European Commission

Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems

SMART 2016/0071

TNO 2019-R10095

Final Study Report regarding CAD/CCAM and Industrial Robots

A study prepared for the European Commission
DG Communications Networks, Content & Technology
by:

TNO innovation for life
VVA CONSULTING
Sant'Anna Scuola Universitaria Superiore Pisa

Digital Single Market

This study was carried out for the European Commission by

Authors:

TNO:	Marc van Lieshout, Tjerk Timan, Kristina Karanilokova, Ming Chen, Sven Jansen, Ron Snijders, Rino Brouwer, Arturo Tejada, Sjef van Montfort
VVA:	Marco Bolchi, Stefano Suardi, Maria Kirova, Patrisia Costenco
SSSA:	Andrea Bertolini, Francesca Episcopo, Stefano Alberti, Erica Palmerini

Internal identification

Contract number: 30-CE-0887241/00-16

SMART number: 2016/0071

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN number 978-92-79-99495-1

DOI:number 10.2759/448974

Catalogue number: KK-04-19-076-EN-N

ABSTRACT (EN)

As part of the 'Study on Safety of non-embedded software' TNO, VVA, and SSSA analysed the legal and business landscape and the challenges and opportunities related to new advanced technologies associated with digitisation and AI. The team studied:

- The safety of non-embedded software by gathering evidence and analysing the key risks, focusing on CAD-CCAM (Collaborative Automated Driving - Cooperative, Connected and Automated Mobility). The team also mapped the legal framework surrounding those risks in eight Member States.
- Different scenarios and conditions for the implementation of CAD-CCAM in Europe. The study identified specific issues which affect the impact of CAD-CCAM and provided empirically founded recommendations for policy measures to facilitate the future business uptake of the technology.
- The testing, certification, and liability framework applicable to industrial robots and CAD-CCAM in Europe and eight Member States. The team analysed how high levels of product quality and safety can be ensured and how liability rules can be shaped in order to provide desirable incentives to all players involved.
- The state-of-art and recommended requirements of Event Data Recorders (EDRs) suited for monitoring the operation of AI systems such as CAD-CCAM.The project provided a prospective foresight study on specifications of EDRs.

ABSTRACT (FR)

Dans le cadre de l'étude sur "la sécurité des logiciels non-intégrés" TNO, VVA, et SSSA ont analysés le paysage juridique et économique, les difficultés et les opportunités liées aux nouvelles technologies associées à la numérisation et l'intelligence artificielle. L'équipe a étudié :

- La sécurité des logiciels non-intégrés en recueillant des informations et des évidences et en analysant les risques clés, en mettant l'accent sur la CCA-MCCA (Conduite Connectée et Automatisée -Mobilité Coopérative, Connectée et Automatisée). L'équipe a également pointé le cadre juridique entourant ces risques dans huit États membres.
- Différents scénarios et conditions pour la mise en œuvre du CCA-MCCA en Europe. L'étude a identifié des enjeux spécifiques qui ont un impact sur le MCCA et a fourni des recommandations empiriques fondées sur des mesures politiques visant à faciliter l'adoption future de la technologie par les entreprises.
- Les essais, la certification et la responsabilité civile applicable aux robots industriels et aux CCA-MCCA en Europe et à huit États membres. L'équipe a analysé comment les niveaux élevés de qualité et de sécurité des produits peuvent être assurés et comment les règles de responsabilité civile peuvent être façonnées afin de convenir à tous les acteurs concernés.
- L'état actuel et les exigences recommandées pour les Enregistreurs de Données d'Evénement (EDE), adaptés pour surveiller le fonctionnement des systèmes d'intelligence artificielle tels que CCA-MCCA. Le projet a permis une étude potentielle sur les spécifications du EDE.

EXECUTIVE SUMMARY (EN)

Progress in digital technologies, in combination with other key enabling technologies, is quickly changing the way products are developed and used. Within the framework of the DG CONNECT "Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems (SMART number 2016/0071)", TNO, VVA, and SSSA analysed the legal and business landscape as well as the complexities, challenges and opportunities related to such new technologies. The project was focused on two quickly developing application domains, namely:

1. Cooperative, Connected, and Automated Mobility (CAD-CCAM) and
2. Industrial robots (IR), and more specifically exoskeletons, mobile and collaborative robots.

The results and recommendations in the study have been based on an extensive literature review, stakeholder interviews and a stakeholder workshop. The widespread stakeholder consultation has ensured that the results of the study have been validated with a large number of experts, companies and policy-makers.

Cooperative, Connected and Automated mobility (CAD-CCAM)

As a first task within the project, the team **gathered evidence and analysed key risks with respect to the safety of non-embedded software in the field of CAD-CCAM**. The main findings of the exploratory analysis showed that in the eight researched Member States (Austria, France, Germany, Italy, The Netherlands, Spain, Sweden and the United Kingdom), there are well-developed programmes and sites for testing autonomous vehicles. At these testing sites, scenarios are being tested either physically or via simulations. Incidents on such testing sites are not, to our knowledge, widely reported. The main challenge regarding non-embedded software is that once a car-OS (Operating System) is connected, the difference between embedded and non-embedded software from a cyber-security point of view is diminishing.
Analysing the broader CCAM technology and framework conditions in Europe, it has been concluded that the uptake of CCAM is being affected by a number of elements such as technical challenges, regulatory aspects (regarding testing, certification and liability liability, insurance and risk management) and commercial bottlenecks. The following conclusions and recommendations can be made:

- **Presence of a human driver**: Both the definition of vehicle set out in the Framework Directive (FD) and in the Motor Insurance Directive (MID) do not require the presence of a human driver. Likewise, many – but not all – MSs possess a definition of vehicle, that would accommodate CADs.
- **Testing**: Fragmented regulation, unharmonized testing activities and different testing procedures limit the possibility to test among MSs, create additional burdens on companies, and hinder technological innovation. The amended Vienna Convention on Road Traffic allows automated driving, provided that the technologies used comply with the UN regulations, or can be overridden by the driver. At the same time, many MSs have regulated testing of CADs on public roads, often excluding fully-autonomous devices. Testing resorts to multiple techniques, including simulation and computer modelling, primarily aimed at assessing those specific risks about which relevant actuarial data is still absent, such as those related to cyber-security, the use of machine-learning techniques, as well as, the unpredictability of the driving environment.
  The observed regulatory fragmentation suggests that an intervention at EU level could tackle the aforementioned issues, and provide a level playing field, enhancing innovation. The creation of Tokku zones and regulatory sandboxes is suggested as a way of facilitating trials in real life conditions. The Commission could also encourage Member States to improve the transparency of testing requirements/principles/

guidelines, by means of recommendations, by monitoring and analysing the different interpretations of testing requirements, and by cross-fertilisation actions aimed at directing Member States towards a more homogeneous approach where neccessary.

- **Certification**: For purposes of certification CADs are compared to road vehicles, therefore the relevant conformity assessment procedure is the type approval, which in turn makes reference to UNECE Regulations. These, indeed, have gradually been amended in order to allow advanced devices involving automation, concerning steering, braking and lighting features.
  On a more global level, nonetheless, the type approval procedure does not seem wholly consistent with CADs' peculiar features, because type approval is focused on a static evaluation and fails to consider that CADs evolve their functioning and receive updates over time, and that CADs communicate and interact with one another and with the infrastructure Therefore, it is suggested that the Commission should actively participate in the work that is currently ongoing on this topic at UNECE level by the specific Task Force under the ITS/AD Informal Group within WP.29, so to obtain in the final certification scheme an optimal balance between the extension, approach and stringency of the testing (and associated levels of safety and security), and the administrative burden on the industry.
- **Liability**: With respect to liability, since CADs are road vehicles, motor liability and insurance regulation apply, as primarily defined at MSs' level. Such rules typically hold both the driver (fault) and the owner (semi-strictly) liable, often jointly and severally. Some MSs opt for no-fault systems and automatic compensation plans . At the same time, CADs are subject to product liability regulation, holding the manufacturer liable for damages deriving form a defect in their products.
  The complex human-machine interaction causes the apportionment of liability among the possible responsible subjects (driver, owner, producer, service providers) to become ever more complex, and further exacerbating the general concerns the Defective Product Directive gives rise to.
  Ad-hoc enacted legislation, such as that put forth by Germany and the United Kingdom, does not appear to radically solve such issues, since – despite some degrees of variations – still resorts to considerations of fault on the side of the user – for failing to resume control when prompted to do so, or for failing to install safety-critical updates. Moreover, legislation at MSs level could cause relevant fragmentation that could impair the possibility to use the same vehicle across EU.
  Ad-hoc EU legislation would thus be beneficial, especially if it implemented a Risk-Management Approach (RMA), by holding the party who is best positioned to minimize risks, ensure compliance, as well as acquire insurance. RMA, in combination with strict (or absolute) liability, would identify a clearly responsible party (one-stop-shop) easing prima facie victim compensation, and subsequent distribution of all associated costs along the value chain
- **Cybersecurity**: there are different types of additional risks associated to CCAM: on one side, the risk of intrusion (e.g. data or privacy related), and, on the other, risk related to the effects of malware (i.e. traffic safety related). The management of cybersecurity is becoming a challenging topic and divergent cybersecurity approaches exist. ENISA should use the finalized UNECE WP.29 guidelines on cybersecurity to implement an EU-wide certification scheme. Furthermore, the report welcomes the initiative to create a network of competence centres across Member States as well as a European Cybersecurity Research and Competence Centre to aid the development of respective tools and technologies necessary to ensure a continuous monitoring and evaluation of cyber-threats.
- **Access to data:** the establishment of a clear, full, transparent data-sets categorisation should be a priority, as it represents an enabler for policy decisions. Within the Recommendation planned to be issued at the end of 2018, the Commission should stress the importance of ensuring that data access solutions developed and made available by OEMs enable the generation of innovative downstream services, while guaranteeing a level playing field for players competing in their provision. The Commission should then

continue analysing the service market enabled by vehicle data. Should the monitoring activity identify, within 1 or 2 years, that downstream competition is impacted by asymmetric data access and that development of new data-based services is limited by the dominant position of OEMs, a regulatory approach on data access should be pursued.
- **Infrastructure evolution:** priority, in terms of policy action and public fund allocation, should be given to maintenance and refurbishment of signalling across EU roads, as well as to the alignment of signalling across the Member States. Furthermore, the Commission should recommend national institutions to investigate the opportunity to regulate how road network and road infrastructure operators grant access to third parties including telecommunication operators, so to ensure fair access to road infrastructure to these actors.

Regarding the identified technical challenges, the research team has put forward the following conclusions:

- **Artificial intelligence**: AI will find its application in scenario assessment and decision making, both of which are safety related. It is suggested to create a multi-stakeholder communication platform to guarantee competitiveness and creation of ethical guidelines, as well as continuing the coordination of research and investments at EU level.
- **Positioning technology**: participate in international and European standardisation fora to ensure that specific differentiators of European systems (e.g. European GNSS) are taken into account. Furthermore, the opportunity to consider positioning and GNSS related requirements and aspects in the ongoing process of update of certification at UNECE level[1] should be strongly considered by European institutions, as UNECE has started regulatory drafting activities on certification to accommodate the specificities of automated driving.
- **HD maps**: these represent an essential input for automated driving. Their development requires significant investments and continuous updates. It is suggested that the Commission should promote public/private partnerships to cover market failures resulting from scarcely populated/rural areas. Furthermore, focus on helping the coordination between international business players in developing a single format for HD maps, to increase the compatibility across different OEMs and potentially enable economies of scale.
- **Absence of a dominant V2X communication standard**: the European Commission should not to delay a decision on the standard of communication that should be followed in Europe for V2X communication. As the current situation is restraining technological development in the field, a clarification on the issue from the EC will provide a strong signal to the automotive industry.

One option to address some of these issues is the use of Event Data Recorders (EDRs). EDRs, popularly known as "black boxes", are devices that record and process information from a vehicle or system while it is in operation. The recorded data can be used for multiple purposes, for instance, training, safety assessment, surveillance, vehicle diagnostics, testing and development, etc. One important use of EDRs is to determine event causation and contributing factors, for example for legal liability after accidents occur.

The analysis showed that **the use of EDRs is very common in the automotive sector**. Almost all new vehicles have EDR functions installed (i.e. not always a separate black box unit, can also be integrated using software). However, these EDRs often only measure basic sensory information such as seat belt status, acceleration and speed. Storage of high-bandwidth information and decision-making processes from advanced (AI-based) systems inside existing EDRs is limited (or at least not publicly known).

[1] Activities are covered by the Task Force "AutoVeh" under the ITS/AD informal working group of UNECE WP.29.

Future EDRs should record relevant information from these AI-based systems, including the operational situation. This allows researchers to investigate a) whether or not the system was used in the right (environmental) conditions and b) how the relevant AI-based algorithms were trained and tested and c) whether or not the datasets used for training and testing were representative for the situation in which the event occurred. Furthermore, AI-based systems should be designed with explainability and situational awareness in mind. Basic information about decision making processes (the what, where, why and why-not) of AI-based systems should be stored inside the EDR itself.

Industrial robots (IR)
With regard to IR, the research team studied the testing, certification and liability, insurance and risk management aspects.

International standards (ISO 10218-1:2011, ISO 8373:2012) define an **industrial robot** as an "automatically controlled, reprogrammable, multipurpose manipulator […] which can be either fixed in place or mobile for use in industrial automation applications".

Given the breadth of the category so defined, three specific case studies are considered in order to pursue the analysis, namely **collaborative** robots, "designed for direct interaction with a human" (ISO 8373:2012, ISO 10218-2:2011), **mobile** robots, which are "able to travel under [their] own control" (ISO (8373:2012, ISO 19649:2017) and **exoskeletons**, external structural mechanisms (see ISO 13482:2014) featuring joints and links corresponding to those of the human body. Moreover, the study identifies and **describes subjects who bear a direct safety-related duty** and other subjects, such as potential victims, certification bodies and insurance companies that are considered in the assessment.

As far as **testing** is concerned, both procedures intended to assess functionalities – "performance testing" –and risks – "reliability testing" are considered. Despite a general duty to perform testing can be identified as underlying the overall framework on product safety, **no specific regulation at EU or MS level applies**, but only general obligations related to the health and safety at work.

Different **testing techniques** are considered, starting from computerized solutions and then inserting real-life trials, especially in order to enforce preventive measures against unforeseen occurrences. Specific **emerging risks** are described, in particular those depending upon cybersecurity threats, loosely structured work environments, as well as the use of machine learning solutions that, given the **absence of data** with respect to the likelihood of their occurrence and possible consequences, **require novel approaches**.

In a regulatory perspective, **since testing is performed in private locations**, the study concludes that **there is no need to adopt ad-hoc legislation**, that could, instead, limit innovative practices on the side of manufacturers. However, the lack of shared benchmarks and experimental reproducibility, as well as difficulties in accessing data and facilities for SMEs and researchers, yield for the creation of **good practices** that could act as instruments of soft law, as well as the establishment of **Digital Innovation Hubs** (DIH), across Europe.

As per purposes of product **certification**, all IRs fall within the scope of the **Machinery Directive**, while exoskeletons may also be considered as "personal protective equipment", and medical devices, thus may be subject to the **Personal Protective Equipment Directive** or **Medical Device Directive**, and the Regulations repealing them.

IRs may need **multiple certifications**, when falling within different classes of devices, or when further modified and adapted by a system integrator or a business user, after their first assessment. Regulations and standards concerning cobots and mobile robots appear adequate. Exoskeletons would instead benefit from ad-hoc legal provisions that might help

clarifying duties that lie on manufactures and on the other subjects involved, as well as from narrow-tailored standards.

Liability issues are tackled by legislative provisions on **safety and health on the workplace** and on general **liability for defective products** since manufacturers, suppliers and integrators may qualify as producers, pursuant to the Product Liability Directive (PLD).

The current liability and insurance framework seems sufficient, because **the victim may clearly identify the party who is called in to provide compensation** – namely the business user –, while **contractual agreements and business relations** bind relevant stakeholders, ensuring the possibility to **distribute costs** arising from possible accidents **along the entire value chain.**

EXECUTIVE SUMMARY (FR)

Les progrès des technologies numériques, combinés à d'autres technologies clés, changent rapidement la façon dont les produits sont développés et utilisés. Dans le cadre de l'étude de DG CONNECT "Etude sur la sécurité des logiciels non-intégrés ; le service, l'accès aux données et les questions juridiques des robots, des véhicules et des systèmes autonomes, connectés et basés sur l'intelligence artificielle (SMART Number 2016/0071)", TNO, VVA et SSSA ont analysés le paysage juridique et commercial ainsi que les complexités, les défis et les opportunités liés à ces nouvelles technologies. Le projet a été axé sur deux domaines d'application en rapide développement, à savoir :

- Conduite Connectée et Automatisée -Mobilité Coopérative, Connectée et Automatisée (CCA-MCCA)
- Robots industriels, et plus précisément exosquelettes, robots mobiles et collaboratifs

Les résultats et les recommandations de l'étude ont été fondés sur une vaste recherche de documentations, des entretiens avec des parties prenantes et un séminaire organisé pour tous les acteurs liés à la MCCA. Le grand nombre d'entretiens garanti que les résultats soient fiables et validés auprès des experts, des industries et des régulateurs.

Mobilité Coopérative, Connectée et Automatisée (CCA-MCCA)

En tant que première tâche au sein du projet, l'équipe a **rassemblé des preuves et analysé les risques clés en ce qui concerne la sécurité des logiciels non-intégrés dans le domaine de la CCA-MCCA**. Les principales conclusions de l'analyse ont montré que dans les huit États membres recherchés (Autriche, France, Allemagne, Italie, Pays-Bas, Espagne, Suède et Royaume-Uni), il existe des programmes et des sites bien développés pour tester les Véhicules Autonomes. Sur ces sites d'essais, diffèrents types de scénarios sont testés physiquement ou via des simulations. Les incidents sur tels sites d'essais ne sont pas, à notre connaissance, largement rapportés. Le principal défi concernant les logiciels non-intégrés est qu'une fois que le système d'opération est connecté à la voiture, la différence entre les logiciels intégrés et non intégrés, d'un point de vue de la cybersécurité, diminue.

En analysant l'ensemble de la technologie MCCA, le cadre et les conditions global en Europe, il a été conclu que l'adoption de MCCA est affectée par un certain nombre d'éléments tels que les défis techniques, les aspects réglementaires (en ce qui concerne les essais, la certification et la responsabilité civil, assurance et gestion des risques) et des goulets d'étranglement commerciaux. Les conclusions et recommandations suivantes peuvent être formulées:

- **Présence d'un conducteur humain** : la définition du véhicule énoncée dans la directive-cadre (DC) et dans la directive sur l'assurance automobile, n'exige pas la présence d'un conducteur humain. De même, de nombreux États membres possèdent une définition du véhicule, qui pourrait accueillir CCA.
- **Les Essais :** la réglementation fragmentée, les activités d'essais non harmonisées et les différences dans les procédures d'essai freinent les possibilités de tester les véhicules entre les Etats membres. Cela crée des fardeaux supplémentaires pour les entreprises et entrave l'innovation technologique. La Convention de Vienne modifiée sur la circulation routière autorise la conduite automatisée, à condition que les technologies utilisées respectent les réglementations de l'ONU ou puissent être substituées par le conducteur. En même temps, de nombreux Etats membres ont réglementé les essais de CCA sur les routes publiques, en excluant souvent les dispositifs entièrement autonomes. Les essais ont recours à de multiples techniques, y compris la simulation et la modélisation informatique, visant principalement à évaluer les risques spécifiques sur lesquels les données actuarielles pertinentes sont encore absentes, telles que celles liées

à la cybersécurité, les techniques d'apprentissage automatique, ainsi que l'imprévisibilité de l'environnement de conduite.
La fragmentation réglementaire observée suggère qu'une intervention au niveau de l'UE pourrait traiter les problèmes évoqués et uniformiser les règles du jeu, en favorisant l'innovation. La création de zones "Tokku" et de sas réglementaires est suggérée comme un moyen de faciliter les essais dans des conditions de vie réelles. La Commission pourrait également encourager les États membres à améliorer la transparence des besoins/principes/lignes directrices en matière d'essais, par le biais de recommandations, en surveillant et en analysant les différentes interprétations des exigences et besoins en matière d'essais, et en encourageant le brassage entre les Etats membres, visant à les orienter vers une approche plus homogène, si nécessaire.

- **Certification** : A fin de la certification les CCA sont comparés aux véhicules routiers, la procédure d'évaluation de la conformité pertinente est donc l'homologation de type, qui à son tour fait référence aux réglementations CEE-ONU. Ceux-ci, en effet, ont été progressivement modifiés afin de permettre des dispositifs avancés portant sur l'automatisation, concernant les dispositifs de direction, de freinage et d'éclairage.
  À un niveau plus global, néanmoins, la procédure de réception par type des véhicules ne semble pas entièrement compatible avec les caractéristiques particulières des CCA, car l'approbation de type est axée sur une évaluation statique et ne considère pas que le fonctionnement des CCA va évoluer et recevoir des mises à jour au fil du temps, et que les CCA communiquent et interagissent entre eux et avec l'infrastructure. Par conséquent, il est suggéré que la Commission participe activement aux travaux actuellement en cours sur ce sujet au niveau de la CEE et plus précisément dans l'équipe spéciale sous le groupe informel des systèmes de transport intelligents (STI)/CA au sein du WP.29, afin d'obtenir dans le système de certification final, un équilibre optimal entre l'élargissement, l'approche et la rigueur des essais (et les niveaux associés de sûreté et de sécurité), et la charge administrative sur l'industrie.
- **Responsabilité civile** : En ce qui concerne la responsabilité civile, puisque les CCA sont des véhicules routiers, la responsabilité civile automobile et la réglementation en matière d'assurance s'appliquent, comme défini par les Etats membres. Ces règles détiennent généralement le conducteur et le propriétaire responsable, souvent conjointement et solidairement. Certains Etats membres optent pour des systèmes d'indemnisation en cas d'accidents, sans égard à la faute. En même temps, les CCA sont soumis à la réglementation de la responsabilité du fait des produits défectueux, ce qui tient le producteur responsable pour les dommages causés par le caractère défectueux de ses produits.
  L'interaction complexe homme-machine provoque la répartition de la responsabilité civile automobile parmi les sujets responsables possibles (conducteur, propriétaire, producteur, prestataires de services) encore plus complexe et provoque d'avantage des préoccupations liés cette réglementation de la responsabilité du fait des produits défectueux.
  La législation ad hoc promulguée, comme celle présentée par l'Allemagne et le Royaume-Uni, ne semble pas résoudre de manière radicale ces problèmes, puisque malgré quelques degrés de variations-elle recourt toujours à des considérations de faute du côté de l'utilisateur-pour ne pas reprendre le contrôle du véhicule quand il se doit, ou pour avoir omis d'installer des mises à jour critiques pour la sécurité du véhicule. En outre, la législation au niveau des Etats membres pourrait entraîner une considérable fragmentation qui pourrait nuire à la possibilité d'utiliser le même véhicule partout dans l'UE.
  La législation ad-hoc de l'UE serait donc bénéfique, en particulier si elle met en œuvre une politique de gestion des risques, en tenant la partie qui est la mieux placée pour minimiser les risques, assurer la conformité, ainsi que d'acquérir une assurance. Une politique de gestion des risques, en combinaison avec une responsabilité civile automobile stricte (ou absolue), identifierait une seule partie clairement responsable, facilitant l'indemnisation prima facie des victimes, et la distribution subséquente de tous les coûts associés le long de la chaîne de valeur.

- **Cybersécurité :** il existe différents types de risques supplémentaires associés aux MCCA : d'un côté, le risque d'intrusion (lié aux données privées), et d'un autre côté, le risque lié aux effets des logiciels malveillants (relatif à la sécurité routière). La gestion de la cybersécurité devient un défi et des approches divergentes en matière de cybersécurité existent. L'ENISA devrait utiliser les lignes directives du CEE-ONU WP. 29 sur la cybersécurité pour mettre en œuvre un système de certification à l'échelle de l'UE. En outre, le rapport salue l'initiative visant à créer un réseau de centres de compétences dans les États membres ainsi qu'un Centre Européen de Recherche et de Compétences sur la cybersécurité afin d'aider au développement des outils et des technologies nécessaires pour assurer une surveillance et une évaluation des cyber-menaces en continue.
- **Accès aux données :** la création d'une catégorisation claire, complète et transparente des ensembles de données devrait être une priorité, car elle représente un mécanisme permettant de prendre des décisions en matière de politiques. Dans le cadre de la recommandation prévue à la fin du 2018, la Commission devrait insister sur l'importance de veiller à ce que les solutions d'accès aux données développées et mises à disposition par les producteurs d'automobiles permettent la création de services en aval, tout en garantissant une concurrence loyale. La Commission devrait ensuite poursuivre l'analyse du marché des services générés par les véhicules. Si l'activité de surveillance identifie, dans les 1 ou 2 ans, que la concurrence en aval est influencée par l'accès asymétrique aux données et que le développement de nouveaux services fondés sur les données est limité par la position dominante des fabricants d'automobiles, une approche réglementaire sur l'accès aux données devrait être poursuivi.
- **Évolution de l'infrastructure :** la priorité, en termes d'action politique et de répartition des fonds publics, devrait être accordée à l'entretien et à la remise à neuf de la signalisation sur les routes de l'UE, ainsi qu'à l'alignement de la signalisation dans les États membres. En outre, la Commission devrait recommander aux institutions nationales d'étudier la possibilité de réglementer la façon dont les opérateurs de réseaux routiers et d'infrastructures routières accordent l'accès à des tiers, y compris les opérateurs de télécommunications, afin d'assurer un accès équitable aux infrastructures routières à ces acteurs.

En ce qui concerne les défis techniques identifiés, le consortium a apporté les conclusions suivantes :

- **Intelligence artificielle :** l'IA trouvera son application dans l'évaluation des scénarios et la prise de décisions, qui sont toutes les deux liées à la sécurité. Le consortium propose la création d'une plate-forme de communication multi-parties prenantes pour garantir la compétitivité et la création de lignes directrices éthiques, ainsi que la poursuite de la coordination de la recherche et des investissements au niveau de l'UE.
- **La technologie de positionnement :** participer à des forums internationaux et européens pour la standardisation de la technologie afin de garantir que les différentiateurs spécifiques des systèmes européens (par exemple GNSS européen) soient pris en compte. En outre, la possibilité d'examiner les besoins et les aspects relatifs au positionnement et aux services mondiaux de navigation par satellite (GNSS) dans le processus en cours de mise à jour de la certification au niveau de la CEE devrait être fortement examinée par les institutions européennes, étant donné que la CEE a entamé la rédaction réglementaire de certification pour répondre aux besoins de la conduite automatisée.
- **Les cartes haute définition (HD) :** elles représentent une partie essentielle pour la conduite automatisée. Leur développement nécessite des investissements importants et des mises à jour continues. Le consortium suggère que la Commission encourage les partenariats publics/privés pour couvrir les déficiences du marché résultant des zones à peine peuplées ou très rurales. En outre, le consortium suggère la Commission de se concentrer sur l'aide à la coordination entre les acteurs internationaux dans l'élaboration d'un format unique pour les cartes HD, afin d'accroître la compatibilité entre les

différents constructeurs d'automobiles et potentiellement de permettre des économies d'échelle.

- **Absence d'une norme de communication V2X dominante:** la Commission européenne ne devrait pas retarder une décision sur la norme de communication qui devrait être suivie en Europe pour la communication V2X. Comme la situation actuelle freine le développement technologique sur ce sujet, une clarification sur la question de la part de la Commission fournira un signal fort à l'industrie automobile.

L'une des options pour aborder certaines de ces questions est l'utilisation d'enregistreurs de données d'événements. Les enregistreurs de données d'événements, ou encore appelé " boîtes noires", sont des dispositifs qui enregistrent et traitent l'information d'un véhicule ou d'un système pendant qu'il est en opération. Les données enregistrées peuvent être utilisées à des fins multiples, par exemple la formation, l'évaluation de la sécurité, la surveillance, le diagnostic du véhicule, les essais, etc. Une des utilisations importantes de ces "boite noires" consiste à déterminer la causalité des événements et les facteurs contributifs, par exemple pour la responsabilité civile en cas d'accidents.

L'analyse a montré que **l'utilisation des enregistreurs de données d'événements est très courante dans le secteur de l'automobile**. Presque tous les nouveaux véhicules sont équipés de cette fonction (pas toujours une unité de boîte noire séparée, cela peut également être un logiciel intégré). Cependant, ces enregistreurs de données d'événements ne mesurent souvent que les informations sensorielles de base telles que l'état de la ceinture de siège, l'accélération et la vitesse. Le stockage d'informations à grande largeur de bande et de processus décisionnels à partir de systèmes avancés (IA) à l'intérieur des enregistreurs de données d'événements existants est limité (ou du moins pas publiquement connu).

Les futurs enregistreurs de données d'événements devraient enregistrer les informations pertinentes de ces systèmes basés sur l'IA, y compris la situation opérationnelle du véhicule. Cela permet aux chercheurs d'enquêter sur a) si le système a été utilisé ou non dans les conditions appropriées (environnementales) et b) comment les algorithmes pertinents basés sur l'IA ont été formés et testés et c) si les ensembles de données utilisés pour la formation et les tests ont été représentant pour la situation dans laquelle l'événement s'est produit. En outre, les systèmes basés sur l'IA doivent être conçus avec une explication et une conscience de la situation. Les informations de base sur les processus décisionnels (le quoi, où, pourquoi et pourquoi-pas) des systèmes basés sur l'IA devraient être stockées à l'intérieur de enregistreurs de données d'événements.

Les robots industriel (RI)

En ce qui concerne l'IR, l'équipe de recherche a étudié les aspects des tests, de la certification et de la responsabilité, des assurances et des risques.

Les normes internationales (ISO 10218-1 :2011, ISO 8373 :2012) définissent un **robot industriel** comme un "manipulateur, multi-application, reprogrammable, commandé automatiquement, programmable sur trois axes ou plus, qui peut être fixé sur place ou mobile, destiné à être utilisé dans des applications d'automatisation industrielle".

Compte tenu de la largeur de la catégorie ainsi définie, trois études de cas spécifiques sont envisagées afin de poursuivre l'analyse, à savoir les robots **collaboratifs**, "travaillent en collaboration directe avec un humain à l'intérieur d'un espace de travail défini conçus pour l'interaction directe avec un humain" (ISO 8373:2012, ISO 10218-2:2011), les robots **mobiles**, sont ceux qui "pouvant se déplacer sous son propre contrôle" (ISO (8373:2012, ISO 19649:2017) et **exosquelettes**, robots d'assistance physique qui sont fixés à la personne pendant l'utilisation (voir ISO 13482:2014). En plus, l'étude identifie et décrit dans son évaluation les sujets qui ont un devoir direct en matière de sécurité et d'autres sujets,

tels que les victimes potentielles, les organismes de certification et les compagnies d'assurance.

En ce qui concerne les essais, les deux procédures visant à évaluer les fonctionnalités – " tests de performance " – et les risques – " tests de fiabilité " sont considérées. A part une obligation générale d'effectuer des tests faisant partie de la loi-cadre sur la sécurité générale des produits., aucune réglementation spécifique à l'UE ou au niveau des Etats membres s'applique, à l'exception des obligations générales liées à la santé et la sécurité au travail.

Différentes techniques de tests sont envisagées : des solutions informatisées en collaboration avec des essais réels, afin d'appliquer des mesures préventives contre des événements imprévus. Des risques spécifiques émergents sont décrits, en particulier ceux qui sont liés aux menaces de cybersécurité, des environnements de travail faiblement structurés, ainsi que l'utilisation de solutions d'apprentissage automatique, compte tenu de l'absence de données concernant la probabilité de leurs conséquences possibles, ils nécessitent des approches novatrices.

Dans une perspective réglementaire, puisque les essais sont effectués dans des endroits privés, l'étude conclut qu'il n'est pas nécessaire d'adopter une législation ad hoc, qui pourrait plutôt limiter les pratiques innovatrices des fabricants. Toutefois, le manque de points de repère partagés et de reproductibilité expérimentale, ainsi que les difficultés d'accès aux données et aux facilités pour les petites et moyennes organisations et les chercheurs, évoque le besoin pour la création de bonnes pratiques qui pourraient servir d'instruments de droit souple, ainsi que les créations de Centres d'Innovation Numériques (CIN), à travers l'Europe.

En vertu de la certification des produits, tous les robots industriels entrent dans le champ d'application de **la directive relative aux machines**, tandis que les exosquelettes peuvent également être considérés comme des " équipements de protection individuelle ", et les dispositifs médicaux, peuvent donc être soumis à la **directive des équipements de protection individuelle** ou bien **la directive relative aux dispositifs médicaux** et les règlements les abrogeant.

Les robots industriels peuvent avoir besoin de **plusieurs certifications**, lorsqu'ils tombent dans différents classements de produit, ou lorsqu'ils sont modifiés et adaptés par un intégrateur de système ou un utilisateur professionnel, après leur première certification. Les règlements et les normes concernant les robots et les robots mobiles semblent adéquats. En revanche, les exosquelettes bénéficieraient de dispositions légales ad-hoc qui pourraient aider à clarifier les tâches des fabricants et des autres sujets concernés. Il serait bénéfique pour eux d'avoir aussi des normes étroites sur mesure.

Les problèmes de responsabilité sont abordés par des dispositions législatives sur la sécurité et la santé sur le lieu de travail et sur la responsabilité des produits défectueux puisque les fabricants, les fournisseurs et les intégrateurs peuvent être considérés comme producteurs, conformément à la directive sur la responsabilité des produits défectueux.

Le cadre actuel de la responsabilité civile et de l'assurance semble suffisant, car la victime peut clairement identifier la partie qui doit fournir une indemnisation- à savoir l'utilisateur professionnel-, tandis que les accords contractuels et les relations d'affaires lient les parties prenantes, en assurant la possibilité de distribuer les coûts liés aux accidents éventuels le long de la toute chaîne de valeur.

Table of Contents

1. INTRODUCTION AND OBJECTIVES OF THE STUDY

Progress in digital technologies, in combination with other key enabling technologies, is quickly changing the way products are developed and used. The advances in technologies such as IoT,

data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems (SMART number 2016/0071)", aims to provide the Commission with an analysis of the legal and robotics, data analytics and AI create opportunities in Europe as identified by the Digital Single Market Strategy (COM/2015/0192). Given the fast pace of change however, it is also important to study these technologies to ensure that a transparent and safe playing field is in place.

The present report, in the framework of the DG Connect "Study on Safety of non-embedded software; Service,business landscape as well as the complexities, challenges and opportunities related to such new technologies. The project was focused on two groups of quickly developing application domains, namely:

1. Cooperative, Connected and Automated Mobility (CAD-CCAM), focusing on the autonomous and automated procedures for driving (excluding traffic management applications).
2. Industrial robots, and more precisely exoskeletons, mobile and collaborative robots.

The results and recommendations in the study have been based on an extensive literature review, stakeholder interviews (tasks 1-4) and a stakeholder workshop (task 2). The widespread stakeholder consultation has ensured that the results of the study have been validated with a large number of experts, companies and policy-makers.

The project was structured along five main tasks, briefly described below:
Task 1: Safety of non-embedded software: the task aimed to gather evidence and analyse key risks with respect to the safety of non-embedded software, with a particular focus on CAD-CCAM. Further, the project team mapped the current legal framework surrounding those risks in eight Member States (Austria, France, Germany, Italy, The Netherlands, Spain, Sweden, and the United Kingdom).

Task 2: Scenarios and conditions for the implementation of CAD - CCAM and proactive mapping of policy measures: as part of the task, the team identified specific issues which affect the impact of CCAM and provided empirically founded recommendations for policy measures that will facilitate the future business uptake of the technology.

Task 3 and 4: Testing, certification, and liability and insurance of industrial robots and CAD-CCAM: the two tasks together provide a prospective foresight study and determine how appropriate levels of product quality and safety can be ensured and how liability rules can be shaped in order to provide desirable incentives to all players involved. A framework for robot testing in Europe was determined, which could ease the assessment of risks and their management, as well as technological research. The task also focused on the eight Member States studies in task 1.

Task 5: Prospective foresight study on specifications of event data recorders: as part of this task, the team examined the state-of-art and provided recommended requirements for future Event Data Recorders suited for monitoring the operation of AI systems such as CAD-CCAM.

2. POSITIONING AND ORGANIZATION OF THIS REPORT

This report constitutes the final deliverable of the project related to CAD-CCAM and Industrial Robots.

The following sections provide an overview of the tasks performed withing the project, the conclusions and recommendations. In order to provide more in-depth information per task, the results and objectives of each task are summarised individually in the following sections:

- Overview of activities and results in Task 1: Safety of non-embedded software related to CAD-CCAM.
- Overview of activities and results in Task 2: Scenarios and conditions for the implementation of CAD – CCAM.
- Overview of activities and results in Tasks 3&4: Testing, certification, and liability and insurance of industrial robots and CAD-CCAM.
- Overview of activities and results in Task 5: Prospective foresight study on specifications of event data recorders.

The full reports of the study can be found in the attached Annexes.

3. OVERVIEW OF THE ACTIVITIES AND RESULTS:

3.1. Overview of activities and results in Task 1: Safety of non-embedded software related to CAD-CCAM

The part on CAD-CCAM in Task 1 of this study focused on the inventory of incidents with non-embedded software. The task provides a first overview into reported incidents and accidents of CCAM within Europe or outside, followed by an overview of possible court cases surrounding these incidents (if any). The rationale of this mapping is to distill novel risks related to non-embedded software within automated driving and to see if and how they are related to the current liability regimes.

In identifying the grey zones from a regulatory perspective, the report covered only a first analysis of the Radio Equipment Directive (RED), the General Data Protection Regulation (GDPR) and other directives and regulations that might have an impact on non-embedded software in devices and machines. The task focused on eight Member States (MS): Austria, France, Germany, Italy, The Netherlands, Spain, Sweden and the United Kingdom. This analysis was further elaborated and expanded in the consecutive tasks 2, 3 and 4.

The main findings of our exploratory analysis regarding CCAM showed that in the eight researched Member States there are well-developed programmes and sites for testing autonomous vehicles. At these testing sites, scenarios are being tested either physically or via simulations. Incidents on such testing sites are not widely reported to our knowledge so far. As for novel risks and potential incidents, on the level of AI and autonomy, some of the risks identified were faulty sensor-calibration or underperforming sensors, faulty data from the server-side of for instance route information; hacking and/or data breaches were also mentioned by some recent reports and experts as a new risk. Interaction with infrastructure and other vehicles was seen as a challenge in relation to interoperability and performance, cross-border data flows and also cybersecurity.

The main challenge regarding non-embedded software is that once a car-OS (Operating System) is connected, the difference between embedded and non-embedded software from a cyber-security point of view is diminishing. Where for now, applications such as navigation software or in-car entertainment is seen as non-embedded and non-trivial for the car's performance, it is already possible to reach and manipulate trivial parts of the software via such non-trivial applications. Concerning data, there are different regulations that touch upon or have a say of what can and cannot be shared or transmitted. From the RED to the GDPR and more, the regulatory landscape for data is a complex one in Europe, as it also touches upon non-embedded software-parts of automated vehicles. A next step for this and related projects would be to map out this landscape.

Regarding liability, in all Member States we have looked into, the role of the driver is to be in control of the vehicle at all times and so far this would also hold for (semi) autonomous vehicles. Yet, as witnessed in recent accidents with self-driving cars in the US, users of autonomous vehicles perhaps see themselves more as passengers than as drivers, having (too) high expectations of the car's autonomy and smartness. One solution direction from the industry in response is to add alarm-mechanisms in the car that need to warn the passenger/driver when attention is needed. One MS has proposed a driver's license for AI. This would call for regular testing and updating of such a driver's license for AI before being allowed on the road.

In the report the following conclusions are drawn :

- There are a number of initiatives in Member States which aim to determine what the future liability and safety rules will be. Automation is however currently still widely used at lower automation levels, in which case – as the GEAR 2030 recommendations state – EU Directives on liability for defective products (85/374/EEC) and on motor insurance

(2005/14/EC) are sufficient for upcoming automated systems. There have been a number of studies already prepared which point to the need to revisit some concepts such as a driver when it comes to traffic liability. Clarification on the data storage and data ownership and rights has started in some Member States – France notably. Further automation and future updates of the legislation might be necessary as full autonomous vehicles become operational.

- Accidents currently revolve around the sensors and updates of the technology. It is not reasonable to expect that the transition to autonomous driving will be without accidents.
- Cyber security is frequently cited as a problem – ACEA views additional access points to a vehicle as a problem and recommends the extended vehicle model. Different legislative instruments mention the need to make sure that the systems are protected from cyber-attacks but achieving a 100% seems quite difficult. Implementing safety and security by design approaches has been recommended.

3.2. Overview of activities and results in Task 2: Scenarios and conditions for the implementation of CAD - CCAM

Task 2 has aimed at identifying empirically founded recommendations for policy measures that will facilitate the future business uptake of Cooperative, Connected and Automated Mobility (CCAM) in the EU context.

The uptake of CCAM is being affected by a number of elements such as technical challenges, regulatory hurdles, and commercial bottlenecks, which in turn will impact social and market acceptance. These **issues** are presented below.

Liability: Most Member States have rules that make the driver, who is involved in the driving task, liable. Manufacturers' liability holds for cases where damage is derived from the product's use. With increased automation the rules will start to overlap as the human and vehicle gradually start sharing the driving task. Additional complications include the fact that automation will come in degrees as well as the fact that the substitution will be a time-consuming process given that the car is a long lasting good. In addition, with cooperation (connectivity), apart from the driver and the driver's car manufacturer, there will be additional actors to be considered, which adds complexity. There are different conditions under which the owner, the producer or the human is liable. Even if we have all the information and we have identified the type of situation, it is still a very complex issue that requires litigation and many actors involved.

Cybersecurity: there are different types of additional risks associated to CCAM: on one side, the risk of intrusion (e.g. data or privacy related), and, on the other, risk related to the effects of malware (i.e. traffic safety related). The management of cybersecurity is becoming a challenging topic and divergent cybersecurity approaches exist. OEMs would like to opt for a security-by-design and customised cybersecurity strategy, whereas other stakeholders suggest that a standardised approach following European cybersecurity principles would be optimal. Suppliers and other stakeholders have mixed views, suggesting broad standards and minimum requirements – OEMs would then be free to develop their strategy to meet these.

Data sharing framework and data access: the data generated by the automated cars is, and will increasingly be, a key source of value. Therefore, access to in-vehicle data will represent a vital element to ensure the provision of new services by many categories of current and potential service providers. From the policy standpoint, the key challenge is maximising the socio-economic benefits that can be generated by the access and use of vehicle data. At the present stage, OEMs and partially suppliers have control over most of the data generated by the vehicles and it is not in their best interest to make access to these data fully available to third parties. In contrast, aftermarket services are requesting for direct

in-vehicle access and even if intermediate solutions are proposed such as an extended server, a consensus and a final decision on the solution to adopt is not yet achieved.

Testing on roads: first, unharmonized testing activities and different testing procedures across countries make the overall implementation of testing on roads difficult. This is also linked to the fact that cross-border testing activities are still limited in numbers. Second, incidents on testing cases are not widely reported and communication is lacking between different projects and Member States Initiatives. Third, in the future, further amendment of the Vienna Convention is required for testing and large-scale operation because the current amendment does not allow testing vehicles to run on public roads without a driver in control.

Certification: the current framework for testing and type approval needs to evolve in light of the advent of automated driving, which brought the following challenges: a) automated operation cannot be tested as combination of "vertical" components; b) the definition of a limited number of test cases is not suitable to ensure safety of an artificial intelligence-based system, which needs to take decisions in the real world considering an endless number of possible situations and scenarios; c) in the current framework there is a limited possibility to consider the actual environment in which the vehicle operates; and d) the current framework is not suited to ensure the validity of certification over time, as new threats and issues are likely to emerge over the lifetime of the vehicle and software updates might update and affect fundamental safety functions.

Road infrastructure evolution: the emergence of automated driving will eventually require public institutions and national bodies to upgrade the current road and communication infrastructure network. However, the current commercial and legal practices may impede communication providers to access the physical infrastructure, *de facto* preventing the investments required to implement communication capabilities on already existing infrastructure.

Technical issues: there are several technological challenges that need to be solved to ensure an effective, safe and secure roll out of CCAM:

- **Artificial intelligence**: technologies inside automated vehicles such as LIDAR, cameras, radars that collect scenario information will be required to be processed and used to take precise, immediate decisions. AI will find its application in scenario assessment and decision making, which both are safety related. The use of AI will eventually raise ethical questions, as decisions involving life-threating situations will be taken by the vehicle and not anymore by the driver.
- **Positioning technologies**: the key challenges for the industry are to improve the performance of the single technologies while ensuring cost effectiveness, as well as to advance on sensor and data fusion and processing capabilities to feed the decision to be taken by artificial intelligence.
- **High definition (HD) maps**: these represent an essential input for automated driving. Their development requires significant investments and continuous updates. Furthermore, their coverage should be extended across all territories, and not only across densely populated areas. Finally, common technical formats are currently missing, with HD Maps databases currently limited in terms of interoperability across automotive players and other stakeholders.
- **Absence of a dominant standard for V2X communication**. While a vehicle could implement automated features independently to its capability to communicate and cooperate with the external world, it is undisputable that connectivity will expand the potential of automated vehicles, integrating them in a complex mobility ecosystem characterised by cooperative behaviour among vehicles and infrastructures. Today, the market offers different technologies capable of offering connectivity and cooperative

features, namely ITS-G5 and future cellular based 5G, although testing has already started using the already available LTE-V2X. As the two technologies are currently non-compatible, the traditional approach of the European Commission of "technology neutrality" could result in being counter-productive and even represent a risk for the safety of consumers.

Taking stock of the following challenges and bottlenecks, the reports identifies the **recommendations** outlined below.

Liability: we suggest a revision of the Product Liability Directive and of its scope of application by the relevant authorities. Furthermore, autonomous driving regulation could use compulsory insurance schemes, no-fault plans, as well as a risk-management approach.

Testing on public roads: the Commission could encourage Member States to improve the transparency of testing requirements/principles/guidelines, by means of recommendations, by monitoring and analysing the different interpretations of testing requirements, and by cross-fertilisation actions aimed at driving Member States towards a more homogeneous approach where nessary. The Commission should also establish stronger cooperation on testing across Europe, through the implementation of a European system for sharing testing data, conditions, use cases and best practices related to automated driving.

Certification: The Commission should actively participate in the work that is currently ongoing on this topic at UNECE level by the specific Task Force under the ITS/AD Informal Group within WP.29, so to obtain in the final certification scheme an optimal balance between the extension, approach and stringency of the testing (and associated levels of safety and security), and the administrative burden on the industry. In case of delays in the process, available instruments and options under the EU legal framework could be used as possible mitigation instruments.

Cybersecurity: ENISA should use the finalized UNECE WP.29 guidelines on cybersecurity to implement an EU-wide certification scheme. Furthermore, the report welcomes the initiative to create a network of competence centres across Member States as well as a European Cybersecurity Research and Competence Centre to aid the development of respective tools and technologies necessary to ensure a continuous monitoring and evaluation of cyber-threats.

Access to data: the establishment of a clear, full, transparent data-sets categorisation should be a priority, as it represents an enabler for policy decisions. Within the Recommendation planned to be issued at the end of 2018, the Commission should stress the importance of ensuring that data access solutions developed and made available by OEMs enable the generation of innovative downstream services, while guaranteeing a level playing field for players competing in provisioning these services. The Commission should then continue analysing the service market enabled by vehicle data. Should the monitoring activity identify, within one or two years, that downstream competition is impacted by asymmetric data access and that development of new data-based services is limited by the dominant position of OEMs, a regulatory approach on data access should be pursued.

I**nfrastructure evolution:** priority, in terms of policy action and public funds allocation, should be given to maintenance and refurbishment of signalling across EU roads, as well as to the alignment of signalling across the Member States. Furthermore, the Commission should recommend national Institutions to investigate the opportunity to regulate how road network and road infrastructure operators grant access to third parties including telecommunication operators, so to ensure fair access to road infrastructure to these actors.

Technical challenges: the following conclusions and recommendations are suggested:

- **Artificial intelligence**: create a multi-stakeholder communication platform to guarantee competitiveness and creation of ethical guidelines, as well as continuing the coordination of research and investments at EU level.
- **Positioning technology**: participate in international and European standardisation fora to ensure that specific differentiators of European systems (E.g. European GNSS). Furthermore, the opportunity to consider positioning and GNSS related requirements and aspects in the ongoing process of update of certification at UNECE level[2] should be strongly considered by European Institutions, as UNECE has started regulatory drafting activities on certification to accommodate the specificities of automated driving.
- **HD maps**: promote public/private partnerships to cover market failures resulting from scarcely populated/rural areas as the best approach to solve the commercial issue underlying the creation of HD maps. Furthermore, focus on helping the coordination between international business players in developing a single format for HD maps, to increase the compatibility across different OEMs and potentially enable economies of scale.
- **Absence of a dominant V2X communication standard**: the European Commission should not delay a decision on the standard of communication that should be followed in Europe for V2X communication. As the current situation is restraining technological development in the field, a clarification on the issue from the Institution will provide a strong signal to the automotive industry.

3.3. Overview of activities and results in Task 3 and 4: Testing, certification, and liability and insurance of industrial robots and CAD-CCAM

Tasks 3 and 4 addressed three aspects, namely (i) testing, (ii) certification, and issues regarding (iii) liability, insurance and risk management, concerning both industrial robots (IRs) and connected and automated driving devices (CADs).

Testing. Testing represents the procedures, evaluations and trials performed during the development of the product, to assess the performance and reliability of the device, against a series of benchmarks. The study identifies and assesses the legal framework applicable, and the techniques used, suggesting alternative approaches when needed.

Certification. Certification is the procedure each product has to undergo in order to be traded onto the EU market, assuring compliance with the minimum safety requirements put forth by applicable legislation and easing circulation of goods within the common market. Said requirements can be met through compliance with technical standards, especially if provided with reinforced legal value (such as harmonized ones). The analysis will determine whether IRs and CADs fall within existing safety regulations, whether the latter are adequate, and whether existing standards are sufficient and/or sufficiently narrow tailored for these novel applications.

Liability, insurance and risk management. Civil liability determines who bears the economic consequence of an accident, and – traditionally – provides *ex ante* incentives towards a high-level of product safety, while insurance allows such costs to be internalized and managed, and compensation to be secured.

The Risk Management Approach (RMA) decouples the traditional functions of liability, i.e. deterrence and compensation. It relies on *ex ante* regulations to obtain safety and security of products, and holds strictly liable the party that is best positioned to (i) minimize risks and (ii) acquire insurance, to grant prompt and adequate compensation *ex post*.

[2] Activities are covered by the Task Force "AutoVeh" under the ITS/AD informal working group of UNECE WP.29

The study aims to determine applicable liability rules, identify criticalities and propose solutions to address them – pursuant to a RMA and other approaches when relevant –, while at the same time assessing the availability of technology-specific insurances and their impact on technological development.

3.3.1. Industrial Robots

Introduction. Absent any legal definition, and on the basis of international standards, an **industrial robot** can be defined as an "automatically controlled, reprogrammable, multipurpose manipulator, programmable in three or more axes, which can be either fixed in place or mobile for use in industrial automation applications" (ISO 10218-1:2011, ISO 8373:2012).

Given the breadth of the category, the study is performed on **three case studies**, which display different characterizing features of Industry 4.0 robotics, namely:

- **collaborative robots**: "robot[s] designed for direct interaction with a human" (ISO 8373:2012, ISO 10218-2:2011);
- **mobile robots**: "robot[s] able to travel under [their] own control" both "with or without manipulators" (ISO (8373:2012, ISO 19649:2017);
- **exoskeletons**: external structural mechanism with joints and links corresponding to those of the human body (see, for personal care robots, ISO 13482:2014).

As for the **subjects** involved in the testing, certification, liability and insurance of IRs, the study addresses:

- those who bear a direct **safety-related duty** (ISO 10218:1): **manufacturers**, **suppliers** of individual components, **integrators** and **business-users**;
- **other subjects**, who still play a fundamental role for depicting the general framework: potential victims – non-business-users and by-standers –, certification competent bodies – notified bodies, notifying authorities and notified authorities – and insurance companies.

Testing. Testing of IRs consists of the different procedures performed in the development and production of robotics, with the purpose of verifying goals and functionalities – so called "**performance** testing" –, and gathering knowledge about potential risks and failures connected to their use – so called "**reliability** testing". Despite a general duty to perform testing can be identified as underlying the overall framework on product safety, **there is no specific regulation** neither at the EU nor at the MSs level, establishing how testing should be performed for the purpose of obtaining functional and safe products, or setting procedures to be followed in order to carry out particular activities. However, the **general obligations related to the health and safety at work apply**, thus requiring testing to be performed in a way that does not put at risks operators and other subjects involved.

During the entire production cycle of the IRs, which comprises experiments and design, development, manufacturing and final validation, tests are performed through a series of techniques – such as mathematical modelling and simulation– which are used for each component and the assembled system, in combination with each other and according to a scrum methodology, starting from more computerized solutions and progressively inserting real-life trials.

In this process, **risk assessment and evaluation** take into account the extant **functional and safety requirements,** set in different EU legislative documents and international standards. The general duty to market safe products requires preventive measures against **unforeseen risks**. This is particularly important for Industry 4.0 robotics, as **machine learning solutions, cybersecurity risks and loosely structured work environments**

bring about new scenarios which might make the human-robot interaction more dangerous, and that are, however, difficult to foresee and evaluate. Therefore, testing has to be adapted as to allow greater availability of data for software-training, and requires precautionary measures to avoid damages.

Against this picture, a lack of specific regulation seems to foster rather than hinder testing of IRs, since it allows businesses to develop the solutions which best fit their production without incurring in additional procedures and costs. Moreover, since testing, also when based on real-life scenarios, is performed in private locations, no regulation for ensuring safety, either than the one on working environments already in place, is required. Therefore, **no legislative intervention is needed**. However, the lack of shared benchmarks and experimental reproducibility, as well as the difficulties in accessing data and facilities for SMEs and researchers, and the uncertain realization of available standards, yield for the **creation of good practices** which could act as instruments of soft law, **and the establishment of Digital Innovation Hubs (DIHs)** across Europe, to create synergies and grant further resources.

Certification. Certification is the procedure each product has to undergo in order to be marketed within the EU, and assure compliance with minimum safety requirements.

Absent any rules specifically put into place for IRs, it is necessary to ascertain whether extant rules apply to IRs. On the basis of existing legislation:

- **all IRs** qualify as "machinery" or "partly completed machinery", hence **fall within the scope of the Machinery Directive;**
- **exoskeletons** may also be considered as "personal protective equipment", and, to a more theoretical extent, medical devices, and thus are subject to the **Personal Protective Equipment Directive** or **Medical Device Directive, and the Regulations repealing them**.

IRs may need **multiple certifications**, not only when they are marketed outside Europe, but also when falling within multiple classifications, when other rules – such as those related to certification of low voltage electrical equipment – apply, and even when further modification (e.g. by the business-user) are made to an already certified product.

Pursuant to the rules set out in the aforementioned legislation, harmonization is limited to the essential requirements, with technical specifications being set out in **harmonized standards** that, if applied, grant a **presumption of conformity** with the corresponding essential requirements, and, in some cases, a **simplified conformity assessment**.

As far as **cobots and mobile robots** are concerned, the study demonstrated that they are mostly qualified as machinery or partly completed machinery, and that – since manufacturers often rely on self-certification – the subject who faces the most relevant burden is the SI, who substantially modifies the original product also adding collaborative features, and will thus need to obtain certification again. Likewise, certification will be required also by business-users, should they decide to further adapt and modify the integrated machine.

Despite not specifically adopted for such kind of applications, both the **legal framework and the standards available appear sufficiently defined and enough in number.**

On the contrary, (i) the peculiar nature of industrial **exoskeletons**, (ii) the certification burden resting mainly upon the manufacturer alone, and (iii) the qualification pursuant to the applicable legal framework, are more ambiguous, leading to **uncertainties** and market-driven qualifications, which might create problems in the longer run. Additionally, only general standards apply to exoskeletons, since no specific ones could be found. Thus,

framework amendment would be welcomed by stakeholders: **legal provisions concerning industrial exoskeletons would help clarifying duties that lie on manufacturers and the other involved subjects, issue of more standards would aid in pursuing the same goals**.

Despite mentioned by stakeholders operating primarily in the field of exoskeletons, the suggestion of **creating a public database and repository of already applied certification procedures that could ease the position of those seeking the certification of advanced devices** – which might not fall squarely under a specific regulation –, seems of greater value, and might be generalized to include other kinds of advanced industrial robotic applications. In such a perspective, intellectual property rights and relevant industrial secrets should always be protected and be left unaffected.

***Liability*.** Liability issues are tackled by a legislative and regulatory framework addressing both (i) **safety and health on the workplace** and (ii) **general private law liability burdening producers for defective products**.

Sub (i), a comprehensive set of European normative bodies – and national implementation acts – require business-users to ensure that workplace – to be intended as both working environment, equipment and working conditions – are not only safe, but globally healthy for employees.

Therefore, **in case of relevant accidents or illnesses, workers are entitled to obtain damage recovery**. In most Member States, liability regimes related to work accidents are coupled with **social insurance mechanisms**, so as to strengthen the employee's position and not to discourage entrepreneurship. Given certain conditions, social insurance bodies are then entitled to act in recourse against employers.

Sub (ii), both manufacturers, suppliers and integrators may qualify as producers, pursuant to the **Product Liability Directive** (PLD), which establishes a **semi-strict liability** regime burdening producers. PLD has been shown to offer **insufficient protection to the victims**, providing sometimes difficult liability ascertainment and apportionment, and an uneasy burden of proof concerning defects and causal links.

Nonetheless, besides the general need of a PLD reform, under IRs' point of view **the current liability and insurance *status quo* is sufficient**, because the **victim may clearly identify the party *prima facie* responsible to provide compensation** – namely the business-user –, and **contractual agreements and business relations thoroughly bind relevant stakeholders**. Moreover, the absence of theoretical disproportion in negotiating power or access to technical evidence, and the likelihood that liability-related costs can be sensibly distributed along the value chain, sensibly reduce concerns that would otherwise be present due to some criticalities that emerge from the application of the PLD.

3.3.2. Connected and Automated Driving

Introduction. Automated driving has the **potential to bring many social benefits**, and most importantly to increase road safety by eliminating the major cause of accident, i.e. human error, and its introduction has been supported by the European Union through different policy initiatives.

CADs are vehicles which display two main features: (i) **they are connected with other vehicles, with the infrastructure, and/or with other devices; (ii) they have different degrees of automation**, which, for the purpose of this report, are indicated according to the SAE scale of automation.

At the EU and international level, both the definition of vehicle set out in the Framework Directive 2007/46/EC (FD), and in the Motor Insurance Directive (MID) do not include the human driver as a constitutive element. Likewise, many – but not all – MSs possess a definition of vehicle, that would accommodate CADs.

Testing. The amended **Vienna Convention on Road Traffic** allows automated driving, provided that the technologies used comply with the UN regulations, or can be overridden by the driver. Many MSs have regulated testing of CADs on public roads, according to different requirements and procedures. The majority only allow high automation, while others also accommodate trials of fully autonomous vehicles, or are taking actions in that direction.

Testing is performed both on whole vehicles, on components and on systems of components, usually according to a combination of different techniques. Physical testing can take place indoors, outdoors, in controlled environments and on public roads, while virtual testing involves computer modelling. During trials, it is fundamental to take into account CADs specific risks – related to machine learning, cyber-security, unpredictability of the driving environment (e.g. because of the behaviour of bystanders in real life testing), and the possible fall back of test-drivers.

Fragmented regulation limits the possibility to test among MSs, creates additional burdens on companies, and hinders technological innovation. Only **EU level novel regulation** seems able to tackle the aforementioned issues, build a level playing field and enhance innovation, especially when higher degrees of automation are considered. This should be accompanied by **exploitation of virtual testing and common repositories of benchmarks and data sharing tools**. The creation of **Tokku zones and regulatory sandboxes**, derogating from regulation which is incompatible with testing of CADs, is suggested as a way of facilitating trials in real life condition.

Initiatives to foster research and development of technical solutions incrementing the accuracy, variety and complexity of the scenarios which CADs shall be tested against, especially through virtual testing, as well as tools for data-sharing and common benchmarks and practices, are needed.

Certification. For certificatory purposes CADs are compared to road vehicles, therefore, pursuant to the European applicable framework, the relevant conformity assessment procedure is the **type approval**, which in turn makes reference to **UNECE Regulations**, and is based on the principles of third-party assessment and mutual recognition.

UNECE Regulations, initially established in 1958, have **gradually and partially been amended in order to describe requirements for advanced devices involving automation.** Therefore, even if completely autonomous steering is still forbidden in any case, vehicles featuring steering aids can now be type-approved. As far as the braking function is concerned, as well, automated braking devices – able to prevent accidents and improve the vehicle's safety overall – are allowed and comprehensively regulated in UNECE Regulations. Concerning the lighting devices, on the other hand, UNECE Regulations now allow the automated switching on of emergency lights in case of danger, but still do not allow direction indicators to switch on independently.

Thus, **UNECE regulations appear capable of adapting** over time and encompassing major advancements. **Future reforms to accommodate emerging features could be awaited**, similarly to what already happened and was just described.

More globally, **the whole type approval procedure**, envisaged by the applicable European Framework, **does not seem perfectly consistent with CADs' peculiar features** and the advanced degree of technology shown.

First of all, type approval is focused on a static evaluation of a vehicle specimen at a given time. While this is consistent with the nature of traditional non-automated vehicles, which do not modify or update over time, it **fails to take into account the fact that AI applications – among which CADs – evolve their functioning, learning from previous experiences and receive constant and substantial updates**.

Components which are based on AI, moreover, do not interact among each other simply from a mechanical or electrical perspective, just like traditional road vehicles' parts, but they do so at a wholly different level, involving other CADs and infrastructures.

On side of that, a feature of CAD is not just the increasing degree of automation, but also the **novel connection that occurs both between different vehicles and between vehicle and road infrastructure**. A static evaluation method like traditional type-approval does not take this phenomenon into account.

Therefore, several stakeholders suggest that **the type-approval certification method should be amended, in order to adapt to new AI-based technologies, by introducing a more convenient and less burdensome approach, that may take advantage of virtual testing and modelling techniques, and that requires the monitoring of the performance of the vehicle over time**.

Liability. At a European Union level, relevant bodies of regulation concerning liability issues and CADs are **the Product Liability Directive (PLD) and the Motor Insurance Directive (MID)**, both of which have recently been subject to official evaluation, in order to assess whether technological developments suggest revisions or amendments. As far as the former is concerned, the conclusion was reached that the PLD is fit for purpose, while, as far as the latter, instead, a reform proposal has been developed but it does not address CADs.

More broadly, since almost the totality of CADs is to be legally considered as road vehicles, **regulatory framework concerning motor liability and insurance apply, also at MS level**. Research on different MSs' legal systems showed that the driver and owner are usually held liable, oftentimes in jointly and severally. Some MSs chose fault-based rules for the driver's liability and semi-strict regime for the vehicle's owner, while others opt for no-fault systems and automatic compensation plans, in order to better protect road accident victims.

Some countries enacted **ad-hoc legislative provisions regulating CADs**. **Germany** enacted a system whereby **liability rests upon the driver in case he fails to supervise** the driving task and resume control in case of need. In the United Kingdom, instead, the Automated and Electric Vehicles Act 2018 extends to CADs the insurance duties that typically concern traditional, non-automated vehicles, while the vehicle owner is responsible to ensure that all safety-critical updates are installed in a timely fashion.

Until vehicles reach full automation (SAE level 5), the driving-task is handled both by the autonomous system and the human driver; thence, **both the PLD and traffic liability rules apply, and overlap in determining liability for any given accident**. This circumstance causes the **apportionment of liability** among potentially liable parties to become ever more **complex**. Moreover, some criticalities that are already today displayed by the PLD – namely the complex burden of proof the claimant needs to meet in order to establish defectiveness and the existence of a clear causal nexus between the event and the defect – are further exacerbated by similar scenarios, primarily to the **disadvantage of the victim and even more of the owner of the vehicle**. The latter, indeed, will most likely be sued and won't easily succeed in acting against the manufacturer in recourse.

With respect to the evidentiary burden, it shall be further stressed how the **limited access to the data recorded** by the vehicle, as well as its complex interpretation, requiring access to proprietary information possessed by the manufacturer, might substantially impair the

possibility for the victim – or owner – to successfully bring a claim to court, giving rise to relevant problems of access to justice.

The simple provision of a duty to insure – despite useful – is incapable of successfully addressing the above described issues, for it should be clarified which party bears what risks.

It is argued that **the best solution**, in order to ease penetration of CADs into the market, while at the same time protecting other road users and enhancing innovation, **would come from ad-hoc legislation adopted at EU level**.

Indeed, absent EU initiatives, MSs would adopt different legislative and regulatory frameworks at national level, leading to regulatory and market fragmentation. A reform of the PLD, on the one side, would exceed the purpose, while, on the other side, requiring longer elaboration might induce MSs intending to act early to intervene, leading to a similar conclusion.

Ad-hoc EU legislation would be beneficial, with the aim of **creating a level playing field and to avoid fragmentation, both from a market and a technological point of view**: these two profiles are intertwined, since differing liability rules may yield different technological approaches, limiting cross-border market and operation of advanced AI-based vehicles.

It would be advisable to avoid focusing on the ascertainment of fault, while choosing a **Risk-Management Approach (RMA), therefore establishing *ex ante* to burden the party who is best positioned to minimize risks, to ensure compliance and to get insurance**.

RMA, in combination with **strict liability**, would identify a **clearly responsible party pursuant to a one-stop-shop approach**, easing distribution of costs along the value chain, primarily through contractual agreements, limiting litigation.

A viable example of a RMA, is that which burdens manufacturers and not users – unlike the UK law– with the duty to install safety-critical updates. While on the one hand, one could argue that the negligent user – who had been prompted to act and failed to do so – is to be reprimanded, the manufacturer is better positioned to ensure compliance, already in the way he designs and conceives the system and its updating functionalities.

3.4. Overview of activities and results in Task 5: Prospective foresight study on specifications of event data recorders

The final task of the study focused on **Event Data Recorders (EDRs)**. EDRs, popularly known as "black boxes", are devices that record and process information from a vehicle or system while it is in operation. The recorded data can be used for multiple purposes, for instance, **training, safety assessment, surveillance, vehicle diagnostics, testing and development**, etc.

One important use of EDRs is to determine event causation and contributing factors, for example for **legal liability after accidents occur**. In particular, this study focused on EDRs for road vehicles that make use of Artificial Intelligence (AI)-based algorithms and presented recommendations on the data and information that an EDR might need to record to help establish liability. While the study was focused on road vehicles, many of the findings (especially those related to AI-based systems) can also be relevant to other (semi-) autonomous systems in fields such as Industrial Robots (IR), Medical and Service Robots and Autonomous Shipping.

The analysis showed that the use of EDRs is **very common in the automotive sector**. Almost all new vehicles have EDR functions installed (i.e. not always a separate black box unit, can also be integrated using software). Today's event data recorder in the automotive sector is either a recording device that is retrofitted or is part of an on-board unit. Car manufacturers record a lot of data of their sensors and systems for maintenance purposes. Adding software that records specific data right before and after a specific event can then be seen as an event data recorder. However, these EDRs often **only measure basic sensory information** such as seat belt status, acceleration and speed. Storage of high-bandwidth information and decision-making processes from advanced (AI-based) systems inside existing EDRs is limited (or at least not publicly known).

Future **EDRs should record relevant information from these AI-based systems**, including the **operational situation**. This allows researchers to investigate a) whether or not the system was used in the right (environmental) conditions, b) how the relevant AI-based algorithms were trained and tested, and c) whether or not the datasets used for training and testing were representative for the situation in which the event occurred. Furthermore, AI-based systems should be designed with **explainability and situational awareness** in mind. Basic information about decision making processes (the what, where, why and why-not) of AI-based systems should be **stored inside the EDR itself**.

The study has provided r**eccomendations regarding requirements for future Event Data Recorders,** including a **suggested list of data categories** that a generic EDR should collect to aid establishing liability. Many of these items are also relevant for recording the events of non-AI based systems. In keeping the recommendations generic, the suggestions specify data categories instead of specific signals or physical variables. It is assumed that this data is recorded using the internal sensors of the "ego vehicle" (i.e., the vehicle carrying the EDR) or it is received by the ego vehicle from other traffic participants (including the road infrastructure).

However, **in the possible future legislation of EDRs, cost-effectiviness and the rapid advances in AI-based systems should be taken into account**. Setting **too high demands** on the amount and type of information required to be stored, **might hinder the advancement** and application of AI-based systems. Alternative solutions might involve storing the event data in a distributed way, using cloud solutions or storing the data in the infrastructure itself.

Better regulation on the issue of **who owns the data and how the privacy of the user is protected** is needed. It is at this moment unclear whether the data stored inside EDRs and RSUs is owned by the manufacturer, the owner of the car or the driver of the car. Further, it needs to be clarified how to protect the privacy and validity of the data inside and outside the EDR while allowing access to researchers and authorities. Initiatives such as the International Data Space (IDS) association can be useful to setup a trustworthy architecture to share data in a controlled way.

The **real danger of AI-based systems is that it may generalize poorly** (e.g., due to overfitting) **for previously unseen situations**. This may lead to poor performance or even unpredictable behaviour in critical situations at the onset of an event. The data (such as the version number of both the software and trainingdata being used) stored inside the **EDR should help to investigate whether or not the right testing and validation procedures were executed to account for this risk** during development and deployment of new or updated AI-based systems.

European Commission

Title

Luxembourg, Publications Office of the European Union

2019– 28 pages

ISBN number: 978-92-79-99495-1
DOI number: 10.2759/448974

ANNEXES

Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems

SMART 2016/0071

European Commission

Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems

SMART 2016/0071

Annex 1, Part A

Evidence gathering and analysis of Member States'legislation with respect to the safety of non-embedded software for CAD – CCAM (Task 1)

TNO 2019 R10095

A study prepared for the European Commission
DG Communications Networks, Content & Technology
by:

TNO innovation for life
VVA CONSULTING
Sant'Anna Scuola Universitaria Superiore Pisa

Digital Single Market

This study was carried out for the European Commission by

Authors:

- Tjerk Timan (TNO)
- Kristina Karanilokova (TNO)
- Marc van Lieshout (TNO)
- Andrea Bertolini (SSSA)
- Francesca Episcopo (SSSA)

Internal identification

Contract number: 30-CE-0887241/00-16

SMART number: 2016/0071

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN number 978-92-79-99495-1

DOI:number 10.2759/448974

Catalogue number: KK-04-19-076-EN-N

Table of Contents

List of Tables

No table of figures entries found.

List of Figures

No table of figures entries found.

List of abbreviations

Acronyms	Definition
AI	Artificial intelligence
B2B	Business to Business
CAD	Connected Automated Driving
CCAM	Cooperative Connected and Automated Mobility
C-ITS	Communication and Information Technology Services
C-V2X	Communication Vehicle to everything
ECU	Electronic Control Units
EDR	Event Data Recorders
EV	Electric Vehicle
GM	General Motors
GNSS	Global Navigation Satellite System
IP	Intellectual Property
LiDAR	Light Detection and Ranging
MaaS	Mobility as a Service
MCC	Mobile Computing Cloud
NASA	National Aeronautics and Space Administration's
NHTSA	Highway Traffic Safety Administration
OEMs	Original Equipment Manufacturer
OICA	Organisation Internationale des Constructeurs d'Automobile
R&D	Research and Development
UBI	Usage Based Insurance
V2P	Vehicle-to-Pedestrian
VC	Vienna Convention
TVAF	UN Task Force on Automated Vehicle Testing

1. INTRODUCTION AND BACKGROUND OF TASK 1

This report (part A) describes CAD-CCAM results of task 1 of the Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems. The other task 1 results were reported in the first progress report.

Task 1 of the study firstly focuses on the inventory of incidents with non-embedded software in the domain of health and wellbeing that is not captured by the Medical Device Regulation and with non-embedded software applications in the field of Connected Collaborative Automated Driving (CCAM). Secondly, task 1 provides an overview of regulatory activities in eight Member States in dealing with safety of non-embedded software related to health and wellbeing (not captured by the MDR) and related to CAD. The eight countries that are covered are, in alphabetical order: Austria (AU), France (FR), Germany (GE), Italy (IT), The Netherlands (NL), Spain (ES), Sweden (SW) and the United Kingdom (UK).

The focus will be on safety in a generic manner, understood as the absence of harm or risk and danger to persons. Wherever possible, a delineation of safety caused by harmful failure of technical aspects will be included. The technical aspects will concentrate on the following three sub-questions: what cyber security risks, connectivity risks and risks associated with failures in data management can be identified? This chapter starts by clarifying the meaning of a number of concepts that are relevant in the context of this study. First, the concept of safety will be introduced and elaborated upon (section 1.1). Second, the concept of an incident will be further explained (section 1.2). Thirdly, the concept of non-embedded software is explicated (section 1.3).

Chapter 2 will cover an exploration of safety risks and incidents related to CAD/CCAM After introducing the task, we will discuss risks and incidents and we will provide an overview of reported or known incidents per risk category (section 3.2), followed by a section discussing connectivity in relation to automated driving (3.3), product safety (3.4), liability (3.5) and data protection (3.6) In 3.7 we will provide an overview of regulatory initiatives and reports per Member State, finishing with conclusions and connections to other tasks in section 3.5.

Task 1 focuses on understanding safety risks associated with non-embedded software in a number of distinct domains. In the next sections what should be considered a (serious) incident is outlined (1.2) and what should be understood by non-embedded software (1.3). We start with outlining the methodology followed for the task (1.1).

1.1. Methodology of the tasks

Task 1 is aimed at exploring recent incidents and accidents regarding Health & Wellbeing Apps and CCAM and to find out if and how Member States are responding to these. In order to grasp what is happening in the Member States, we have created a list of experts for each task. Parallel to this contact list, we have performed desk research, looking into recent EU- and MS-specific reports and projects dealing with safety i.r.t. non-embedded software. The experts we have talked to come from industry, government and academia. The work presented in this interim report will flow into consecutive tasks in the project. There is a dedicated expert workshop on CCAM planned in Task (we will provide a list of interviewees, contacts and references).

In terms of research limitations, the following remarks:

- Access to legal expertise in each Member State. We have tried to gather legal expertise through our network and contacts, yet both in terms of time and language, this turned out to be challenging.

- Terminology, scoping and timing. Both in terms of incidents and risks, there is not much to be found as of yet. Since autonomous vehicles are as of yet not allowed on public roads in the EU, court cases are non-existent. There is regulation regarding testing on public roads. However, since some recent serious accidents with autonomous vehicles in the US, actual road testing seems uncertain from an industry point of view.

- Embedded vs non-embedded software. Although the study is based on an EC-provided definition of non-embedded software, especially in CCAM industry, but also in academic literature, such terminology is not always recognized (see conclusions-section)

- Non-response to survey and mitigation plan. In case of CCAM, we have sent out a survey regarding incidents and liability (135). However, the survey responses were low (9). We have since relied on interviews and desk research for CCAM.

1.2. A safe product

In the document that was used for the public consultation on the safety of apps and other non-embedded software, the EU defines safety as the "freedom from unacceptable danger, risk or harm including security-vulnerabilities ("cyber-security") and cover[ing] physical, economic as well as non-material damage." Harm is the manifestation of physical, economic or non-material damage. Risk and danger refer to the probability that harm may be caused. The definition of safety as put forward in the consultation document refers to a level of harm that should not be trespassed in order for the product to remain acceptable. For medical devices, this level is associated with risk classes (see below). For non-medical devices, the classification scheme to determine the level of acceptability of risk and harm needs to be provided by other regulatory schemes.

The most relevant scheme in this respect is the General Product Safety Directive (2001/95/EC). The GPSD defines a 'safe product' as a product that under normal foreseeable conditions of use poses limited and acceptable risks. In case of health and wellbeing applications, risks will be associated with health risks. Other risks are relevant insofar they lead to health risks. In case of CCAM, risks will be associated with harm for persons, either in the vehicle or outside the vehicle. Cybersecurity risks or other technical risks are relevant insofar they have health consequences or impact upon persons in or outside the vehicle in case of CCAM.

Article 2 of the GPSD clarifies how safety requirements should be identified. It stipulates the following sequence of measures (art 2(3)):

a) voluntary national standards transposing relevant European standards;

b) other standards drawn up in the Member State in which the product is marketed;

c) Commission recommendations setting guidelines on product safety assessments;

d) product safety code of good practices in force in the sector concerned;

e) the state of the art and technology;

f) reasonable consumer expectations concerning safety.

The GPSD differentiates between national standards (identified under (a) above) that refer to European standards that have been published in the Official Journal of the European Communities and European standards that have not been published in this Journal. For the first category, the GPSD defines a procedure to be followed (art 15(2)). For software as a service , the GPSD calls upon the European standardisation bodies to come with rules

governing the safety of information society services (defined in Directive 2001/31/EC). Basically, the GPSD thus refers to national standardization bodies to define acceptable levels of risks for non-embedded software.

Concerning guidelines set by the Commission (see 'c)' above), these should refer to how the safety of a product is assessed. This study will check the availability of these guidelines for CCAM.

Codes of conduct and/or good practice may be established by organisations working in the sector under consideration. Such a code could be formally agreed upon and could lead to established quality trust marks. The General Data Protection Regulation, as an example, enables the establishment of Codes of conduct as an instrument to demonstrate accountability (GDRP, art 40). Certification schemes may play a role as well (GDPR, art 42 and 43). The GDPR perceives certification schemes as a trust mark and as a manner to demonstrate compliance.

Regarding the GPSD, state of the art and technology is not properly described in this Directive. It may refer to common and accepted perspectives on risks associated with a specified product or technology. The GPSD does not describe what levels of risks are associated with state of the art and what measures should be adopted. Some technologies will by themselves be associated with a specific risk, such as nuclear technologies. In the situation of health and wellbeing software this could relate to the complexity of the software and common standards associated with mastering this complexity. In the situation of CCAM it could refer for instance to the space for manoeuvring if something goes awry with speed influencing the available response times. But the GPSD does not formulate strict criteria for risks associated with state of the art or technology.

Finally, reasonable consumer expectations play a role in determining risk levels. People will expect that applications behave as expected. The complexity of the environment in which CCAM applications would function, both in a technical and in a 'logical' sense, makes it extremely difficult for laymen to understand what precisely is determining the behaviour of the applications. They should thus act as one would expect them to act. In the case of CCAM this could be in the software that controls basic functions of the vehicle or in the accompanied software application that communicate with the car (navigation software for example). In case of malfunctioning software in-or connected to the vehicle, one of the questions that arise is under which scheme or Directive this would fall.

Regarding the latter, in in a different context, the Commission warns in a Staff Working Document on Lifestyle and Wellbeing apps, for example, on the applicability of the GPSD for these apps. It states: "Due to the fact that both the General Products Safety Directive and the Directive on liability for defective products apply to manufactured products, it is not yet clear if and to what extent they apply to lifestyle and wellbeing apps." The problem relates to the question whether software applications can be considered manufactured products. This is not easily solved. Presuming an application can be considered to be a product that is sold or offered against remuneration (which could exist in access to data on the carrier of the app), it could fall under the GPSD. However, this would be unlikely when taking the history and context of this Directive into account. Relevant in this description is the notion that a product can relate to providing a service. But even then, it still remains to be seen whether the service provides a separate product (a navigation app, for instance) as part of a more extensive package, or whether the service itself should be seen as a product.

Given the presence of a producer of a software, i.e. the person or organization responsible for the design and construction of the software and the accompanying service (usually an information society service, according to the eCommerce directive 2000/13/EC), in this study

we will start from the position that the definition of a safe product as used in the GPSD is potentially applicable to software applications (and to non-embedded software overall).

1.3. A (serious) incident

The second element to cover is what characteristics or constitutive elements of danger, risk or harm can be discerned that could lead to the safety risks being unacceptable. While harm refers to (physical, economic or otherwise) damage that has materialized, danger and risk refers to potential situations, i.e. situations that have a probability of arising. Danger refers to an identifiable threat that could materialize; risk refers to the probability a specific harm is caused. The safety of a software application is thus determined by the probable chance that the use of this application gives rise to an unacceptable situation.

A situation that is different from foreseeable situations, associated with a normal functioning of the application is termed an incident. Malfunctioning of a device may have various origins: defects in the hardware, such as a break-down of connectivity, a short circuit in the electronic components, a loss of power; defects in the software, such as incorrect software or a faulty upgrade of a new software version; defects in the data used for the software, such as lack of qualitatively sound data, missing data, data which are not sufficiently accurate. A device that is hacked may malfunction due to a variety of problems: compromised data, compromised software, or compromised functioning of the device. Incidents may go unnoticed, while causing harm to a subject.

1.4. Definitions of non-embedded software

This study relates to the safety of non-embedded software. A feature of non-embeddedness relates to the role the downloadable software plays. The Commission makes a distinction between functional and non-functional software with respect to the device on which it is downloaded. Functional software is software that is directly supportive to the function of the device or vehicle on which the software is downloaded. A CT-scanner for instance requires software that makes the CT-scanner function as a CT-scanner. Software that is additionally used to analyse and interpret the images delivered by the CT-scanner is an example of non-embedded software, presupposing it is separately installed on a specific device. Another example can be found in the smartphone. The smartphone needs software to function as a (smart) phone, i.e. software to connect the phone to a cell tower and software to help the user making a phone call or an internet connection. Usually, this software is updated every now and then in order to improve the functionality of the software of to close security gaps. The mere fact that this software is downloaded and is frequently updated, does not turn this software in the non-embedded software that is of interest for this study. Software that comes with applications that are different from the basic functionality of – for instance – the smart phone by contrast is non-embedded software. This can be a game, a calendar, a mail programme, a photoshop programme, a text editor, etc. In case of CCAM, software that directly impacts upon the basic functionalities of the car, such as breaking or steering, fall outside the realm of this study. Again, this software may be updated from time to time but this feature does not determine whether the software should be considered non-embedded or not. Only when the software functions as an add-on to the basic functionalities within the car, such as providing additional navigational information or additional information on how the car drives and how the car driver functions, this software should be considered to be non-embedded.

1.5. Summarizing the relevant concepts for the study

All relevant concepts have now been defined:

1. Non-embedded software relates to software that is additional to the primary function of the device on which it is downloaded. This software can be updated, but this is not a distinguishing feature in itself. The distinction is in the function of the software: it adds to the basic functionality of the device om which it is downloaded.

2. Non-embedded software is considered to be safe when it does not give rise to (serious) incidents that compromise the safety of subjects that either directly or indirectly can be confronted with the consequences of these incidents.

    a. Compromising safety means inducing physical, financial or other forms of non-material harm to individuals.

    b. For CCAM, harm could be financial, for instance by an accident with a car that leaves the driver unharmed but causes serious damage to the car.

3. Regulations, guidelines, certification schemes, etc. contribute to reducing the safety risks associated with non-embedded software.

2. AUTOMATED DRIVING/CAD/CAMM

2.1. Introduction: non embedded software and risks in CAD/CAM

Regarding CCAM, this task is a first overview study into reported incidents and accidents of CCAM within Europe or outside, followed by an overview of possible court cases surround these incidents (if any). The point of this mapping is to then distil novel risks related to non-embedded software within automated driving and to see if and how there are novel angles to liability. As this part of task one is a first mapping of a longer and larger legal task regarding liability, we have done a first overview / mapping only – more detailed analysis will take place in task 2 and beyond. In identifying the grey zones from a regulatory perspective, the report here covers only a first analysis of the RED, the GDPR and other directives and regulation that tough upon non-embedded software in devices and machines – this analysis will be taken a step further during consecutive tasks.

Regarding novel risks in relation to non-embedded software, we have looked for aspects of non-embedded software that could pose a risk. The dilemma here is that, as stated in section 1, the notion of non-embedded software assumes that this software is non-vital or non-trivial for the working of the vehicle. However, this assumption automatically leads to a category of risks that are very low, or that cause for indirect risks (e.g. being distracted by meddling with the in-vehicle entertainment system, trusting too much on the automated vehicle to do the driving etc). Such a reading would broaden the risk-scope or landscape too much in our view. On the other hand, based on a fist set of interviews and readings the distinction between embedded and non-embedded software becomes blurry when realizing the context of CCAM on the public road: vehicles would need to communicate constantly and (near) real-time with other vehicles, with back-end servers, with the surrounding infrastructures, with the passengers of the vehicles etc. Moreover, they would increasingly monitor and communicate their own status, be it for performance, maintenance and/or insurance reasons. Many players of software and networked "smartness" would be involved that would run across current divisions of embedded-and non-embedded. As such, the risk-landscape i.r.t. non-embedded software should be expanded to also external networks and/or infrastructures – basically to the network of things and people the automated car is sending data to and getting data from.

In terms of methodology, at the beginning of the project a short exploratory survey was conducted among various stakeholders (industrial organizations, academics, etc). The survey included a small set of questions; asking if the person is aware of non-embedded software incidents, the national legislative frameworks, as well as their opinion on the most pressing issues regarding non-embedded software in relation to safety.

In total 135 invitations to fill in the questionnaire were sent out by the end of January. Unfortunately the survey resulted in only 9 replies which number is insufficient to draw conclusions from.

Due to the low response rate, it has been decided that this line of data collection method would not be continued. Instead, information will be gathered via desk research and where possible interviews. The experts we have contacted were provided by the Commission, by in-house experts at TNO and through contacting authors of reports. We have used this information to base our first findings on.

2.2. Risk and Incidents

2.2.1. Incidents

The team performed an initial online search for publicly announced incidents related to connected and autonomous driving. Based on the results, so far it appears that most of the incidents are related to cybersecurity (hacking a car) and data access and confidentiality. The main incidents found until this moment relate to:

- Cybersecurity – the best documented case is of the hijack of a Jeep's digital systems and disable the brakes (2015)

- Data management and access – mainly cases of leaked data from various providers – Uber users data and drivers data leaked, information for car tracking devices Stolen Vehicle Records were leaked online, possibility (not real case) to use proprietary mobile apps to get the GPS coordinates of a car, trace its route, open its doors, start its engine, and turn on its auxiliary devices.

- Interaction with autonomous cars with human-operated cars- e.g. due to the car following the traffic rules completely and not accounting for other actors erroneous behaviour.

2.2.2. Risks

With the introduction of new technologies moving towards connected, collaborative and later on autonomous driving requires that the operating software is continuously updated to meet the complex environment on the road. Not only would vehicles need to account for traffic rules, traffic conditions and other participants in the traffic but the software might need to take into account unexpected behaviour of the other road participants and new situations. Looking at autonomous driving, Litman notes that ensuring that such complex software never experiences problems is impossible as the system complexity can lead to potential failures.

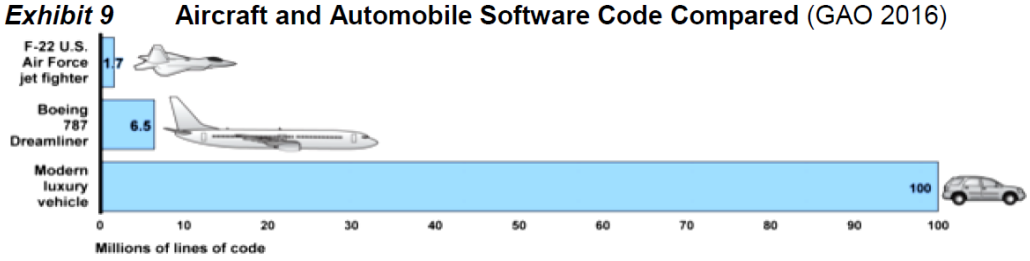


Figure 1: complexity of cars. Source: Litman (2018), p 13

From the literature search on recent academic literature and study reports, as well as posts in popular media, the following table of incidents and risks regarding CAD/CCAM could be made. Note here that due to the fact that self-driving cars are not allowed yet on the European motorways, actual incidents of autonomous vehicle stem mainly from the US and range from busted taillights due to the automated vehicle breaking too abruptly before a traffic light (surprising the human driver that was behind the automated vehicle) to the recent fatal accident involving a pedestrian crossing a street in the dark, unseen by the

sensors on the automated vehicle[1]. Keeping this in mind, we have mapped the incidents, accidents and risks we have found in literature according to a set of categories (which we will elaborate on in the following sections). Regarding the incidents, literature studies distinguish among vehicle to vehicle, vehicle to infrastructure and vehicle to everything possible risks.[2] As the incidents recorded so far generally involve self-driving testing cars or cars using autopilot functions, we have not made that distinction. In the future however, it might make sense to distinguish the different incidents based on which level the problem occurred. Regarding the risks, we have tried to categorize risks found in literature among the three sub-categories of digitisation in relation to automated driving, being cyber security, connectivity and data management. Also here we have added an 'other' category to capture all types of risks that did not fit these categories, yet were identified in literature as a CCAM risk. Provisionally, this lead to the following table:

Table 1: Reported Incidents

Description of the accident/risk	Risk category low, medium, high (explanation)	Reported where?	Reference
in 2016 Tesla Model S in autopilot crashes into a tractor trailer. The Tesla was travelling on a highway and did not detect a crossing tractor trailer. It is believed that the combination of a bright day and the white colour of the tractor trailer made it difficult to see. Neither the Tesla Autopilot nor the driver of the Tesla engaged the brakes	High - the accident was fatal	US	https://www.engadget.com/2016/06/30/tesla-under-investigation-after-first-autopilot-related-death/
In 2017, Tesla Model S crashed into a stopped firetruck. The driver claimed that the car was on autopilot. Other non-fatal accidents have occurred (eg. drunk driving on autopilot, accidents reported in California, etc)	High - the accident was fatal - accident was not fatal but the crush occurred	US	https://www.wired.com/story/tesla-autopilot-crash-dui/
In 2018, a UBER self-driving car hit a pedestrian. The accident was fatal for the pedestrian. It is still not a 100% clear if the accident could have been prevented from a driver or the safety driver in the car.	High- the accident was fatal	US	https://www.wired.com/story/uber-self-driving-crash-explanation-lidar-sensors/ https://www.reuters.com/article/us-autos-selfdriving-uber-trust/self-driving-car-industry-

[1] https://www.theguardian.com/technology/2018/mar/31/tesla-car-crash-autopilot-mountain-view

[2] See in general "C-ITS Platform – Final Report Phase II, September 2017" or REGULATING AUTOMATED DRIVING THE UK INSURER VIEW – Thatcham Research report, 2017

			confronts-trust-issues-after-uber-crash-idUSKBN1GY15F
In 2018, a Tesla Model X SUV crushed into a concrete barrier while on Autopilot. The car burst into flames and resulted in a fatality. Investigation is ongoing but Tesla has reported that the driver should have been able to see the barrier and respond before the crush as well as the driver's hands were off the steering wheel.	High- the accident resulted in a fatality	US	https://www.wired.com/story/tesla-autopilot-self-driving-crash-california/
In 2011, Nissan Leaf Carwings was found to leak driver's location, direction, and speed to third parties. The systms uses GSM celluar internet connection which provide voluntary telemetry information to Nissan and has been reported to then be leaked to third parties without the knowledge of the driver.	Moderate to high as the data can help identify an individual and can be classified as personal data.	worldwide	https://www.computerworld.com/article/2470123/endpoint-security/nissan-leaf-secretly-leaks-driver-location--speed-to-websites.html
In 2015, personal data of 674 Uber drivers was exposed. The leak was connected to the "Uber Partner" app and lead to the exposure of information such as vehicle registration number, social security numbers and others.		US/world wide	https://www.theverge.com/2015/10/14/9529095/uber-leaks-personal-information-hundreds-drivers
In 2015, sensitive personal data for 50,000 Uber drivers was exposed as sensitive database key on public GitHub page		US	https://arstechnica.com/information-technology/2015/03/in-major-goof-uber-stored-sensitive-database-key-on-public-github-page/
In 2017, Mashable reported that "login data for more than half a million records tied to vehicle tracking device company SVR Tracking have leaked online". Data might have exposed vehicle ID numbers, license plates, GPS data			https://mashable.com/2017/09/21/vehicle-tracker-user-data-leak/#mB17Licptmqn https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/tracking-device-information-for-over-500-000-vehicles-leaked-online
Data in connected cars might survive being wiped and might share sensitive information, even could still be accessed via the management app		potentially worldwide	https://www.iottechnews.com/news/2017/feb/20/connected-cars-and-iot-devices-leak-previous-owners-data/

			https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack
In 2016, Charlie Miller and Chris Valasek demonstrated that when a laptop is directly plugged in the CAN network they can bypass some of the safeguards and override contradicting signals.	potentially high if a computer is connected	potentially worldwide	https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/
In 2015, Charlie Miller and Chris Valasek demonstrated that "they could remotely hijack a Jeep's digital systems over the Internet" and paralyze it. This led to Chrysler recalling 1.4 million vehicles.	high- control over vital parts of the car (brakes at low speed for example)	potentially worldwide	https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/
The Epoch Times reported, "For years now Chinese authorities have been installing spying devices on all dual-plate Chinese-Hong Kong vehicles, enabling a vast network of eavesdropping."		China/Hong Kong	https://www.computerworld.com/article/2470123/endpoint-security/nissan-leaf-secretly-leaks-driver-location--speed-to-websites.html https://www.infowars.com/chinese-spying-devices-installed-on-hong-kong-cars/

Table 2: Risks identified in literature

Risks identified	Risk category-detail	Risk description	Risk level (high/medium/low)	Where
	sensors performance and risk of damage	sensor damage due to AV braking too well /rapidly – a consequence is that the sensors necessary for AV mode are damaged		US
data management	data collection, potential security risks of the data	In 2015, senator Edward J. Markey contacted major car manufacturers to enquire about their security measures arising from connectivity and data management. The conclusion was that almost 100% of all cars use wireless technologies which might lead to hacking or data privacy issues, that customers are often not explicitly aware of the data collection, car manufacturers were unaware of or unable to report on past hacking, security measures to prevent remote access to vehicle electronics are inconsistent incidents, it is not clear how data security is ensured for data collected and wirelessly transmitted to data centers.		US
data management	data collection and management of personal data	A study looking at the data collected by the infotainment system of connected rental companies and/or car share schemes found that personal information of the drivers could be found. The policies of the companies state that it is the responsibility of the drivers to delete such information but the restore factory settings option is generally difficult to find. Some of the information might be personal data.		US/EU/UK
data management and cybersecurity	data from apps to encrypted and susceptible to reverse engineering	IoTtechnews reported that findings of a researcher related to connected cars apps showed that "six of the applications did not encrypt usernames and were susceptible to reverse engineering techniques or hijacking by malware. "		potentially worldwide
cybersecurity	hacking, physical integrity	Kuzin and Chebyshev note that car-controlling apps are popular but studying 7 popular apps of different brand showed that all of the apps turned out to be		potentially worldwide

		vulnerable to attacks (easily infected to get log in details for example)		
cyber security	hacking, manipulation and malware	ACEA notes that currently, the safety of critical systems of cars is constantly being refined by separating control circuits and using the latest encryption methods – from the vehicle's telematics interface all the way to the vehicle manufacturer's backend – combined with various security tests Similarly, T.Litman notes that self-driving technologies might become target for malicious hacking for amusement or crime.		EU/potentially worldwide
cyber security		After a group of attackers has done the work to identify an attack vector, they may share that attack publicly, simplifying follow-up attacks. Several workshop panelists raised the possibility of remote attacks that could involve large numbers of connected vehicles.		potentially worldwide
		hackers get into core of the car via third-party applications		US
		Some stakeholders warned that there are potential risks to security and safety involved in any method of obtaining in-vehicle data and that the system established to access in-vehicle data could have large effects in terms of market fairness and equality.		EU
other, being:	coordination with other participants in the traffic	connected and automated driving in a mix environment where different levels of compliance with the traffic rules/ behaviour exist	medium - generally accidents occur with low speed areas	potentially worldwide
	fraud and theft as a result of networking and third party access	uncontrolled access to vehicle data or functions by third parties brings secondary security risks through networking (eg. enabling vehicle theft and remote door unlock, mileage manipulation, improper creation and misuse of movement profiles or sale of personal data)		potentially worldwide

	driver distraction	apps visualized in the head-up display are considered safety-critical due to broad networking with other vehicle functions and consequently uncontrolled access to on-board systems and interfaces and function displays might need to be left in the control of the manufacturer		EU/potentially worldwide
	Hardware and software failures	CCAM involves complex systems and as with any other complex electronic system are likely to experience system fails. These might involve different be related to software errors or sensor malfunction, distorted signal, etc.		potentially worldwide
	increased risk taking and platooning effects	a more indirect consequence of the technology is that drivers might become too confident in the performance of the vehicles and might start taking additional risks - less attention on the road, not wearing a seatbelt or joining potential dedicated roads for automated cars		potentially worldwide
	overconfidence of assistive but not yet autonomous systems	while many of the semi-autonomous, self-steering systems reiterate the driver should keep his attention on the road and include safety measures (detecting if the driver's hands are on the wheel, beeping, etc), there is a risk that drivers become overconfident in the systems and stop supervising and actively paying attention to the traffic. Some confusion between autonomous and semi-autonomous systems among customers could be expected. There have been instances in which drivers have claimed the autopilot is on as an explanation for a misconduct on the road (driving with higher alcohol levels)	potentially high as this might lead to putting too much trust in the system and allowing distraction on the road	potentially worldwide
	Always-on data connection might increase the risk of autonomous cars being hacked	Always-on data connection might increase the risk of autonomous cars being hacked as new ways to hack a car are expected to continue to be developed by hackers. For now, Waymo simply keeps the car offline as much of the time as possible.		potentially worldwide

cybersecurity	risks related to multiple access point to the software of a self-driving car	MIT Technology Review, published an article where a researcher claims that " once an attacker can get inside the Internet network linking the roughly 30 different computers inside, he or she can take over just about any component, from the brakes to the radio, [...] It's not possible to isolate the "important" parts such as the brakes because everything must be connected to enable many functions people expect of cars, as well as to allow repairs and software upgrades". The research points that control can be taken by dialing into a car's built-in cellular connection or using an infected CD.		potentially worldwide

2.3. Connectivity and access to data

The general risks associated with connected driving and cars has been addressed by many organizations. Already in 2016, ACEA published a Strategy Paper of Connectivity which outlines some risks associated with third party access to data.[3] The paper notes that there are up to 100 control units and different measures – such as separating control circuits, using encryption, and testing- are taken to protect safety-critical functions from risks such as hacking, manipulation and malware.
Uncontrolled access to data is seen as a potential opening of access points to the safety-critical systems and even in the case when the access to data is non-security related, risks of theft, fraud, hacker attacks and distraction of the driver might emerge.
According to the strategy paper, an appropriate technical solution is the 'extended vehicle' approach, which "provides access to vehicle data in accordance with clearly defined technical, data protection and competition rules through various interfaces and means of data storage, embedded and/or off-board, managed by the vehicle manufacturer".[4]

[3] ACEA (2016), "ACEA Strategy Paper on Connectivity - April 2016"
[4] ACEA (2016), "ACEA Strategy Paper on Connectivity - April 2016"

2.3.1. Scoping the framework of connected and cooperative automated mobility

Cooperative and Connected Automated Mobility (CCAM) involves three different components. To make a distinction among the different terms, ACEA had developed a roadmap of potential developments in all of the three notions in the next 20 years:

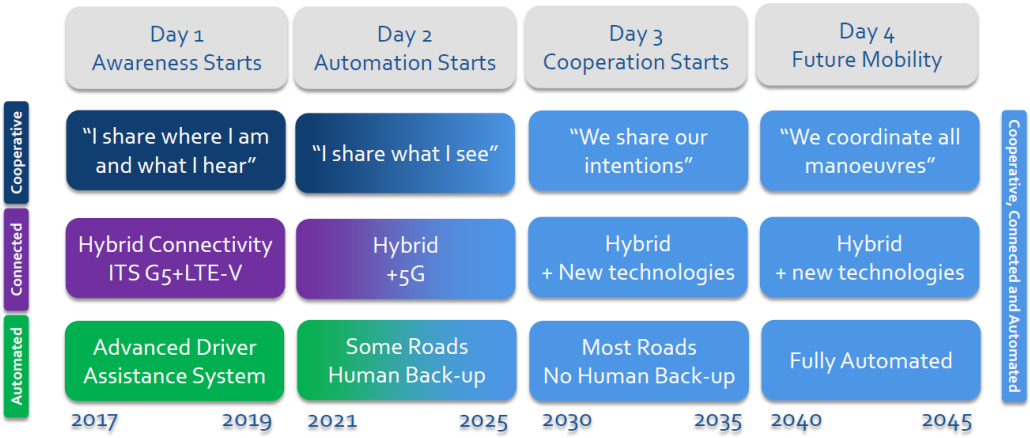


Figure 2: Joost Vantomme, ACEA (26 February 2018)

Based on this overview, it becomes clear that the term refers to autonomous vehicles as well as connected vehicles which communicate with nearby infrastructure and other vehicles. The topic is very broad and new developments and risk associated with connectivity, data management, privacy and cybersecurity are continuously evolving. To study this complex system, the following chapters outline the framework and the national development when it comes to CCAM.

As described above, the current state of play indicates that the majority of the software currently used in vehicles is embedded. Yet, the distinction between embedded and non-embedded software is quite difficult to make especially given the constant technological development and the possibility to introduce over the air updates managed by manufacturers and the introduction of proprietary apps by many car manufacturers. Therefore, we take the perspective of connected and cooperative automated driving as a whole and examine potential risks emerging with respect to cybersecurity, data management and connectivity. In this regard, it should be mentioned that there are many initiates and projects studying the impact of connected vehicles and the regulatory environment in Europe. Notably, a study by the ADAPTIVE project finalized a legal analysis in 2017.[5] The information below provides an overview of the applicable legislative framework as well as some developments in the Member States. We start with an overview of the EU framework as in many cases it is the basis for national initiatives.
On an internal level, several developments have had impact on the issue of cooperative and connected automated mobility. Recently (as of 2016), the Vienna Convention of Road Traffic has been amended to recognize that automated driving technologies are allowed provided that there is a driver who can take control/override the system or these systems are in

[5] AdaptiVe (2017), "Deliverable D2.3: Legal aspects on automated driving"

conformity with the relevant UN vehicle regulations.[6] This development has been seen as a milestone for the deployment of automated driving. In addition, in October 2017, the Informal WG on Intelligent Transport Systems presented proposal for definitions of Automated Driving under WP.29 and the General Principles for developing a UN Regulation on automated vehicles.[7]The proposal has been presented at the March 2018 meeting.[8]
Another currently ongoing discussion and revision affecting CCAM are the discussions on the UNECE Regulation 79 on Steering Equipment. Currently, Regulation 79 allows for Automatically Commanded Steering function to be operational only up to vehicle speed limit of 10 km/h.[9] Proposals for amendments of Regulation 79 have been presented to the WP29 meeting in March 2018.[10]

Connected and autonomous vehicles have been in the spotlight in the past several years. On European level, the Declaration of Amsterdam of April 2016 by national transport ministries called for a development of a European strategy on cooperative, connected and automated vehicles.[11] Agreements with industry and policy representatives of next steps needed to launch connected and cooperative vehicles on the EU roads were initiated.

A High Level Group GEAR 2030 was established and worked on developing medium and long-term actions and recommendations 'address the main challenges and opportunities for the European automotive industry in the run-up to 2030 and beyond.'[12] One of the conclusions of the HLG is that Europe should advance in two main areas: **connected and automated driving** (CAD) and zero emission capable vehicles. GEAR 2030 included a special working group that worked on a Roadmap on automated and connected vehicles. The WG also addressed and assessed the legal framework in place in order to determine if specific actions are necessary. The Working Group concluded, among others, concluded that:[13]

- EU Directives on liability for defective products (85/374/EEC) and on motor insurance (2005/14/EC) are sufficient for upcoming automated systems

---

[6] Article 8 paragraph 5bis of the Vienna Convention on Road Traffic, reads: "5bis. Vehicle systems which influence the way vehicles are driven shall be deemed to be in conformity with paragraph 5 of this Article and with paragraph 1 of Article 13, when they are in conformity with the conditions of construction, fitting and utilization according to international legal instruments concerning wheeled vehicles, equipment and parts which can be fitted and/or be used on wheeled vehicles*
Vehicle systems which influence the way vehicles are driven and are not in conformity with the aforementioned conditions of construction, fitting and utilization, shall be deemed to be in conformity with paragraph 5 of this Article and with paragraph 1 of Article 13, when such systems can be overridden or switched off by the driver" , see http://www.unece.org/fileadmin/DAM/trans/doc/2014/wp1/ECE-TRANS-WP1-145e.pdf

[7] http://www.unece.org/fileadmin/DAM/trans/doc/2017/wp29/ECE-TRANS-WP29-2017-145e.pdf

[8] https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29/ECE-TRANS-WP29-2018-2e.pdf

[9] See 5.1.6.1. of Regulation No 79 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of vehicles with regard to steering equipment, OJ L 137, 27.5.2008

[10] Proposal for the 03 series of amendments to UN Regulation No. 79 (Steering equipment), available at https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29/ECE-TRANS-WP29-2018-35e.pdf

[11] Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility

[12] https://ec.europa.eu/growth/content/high-level-group-gear-2030-report-on-automotive-competitiveness-and-sustainability_en

[13] https://circabc.europa.eu/webdav/CircaBC/GROW/automotive/Library/GEAR%202030/2017-07-10%20-%205th%20GEAR%202030%20Sherpa%20Meeting%20on%2010%20July%202017/2017%2007%2005%20GEAR%202030%20WG2%20PT1%20Draft%20recommendations.pdf, https://ec.europa.eu/growth/content/high-level-group-gear-2030-report-on-automotive-competitiveness-and-sustainability_en

- The ITS Directive 2010/40/EU[14] should be implemented by Member States and service providers. It should be strengthened for automated vehicle needs.
- There is no need to legally harmonize the national testing requirements for Large-scale tests of ACV
- There is a need to clarify liability and data storage and these should be included in the type approval legislation, the group considered that the rules on data recording (black boxes) and associated data access rules should be in the type-approval legislation
- There is also recommendation that preparation by the European Commission of the EU type-approval framework for the certification of automated vehicles, including alternative assessment methods and identification of work priorities at the UNECE, EU and Member State levels should be continued
- On traffic rules, no major changes are expected for mass market systems by 2020;

2.4. Product safety

Product safety has been addressed in a number of different regulatory instruments. Next to the General Product Safety Directive, relevant instruments regulating connected and cooperative vehicles are the provisions of the Radio Equipment Directive (RED), the Low Voltage Directive and the General Product Safety Directive rules may apply.
The RED Guidelines specifically mention the use of radio equipment in vehicles (section 6.3.11). According to the Guide, radio equipment installed in vehicles has to comply with the RED (unless this equipment is specifically excluded from the RED scope) and all other applicable EU acts. Further, it is clarified that the *"risk assessment should take into account the intended purpose*".[15]

The Radio Equipment Directive (RED) has been applicable since June 2016 (with one year of adjustment period) and has a large scope applying to "*electrical or electronic product, which **intentionally** emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination" or uses accessories to intentionally emit/receive radio waves*. The intentionality requirement therefore refers to the use of radio waves rather than the function of the equipment.[16] Nonetheless, the conformity of the radio equipment should be evaluated based on all intended operating conditions, reasonably foreseeable conditions and the requirement for health and safety of humans and animals. If different configurations are possible, all configurations should be assessed against the essential requirements.[17]

The Directive distinguishes between 2 types of essential requirements before a product incorporating radio communication and/or radiodetermination can be placed on the market:

- Essential requirements applicable to all radio equipment requiring that the health and safety of both humans and animals is protected as well as that the safety requirements set in the Low Voltage Directive (without voltage limit)[18] and the

[14] The ITS directive establishes the framework for the coordinated deployment of intelligent Transport systems in the EU. The Directive provides for the development of legally binding specifications for interoperability and continuity through delegated acts in four areas.

[15] RED Guide, page 14
[16] http://www.etsi.org/technologies-clusters/technologies/regulation-legislation/red
[17] Directive 2014/53/EU, Article 17(1)
[18] Directive 2014/35/EU , Article 3 claims that "Electrical equipment may be made available on the Union market only if, having been constructed in accordance with good engineering practice in safety matters in force in the Union, it does not endanger the health and safety of persons and domestic animals, or property, when properly

electromagnetic compatibility are ensured. [19] Related to the scope of application of the safety requirements, BEUC and ANEC have noted that product safety is often understood in a traditional and narrow way, thus excluding cybersecurity and safety of connected products.[20]

- Next to these requirements, the Directive also envisions essential requirements applicable only to specific equipment following the adoption of Commission Delegated acts.[21] As of August 2017, only the requirement that radio equipment supports certain features ensuring access to emergency services has been specified in delegated acts (automatic identification system used by ships for instance).[22] One of the requirements of RED are that radio equipment incorporates safeguards to protect users' personal data and privacy. While very applicable to the current project, the requirement is not yet enforced as no delegated acts have been adopted as of yet.

The RED envisions that the compliance of radio equipment with the essential requirements might be affected by the inclusion or modification of software.[23] Therefore, manufacturers should, in a statement of compliance, provide the MS and EC with information on the compliance of the intended combinations of radio equipment and software with the essential requirements.[24] In addition, the software/radio equipment combination needs to be described in the instructions manuals only when these combinations:

- "have an influence on the conformity of the radio equipment, and
- are intended to be installed or changed by the user without the control of the manufacturer"[25]

Consequently, as the RED Guide explains, where the software is installed under the full control of the manufacturer (e.g. software updates over the air), there is no need to describe the relationship in the manuals as the compliance with the essential requirements has been reflected in the technical documentation.

installed and maintained and used in applications for which it was made. The principal elements of the safety objectives are listed in Annex I."

[19] Directive 2014/53/EU, Article 3.1.a-b

[20] BEUC and ANEC (2018), "Cybersecurity For Connected Products: Position Paper", ANEC-DIGITAL-2018-G-001final - BEUC-X-2018-017 07/03/2018, page 10

[21] See Directive 2014/53/EU, Article 3.3 (a-i)

[22] RED Guide

[23] Directive 2014/53/EU, Recital (16-19), Article 4(1)

[24] Directive 2014/53/EU, Article 4(1)

[25] RED Guide, page 27

2.5. Liability of defective products

The liability framework in Europe is harmonized via the Product Liability Directive[26] which establishes the conditions under which the producer is liable for damages caused by defects caused in his products.

A study for the European Parliament (later incorporated in European Parliament Research Unit report) has concluded that while of great importance, "pre-emptive legislation of the Product Liability Directive (PLD) to encourage deployment of connected and autonomous vehicles is not required at this time" as there is a significant push to introduce connected vehicles and as manufacturers are likely to introduce their products in markets outside the EU as well and have to comply with different liability rules.[27]
The analysis for the European Parliament argues that while the current regulatory framework of the PLD seems to provide a well-balanced system, if not refined to reflect the changing system incorporating autonomous driving, "the application of the PLD to AVs will have a significant negative impact on consumer protection".[28] This is due to a few shortcomings when it comes to autonomous vehicles:

- The report notes that the scope of a product and whether it encompasses software are not technically defined. PLD (Directive 85/374/EEC) would most probably be able to encompass software within its scope, as a broad scope of the term product has been argued for from academics and the Commission.[29] The Directive includes in the definition of a product all movables, even though incorporated into another movable or into an immovable, and includes electricity.[30] However, the report notes that for this, the injured party would have to prove a defect in the software which might pose problems for consumers, especially taking into account that it is often not easy to trace the software producer.[31]
    i. BEUC on the other hand notes that software which is not included in a physical mobile data carrier will be difficult to include in the definition of movable as included in Article 2 of Directive 85/374/EEC (eg. Cloud technology and data).[32]
- A second obstacle is the definition of a 'defect' which refers to a situation where the product does not provide the safety which a person is entitled to expect.[33] The report by the European Parliament Research Unit argues that it will be difficult for users to

---

[26] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

[27] Charlene Rohr, Fay Dunkerley, and David Howarth, "Socio-economic analysis of the EU Common approach on liability rules and insurance related to connected and autonomous vehicles" Research Paper of RAND Europe, published in European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment"

[28] European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment", p.24

[29] Charlene Rohr, Fay Dunkerley, and David Howarth, "Socio-economic analysis of the EU Common approach on liability rules and insurance related to connected and autonomous vehicles" Research Paper of RAND Europe, published in European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment"

[29] European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment", p. 56

[30] Article 2 of Directive 85/374/EEC

[31] E.F.D. Engelhard and R.W. de Bruin (2017), "EU Common Approach on the liability rules and insurance related to Connected and Autonomous Vehicles", p 56, published in European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment"

[32] BEUC (2017), "Review Of Product Liability Rules: BEUC Position Paper", available at http://www.beuc.eu/publications/beuc-x-2017-039_csc_review_of_product_liability_rules.pdf

[33] Article 6(1), PLD

argue that it is reasonable to expect a perfect product,[34] especially in a complex systems such as autonomous cars. Additionally, different producers might 'have a wide margin of possibilities to shift costs of scientifically unknown risks through 'compliance risk' and 'development risk' defences to the consumer".[35] This combined with a few other gaps might lead to insufficient protection to the consumer.

The legal analysis for the European Parliament also identified 4 specific risks for which neither the PLD not the traffic liability rules provide sufficient clarity in light of autonomous vehicles:
(1) risks relating to the failure of the operating software and whether these could have been detected upon initiating the circulation on the market and what the reason for the failure was[36]
(2) "risks relating to network failures,
(3) risks relating to hacking and cybercrime, and
(4) risks/externalities relating to programming choice".

Traffic Liability Rules
The EU harmonization provided by the Motor Insurance Directive[37] mainly focuses on compulsory third party liability insurance and is argued to provide limited harmonization.. The report notes that with the exception of Sweden, most national frameworks based their traffic liability rules on personal responsibility of the driver or owner.[38]One of the conclusions of the report is that the national systems might need to be re-examined in view of the fact that the concept of a driver, owner and possessor of the vehicle is changing in the framework of autonomous vehicles where the driver will not always to be in control to create or limit the risk.

2.6. Data Protection and cybersecurity

With the entry into force of the GDPR from 25 May 2018 (superseding Directive 95/46/EC), becomes the leading data protection legislation on EU level. It provides, among other, for the protection of personal data processed wholly or partly by automated means (Article 2) and calls for data protection by design and by default (Article 25). Close attention should be paid by data controllers to determine which data is personal in the context of a connected vehicle. According to Störing, "for such a qualification it is neither relevant whether data compromises technical data, nor whether data is vehicle generated or provided by the

[34] Article 6(1)(b), PLD
[35] European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment", p. 23
[36] See Article 7 PLD (specifically b and e) which state that "The producer shall not be liable as a result of this Directive if he proves:
(b) that, having regard to the circumstances, it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterwards; or
(d) that the defect is due to compliance of the product with mandatory regulations issued by the public authorities; or
(e) that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered;"
[37] Directive 2009/103/EC Of The European Parliament And Of The Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability

[38] Charlene Rohr, Fay Dunkerley, and David Howarth, "Socio-economic analysis of the EU Common approach on liability rules and insurance related to connected and autonomous vehicles" Research Paper of RAND Europe, published in European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment

customer".[39] There have already been industry resolutions to protect privacy and ensure security and integrity of the data as much as possible.[40] Data protection authorities have also started to develop guidelines on how the data protection legislation (GDPR and national rules) are applicable in the framework of connected cars (see CNIL below). Generally, it is stressed that privacy rules need to be respected, best efforts employed to protect the data from unauthorized interference, information to the data subject should be easily understandable and complete, and the data subject's sovereignty to their data reiterated.

When it comes to data sharing, the debate of what data should be share and with whom is still ongoing. A recent workshop on the topic concludes that view on what model to use for the conditions to share data are still divergent.[41] A report by TRL on the topic of data sharing and the connected vehicles examined the legal consequences of the three solutions offered by the WG6 of the C-ITS platform (using Data Server Platform, In-vehicle Interface, or On-board Application Platform). The report concludes that "each option is likely to give rise to a range of legal obstacles that will need to be navigated by market participants and there is a risk that the current legal framework may allow the market to develop in a way that is inconsistent with the five guiding principles agreed by WG6 and with relevant European legislation in general (e.g. competition legislation)."[42]
When it comes to cybersecurity, the Directive on security of network and information systems (the NIS Directive) addresses cybersecurity and proposes measures 'with a view to achieving a high common level of security of network and information systems'. [43]The Directive will require, among others, for Member States to adopt national strategies on security of NIS, creation of computer security incident response teams and network; and sets security and notification requirements for operators of essential services and for digital service providers. Operators of essential services could be ITS operators and road authorities[44] which fulfil the criteria[45] of an:
"(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
(b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service".[46]

[39] Dr. Marc Störing (2017), "What EU legislation says about car data Legal Memorandum on connected vehicles and data", available at http://mycarmydata.eu/wp-content/uploads/2017/06/20170516-Legal-Memorandum-on-Personal-Data-in-Connected-Vehicles-www.pdf

[40] See WP29 Consolidated Resolution on the Construction of Vehicles (R.E.3) Revision 5 (June 2017) regarding Annex 6: "Guideline on measures ensuring cybersecurity and data protection of connected vehicles and vehicles with Automated Driving Technologies"; ACEA 2015 Principles of Data Protection in Relation to Connected Vehicles and Services, the 39th International Conference of Data Protection and Privacy Commissioners resolution: "Resolution on Data Protection in Automated and Connected Vehicles"

[41] https://ec.europa.eu/digital-single-market/en/news/workshop-towards-harmonised-deployment-cooperative-connected-and-automated-mobility-ccam-data-0

[42] TRL (2017), "Access to In-vehicle Data and Resources", available at https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf

[43] Directive EU 2016/1148

[44] Annex II of Directive (EU) 2016/1148

[45] Article 4(4) of Directive (EU) 2016/1148

[46] Article 5(2), of Directive (Eu) 2016/1148 Of The European Parliament And Of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

2.7. National Frameworks

2.7.1. Austria

In 2016, Austria adopted a new Action Plan "Automated - Connected - Mobile"[47] which aims to address a number of key questions surrounding the automation of mobility, organize the proper response in Austria and involve the relevant stakeholders. The action plan centres around the development and prioritization of use cases. In addition, test environments have been anticipated and questions surrounding the legal framework for these tests has been examined. The legal actions included the screening of the relevant national and international framework and the amendments to national legislation to allow for testing of autonomous vehicles.

In addition, Austria has been part of a number of European Groups where discussions on adapting the legal framework has been discussed. Internally, discussions are held on issues such as vehicle and test certification but also software certification and additional issues such as data protection, changes in insurance and liability.[48]

2.7.2. France

Automated driving in France is addressed in the "New France for industry" plan which envisions that a new legal framework will be developed to address autonomous driving experimentation. In February 2017 by the Ministry of the Interior and the Secretary of State expressed their readiness to work on issues such as the Road Traffic Code to allow to autonomous cars on public roads, update liability framework, and addresses data protection (CNIL).[49]

An interesting development in the realm of testing autonomous vehicles in France is that there is intention for testing autonomous driving in a cross-country environment: State authorities of France and Germany have adopted a letter of intent for the implementation of an itinerary between Metz and the Sarre for the testing of autonomous vehicles.[50]

When it comes to data access and connected vehicles (i.e vehicles which interact with other participants in the transport system such as other cars or infrastructure), a recent report has been published by CNIL – the French Data Protection Authority – on access to data and connected vehicles.[51] The authority looked into three use cases of connected cars and based on these developed a compliance package describing the rules on processing of personal data collected via vehicle sensors, telematics boxes, or mobile applications. The compliance package aims to address the current state of use and therefore excludes issues such as ITS the conditions for roll-out for which have not yet been set out.
The compliance package provides an overview of the French Data Protection Legislation and the GDPR and outlines a list of questions that should be asked prior to the processing of personal data. The recommended questions are shown in Figure 3.

---

[47] Action Plan Automated Driving - Executive Summary June 2016, available at http://www.smart-mobility.at/fileadmin/media_data/services/Thematisches/Actionplan_automated_driving.pdf

[48] Based on interview with Mr Russ

[49] https://connectedautomateddriving.eu/wp-content/uploads/2017/02/20161216_CARTRE_MS_Workshop_v1.1-1.pdf; https://www.twobirds.com/en/news/articles/2017/global/at-a-glance-autonomous-vehicles

[50] https://www.twobirds.com/en/news/articles/2017/global/at-a-glance-autonomous-vehicles

[51] CNIL(2017), Connected Vehicles and personal data: Compliance Package, October 2017 Edition

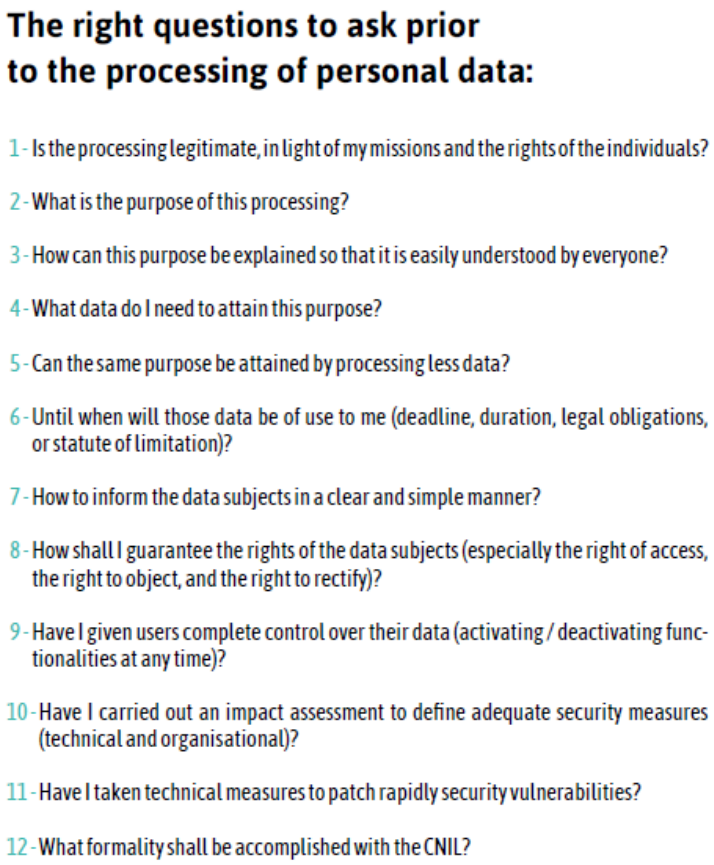


Figure 3; CNIL(2017), Connected Vehicles and personal data: Compliance Package, October 2017 Edition

Interestingly, the report addresses the applicable data protection rules and their implications in three use cases, for each looking at the legal basis, rights of the user, implications for security, etc. CNIL also addresses infrastructures outside the vehicle and has developed a method for the assessment risks associated with protecting people's privacy. The following summarizes the scenarios and some (not all) point related to security:

1) The vehicle's data are not transmitted to the service provider in which case either no data form application is transferred outside the vehicle or the used application involve transfer of data from the vehicle but without being transferred to the service provider (in which case personal data is confined to the communication network but is under the user control or uses telecommunication network open to the public). In such situation, and provided that indeed the user has full control over the data, the performance of purely personal activities is not subject to data protection regulations.[52] Yet, recommendation related to authentication of data-receiving devices and user authentication tailored to the level of data sensitivity have been outlined.
2) The second use case refers to situations in which applications transmit data to the service provider to provide additional services but without automatic action being triggered in the vehicle (e.g. E-Call, product optimization, breakdown assistance). For these purposes only personal data that is strictly relevant for the service should

[52] CNIL (2017), Connected Vehicles and personal data: Compliance Package, October 2017 Edition, pp. 19-20

be collected. The guidelines also refer to the fact that the service providers should establish measures to ensure the security and confidentiality of the processed personal data and are advised to adopt a 'privacy by design' approach.

3) The third use case scenario is referred to as ""in->out->in" and "covers cases in which the data collected are passed on to the service provider to remotely trigger an automatic action in the vehicle" (e.g. dynamic traffic information with continuously updated traffic situation).

2.7.3. Germany

Germany has adopted amendments of the Road Traffic Act ((Straßenverkehrsgesetz) to recognise the automated driving systems in vehicles with high automation. Yet, the driver is still defined as the person operating and activating the vehicle, and should be able to immediately take control in case the system requires him to do so or the requirements for the use of the automated driving systems are no longer fulfilled.[53] In that sense, the law does not cover autonomous (entirely self-driving) vehicles.[54] As Freshfields explains in detail in an article, the allocation of fault and liability (i.e. whether the driver was vigilant to take control of the situation or the accident was caused based on failure of the system when the driver was relying on it properly) are to be ensured by the inclusion of a black box in automated driving systems vehicles.[55] As the article points, liability towards an accident victim would still be governed by the existing German car owner framework putting the liability with the vehicle owner.
When it comes to data protection, a dedicated recommendation related to data collection in automated and connected vehicles has been published by the German Commissioner for Data Protection.[56]

Germany also the first country to commission a ethics report on connected and automated driving.[57] The Ethics Commission developed a total of 20 rules of rules for automated and connected vehicular traffic. The rules point that the main aim of automated systems should be to improve safety of the road users (rule 1) and the protection of individuals should take precedence. When it comes to accountability and liability, the rules state that 'It must be possible to clearly distinguish whether a driverless system is being used or whether a driver retains accountability with the option of overruling the system' (rule 16) and that the legislation should reflect the shifting accountability 'from the motorist to the manufacturers and operators of the technological systems and to the bodies responsible for taking infrastructure, policy and legal decisions' (rule 10). When it comes to product liability, as the same rules apply as to other products, 'manufacturers or operators are obliged to continuously optimize their systems and also to observe systems they have already delivered and to improve them where this is technologically possible and reasonable' (rule 11). In addition, the public sector is seen as the responsible party to ensure 'the safety of the automated and connected systems introduced and licensed in the public street environment'' (rules 3).

---

[53] https://www.researchgate.net/profile/Krzysztof_Czarnecki3/publication/320813344_English_Translation_of_the_German_Road_Traffic_Act_Amendment_Regulating_the_Use_of_Motor_Vehicles_with_Highly_or_Fully_Automated_Driving_Function_from_July_17_2017/links/59fbbe680f7e9b9968bb5a0f/English-Translation-of-the-German-Road-Traffic-Act-Amendment-Regulating-the-Use-of-Motor-Vehicles-with-Highly-or-Fully-Automated-Driving-Function-from-July-17-2017.pdf

[54] Freshfields Bruckhaus Deringer (21 June 2017), "Automated driving law passed in Germany", available at https://www.freshfields.com/en-us/our-thinking/campaigns/digital/internet-of-things/connected-cars/automated-driving-law-passed-in-germany/

[55] Freshfields Bruckhaus Deringer (21 June 2017), "Automated driving law passed in Germany", available at https://www.freshfields.com/en-us/our-thinking/campaigns/digital/internet-of-things/connected-cars/automated-driving-law-passed-in-germany/

[56] file:///C:/Users/karanikolovakn/Downloads/DatenschutzrechtlicheEmpfehlungenVernetztesAuto.pdf

[57] Ethics Commission appointed by Federal Ministry of Transport and Digital Infrastructure (2017), "Automated And Connected Driving", available at: https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile

Data management recommendations have also been research and published, with the recommendations pointing to (among others) the importance of data minimization and transparency, developing products following privacy-by-design and default principles (recommendation 9), reliable online communication component providing protection against attacks (recommendation 13).[58]

Regarding the non-embedded software specific legislations, the following reply from the Federal Ministry of infrastructure was provided:
"The existing German rules on automated and connected driving (Eight Act amending the Road Traffic Act) and intelligent transport systems (Intelligent Transport Systems Act) do not contain requirements regarding non-embedded software. Thus, a more detailed discussion of the issue of non-embedded software has not yet been undertaken".[59].

2.7.4. Italy

According to Rinaldi, in Italy, autonomous driving is restricted by the definition of a driver. Definition in article 46 of the Highway code refers to the driver as the human driver. Therefore, high automation vehicles are not permitted on the streets. Likewise, this has effect on the liability framework. In Italy, liability is governed by the Civil Code (art. 2054) and driver is liable for damages unless they can prove they everything possible to stop the accident[60] As fully automated vehicles are not permitted and provided that the driver had a choice to take control, it is likely that drivers would still be held liable for damages caused.

A testing site at the Florence–Livorno freeway has been dedicated for testing of connected vehicles as part of the AUTOPILOT EU project. The stretch of the pilot site is equipped with ITS technology for control and data analysis and results are expected to provide ITS stakeholders with information on different complex scenarios and how AUTOPILOT technologies are performing.[61]

2.7.5. The Netherlands

The Netherlands has actively supported the development of an infrastructure to initiate testing of connected and automated vehicles. During the Dutch presidency the topic was put forward.[62] In 2017, the Dutch Cabinet approved legislation that makes it possible for manufacturers to carry out much more extensive testing of self-driving vehicles, with remote drivers. A Taskforce supporting the Dutch road authorities by developing knowledge and sharing experiences of tests with self-driving vehicles has also been established.[63]

---

[58] Alex van der Wolk, Philip Radlanski, and Jens Wollesen (July 2017), "Germany's Federal Commissioner for Data Protection Issues Recommendations for Self-Driving Cars; MoFo Privacy Minute", available at https://www.mofo.com/resources/publications/170720-germany-data-protection-self-driving-cars.html and "Datenschutzrechtliche Empfehlungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum automatisierten und vernetzten Fahren"

[59] Email from Arne Zielonka, Federal Ministry of Transport and Digital Infrastructure, Division DG 24 – Intelligent Transport Systems and Automated Driving, received on 23.03.2018

[60] https://www.twobirds.com/en/news/articles/2017/global/at-a-glance-autonomous-vehicles

[61] http://erticonetwork.com/italian-pilot-site-large-scale-testing-ground-for-autopilot-iot-e-nabled-autonomous-driving/

[62] See Ministry of Infrastructure and the Environment (2017), "On our way towards connected and automated driving in Europe: Outcome of the first High Level Meeting" available here and Florien van der Windt and Frans op de Beek (2015), "European Cooperation in the Field of connected and automated driving, in view of the Dutch EU Presidency (abstract NON-paper, concept 25 September 2015)"

[63] http://www.connekt.nl/wp-content/uploads/2016/03/Flyer-Taskforce-Dutch-Roads.pdf

Different parties can gain experience with intelligent traffic systems on the Dutch public roads under some conditions. The RDW - Netherlands Vehicle Authority – is willingly searching for cooperation on the matter. Some of the technologies tested are:[64]

- automatic following;
- connected adaptive cruise control;
- lane-keeping assist;
- vehicle following;
- lane change;
- traffic jam assist;
- overtaking;
- valet parking;
- collision avoidance;
- emergency stop;
- self-driving vehicles.

What is more, the Dutch Vehicle Authority (RDW) has initiated a "Digital Driving License Project"[65] The project aims to contribute towards an international standard (ISO) methodology for assessment of autonomous vehicles.

2.7.6. Spain

Spain has introduced regulations from November 2015 that establish a legal framework allowing for tests to be conducted with autonomous driving vehicles on public roads.[66] The general responsible body that oversees the test is the Directorate General of Traffic (DGT). The Spanish DGT is involved in many different working groups and fore on the subject of automated driving, both at EU level and the UN level.

When testing CAD , any issue or incident must be immediately communicated to DGT. DGT is also financing research projects in this field, however all projects are still on going and results are not yet available..[67]

An article has reported that DGT intends to work on a so-called '21st century Traffic Act' which will regulate the driverless cars regime in detail.[68] The amendments of the Traffic Law are still in a draft form and not publicly available. However, the first drafts are expected to allow for automated driving up to level 5. The draft is expected to be presented to the Parliament by the end of 2018.[69]

In general, cybersecurity issues are covered by the Ministry of Enterprise but the DGT is working closely with the Ministry when it comes to CCAM.

2.7.7. Sweden

Sweden has launched the biggest large-scale pilot project in autonomous driving with Volvo cars and the support of the government which see autonomous driving as a solution to zero

---

[64] https://www.rdw.nl/information-in-english/information-in-english/information-in-english/intelligent-transport-system/practical-testing-of-its-in-the-netherlands
[65] http://on-demand.gputechconf.com/gtc/2017/presentation/s7559-jorrit-kuipers-digital-driving-license.pdf
[66] http://www.lamoncloa.gob.es/lang/en/gobierno/news/Paginas/2016/20160414-eu-transport-min.aspx
[67] Reply to request for information from Mr Arriola
[68] https://www.twobirds.com/en/news/articles/2017/global/at-a-glance-autonomous-vehicles
[69] Reply to request for information from Mr Arriola, 28.03.2018

fatalities aim: Drive Me - Self driving cars for sustainable mobility[70] In addition, trials self-driving vehicles in real life environment have been announced for variety of vehicles, including buses and passenger cars[71]The Swedish Government has adopted an ordinance referring to trials of self-driving vehicles.[72] The ordinance entered into force on 1 July 2017 and stipulates that a driver still needs to be present in or outside of the vehicle. A permit for testing needs to be issued and relevant authority for this is the Swedish Transport Agency.[73]

Regarding liability issues, the European Parliament Research Service study reported that in Sweden a proposal for regulation for the testing of autonomous vehicles has evaluated that the laws on compensation for traffic accidents can be applied to all levels of automated vehicles.[74] The Swedish Traffic Damage Act (Trafikskadelagen, 1975/1410) also provides that injured parties in a motor vehicle accident may seek compensation from the liability-motor-insurance (it is the insurer's liability that is the basis for the claim).[75]

2.7.8. The United Kingdom

According to a study conducted in 2015, the review of the (already at that point) existing legislation pointed that driverless vehicles can be legally tested on public roads in the UK.[76] Yet, a test driver is still required to be present and take responsibility of the operations of the safe vehicle.[77]
In the UK, several interesting and recent regulatory developments have taken place in the realm of connected, automated and self-driving vehicles.

In the end of January 2018, the **Automated and Electric Vehicles Bill** has been scrutinized by the House of Commons and has been passed to the House of Lords.[78] The Bill includes a specific section on the Automated vehicles and regulates the liability of insurers in case of automated vehicles. The text stipulates that (text as introduced on 30.01.2018 to the House of Lords):
"(1)Where—
(a)an accident is caused by an automated vehicle when driving itself,
(b)the vehicle is insured at the time of the accident, and
(c)an insured person or any other person suffers damage as a result of the accident, the insurer is liable for that damage."[79]

---

[70] https://international.goteborg.se/smart-cities-and-sustainable-solutions/driveme-self-driving-cars-sustainable-mobility
[71] https://sputniknews.com/science/201711281059504905-sweden-driverless-cars/
[72] http://www.government.se/articles/2017/05/government-paves-the-way-for-self-driving-vehicles/

[73] ibid

[74] Charlene Rohr, Fay Dunkerley, and David Howarth, "Socio-economic analysis of the EU Common approach on liability rules and insurance related to connected and autonomous vehicles" Research Paper of RAND Europe, published in European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment"
[74] European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment", p.77
[75] Ibid

[76] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/446316/pathway-driverless-cars.pdf
[77] http://www.legco.gov.hk/general/english/library/stay_informed_overseas_policy_updates/the_pathway_to_driverless_cars_esum.pdf
[78] https://services.parliament.uk/bills/2017-19/automatedandelectricvehicles/documents.html
[79] https://publications.parliament.uk/pa/bills/lbill/2017-2019/0082/lbill_2017-20190082_en_2.htm#pt1-l1g1

According to the proposed bill however, the motor insurer will have the right of recovery against any other person also liable (Section 5(1)). Additionally, the liability of the insurer can be limited in case of an accident resulting from unauthorised software alterations or failure to update software (Section 4(1)). The article will be applicable in situation in which a vehicle is driving itself, meaning that it "is not being controlled, and does not need to be monitored, by an individual"[80] While the Bill has been delated (in 2017 under Vehicle Technology and Aviation Bill name and due to general election). Yet, according to Kerris Dale and Alistair Kinley, it has been largely supported and accepted by the insurance industry and the different political parties.[81]

Other legislative proposals are looking at amendments of the Highway Code and regulations and might have an impact on automated driving systems. For example, a public consultation on the proposed changes to regulations to allow parking via a remote device closed on 30 January 2018. Still, while the proposal includes clarifications and amendments of the Highway Code, it still proposes that the responsibility still lies with the driver when using advanced driver assistance systems stating that "*If you are using advanced driver assistance systems, like motorway assist, or a remote control parking application or device, then you as the driver are still responsible for the vehicle and MUST exercise full control over these systems at all times*"[82]

In March 2018, the UK Roads Minister has announced the start of a three-year **project to review the legal obstacles to the introduction of self-driving vehicles** in order to develop a regulatory framework appropriate for self-driving vehicles.[83] The specific questions to be addressed include issues of criminal and civil liability, and who the responsible driver or person is, as well as what is the expected impact on road users.

2.8. Conclusions and connections to other tasks

2.8.1. Conclusions: CCAM

The main findings of our exploratory analysis regarding CCAM show that in researched member states, there are well-developed programs and sites for testing autonomous vehicles. At these testing sites, scenarios are being tested either physically or via simulations. Incidents on such testing sites are not widely reported to our knowledge so far. As for novel risks and potential incidents, on the level of AI and autonomy, some of the risks identified were wrong sensors calibration or underperforming sensors, faulty data from the server-side of for instance route information, hacking and/or data breaches were also mentioned by some recent reports and experts. Interaction with infrastructure and other vehicles was also seen as a challenge in relation to interoperability and performance, cross—border data flows and also cybersecurity.

---

[80] Section 7 (1)(a), https://publications.parliament.uk/pa/bills/lbill/2017-2019/0082/lbill_2017-20190082_en_2.htm#pt1-l1g1

[81] Kerris Dale and Alistair Kinley (30 January 2018)," Automated driving legislation heads to Lords - a third Bill at its third reading", available at: https://www.lexology.com/library/detail.aspx?g=ef6698ab-87f3-4549-932a-c72c4cf11380

[82] The Highway Code Rule 150 proposed changes of the Centre for Connected and Autonomous Vehicles (2017), "Remote Control Parking and Motorway Assist: Proposals for Amending Regulations and the Highway Code", p 15, available here

[83] Department of Transport (March 2018), "Government to review driving laws in preparation for self-driving vehicles", available here

The main challenge regarding non-embedded software is that once a car-OS is connected, the difference from a cyber-security point of view is diminishing (between embedded and non-embedded software). Where for now, applications such as navigation software or in-car entertainment is seen as non-embedded and non-trivial for the car's performance, it is already possible to reach and manipulate trivial parts of the software via such non-trivial applications. On the topic of data, there are different regulations that touch upon or have say of what can and cannot be shared or transmitted. From the RED to the GDPR and more, the regulatory landscape for data is a complex one in Europe and it will also touch upon non-embedded software-parts of automated vehicles. A next step for this and related projects would be to map out this landscape[84].

Regarding liability, in all Member States we have looked into, the role of the driver is to be– in control – of the vehicle at all times and so far this would also hold for (semi) autonomous vehicles. Yet, as witnessed in recent accidents with self-driving cars in the US, users of autonomous vehicles perhaps see themselves more as passengers than as drivers, having (too) high expectations of the car's autonomy and smartness. The (almost Pavlovian) response from industry is to add more alarm bells and warning signs or mechanisms in the car, which is a doubtful direction. A more interesting direction perhaps stems from one MS, who has proposed a driver's license for AI, Tis would call for regular testing and updating of such a driver license for AI before being allowed on the road.

2.8.2. Recommendations and continuation in Tasks 2 and 4.

- There are a number of initiatives and MS who aim to determine what the future liability and safety rules will be. Automation is however currently still widely used at lower automation levels, in which case as the GEAR 2030 recommendations state, EU Directives on liability for defective products (85/374/EEC) and on motor insurance (2005/14/EC) are sufficient for upcoming automated systems. There have been a number of studies already prepared which point to the need to revisit some concepts such as a driver when it comes to traffic liability. Clarification on the data storage and data ownership and rights has started in some MS – FR notably. Further automation and future updates of the legislation might be necessary as full autonomous vehicles become operational.
- Accidents currently revolve around the sensors and updates of the technology. It is not reasonable to expect that the transition to autonomous driving will be without accidents.
- Cyber security is frequently cited as a problem – ACEA views additional access point as a problem and recommends the extended vehicle model. Different legislative instruments mention the need to make sure that the systems are protected from cyber-attacks but achieving a 100% seems quite difficult to achieve. Implementing safety and security by design approach has been recommended.

[84] See "Access to In-vehicle Data and Resources" report, p 12 and onwards. EC, DG Grow, May 2017

3. ANNEX 1: REFERENCES

Popular literature

- Rich McCormick (14 October 2015), "Uber accidentally leaks personal data for hundreds of drivers", The Verge, available at https://www.theverge.com/2015/10/14/9529095/uber-leaks-personal-information-hundreds-drivers
- Andy Greenberg (08 January 2016), "The jeep hackers are back to prove car hacking can get much worse", WIRED, available at: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/
- Julia Carrie Wong (22 November 2017), "Uber concealed massive hack that exposed data of 57m users and drivers", the Guardian, available at: https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack
- Trend Micro (22 September 2017), "Tracking Device Information for Over 500,000 Vehicles Leaked Online", available at: Tracking Device Information for Over 500,000 Vehicles Leaked Online
- Mikhail Kuzin, Victor Chebyshev (16 February 2017), "Mobile apps and stealing a connected car", SecureList, available at https://securelist.com/mobile-apps-and-stealing-a-connected-car/77576/
- Eric Brandt (10 October 2017), "Autonomous Cars Are Getting into Accidents Because They Drive Too Well", The Drive, available at: http://www.thedrive.com/sheetmetal/15023/autonomous-cars-are-getting-into-accidents-because-they-drive-too-well
- SPUTNIK NEWS (28 November 2017), "Sweden Kick-Starts Major Trial Run of Self-Driving Cars, Buses", available at: https://sputniknews.com/science/201711281059504905-sweden-driverless-cars/

Articles, reports, and position papers:

- T. Litman (2018), "Autonomous Vehicle Implementation Predictions Implications for Transport Planning", Victoria Transport Policy Institute
- ACEA (2016), "ACEA Strategy Paper on Connectivity - April 2016"
- AdaptiVe (2017), "Deliverable D2.3: Legal aspects on automated driving", coordinator: Aria Etemad Volkswagen Group Research, authors: Jörg Bienzeisler, et al, available at https://www.adaptive-ip.eu/index.php/deliverables_papers.html
- DG GROWTH (18 October 2017), "High Level Group GEAR 2030 report on automotive competitiveness and sustainability", available at: https://ec.europa.eu/growth/content/high-level-group-gear-2030-report-on-automotive-competitiveness-and-sustainability_en
- GEAR 2030 Working Group 2 Project Team 1 (5 July 2017), "Policy and regulatory issues for Automated and connected vehicles' Summary of the draft final recommendations.", available here
- ETSI, "The Radio Equipment Directive 2014/53/EU", available at http://www.etsi.org/technologies-clusters/technologies/regulation-legislation/red
- BEUC and ANEC (2018), "Cybersecurity For Connected Products: Position Paper", ANEC-DIGITAL-2018-G-001final - BEUC-X-2018-017 07/03/2018
- Charlene Rohr, Fay Dunkerley, and David Howarth, "Socio-economic analysis of the EU Common approach on liability rules and insurance related to connected and autonomous vehicles" Research Paper of RAND Europe, published in European

Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment

- European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment"
- E.F.D. Engelhard and R.W. de Bruin (2017), "EU Common Approach on the liability rules and insurance related to Connected and Autonomous Vehicles", published in European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment"
- BEUC (2017), "Review Of Product Liability Rules: BEUC Position Paper", available at http://www.beuc.eu/publications/beuc-x-2017-039_csc_review_of_product_liability_rules.pdf
- Dr. Marc Störing (2017), "What EU legislation says about car data Legal Memorandum on connected vehicles and data", available at http://mycarmydata.eu/wp-content/uploads/2017/06/20170516-Legal-Memorandum-on-Personal-Data-in-Connected-Vehicles-www.pdf
- WP29 Consolidated Resolution on the Construction of Vehicles (R.E.3) Revision 5 (June 2017) regarding Annex 6: "Guideline on measures ensuring cybersecurity and data protection of connected vehicles and vehicles with Automated Driving Technologies"
- ACEA (2015), "Principles of Data Protection in Relation to Connected Vehicles and Services"
- the 39th International Conference of Data Protection and Privacy Commissioners resolution (25-29 September 2017),"Resolution on Data Protection in Automated and Connected Vehicles"
- TRL (2017), "Access to In-vehicle Data and Resources", available at https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf
- European Commission (31 January 2018), "Workshop "Towards a harmonised deployment of Cooperative, Connected and Automated Mobility (CCAM): Data", available at https://ec.europa.eu/digital-single-market/en/news/workshop-towards-harmonised-deployment-cooperative-connected-and-automated-mobility-ccam-data-0
- bmvit - Austrian Ministry for Transport, Innovation and Technology (2016), Action Plan Automated Driving - Executive Summary June 2016, available at http://www.smart-mobility.at/fileadmin/media_data/services/Thematisches/Actionplan_automated_driving.pdf
- CARTRE - Coordination of Automated Road Transport Deployment for Europe (16 December 2016), "Workshop on Automation Pilots on Public Roads" European Commission Brussels, Covent Garden, Room 05/183, Summary of Meeting, available here
- Bird and Bird (25 July 2017), "At a Glance: Autonomous Vehicles", available at https://www.twobirds.com/en/news/articles/2017/global/at-a-glance-autonomous-vehicles
- CNIL(2017), Connected Vehicles and personal data: Compliance Package, October 2017 Edition
- Freshfields Bruckhaus Deringer (21 June 2017), "Automated driving law passed in Germany", available at https://www.freshfields.com/en-us/our-

thinking/campaigns/digital/internet-of-things/connected-cars/automated-driving-law-passed-in-germany/

- Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2017), "Datenschutzrechtliche Empfehlungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum automatisierten und vernetzten Fahren", available here
- Ethics Commission appointed by Federal Ministry of Transport and Digital Infrastructure (2017), "Automated And Connected Driving", available at: https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile
- Alex van der Wolk, Philip Radlanski, and Jens Wollesen (July 2017), "Germany's Federal Commissioner for Data Protection Issues Recommendations for Self-Driving Cars; MoFo Privacy Minute", available at https://www.mofo.com/resources/publications/170720-germany-data-protection-self-driving-cars.html
- ERTICO (2017), "Italian pilot site: large-scale testing ground for autopilot iot e nabled autonomous driving", available at http://erticonetwork.com/italian-pilot-site-large-scale-testing-ground-for-autopilot-iot-e-nabled-autonomous-driving/
- Ministry of Infrastructure and the Environment (2017), "On our way towards connected and automated driving in Europe: Outcome of the first High Level Meeting" available here
- Florien van der Windt and Frans op de Beek (2015), "European Cooperation in the Field of connected and automated driving, in view of the Dutch EU Presidency (abstract NON-paper, concept 25 September 2015)"
- Connekt, Ministry of Infrastructure and the Environment, RDW, (2016) "Taskforce Dutch Roads for self-driving vehicles", http://www.connekt.nl/wp-content/uploads/2016/03/Flyer-Taskforce-Dutch-Roads.pdf
- RDW, Practical testing of ITS in the Netherlands, available at: https://www.rdw.nl/information-in-english/information-in-english/information-in-english/intelligent-transport-system/practical-testing-of-its-in-the-netherlands
- Jorrit Kuipers, "Digital Driving License", available at: http://on-demand.gputechconf.com/gtc/2017/presentation/s7559-jorrit-kuipers-digital-driving-license.pdf
- Complejo de la Moncloa (14 April 2016), "Spain backs EU encouragement of automated and driverless vehicles", available at http://www.lamoncloa.gob.es/lang/en/gobierno/news/Paginas/2016/20160414-eu-transport-min.aspx
- City of Gothenburg, "DriveME self-driving cars for sustainable mobility", available at https://international.goteborg.se/smart-cities-and-sustainable-solutions/driveme-self-driving-cars-sustainable-mobility
- The Highway Code Rule 150 proposed changes of the Centre for Connected and Autonomous Vehicles (2017), "Remote Control Parking and Motorway Assist: Proposals for Amending Regulations and the Highway Code", p 15, available here
- Department of Transport (March 2018), "Government to review driving laws in preparation for self-driving vehicles", available here
- Kerris Dale and Alistair Kinley (30 January 2018)," Automated driving legislation heads to Lords - a third Bill at its third reading", available at: https://www.lexology.com/library/detail.aspx?g=ef6698ab-87f3-4549-932a-c72c4cf11380

Legislative texts:

- Vienna Convention of 8 November 1968, concluded under the auspices of the United Nations Economic Commission for Europe, available at https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XI-B-19&chapter=11&Temp=mtdsg3&clang=_en
- Working party on Road Traffic Safety (2017), "Report of the sixty-eighth session of the Working Party on Road Traffic Safety", ECE/TRANS/WP.1/145, available at: http://www.unece.org/fileadmin/DAM/trans/doc/2014/wp1/ECE-TRANS-WP1-145e.pdf
- Informal Working Group on Intelligent Transport Systems / Automated Driving (2017), "Proposal for the Definitions of Automated Driving under WP.29 and the General Principles for developing a UN Regulation on automated vehicles", ECE/TRANS/WP.29/2017/145, available at http://www.unece.org/fileadmin/DAM/trans/doc/2017/wp29/ECE-TRANS-WP29-2017-145e.pdf
- Informal Working Group on Intelligent Transport Systems / Automated Driving (2018), "Proposal for the Definitions of Automated Driving under WP.29 and the General Principles for developing a UN Regulation on automated vehicles", ECE/TRANS/WP.29/2018/2, available at https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29/ECE-TRANS-WP29-2018-2e.pdf
- Regulation No 79 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of vehicles with regard to steering equipment, OJ L 137, 27.5.2008
- Working Party on Brakes and Running Gear (2018), "Proposal for the 03 series of amendments to UN Regulation No. 79 (Steering equipment)", ECE/TRANS/WP.29/2018/35, available at: https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29/ECE-TRANS-WP29-2018-35e.pdf
- Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility", COM/2016/0766 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0766
- Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, OJ L 207/1, available here
- Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, OJ L 153/62
- Guide to the Radio Equipment Directive 2014/53/EU Version of 19th May 2017, Ref. Ares(2017)2560531 - 19/05/2017
- Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits Text with EEA relevance, *OJ L 96*

- Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210
- Directive 2009/103/EC Of The European Parliament And Of The Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability, OJ L 263
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, *OJ L 194*
- Krzysztof Czarnecki (2017), English Translation of the German Road Traffic Act Amendment Regulating the Use of "Motor Vehicles with Highly or Fully Automated Driving Function", available here
- Department of Transport (2015), "The Pathway to Driveless Cars: A Code of Practice for Testing"https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/446316/pathway-driverless-cars.pdf; Executive Summary available here: http://www.legco.gov.hk/general/english/library/stay_informed_overseas_policy_updates/the_pathway_to_driverless_cars_esum.pdf
- Bill documents — Automated and Electric Vehicles Bill 2017-19, available at https://services.parliament.uk/bills/2017-19/automatedandelectricvehicles/documents.html
- Automated and Electric Vehicles Bill (HL Bill 82), https://publications.parliament.uk/pa/bills/lbill/2017-2019/0082/lbill_2017-20190082_en_2.htm#pt1-l1g1

European Commission

Title
Luxembourg, Publications Office of the European Union

2019– 39 pages

ISBN number: 978-92-79-99495-1
DOI number: 10.2759/448974

European Commission

Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems

SMART 2016/0071

Annex 2, Part B

Scenarios and conditions for the implementation of CAD - CCAM and proactive mapping of policy measures (Task 2)

TNO 2019 R10095

A study prepared for the European Commission
DG Communications Networks, Content & Technology
by:

TNO innovation for life
VVA CONSULTING
Sant'Anna Scuola Universitaria Superiore Pisa

Digital Single Market

This study was carried out for the European Commission by

Authors:

- Marco Bolchi (VVA)
- Stefano Suardi (VVA)
- Maria Kirova (VVA)
- Patrisia Costenco (VVA)
- Andrea Bertolini (SSSA)
- Francesca Episcopo (SSSA)
- Sven Jansen (TNO)
- Tjerk Timan (TNO)
- Kristina Karanilokova (TNO)

Internal identification

Contract number: 30-CE-0887241/00-16

SMART number: 2016/0071

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN number 978-92-79-99495-1

DOI:number 10.2759/448974

Catalogue number: KK-04-19-076-EN-N

Table of Contents

List of Tables

List of Figures

List of abbreviations

Acronyms	Definition
AI	Artificial intelligence
B2B	Business to Business
CAD	Connected Automated Driving
CCAM	Cooperative Connected and Automated Mobility
C-ITS	Communication and Information Technology Services
C-V2X	Communication Vehicle to everything
ECU	Electronic Control Units
EDR	Event Data Recorders
EV	Electric Vehicle
GM	General Motors
GNSS	Global Navigation Satellite System
IP	Intellectual Property
LiDAR	Light Detection and Ranging
MaaS	Mobility as a Service
MCC	Mobile Computing Cloud
NASA	National Aeronautics and Space Administration's
NHTSA	Highway Traffic Safety Administration
OEMs	Original Equipment Manufacturer
OICA	Organisation Internationale des Constructeurs d'Automobile
R&D	Research and Development
UBI	Usage Based Insurance
V2P	Vehicle-to-Pedestrian
VC	Vienna Convention
TVAF	UN Task Force on Automated Vehicle Testing

Executive Summary

Connected and Automated Driving (CAD), and the consequent Cooperative and Connected Autonomous Mobility (CCAM) concept, will inevitably revolutionize the way European and Global citizens will drive and move across cities. The present report, in the framework of DG Connect Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems (SMART number 2016/0071), aims at identifying empirically founded recommendations for policy measures that will facilitate the future business uptake of Connected, Cooperative and Automated Mobility (CCAM) in the EU context.

The uptake of CCAM is being affected by a number of elements such as technical challenges, regulatory hurdles, and commercial bottlenecks, which in turn will impact social and market acceptance. These **issues** are presented below.

Liability: Most Member States have rules that make the driver, who is involved in the driving task, liable. Manufacturers' liability holds for cases where damage is derived from the product's use. With increased automation the rules will start to overlap as the human and vehicle gradually start sharing the driving task. Additional complications include the fact that automation will come in degrees as well as the fact that the substitution will be a time-consuming process given that the car is a long lasting good. In addition, with cooperation (connectivity), apart from the driver and the driver's car manufacturer, there will be additional actors to be considered, which adds complexity. There are different conditions under which the owner, the producer or the human is liable. Even if we have all the information and we have identified the type of situation, it is still a very complex issue that requires litigation and many actors involved.

Cybersecurity: there are different types of additional risks associated to CCAM: on one side, the risk of intrusion (e.g. data or privacy related), and, on the other, risk related to the effects of malware (i.e. traffic safety related). The management of cybersecurity is becoming challenging topic and divergent cybersecurity approaches exist. OEMs would like to opt for a security-by-design and customised CS strategy, whereas other stakeholders suggest that a standardised approach following European CS principles would be optimal. Suppliers and other stakeholders have mixed views, suggesting broad standards and minimum requirements – OEMs would then be free to develop their strategy to meet these.

Data sharing framework and data access: the data generated by the automated cars is, and will increasingly be, a key source of value. Therefore, access to in-vehicle data will represent a vital element to ensure the provision of new services by many categories of current and potential service providers. From the policy standpoint standpoint, the key challenge is maximising the socio-economic benefits that can be generated by the access and use of vehicle data. At the present stage, OEMs and partially suppliers have control over most of the data generated by the vehicles and it is not in their best interest to make access to these data fully available to third parties. In contrast, aftermarket services are requesting for direct in-vehicle access and even if intermediate solutions are proposed such as an extended server, a consensus and a final decision on the solution to adopt is not yet achieved.

Testing on roads: first, unharmonized testing activities and different testing procedures across countries, make the overall implementation of testing on roads difficult for. This is also linked to the fact that cross-border testing activities are still limited in numbers. Second, incidents on testing cases are not widely reported and communication is lacking between different projects and Member States Initiatives. Third, further amendment of the Vienna Convention is required for testing and large-scale operation because the current amendment does not allow testing vehicles to run on public roads without a driver in control.

Certification: the current framework for testing and type approval needs to evolve in light of the advent of automated driving, which brought the following challeges: a) automated operation cannot be tested as combination of "vertical" components; b) The definition of a limited number of test cases is not suitable to ensure safety of an artificial intelligence-based system, which needs to take decisions in the real world considering an endless number of possible situations and scenario; and c) In the current framework there is a limited possibility to consider the actual environment in which the vehicle operates. D) the current framework is not suited to ensure the validity of certification over time, as new threats and issues are likely to emerge over the lifetime of the vehicle and software updates might update and affect fundamental safety functions.

Road infrastructure evolution: the emergence of automated driving will eventually require public Institutions and national bodies to upgrade the current road and communication infrastructure network. However, the current commercial and legal practices may impede communication providers to access the physical infrastructure, *de facto* preventing the investments required to implement communication capabilities on already existing infrastructure.

Technical issues: there are several technological challenges that need to be solved to ensure an effective, safe and secure roll out of CCAM:

- **Artificial intelligence**: technologies inside automated vehicles such as LIDAR, cameras, radars that collect scenario information will required to be processed and used to take precise, immediate decisions. AI will find its application in scenario assessment and decision making, which both are safety related. The use of AI will eventually raise ethical questions, as decisions involving life-threating situation will be taken by the vehicle and, not anymore, by the driver.
- **Positioning technologies**: the key challenges for the industry are to improve the performance of the single technologies while ensuring cost effectiveness, as well as to advance on sensor and data fusion and processing capabilities to feed then the decision to be taken by the artificial intelligence.
- **High definition (HD) maps**: these represent an essential input for automated driving. Their development requires significant investments and continuous updates. Furthermore, their coverage should be extended across all territory, and not only on densely populated areas. Finally, common technical formats are currently missing, with HD Maps databases currently limited in terms of interoperability across automotive players and other stakeholders.
- **Absence of a dominant standard for V2X communication**. While a vehicle could implement automated features independently to its capability to communicate and cooperate with the external world, it is undisputable that connectivity will expand the potential of automated vehicles, integrating them in a complex mobility ecosystem characterised by cooperative behaviour among vehicles and infrastructures. Today, the market offers different technologies capable of offering connectivity and cooperative features, namely ITS-G5 and future cellular based 5G, although testing has already started using the already available LTE-V2X. As the two technologies are currently non-compatible, European Commission traditional approach of "technology neutrality" could result counter-productive and even represent a risk for the safety of consumers.

Taking stock of the following challenges and bottlenecks, the reports identifies the **recommendations** outlined below.

Liability: we suggest a revision of the Product Liability Directive and of its scope of application by the relevant authorities. Furthermore, autonomous driving regulation could use compulsory insurance schemes, no-fault plans, as well as a risk-management approach.

Testing on public roads: the Commission could encourage Member States to improve the transparency of testing requirements/principles/guidelines, by means of recommendations, by monitoring and analysing the different interpretations of testing requirements, and by cross-fertilisation actions aimed at driving Member States towards a more homogeneous approach where nessary. The Commission should also establish stronger cooperation on testing across Europe, through the implementation of a European system for sharing testing data, conditions, use cases and best practices related to automated driving.

Certification: The Commission should actively participate in the work that is currently ongoing on this topic at UNECE level by the specific Task Force under the ITS/AD Informal Group within WP.29, so to obtain in the final certification scheme an optimal balance between the extension, approach and stringency of the testing (and associated levels of safety and security), and the administrative burden on the industry. In case of delays in the process, available instruments and options under the EU legal framework could be used as possible mitigation instruments.

Cybersecurity: ENISA should use the finalized UNECE WP.29 guidelines on cybersecurity to implement an EU-wide certification scheme. Furthermore, the report welcomes the initiative to create a network of competence centres across Member States as well as a European Cybersecurity Research and Competence Centre to aid the development of respective tools and technologies necessary to ensure a continuous monitoring and evaluation of cyber-threats.

Access to data: the establishment of a clear, full, transparent data-sets categorisation should be a priority, as it represents an enabler for policy decisions. Within the Recommendation planned to be issued at the end of 2018, the Commission should stress the importance of ensuring that data access solutions developed and made available by OEMs enable the generation of innovative downstream services, while guaranteeing a level playing field for players competing in their provision. The Commission should then continue analysing the service market enabled by vehicle data. Should the monitoring activity identify, within 1 or 2 years, that downstream competition is impacted by asymmetric data access and that development of new data-based services is limited by the dominant position of OEMs, a regulatory approach on data access should be pursued.

I**nfrastructure evolution:** priority, in terms of policy action and public fund allocation, should be given to maintenance and refurbishment of signalling across EU roads, as well as to the alignment of signalling across the Member States. Furthermore, the Commission should recommend national Institutions to investigate the opportunity to regulate how road network and road infrastructure operators grant access to third parties including telecommunication operators, so to ensure fair access to road infrastructure to these actors.

Technical challenges: the following conclusions and recommendations are suggested:

- **Artificial intelligence**: create a multi-stakeholder communication platform to guarantee competitiveness and creation of ethical guidelines, as well as continuing the coordination of research and investments at EU level.

- **Positioning technology**: participate in international and European standardisation fora to ensure that specific differentiators of European systems (E.g. European GNSS). Furthermore, the opportunity to consider positioning and GNSS related requirements and aspects in the ongoing process of update of certification at UNECE level

- [1] should be strongly considered by European Institutions, as UNECE has started regulatory drafting activities on certification to accommodate the specificities of automated driving.
- **HD maps**: promote public/private partnerships to cover market failures resulting from scarcely populated/ rural areas as the best approach to solve the commercial issue underlying the creation of HD maps. Furthermore, focus on helping the coordination between international business players in developing a single format for HD maps, to increase the compatibility across different OEMs and potentially enable economies of scale.
- **Absence of a dominant V2X communication standard**: the European Commission should not to delay a decision on the standard of communication that should be followed in Europe for V2X communication. As the current situation is restraining technological development in the field, a clarification on the issue from the Institution will provide a strong signal to the automotive industry.

[1] Activities are covered by the Task Force "AutoVeh" under the ITS/AD informal working group of UNECE WP.29

1. INTRODUCTION

1.1. Objectives of the report

Connected and Automated Driving (CAD), and the consequent Cooperative and Connected Autonomous Mobility (CCAM) concept, will inevitably revolutionize the way European and Global citizens will drive and move across cities. The present report, in the framework of DG Connect Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems, aims at identifying empirically founded recommendations for policy measures that will facilitate the future business uptake of Connected and Automated Driving (CAD) in the EU context. For this purpose, this study includes the:

- triangulation of key information on the expected evolution of the market landscape, emerging services related to CAD;
- analysis of the identified technical, commercial and regulatory bottlenecks, obstacles, and risks that affect the business roll-out of CAD in the EU context; along with
- justified recommendations for measures that would support timely and effective action in avoiding setbacks in the business roll-out of CAD and related services in the EU context.

1.2. Methodological approach

The methodological approach of this study was based on the combination of five different tasks, specified here below:

- Definition of CAD **key market trends**;
- Definition of CAD **service and business model** scenarios;
- Assessment of **technical, regulatory and commercial bottlenecks**;
- Identification of **policy measures** to avoid setbacks;
- Organisation of a **stakeholder consultation workshop** to discuss and validate the findings of the study.

To gather the necessary data to answer the complex questions of the subtasks, the following data gathering activities have been conducted:

- **Desk research** and an **interview campaign** of more than 30 in-depth interviews with stakeholders across the value chain, complemented by a validation round with at least 12 experts previously consulted. The interview campaign focused on key market trends, service and business model scenarios and the assessment of bottlenecks. The outcomes of the consultation are included in Annex B;
- An analysis, based on the outcomes of the interviews and complemented by desk research, of **strategic orientations** of CCAM decision makers (Annex C) and of the positions of key stakeholders (Annex D);
- A **stakeholder survey**, focusing on validating the first outcomes of the study as well as on exploring the case for potential policy measures. The results of the survey are included in Annex E.
- A **stakeholder workshop**, to discuss and validate with stakeholders the bottlenecks and potential policy measures identified in the study. Following the

workshop, additional interviews have been conducted with participants that contacted the consortium to provide a more detailed view on the workshop topics.

1.3. Structure of this report

The document is organised as follows:

- **Section 1** includes the introduction to the study, its objectives and the methodological approach.
- **Section 2** presents the background and context, consisting in an overview on the trends affecting the industry, the evolution of synergies between sectors, an analysis of the market trends and the potential evolution of CCAM uptake.
- **Section 3** presents an overview of the main issues identified across the study regarging CCAM. The following bottlenecks are addressed in the report: liability, testing, certification, cybersecurity, access to data, infrastructure evolution and a range of relevant technical challenges. Each of these issues is described in a dedicated section of the report (**Sections 4 to 10**), by covering the following elements:
    a. Description of the issue;
    b. Key market and industry trends;
    c. State of the art, presenting the legal and/or technical framework according with the type of issue;
    d. Policy initiatives and strategic orientations;
    e. Impact of the issue and of possible solutions on business models;
    f. Conclusions and recommendations.
- **Section 11**, covers the overall conclusions and a set of policy measures.

This report also contains Annexes consisting of the following:

- Annex A: the bibliography (Section 12.1)
- Annex B: Stakeholder consultation report (Section 12.2)
- Annex C: Mapping of strategic orientations (Section 12.3)
- Annex D: Mapping of stakeholders'positions (Section **Error! Reference source not found.**)
- Annex E: Survey Report (Section 12.5)
- Annex F: Appendix to the Assessment of the evolution of CCAM Market (Section 12.6)

1.4. Definitions

The following definitions are adopted in the study for the concept of Cooperative, Connected and Automated Mobility (CCAM), discussing for the latter the understanding of Mobility as a Service (MaaS). These definitions have been shared and validated with consulted stakeholders, to ensure alignment on the discussion of key trends, bottlenecks and the potential need for policy measures.

- **Cooperative**: The vehicle interacts directly with each other and with the road infrastructure referred to Cooperative Intelligent Transport Systems (C-ITS). This VtoV and VtoX communication is defined as the cooperative element of the CCAM. Vehicle cooperation is enabled by digital connectivity between vehicles and between vehicles and transport infrastructure.
- **Connected**: The vehicles are already connected devices, meaning that they are connected to Smartphones, having infotainments and other services services, internet and GNSS. A connected car is a car that is equipped with Internet access, and usually also with a wireless local area network. This allows the car to share internet access with other devices both inside as well as outside the vehicle.
- **Automated**: Refers to self-driving cars, autonomous cars, vehicles that can guide themselves without human conduction. It is a vehicle that can sense its environment and navigating without human input. In terms of level of automation, the classification below corresponds to the one established by the SAE International (SAE J 3016):
    g. At level 0, the driver performs all operating tasks like steering, braking, accelerating or slowing down, and so forth.
    h. At level 1, the vehicle can assist with some functions, but the driver still handles all accelerating, braking, and monitoring of the surrounding environment.
    i. At level 2, the vehicle can assist with steering or acceleration functions and allow the driver to disengage from some of their tasks.
    j. At level 3, the vehicle itself controls all monitoring of the environment (using sensors like LiDAR). The driver's attention is still critical at this level, but, in safe conditions, technology allows the user to disengage from "safety critical" functions such as braking.
    k. At level 4, the vehicle is capable of steering, braking, accelerating, monitoring the vehicle and roadway as well as responding to events, determining when to change lanes, turn, and use signals.
    l. At level 5, there is no need for pedals, brakes, or a steering wheel, as the autonomous vehicle system controls all critical tasks, monitoring of the environment and identification of unique driving conditions like traffic jams.

- **Mobility as a Service (MaaS)**: A mobility distribution model in which all a customer's major transportation needs are met via a single platform by a single service provider that orchestrates each individual transport service component to meet a customer's end-to-end service expectations. This is enabled by combining transportation services from public and private transportation providers through a unified gateway that creates and manages the trip, which users can pay for with a single account. Users can pay per trip or a monthly fee for a limited distance.

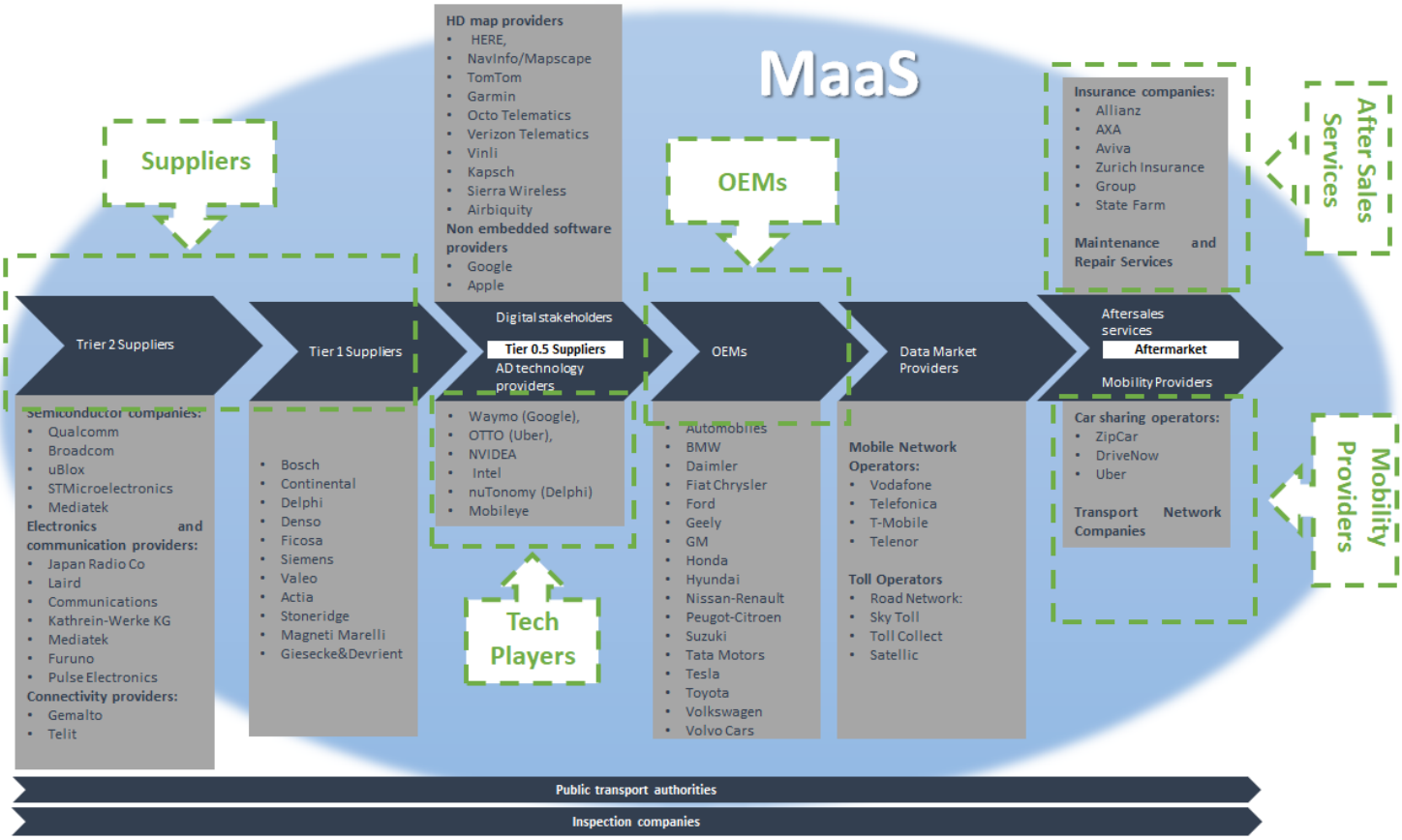
2. BACKGROUND AND CONTEXT

2.1. The value chain of cooperative, connected and automated mobility

The automotive industry is being significantly impacted by the growing innovation speed in technology applied to vehicles. Alongside the industry incumbents, including the few large OEMs, owning dozens of different brands, large Tier 1 suppliers and their Tier 2 suppliers, and the already existing downstream players, nowadays there are companies from different sectors and start-ups competing with new innovative solutions at all levels. Driven by the new business opportunities enabled by connectivity and automation, the automotive industry is becoming more complex and is converging with other sectors ICT and mobility being the most prominent ones.

The figure below is a representation of the current state of the value chain. The list of stakeholders given as an example is non- exhaustive. Compared to the traditional value chain, new entrants are appearing such as Tier 0.5 suppliers and the "Mobility-as-a-Service" providers. During consultation phase, stakeholders provided feedback on the value chain, and shared their opinion on its future evolution in the next 10-15 years. A large amount think that the value chain will be populated by emerging new services. The main actors will remain in place, but their role will evolve, in line with the shift of revenue and profit pools from products (vehicles) to data-enabled services.

Figure-1 Automotive Value Chain*

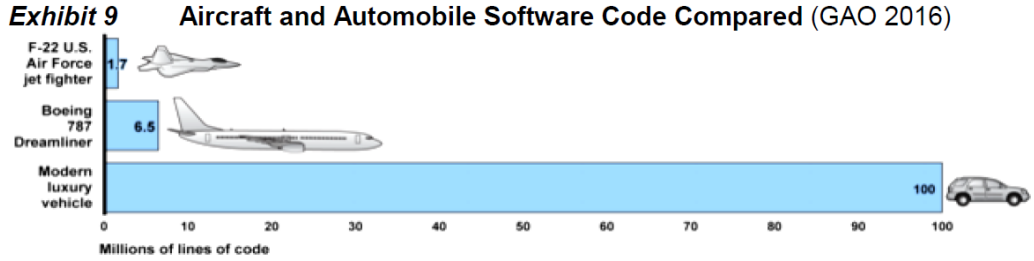


The major trends impacting the value chain are explained in the sections below.

Entry of technology companies in the automotive sector. Technology companies of different size are entering or trying to address the automotive industry. Obvious examples include Google with its self-driving car Waymo, Apple working working on the Titan project for self-driving cars, and many other Tier 0.5" suppliers of automated driving technology.

The window of opportunity for technology companies comes from the fact that the car itself is becoming more and more sophisticated in terms of connectivity and software presence. As a consequence, technology companies are entering the value chain leveraging on their software and or product capabilities.

Figure 2 Complexity of cars



Vehicles have more complex computer systems than aircraft, due to complex roadway interactions.

Source: Litman (2018), p 13

Mobility becomes a service. Another big change in the sector is the increasing mobility of "mobility services", with their business models leveraging, among others, on the increased connectivity capabilities. Also, mobility providers such as Uber is heavily investing in automated vehicles and is in partnership with one of the main OEM players. In December 2017, Uber was even recognised as a transportation company by an official ruling of the European Court of Justice.

Data availability fuels the development of new services. The number of service providers in the value chain increases due to the new embedded software in the car creating a large amount of data, which in itself creates opportunities for new services and markets as well as a redefinition of well-known services such as maintenance and diagnostic. New entrants in the automotive supply chain in areas such as telecommunication are also providing new services related to infotainment and entertainment for example.

Partnerships are created as no single player retains all competences. While the presence of new players in the sector makes the landscape very competitive, the width of competences required by CCAM, the pace of innovation, as well as the magnitude of necessary R&D investments, make synergies and collaboration crucial elements for success. Across the market we can observe different types of partnerships, as summarised in the table below.

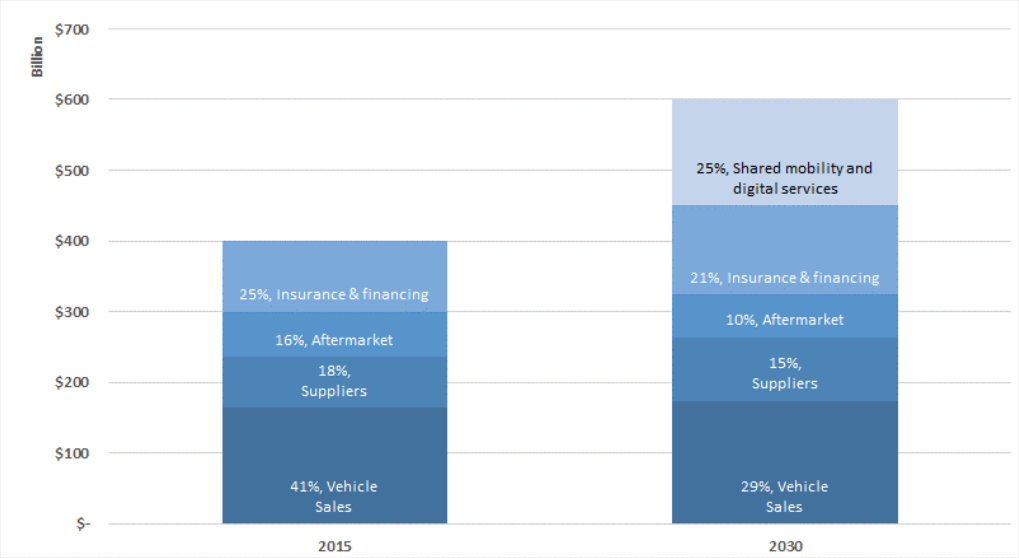
Table 1 Partnerships in CCAM

Type of Partnership	Objective	Examples
Automakers and Technology providers	Exchange knowledge, OEMs covering the traditional high expertise on car production and technology providers filling the technology software knowledge gap.	BMW with Intel-Mobileye and Delphi Fiat Chrysler and Google Toyota with Microsoft
Two or more Automakers	OEMs are jointly developing automated car technologies or creating partnerships for Research and Development purposes.	BMW, Audi and Daimler GM with Honda
Automakers and ride-sharing firms	Commercialization of the automated vehicles.	Volvo with Uber; GM with Lyft Volkswagen with Gett
Automakers with academic or government institutions	Exchange of technical expertise through joint research and development programs or joint development agreements. Incentives for public support.	Nissan with NASA
Suppliers of automakers and technology providers	Development of automated technology, making the link between software and hardware automated components. Common development of systems.	Continental with Baidu; Bosch with Nvidia

During the stakeholder consultation, participants suggested that these partnerships are not expected to be just short-term ventures, but rather a new concept and a tangible business opportunity for the future. During the consultation it was stated that individual market players will cooperate in order to complement each other's skills and develop complete solutions. However, the presence of different business models and the convergence by different players on the use of CCAM, generate risks and challenges. One of the risks could be the jointly developed IP and the dispute of ownership. Another potential risk is the control over the data generated by CCAM. Also, the shared liability among players cooperating to provide automated driving solution is a topic to be addressed.

Shift of value creation: from hardware to software and from product to service. In the future, technology suppliers will increasingly play a role alongside traditional suppliers. While new companies enter the market leveraging on digital expertise, key suppliers sign partnerships and perform acquisition to extend their capabilities. In the upcoming years, relevant growth in terms of added value is foreseen to arise from the emergence of new "downstream" services related to mobility and the data economy. Mobility as a service is another significant source of value. Also, as automated vehicles developments are in line with the evolution of the shared mobility paradigm, this could result in a reduction of cars owned by households and reduction of the demand of vehicles. As a consequence of these trends, at least in relative terms, the share of added value related to business such as vehicle or "traditional" component manufacturing could shrink. Accordingly, the strategies by key incumbents foresee the extension of business models so to encompass provision of connectivity related services or partnership in the provision of mobility solutions.

Figure 3 Global value shifts in the automotive industry - profits, 2015-2030



Source: PwC Connected Car Report, based on IHS; Autofacts; Frost & Sullivan; KPMG; HBR; Bain; McKinsey; NHTSA; Technavio; National Automobile Dealers Association; OEM reports; Capgemini; Thomson Reuters; Gartner; Oxford Economics; Strategy& analysis.

2.2. Assessment of the evolution of CCAM market

2.2.1. *Overview of current automated vehicle roadmaps by key OEMs*

As today, all major vehicle groups worldwide are independently or in the form of *ad-hoc* collaborations working at different degree of the integration of CCAM technologies in their fleet. In the table below we present the state of the art and the announcements by the major actors of the automotive industry.

Table 2 Announcements on forecasted CAD penetration*

Manufacturer	Region (HQ)	Positioning	Level 1	Level 2	Level 3	Level 4	Level 5
BMW Group	Europe	Premium	already onboard	already onboard	Forecasted for 2021	/	/
Daimler	Europe	Premium	already onboard	already onboard	/	Forecasted for early 2020s	/
Fiat Chrysler Automobiles	Europe North America	Volume and Premium	already onboard	already onboard	/	/	/
Ford	North America	Volume	already onboard	already onboard	/	Forecasted for 2020	/
General Motors	North America	Volume	already onboard	already onboard	Forecasted for 2019	/	/
Hyundai-Kia	Asia	Volume	already onboard	already onboard	/	Forecasted for 2022	/
Nissan Motor Co	Asia	Volume and Premium	already onboard	already onboard	/	Forecasted for 2022	/
PSA Group	Europe	Volume	already onboard	already onboard	Forecasted for 2020	Forecasted for 2025	/
Renault	Europe	Volume	already onboard	already onboard	/	/	/
Tesla	North America	Premium	already onboard	already onboard	2018	Forecasted for 2021	/
Toyota	Asia	Volume and Premium	already onboard	already onboard	Forecasted for 2020	/	/
Volkswagen group	Europe	Volume and Premium	already onboard	already onboard	Forecasted for 2019	/	Forecasted for 2025
Volvo	Europe	Premium	already onboard	already onboard	/	Forecasted for 2021	/

* As of beginning of 2018

As summarised above, level 2 of automation has now been achieved and all OEMs are offering at least some models and/or configurations implemented automated driving functions.

A very different situation applies to level 3 onwards. OEMs are adopting different strategies, with some of them working on the achievement of the third level of automation and others "leapfrogging" to level 4. The reasons behind include specific issues with level 3, where the driver must be prepared to take back control of the vehicle in a relatively short time frame:

- Liability-related aspects are particularly difficult to address, as regards the determination of the responsibility of incidents;
- Stakeholders suggest that the situation in which a driver is not performing any operations but must in theory be ready to take back control at all times is not optimal in terms of safety;
- Focusing on commercial vehicles, one of the goals of automated trucking should be to "influence hours of service," and allow drivers to extend their days as an effect of legislation updates. This is not deemed to be likely under level 3, questioning the economic viability of the investments in automated technology.

A more detailed analysis of the announcements and plans by OEMs is included in Annex F.

2.2.1. Evolution of CCAM uptake

Different studies have been trying to investigate the impact Automated Driving Technology will have on the automotive sector. Forecasting the evolution of CCAM uptake represents a challenging exercise mostly due to two factors:

- Firstly, the emergence of new means of transportation, as well as of new concepts of mobility, that may heavily affect the number of vehicles sold in the future.
- Secondly, and most importantly in the scope of this study, there are a range of technical, economical, and legal challenges and obstacles that could play an important role in slowing down the uptake of such technology in the sector.

A synthetic review of a selection of CCAM market uptake estimations is provided in the sub-sections below.

ERTRAC Roadmaps for automated driving

The European Road Transport Research Advisory Council (ERTRAC) is the European Technology Platform (ETP) for Road Transport. Among the tasks of ERTRAC to provide define strategies and roadmaps to achieve the strategic vision for European research and Innovation for road transport, among others through the definition and update of roadmaps. A dedicated roadmap for automated driving was published in mid-2017[2]. The roadmap includes a high level overview of development paths towards full automation, which foresees a progressive step-wise increase of automation level during the upcoming decade. More into detail the Roadmap outlines that:

- SAE level 1 has already been achieved;
- Specific functions belonging to SAE level 2 are already available, and full maturity will be reached in terms of driving assistance functions by 2022;

[2] ERTRAC, Automated Driving Roadmap, May 2017

- SAE level 3 functions (automated driving as "chauffeur") should reach maturity by 2024-25;
- Level 4 functions (AD through auto-pilot) will be established by 2028-2029;
- Full automation (SAE level 5) will take more time and could be achieved by 2035.

Synthetic review of other studies

A comprehensive evaluation of potential CCAM vehicles has been published by Transport System Capital, an innovation centre established and overseen by the UK's innovation agency, Innovate UK, in their report "Market forecast for Connected and Automated Vehicles"[3], published in July 2017. The report acknowledges the potential disruptive effects, which new technologies and trends may have on the sales of vehicles. However, it makes the assumption that sales trend will follow a "business as usual" approach, with an average annual increase for the global market of approximately 2%.

A range of reports provide forecasts for the uptake of automated driving technology in the automotive sector in Europe. As an example, figures from Goldman Sachs Global Investment Research are reported below.

Table 3 Example of forecasted shares of new vehicle sales in Europe by SAE automation level

	2030	2040	2050
Level 1 and 2	*41%*	*0%*	*0%*
Level 3	*34%*	*6%*	*0%*
Level 4 or higher	*25%*	*94%*	*100%*

Source: Goldman Sachs Global Investment Research

Stakeholder views

Existing literature and forecasts were submitted to stakeholders consultend in the study. Interviewees in general confirmed the trends, while the timeframes were considered by part of the stakeholders optimistic.

The uptake levels for higher automation (L3-4) may depend on business and service models, including for instance on whether CCAM is delivered: as a service or privately. If the automated driving is adopted as part of the mobility as a service, the uptake will take less time and will be implemented "by bulks". On the other hand if automated driving is adopted only as part of personal car ownership, the uptake could be slow taking into consideration the consumer acceptance and the higher cost a single end-user should pay to obtain such a vehicle.

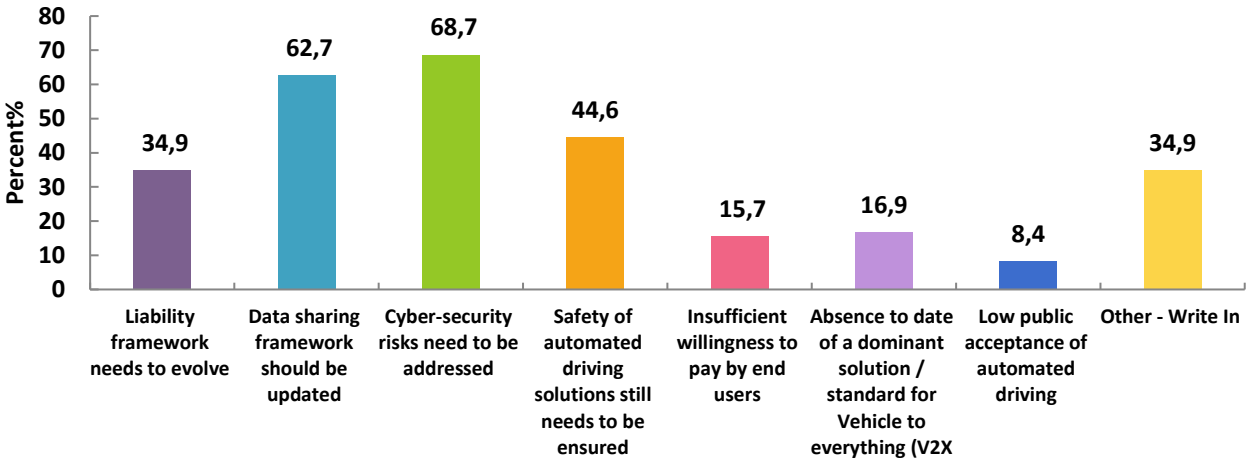
More importantly, stakeholders remarked that **the uptake will be determined by a number of elements such as technical challenges, the regulatory framework, and commercial bottlenecks,** which in turn will impact social and market acceptance. The main issues identified are first presented and then outlined in detail in the next sections.

[3] https://www.gov.uk/government/publications/connected-and-autonomous-vehicles-market-forcecast

3. OVERVIEW OF THE MAIN ISSUES

The following section presents a summary of the assessment of the main issues related to Cooperative, Connected and Automated Mobility (CCAM). These issues have been identified in the first phases of the study and then validated within the stakeholder survey conducted in the study.Respondents were asked to specify, the three most relevant issues affecting the uptake of CCAM. The outcomes of the survey are reported in the figure below.

Figure 4 CCAM issues identified by the survey



Source: VVA Survey on CCAM, July 2018

Stakeholders widely agreed with the identification of the issues, adding as an additional relevant point the need to update the road infrastructure. The identified issues are syntethically described below.

In terms of **liability**, most Member States have rules that make the driver, who is involved in the driving task, liable. Manufacturers' liability holds for cases where damage is derived from the product's use. With increased automation the rules will start to overlap as the human and vehicle gradually start sharing the driving task. Additional complications include the fact that automation will come in degrees as well as the fact that the substitution will be a time-consuming process given that the car is a long lasting good. In addition, with cooperation (connectivity), apart from the driver and the driver's car manufacturer, there will be additional actors to be considered, which adds complexity. There are different conditions under which the owner, the producer or the human is liable. Even if we have all the information and we have identified the type of situation, it is still a very complex issue that requires litigation and many actors involved.

In terms of **cybersecurity**, there are different types of additional risks associated to CCAM: on one side, the risk of intrusion (e.g. data or privacy related), and, on the other, risk related to the effects of malware (i.e. traffic safety related). The management of cybersecurity is becoming challenging topic and divergent cybersecurity approaches exist. OEMs would like to opt for a security-by-design and customised CS strategy, whereas other stakeholders suggest that a standardised approach following European CS principles would be optimal. Suppliers and other stakeholders have mixed views, suggesting broad standards and minimum requirements – OEMs would then be free to develop their strategy to meet these.

Considering the data sharing framework and **data access**, the data generated by the automated cars is, and will increasingly be, a key source of value. Therefore, access to in-

vehicle data will represent a vital element to ensure the provision of new services by many categories of current and potential service providers. From the policy standpoint standpoint, the key challenge is maximising the socio-economic benefits that can be generated by the access and use of vehicle data. At the present stage, OEMs and partially suppliers have control over most of the data generated by the vehicles and it is not in their best interest to make access to these data fully available to third parties. In contrast, aftermarket services are requesting for direct in-vehicle access and even if intermediate solutions are proposed such as an extended server, a consensus and a final decision on the solution to adopt is not yet achieved.

The topic of **safety** was covered in the study through the investigation of several underlying conditions and bottlenecks to be overcome, namely ensuring the conditions for testing of automated driving vehicles, progressing on certification, and overcoming a number of technical challenges.

Regarding **testing on roads**, first, unharmonized testing activities and different testing procedures across countries, make the overall implementation of testing on roads difficult for. This is also linked to the fact that cross-border testing activities are still limited in numbers. Second, incidents on testing cases are not widely reported and communication is lacking between different projects and Member States Initiatives. Third, further amendment of the Vienna Convention is required for testing and large-scale operation because the current amendment does not allow testing vehicles to run on public roads without a driver in control.

Certification challenges are faced as the current framework for testing and type approval needs to evolve in light of the advent of automated driving, which brought the following challeges: a) automated operation cannot be tested as combination of "vertical" components; b) The definition of a limited number of test cases is not suitable to ensure safety of an artificial intelligence-based system, which needs to take decisions in the real world considering an endless number of possible situations and scenario; and c) In the current framework there is a limited possibility to consider the actual environment in which the vehicle operates. D) the current framework is not suited to ensure the validity of certification over time, as new threats and issues are likely to emerge over the lifetime of the vehicle and software updates might update and affect fundamental safety functions.

In addition, there are several **technical issues** that need to be solved to ensure an effective, safe and secure roll out of CCAM:

- Improvement of **artificial intelligence**: technologies inside the automated car such as LIDAR, cameras, radars that collect scenario information will required to be processed and used to take precise, immediate decisions. AI will find its application in scenario assessment and decision making, which both are safety related. The use of AI will eventually raise ethical questions, as decisions involving life-threating situation will be taken by the vehicle and, not anymore, by the driver.
- Considering **positioning technologies**, the key challenges for the industry are to improve the performance of the single technologies while ensuring cost effectiveness, as well as to advance on sensor and data fusion and processing capabilities to feed then the decision to be taken by the artificial intelligence.
- Another technical challenge is releted to the **high definition (HD) maps**, which represent an essential input for automated driving. Their development requires significant investments and continuous updates. Furthermore, their coverage should be extended across all territory, and not only on densely populated areas. Finally, common technical formats are currently missing, with HD Maps databases

currently limited in terms of interoperability across automotive players and other stakeholders.

- Another technical issue is related to **V2X communication**. While a vehicle could implement automated features independently to its capability to communicate and cooperate with the external world, it is undisputable that connectivity will expand the potential of automated vehicles, integrating them in a complex mobility ecosystem characterised by cooperative behaviour among vehicles and infrastructures. Today, the market offers different technologies capable of offering connectivity and cooperative features, namely ITS-G5 and future cellular based 5G, although testing has already started using the already available LTE-V2X. As the two technologies are currently non-compatible, European Commission traditional approach of "technology neutrality" could result counter-productive and even represent a risk for the safety of consumers.

Moving to the need to **update the road infrastructure**, the emergence of automated driving will eventually require public Institutions and national bodies to upgrade the current road and communication infrastructure network. However, the current commercial and legal practices may impede communication providers to access the physical infrastructure, *de facto* preventing the investments required to implement communication capabilities on already existing infrastructure.

Each of the issues outlined above is presented more into details in the following sections.

4. LIABILITY

4.1. Issue definition

Increased automation in driving is intended to reduce the overall number of accidents considering that most are today due to human error, and only a small percentage to mechanical failures in the vehicles [4]. Such a common statement is however not statistically supported, for the data today available as per CADs' safety is not sufficient to conclude so, given the limited number of miles driven by – partially – autonomous vehicles[5]. Moreover, new risks specific to CADs will emerge, due to the peculiarities associated with their functioning, including so called cyber risk (see Section 7), as well as the possibility that failures in the infrastructures and services provided that are necessary for the functioning of the device.

At the same time, traditional vehicles will only over time be replaced by CADs, forcing the coexistence on public roads of vehicles with different levels of automation. This, in turn, together with the increased human-machine interaction in the completion of the driving tasks – for all vehicles of SAE levels 2, 3 and 4 – will cause the **overlapping of different sets of rules that until today hardly ever happened to regulate the same hypothesis, namely product liability and liability for traffic accidents.** The former is regulated at EU level through the Product Liability Directive (85/374/EEC, henceforth PLD)[6], the latter are primarily regulated at national level by each single MS. **Uncertainty with respect to which subject is going to be held liable and under what conditions might result as a consequence thereof, further exacerbating the criticalities that some parts of the legislation already today display** (see section 4.2 below).

Finally, **the increased number of subjects involved in the completion of the driving task**, ranging from the OEM, the user, and the different – internet and infrastructure – service providers, **causes the apportionment of liability to become ever more problematic,** potentially triggering relevant litigation.

These three issues represent the major concerns with respect to the application of the extant legal framework to CADs[7].

4.2. State of the art – legislative frameworks

The liability framework in Europe is harmonized via the **Product Liability Directive**[8] which establishes the conditions under which the producer is liable for damages caused by defects caused in his products.

A study for the European Parliament has concluded that while of great importance, "pre-emptive legislation of the Product Liability Directive (PLD) to encourage deployment of connected and autonomous vehicles is not required at this time" as there is a significant push to introduce connected vehicles and as manufacturers are likely to introduce their

---

[4] Broggi, A., A. Zelinsky, M. Parent and C. E. Torpe (2008). Intelligent Vehicles. Handbook of Robotics. B. Siciliano and O. Khatib, Springer.
[5] Kalra, N. and S. M. Paddock (2016). Driving to Safety. How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?, Rand.
[6] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29–33).
[7] Bertolini, A. (2016). "Insurance and Risk Management for Robotic Devices: Identifying the Problems." Global Jourist(2): 1-24
[8] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

products in markets outside the EU as well and have to comply with different liability rules.[9] The analysis for the European Parliament argues that while the current regulatory framework of the PLD seems to provide a well-balanced system, if not refined to reflect the changing system incorporating autonomous driving, "the application of the PLD to AVs will have a significant negative impact on consumer protection".[10]

The EU harmonization is provided also by the **Motor Insurance Directive**[11], which mainly focuses on compulsory third party liability insurance and is argued to provide limited harmonization. The same report notes that with the exception of Sweden, most national frameworks based their traffic liability rules on personal responsibility of the driver or owner.[12]One of the conclusions of the report is that the national systems might need to be re-examined in view of the fact that the concept of a driver, owner and possessor of the vehicle is changing in the framework of autonomous vehicles where the driver will not always to be in control to create or limit the risk.

2.4.1. EU framework

Liability form damages arising from accidents caused by motor vehicles are regulated by MS, with different degrees of harmonized rules on insurance for civil liability in respect of such damages, according to the Motor Insurance Directive (2009/103/EC, henceforth MID)[13], and for damages arising from a defect of the vehicle or its components, under the PLD.

Pursuant to art. 3 of the MID, each MS has the duty to take appropriate measures to ensure that civil liability in respect of the use of vehicle base in its territory is covered by third parties' insurance. The extent of the liability covered and the terms and conditions of the insurance cover are determined on the basis of those measures. However, insurance shall cover damages to property, loss and personal injury inflicted on another party because of the actions of the policyholder[14], and the victim shall enjoy a direct right of action against the insurance undertaking of the policyholder[15]. Each Member State shall require compulsory third parties' insurance to cover a minimum amount in case of both personal injury (1 million € 000 000 per victim or 5 million € per claim), and of damage to property (€ 1 million per claim) [16]. Issues of civil liability including compensation awards, as well as "comprehensive cover" for physical injury of the driver or damage to vehicles, on the contrary, fall outside the scope of the directive. MS are also obliged to institute specific guarantee funds for accidents caused by unidentified vehicles or vehicles not insured

---

[9] Charlene Rohr, Fay Dunkerley, and David Howarth, "Socio-economic analysis of the EU Common approach on liability rules and insurance related to connected and autonomous vehicles" Research Paper of RAND Europe, published in European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment"
[10] European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment", p.24
[11] Directive 2009/103/EC Of The European Parliament And Of The Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability
[12] Charlene Rohr, Fay Dunkerley, and David Howarth, "Socio-economic analysis of the EU Common approach on liability rules and insurance related to connected and autonomous vehicles" Research Paper of RAND Europe, published in European Parliament Research Unit (2018), "A common EU approach to liability rules and insurance for connected and autonomous vehicles European Added Value Assessment
[13] Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability (OJ L 263, 7.10.2009, p. 11–31).
[14] With the only exemption of the subjects and vehicles set out in art. 5 MID.
[15] Art. 18 MID
[16] Art. 9 MID.

according to art. 3 MID[17], as well as for accident caused by a third-country vehicle[18]. In addition to that, the directive abolishes border checks on insurance[19], specifies the authorities responsible for compensation and some fundamental feature of the compensatory procedures[20], as and introduces a mechanism to compensate local victims of accidents caused by vehicles from another EU country[21]. The directive also requires the quick settlement of claims arising from accidents occurring outside the victim's EU country of residence[22], and entitles policyholders to request a statement concerning the claims (or absence of claims) involving their vehicle during the 5 years preceding the contract[23].

Being a minimum-harmonization directive, the MID states that MS may maintain or adopt provision which are more favorable to the injured parties[24]. Various Member States have indeed adopted differing liability systems, for example, the Netherlands has a semi strict liability system, France has very strict liability system (no fault regime), and the United Kingdom system has a 'no strict liability' regime based on negligence rules[25].

The PLD establishes a – semi – strict standard of liability on the manufacturer for all damages that derive from the use of his product, so long as a causal nexus between the fact and the damage can be established. Thence it is not required to demonstrate the fault of the manufacturer. Pursuant to art. 2 of the directive any good might qualify as a product, yet it is disputed whether software shall not instead be qualified as a service, thence escaping the application of the directive. This is clearly one of the problematic aspects with the application of the directive to technologically advanced devices – such as CADs – where the software component is of the outmost importance.

A product might be deemed defective, either because the manufacturing of the single specimen deviates from the intended design – a typical failure of mass-production techniques – or because warnings about the potential dangers arising from the use of the device were not adequately signalled, or because the design is deemed defective, for it does not provide necessary safeties or is unreasonably dangerous.

The latter hypothesis is for sure the most problematic to establish, for a claimant needs to show that the erroneous design of the device is the cause that led to the accident. Satisfying such a burden of proof entails acquiring the expert opinion of a technician whom, once he has accessed data regarding the functioning of the device[26], is capable of analysing it and demonstrating the existence of a defect in the way the product was conceived. The more technologically complex the product, the harder satisfying such a requirement is going to be. Moreover, manufacturers – pursuant to art. 7, let. E) PLD – might advance a «development risk defence», maintaining that the status of technical and scientific knowledge at the time the product was designed was such as not to allow the defect to be identified and addressed. This defence, when implemented, substantially lowers the standard of liability, causing

[17] Art. 10, 11 MID.
[18] Art. 7, 8 MID.
[19] Art. 4 MID.
[20] Art. 19, 22, 24 MID.
[21] Art. 20 MID.
[22] Art. 11 MID.
[23] Art. 26 MID.
[24] Art. 28 MID.
[25] Evas, T. (2018). A common EU approach to liability rules and insurance for connected and autonomous vehicles. European Added Value Assessment Accompanying the European Parliament's legislative own-initiative report (Rapporteur: Mady Delvaux), EPRS European Parliamentary Research Service.
[26] This in particular might be problematic, for the data generated by the sensors and eventually recorded by an EDR could be claimed as proprietor information by the manufacturer, who opposes its disclosure for the purpose of protecting its industrial secrets.

The PLD is applicable across all MS, having been enacted, at times with some variations that cannot be fully detailed for the purposes of the current analysis. The PLD is certainly applicable to driverless cars, theoretically holding manufacturers liable in all cases where the accident can be traced back to a defect in the vehicle.However, demonstrating the existence of a defect in design, and determining that this was the cause of the accident might be extremely problematic for the victim and, depending on the value of the claim, economically inefficient. Even serious accidents, where substantial bodily injuries are suffered, the cost of evidentiary acquisition might exceed the amount of damages to be liquidated. The risk associated with losing in court litigation – despite attempts are made to acquire necessary evidence – might further discourage actions from being brought against manufacturers.

As anticipated above accidents involving the use of a partially autonomous vehicle might be due to human intervention or misuse of the vehicle and of its autonomous functions. In such a perspective, it shall suffice to recall how each MS provides for tort law rules that, primarily grounded on a notion of fault[27], hold the driver liable, who caused the accident, and in some cases the owner of the vehicle[28], jointly and severally, in an objective fashion.

When an accident involving traditional vehicles occurs the liability has to be apportioned among the two, based on material observations of the accident's dynamics. This entails determining which is responsible, having violated the street code, norms of prudence and diligence[29], ultimately failing to comply with a desirable conduct that theoretically may be identified.

When even just one partially autonomous vehicle is involved, instead, the possibility that the accident is due to a malfunctioning of the device needs to be considered. This might be the case when the accident occurs while the autonomous function is being utilized – which would not always be the case when level 2-4 SAE are considered –[30], yet the very decision to activate such a function in the given circumstances might in and by itself be deemed erratic, that being once again the responsibility of the human driver. Moreover, if the interaction takes into account the possibility that the crash is a consequence of a failure of the various systems – connection and infrastructure – involved in the management of the driving task, the picture is further complicated.

As a result, liability apportionment might become extremely complex and costly, requiring substantial litigation, which ultimately might be – inefficiently – prevented leaving the economic burden of damage compensation either upon the user – even in cases where he is not responsible – or the owner. They, indeed might have no sufficient economic

[27] With the relevant exception of France where Loi n. 85-677 of July 5th, 1985, "Tendant à l'amélioration de la situation des victimes d'accidents de la circulation et à l'accélération des procédures d'indemnisation", also known as "Loi Badinter", puts forth a form of strict liability, very similar to a no-fault plan, since victims are entitled to compensation if the vehicle is simply involved in the accident (see Le Tourneau, P. (2012). Droit de la responsabilité et des contrats. Régime d'indemnisation. Paris, Dalloz., 8102.

[28] Such as art. 2054, of the Italian civil code, that holds the owner of the vehicle liable in an objective way, unless he can show that circulation occurred against his consent. The rationale of the law is that of ensuring the victim's compensation by holding the party liable that might have a larger estate, see Bona, M. (2011). Art. 2054. Commentario del Codice civile. E. Gabrielli and U. Carnevali. Turin, UTET., 378. The same rule is applicable, for instance, under French law, where the aforementioned Loi Badinter mentions at the same time the conducteur and the gardien, and, to a lesser extent, under Spanish law, where Ley 35/2015 (of the 22th of September) states (art. 1, 3) that the owner is liable too if he also is a parent, tutor, teacher or director of the driver.

[29] For a detailed analysis see Bertolini, A. and M. Riccaboni (2018). The Regulation of Connected and Automated Driving. A Law and Economics Analysis of Liability Rules. W. Paper.

[30] For a detailed analysis see ibid.

incentives and resources to ascertain the liability of the other parties, and thence pursue actions in recourse against them[31].

Uncertainty with respect to liability apportionment reflects upon the very possibility of identifying ex ante whom shall insure and against which risks[32]. Therefore, despite the compulsory insurance of vehicles prescribed under the MID, this might be insufficient in the case at hand, unless the party that needs to insure is clearly identified. Indeed, most MS require the owner of the vehicle to purchase insurance. Yet in the current system, given the potential liability of the producer and various services providers, who shall bear which risks is unclear. Moreover, the potential existence of unforeseeable new risks, and the lack of statistically significant information in that respect might cause the calculation of premiums to become even more complex.

Some form of intervention is probably required to simplify the system, easing the uptake of CADs.

2.4.1. National frameworks

The analysis of a selected number of national frameworks is provided below.

Germany

Germany has adopted amendments of the Road Traffic Act ((Straßenverkehrsgesetz) to recognise the automated driving systems in vehicles with high automation. Yet, the driver is still defined as the person operating and activating the vehicle, and should be able to immediately take control in case the system requires him to do so or the requirements for the use of the automated driving systems are no longer fulfilled. In that sense, the law does not cover autonomous (entirely self-driving) vehicles. As Freshfields explains in detail in an article, the allocation of **fault and liability** (i.e. whether the driver was vigilant to take control of the situation or the accident was caused based on failure of the system when the driver was relying on it properly) **are to be ensured by the inclusion of a black box in automated driving systems vehicles. As the article points, liability towards an accident victim would still be governed by the existing German car owner framework putting the liability with the vehicle owner.**According to the general rules governing private law, the owner may sue the manufacturer of the vehicle, according to **product liability**.

Italy

According to Rinaldi, in Italy, autonomous driving is restricted by the definition of a driver. Definition in article 46 of the Highway code refers to the driver as the human driver. Therefore, high automation vehicles are not permitted on the streets. Likewise, this has effect on the liability framework**. In Italy, liability is governed by the Civil Code (art. 2054) and driver is liable for damages unless they can prove they did everything possible to stop the accident**. Currently, as fully automated vehicles are not permitted and provided that the driver had a choice to take control, it is likely that drivers would still be held liable for damages caused.

---

[31] This might very much discourage the transition towards higher levels of automation, since the potential consumer might still prefer more traditional vehicles in order to avoid potential risks associated with the use of CADs, see ibid.

[32] Bertolini, A. (2016). "Insurance and Risk Management for Robotic Devices: Identifying the Problems." Global Jourist(2): 1-24.

Sweden

Regarding liability issues, the European Parliament Research Service study reported that in Sweden a proposal for regulation for the testing of autonomous vehicles has evaluated that the laws on compensation for traffic accidents can be applied to all levels of automated vehicles. The Swedish Traffic Damage Act (Trafikskadelagen, 1975/1410) also provides that injured parties in a motor vehicle accident may seek compensation from the liability-motor-insurance (it is the insurer's liability that is the basis for the claim). In addition, when vehicles are in self-driving mode, **criminal liability** shall be borne by permit holders. Drivers will bear criminal liabilities in the cases where vehicles operate at lower levels of automation. **Permit holders will be responsible for submitting information available from the vehicles' sensors to insurance policyholders in cases where investigations are necessary**. Corresponding laws governing the operation of mass-produced automated vehicles are currently in preparation.

United Kingdom

In the UK, several interesting and recent regulatory developments have taken place in the realm of connected, automated and self-driving vehicles. In the end of January 2018, the Automated and Electric Vehicles Bill has been scrutinized by the House of Commons and has been passed to the House of Lords. The Bill includes a specific section on the Automated vehicles and regulates the liability of insurers in case of automated vehicles. The text stipulates that "(1)**Where**—(a)**an accident is caused by an automated vehicle when driving itself**,(b)**the vehicle is insured at the time of the accident**, and (c)**an insured person or any other person suffers damage as a result of the accident**, **the insurer is liable for that damage."** According to the proposed bill however, the motor insurer will have the right of recovery against any other person also liable. Additionally**, the liability of the insurer can be limited in case of an accident resulting from unauthorised software alterations or failure to update software**. **Insurance company are left free to regulate the policy market as they prefer, but insurance would be compulsory.**

Other legislative proposals are looking at amendments of the Highway Code and regulations and might have an impact on automated driving systems. Still, while the proposal includes clarifications and amendments of the Highway Code, it still proposes that **the responsibility still lies with the driver when using advanced driver assistance systems stating that "If you are using advanced driver assistance systems, like motorway assist, or a remote control parking application or device, then you as the driver are still responsible for the vehicle and MUST exercise full control over these systems at all times"**

In March 2018, the UK Roads Minister has announced the start of a three-year project to review the legal obstacles to the introduction of self-driving vehicles in order to develop a regulatory framework appropriate for self-driving vehicles. The specific questions to be addressed include issues of criminal and civil liability, and who the responsible driver or person is, as well as what is the expected impact on road users.

Denmark

A project license will impose an obligation on **the licensee to have insurance in place covering possible damages, and the licensee will have strict liability for all damages caused by the vehicle.** The driver (present or remote) together with the

licensee could also be held responsible for any criminal offence or violation of the Road Traffic Act committed during the test driving in accordance with normal liability rules[33].

4.3. Policy initiatives and strategic orientations

3.4.1. European level

The European commission recently carried out an **evaluation of the PLD[34] and the REFIT of the MID[35].**

As for the **MID**, the analysis focuses on ascertaining the "suitability of the directive in light of the technological development". The results of the public consultation seem to suggest that further in-depth analysis on the topic is necessary, and in May 2018 the European Commission presented **a proposal to amend the motor insurance directive[36]**, suggesting, in particular, that full compensation should be granted to the victims of motor vehicle accidents even when the insurer is insolvent, that drivers who have a previous claims history in another EU country will be treated equally to domestic policyholders, and will potentially benefit from better insurance conditions. The proposed amendment also makes it easier for authorities to combat uninsured driving, aligns the minimum levels of cover by motor insurance across the EU, and incorporates case law of the EU Court of Justice on the scope of the directive. In the proposal, no amendment addresses CAD, which are considered burned by the motor-third party liability insurance, just like ordinary vehicles, and thus are deemed adequately regulated under the current state of the MID.

The **PLD**, instead, was evaluated through an external study and a public consultation[37], "with the specific focus on its continued effectiveness and relevance for emerging digital technologies", coming to the conclusion that the directive strikes a good balance between consumer protection and encouraging innovation in the Eu, and thus "continues – to some extent – to be adequate for the current state of technological developments"[38]. However, the final report identified some critical features of the PLD, which affect its overall application both at the current stage, and in light of future technological development. Firstly, it is not clear whether a software, particularly if non –embedded, constitutes a product for the purpose of the directive. Secondly, with digital evolution the producer will have less control on the features of the product, making the application of the directive diverge from its original rationale. Thirdly, with new technologies the consumer will be in a much more difficult position when asked to prove the defectiveness of the product, and, fourthly, his claim could still be paralyzed by the development risk defence. More generally, the study identified broader challenges to be further assessed in the future, namely the

---

[33] https://www.twobirds.com/en/news/articles/2017/global/at-a-glance-automated-vehicles
[34] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29–33).
[35] Information about the REFIT of the MID can be found at the following link https://ec.europa.eu/info/consultations/finance-2017-motor-insurance_en
(last accessed 1st August 2018).
[36] European Commission, Proposal for a Directive of the European Parliament and of the Council amending Directive 2009/103/EC, Brussels, 24.5.2018 COM(2018) 336 final 2018/0168 (COD).
[37] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), COM/2018/246 final.
Commission Staff Working Document, Evaluation of Council Directive 85/374/EEC of 25 July 1985, SWD/2018/157 final.
[38] Ibid.

possibility to reconsider the general ground for product liability (from fault based to strict liability, also in connection with the capacity of avoiding damages) – and particularly in case of cybersecurity breach –, to reverse the burden of proof, to include compensation for non-material damage, and eventually to strengthen the system of redress among different actors of the value chain.

For this purpose, the Commission has set up an **Expert Group on Liability**, with a formation on Product Liability and one on New Technology[39], to continue an in-depth analysis of such issues and evaluate if a regulatory intervention is necessary, and, if so, which shape it should take. In mid-2019, the Commission will issue guidance on the PLD and a report on the broader implications for, potential gaps in and orientations for, the liability and safety frameworks for artificial intelligence, the Internet of Things and robotics[40].

3.4.1. National level

Some MS have already taken action, namely Germany and the UK.

Germany

Germany has recently amended its *Straßenverkehrsgesetz*[41], thus established itself as the first EU member State adopting a legal framework on CADs. The human-driver is now allowed[42], while performing medium-high or fully-automated functions, to avert his eyes from the road and defer control of the vehicle, but only so long as he remains vigilant, and ready to resume control, (i) when the highly or fully automated system prompts him to do so, or (ii) if he recognizes or, due to obvious circumstances, must recognize that the prerequisites for the intended use of the highly or fully automated driving functions no longer exist[43]. If he causes an accident in breach his duties, he will be held liable according to ordinary fault-based liability rules, although specific caps apply[44]. If a damage is caused by the vehicle operating in automated mode, absent any fault of the driver, the owner of the vehicle will be held accountable, just as it would occur with ordinary driving[45]. According to the general private law, the owner may sue the manufacturer of the vehicle, in case a product liability claim could be made. For this purpose, the law indeed prescribes that automated motor vehicles shall be designed as to allow, through data-recording-equipment, storage of the position and time when control of the vehicle changes from the vehicle driver to the highly or fully automated system, as well as when the driver is requested to take over control of the vehicle control or a technical disturbance of the system occurs[46]. However, the supervision required to the human driver is incoherent with the very purpose of relying on automation to avoid accidents – namely, the tendency in getting distracted – and would require a signal anticipated enough as to permit prompt

[39] Information available at https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1
[40] Information available at https://ec.europa.eu/growth/single-market/goods/free-movement-sectors/liability-defective-products_en
[41] The Law of June 11, 2017 (Federal Law Gazette. I pg. 1607 BGBI. I pg. 160), amending The Road Traffic Act, as announced on 5 March 2003 (Federal Law Gazette. 1 pg. 310, 919) https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl216s1306.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl216s1306.pdf%27%5D__1516706616435, last access on the 23rd of January 2018.
[42] Before this law was enacted, adaptive cruise control was allowed only under constant supervision.
[43] §1b StVG.
[44] § 12 StVG.
[45] § 7 and § 18 StVG.
[46] §63a StVG.

reaction, also taking into account reasonable consumers' expectations. This two aspects aspect combined could indeed ground substantial product liability litigation, discouraging legal claims against manufacturers, and thus delaying the roll out of CADs[47].

UK

In UK, no legislation on CADs has been passed yet. However, the Automated and Electric Vehicle Bill[48] (henceforth AEVB) was presented at the House of Commons last October and is currently under reading. As firstly introduced to the Parliament, the AEVB extends the compulsory motor insurance requirement existent under English law, obliging CADs owners to acquire insurance covering the technical failure of the automated driving system[49]: therefore the insurer would cover both damages suffered by third parties (personal injury, death, or property damage) as well as those caused to the driver himself, with the same caps provided for traditional vehicles[50]. If the vehicle not be insured at the time of the accident, the owner will be accountable instead[51]. In any case, both the insurer and the owner can recover from the actual wrongdoer – either the driver who has relied on the automated system when it was not appropriate to do so, or the manufacturer, in the damages where cause by a defect in the product – the amount paid in compensation[52]. The idea behind the UK solution is that a first- and third-party insurance to be purchased by the owner of the vehicle ensures the victim obtains prompt and certain compensation, clearly identifying the subject to be sued, resting liability on the party best position to pay (the insurance company itself), irrespectively of any ascertainment about the details of the accident and, more specifically, the mode – traditional or autonomous – in which the vehicle was driving. However, neither the insurer nor the owner would be held liable, were the accident wholly due to the driver's own negligence in opting for the autonomous mode, when it was not appropriate to do so[53], or were the accident caused by unauthorised software alterations perpetrated by the insured person directly, or with his knowledge, or by a failure to install safety-critical software updates[54]. This, on the one hand, replicates the same problems highlighted for the fault-based liability introduced by the German law and, with specific reference to the failure of updating the software, does not create the adequate incentives for preventing damages to occur in the first place.

However, legislation occurring a MS level risks fragmenting the market. Indeed, liability rules might have a bearing on which technological solution is favoured[55]. Diverging legislations could provide different incentives to manufacturers across Europe, fragmenting the EU market and industry. Most likely intervention ought to occur at EU level, as revising existing regulation, as well as introducing additional regulation on the allocation of risks related to CADs as the economic potential to generate European added value, as explained by the study "A common EU approach to liability rules and insurance for connected and autonomous vehicles - European Added Value Assessment".[56] Legislative measures from

[47] BERTOLINI RICCABONI Bertolini, A. and M. Riccaboni (2018). The Regulation of Connected and Automated Driving. A Law and Economics Analysis of Liability Rules. W. Paper.
[48] Available at https://services.parliament.uk/bills/2017-19/automatedandelectricvehicles.html.
[49] Clause 2(1).
[50] Clause 2(3) and 2(4), referring to section 145(4)(b) the Road Traffic Act 1988 (limit on compulsory insurance for property damage).
[51] Clause 2(2).
[52] Clause 2(7) and 5.
[53] Clause 3(2).
[54] Clause 4.
[55] See Bertolini, A. and M. Riccaboni (2018). The Regulation of Connected and Automated Driving. A Law and Economics Analysis of Liability Rules. W. Paper.
[56] Evas, T. (2018). A common EU approach to liability rules and insurance for connected and autonomous vehicles. European Added Value Assessment Accompanying the European Parliament's legislative own-initiative report (Rapporteur: Mady Delvaux), EPRS European Parliamentary Research Service.

the EU could indeed reduce the **transaction costs resulting from the fragmentation of national legal systems, and minimize litigation costs, thus easing the roll out of CADs on the market[57].**

4.4. Mapping of stakeholders' views

In general, stakeholders view the attribution of the burden of proof in case of accidents related to CAD as another important challenge to address. Various stakeholders stress the importance of defining responsibilities (e.g. a set of guidelines) to ensure predictability in terms of liability allocation. According to ACEA, legislation should be put in place to define the driver's role across the different driving scenarios. Liability schemes in case of an accident or infringement to the highway code need to be carefully designed for each level of automation and clearly communicated to the users to ensure a smooth transition between full driver liability to full manufacturer and road operator liability.

In terms of event data recorders, some stakeholders suggested that inputs from Event Data Recorders should be used to determine liability allocation in higher levels of automation. Level 3 is flagged as the most problematic one in terms of liability: one stakeholder views it as a "peak" rather than a progression. Some agree to a direct transition to Level 4. There is a broad agreement that higher levels of automation will at least involve additional actors (besides the human driver) if not involve a transfer of responsibility to the software/hardware manufacturer.They were concerned with the reliability and robustness of EDRs over the vehicle's life. According to them, event data recorders (EDR) and data storage systems for automated driving vehicles (DSSA) should be considered for automated vehicles from SAE level 3 onwards and standards should only be defined if they are fitted in vehicles.

When it comes to compulsory insurance schemes, some stakeholders welcome the idea , with one stakeholder suggesting a European Insurance. End users represented by BEUC for example, believe that the EC should analyse the merits to introduce a mandatory insurance system, particularly for risk sectors.Others opt for a preservation of the heterogeneity of liability regimes.

In terms of legal amendments, the end users, represented by BEUC believe that several changes should be made.

- Motor Insurance Directive should be futureproof and ensure the victims' protection with the increasing automation of the driving task.' [58]
- DSSAs (Data Storage Systems for Automated Driving) should be considered for automated vehicles from SAE level 3 onwards and standards should be defined if they are fitted in vehicles[59].
- the Product Liability Directive needs to be reformed in order to build consumer confidence in CCAM; Extension of the scope to all types of products, digital content products, and (digital and other) services; Automotive suppliers represented by

[57] Bertolini, A. and M. Riccaboni (2018). The Regulation of Connected and Automated Driving. A Law and Economics Analysis of Liability Rules. W. Paper.
[58] https://www.fiaregion1.com/wp-content/uploads/2018/02/2018-01-24-FIA-Region-I-Policy-Position-on-Motor-Insurance-Directive_FINAL.pdf
[59] BEUC, 'Protecting European consumers with connected and autonomous cars', http://www.beuc.eu/publications/beuc-x-2017-138_dve_beuc_connected_autonomous_cars.pdf , November 2017, (accessed 23 July 2018).

CLEPA, emphasizes the need to expand the Product Liability Directive's scope to incorporate intangible elements, such as software. Aftermarket service providers also suggested reviewing the Product Liability Directive to incorporate multiple actors in the process of liability identification[60].

4.5. Impact of the issue and possible solutions on business models

5.4.1. Potential impact on uptake of CAD

Policy action will develop a European regulatory framework that clearly allow consumers to identify which actor should be kept responsible in case of accident involving an automated vehicle. This will help the social fostering the social acceptance of automated vehicle, supporting the uptake of CCAM.

Depending on how the liability framework will evolve, it can be expected the **automotive sector to "skip" from level 2, where liability clearly lies on the driver, to level 4, where liability could be hold on OEMs. This in order to avoid the potential legal consequences level 3, a level with shared responsibility between vehicle and driver, could generate.**

On the other side, if an European regulatory framework clearly defining the liability framework for accidents involving automated vehicles is not defined. Consumers will not have the perception of being protected in case of accident, and they will therefore develop a scepticism toward automated vehicle. Consequently, level 3, level 4 and level 5 uptake to be affected.

5.4.1. Potential impact on automotive value chain

Different players of the value chain will be affected, depending on how the future liability framework will allocate the responsibility in case of accident.

If an automated vehicle will be considered anything different than a normal product, liability could be assumed to lie with the vehicle manufacturer, as described under the Product Liability Directive. In this case, **OEMs will heavily invest in data analytics and data recording technology, as well as on partnerships with established players of the insurance industry to provide customers with adequate insurance policies.**

For insurance companies, automated vehicles will require a re-thinking of the traditional insurance business models. The potential reduction of accidents will reduced profit pool. In addition to that, insurers will have to change their way they assess risks and how they set premium. Under this scenario, insurance companies will move from insuring private people to companies and leasing agencies. Furthermore, insurance companies are be expected to start developing partnerships with OEMs to manage new liabilities and risks.

4.6. Conclusions and recommendations

[60] BEUC, 'Review of Product liability rules', http://www.beuc.eu/publications/beuc-x-2017-039_csc_review_of_product_liability_rules.pdf, November 2017.

As a conclusion, any action is advisable to ease the emergence of CADs that clarifies the current liability framework. In terms of precise recommendations, the analysis conducted in the framework of this project, has concluded that:

a) The relevant authorities should consider a **revision of the PLD and its scope of application**. Indeed, CADs could be subject to autonomous regulation at EU level, that would be preferable to leaving the initiative to single MS, so as to avoid fragmentation. The current initiative aiming at delivering new interpretative guidelines on the PLD might, in this respect, prove insufficient, for it would not solve the problem of the complex distribution of liability among all the different subjects involved. Indeed, MSs' ad hoc legislation, presented so far, does move in that direction, attempting to simplify the overall liability framework, by distributing responsibility in a clearer fashion ex ante, causing the outcome of potential litigation to be foreseeable.

b) **Autonomous regulation could use compulsory insurance schemes, no-fault plans, as well as a risk-management approach**. Insurance regulation despite theoretically adequate, falls victim of uncertainty with respect to liability apportionment, as well as of the uncertainty referring to the new kinds of risks – and their likelihood – that might emerge as a consequence of the very function and design of CADs as well as of the complex interaction of vehicles with different levels of automation on public roads.

5. TESTING ON PUBLIC ROADS

5.1. Issue definition

Member States are progressing fast in terms of ongoing testing on roads projects. There are well-developed programs and sites for testing autonomous vehicles. However, there are still very important challenges to overcome and to be covered by a legal framework.

- **Unharmonized testing activities and different testing procedures across countries**, make the overall implementation of testing on roads difficult for stakeholders. It is also linked to the fact that **cross-border testing activities are still limited in numbers.**
- **Incidents on testing cases are not widely reported and communication is lacking between different projects and Member States Initiatives**. Even if Europe is quite advanced in the implementation of testing for CCAM, there is a **lack of cooperation**[61].
- **Further amendment of the Vienna Convention** is required for large-scale operation because the current amendment does not allow testing vehicles to run on public roads without a driver in control[62].

5.2. State of the art – legislative frameworks

In general, the legislation allowing testing on roads is national and takes into account the international agreements in place (such as Vienna Convention).

2.5.1. International and EU framework

At **international level**, The Vienna Convention on Road Traffic regulates the admission of vehicles in international traffic and harmonises traffic rules across countries. An amendment of the Vienna Convention (VC) was initiated in early 2014 by Austria, Belgium, France, Germany and Italy. As an effect of the resulting update (March 2016), the VC currently allows testing. The introduced changes allow Member States to perform testing of automated vehicles and to adapt their national road regulations. However, the current version of the Convention does not remove all barriers to testing, as automated vehicles are not allowed to run on public roads without a driver in control. In this frame, there is a very inhomogeneous situation across Member States, since:

- Not all (21 out of 28 EU countries) Member States signed onto the Vienna Convention on Road Traffic;
- There are different interpretations of the provision of the VC even across these 21 Member States.

Aside the provisions of the Vienna Convention, **the applicable legislation is mainly national** (traffic rules) and derogations to the'normal' traffic rules are possible, which means that in general **it is responsibility to the Member States to allow testing on roads.** Most European countries are acting in terms of CCAM testing; however, currently

[61] GEAR 2030 final report
[62]https://www.euractiv.com/section/transport/news/eu-countries-want-legal-change-for-driverless-cars-but-theyll-have-to-wait/

each Member State has its own testing procedures, principles and rules under the national legislative framework.

2.5.1. National frameworks

There are varied scenarios across Member States with regards to on-road testing. In Europe, a lot of activities have been undertaken in the past years to allow testing on roads[63]. There is a race to create favourable on-road testing environment. As mentioned above, key drivers of these differences involve different factors: legal provisions of national road codes, signature and interpretation of the Vienna Convention, and of course strategic interests in automated driving.

The following examples of national frameworks present the most active Members States in terms of testing of CAD, but it should be noted that this is not an exhaustive list.

France: The French National Assembly authorised automated vehicles for testing purposes. In 2016 the French Ministry of Environment Energy and Sea and the Ministry of Interior launched a decree regarding testing on roads. Authorisation for such testing operations is granted by the Ministry of Transport (heavily restricted in terms of time and location). In 2018 France announced to allow **Level 4 vehicles, to be used for testing on roads with no human operator behind the wheel by 2019**, as a relevant step forward as compared to the current legislation which requires a human operator[64]. Official standards for testing are expected to be published in 2020. France is participating in cross-country environment testing: State authorities of France and Germany have adopted a letter of intent for the implementation of an itinerary between Metz and the Sarre for the testing of autonomous vehicles[65].

United Kingdom: On testing, in 2015 the Department of Transport released its paper The Pathway to Driverless Cars[66], stating that existing regulation is not a barrier to **testing automated vehicles on public roads, if human is sitting in the driver's seat and remains prompt to resume control if needed[67]**. In the same year the Department of Transport released a **Code of practice for testing,** clarifying that responsibility for testing rests with the testing organisation; vehicles under testing must comply with all relevant road traffic law; test drivers must hold the appropriate driving licence and receive training appropriate to the vehicle; testing organisations should conduct risk analyses of any proposed tests and have appropriate risk management strategies; and the statutory requirements on the holding of insurance apply.

Italy: A testing site at the Florence–Livorno freeway has been dedicated for testing of connected vehicles as part of the AUTOPILOT EU project. The stretch of the pilot site is equipped with ITS technology for control and data analysis and results are expected to provide ITS stakeholders with information on different complex scenarios and how AUTOPILOT technologies are performing. As part of the 2018 budget law, a decree was

---

[63] Available at: https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf , page 6
[64] https://www.autovistagroup.com/news-and-insights/france-amend-legislation-autonomous-vehicle-trials
[65] Available at: https://ec.europa.eu/digital-single-market/en/cross-border-corridors-cooperative-connected-and-automated-mobility-ccam
[66] Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401562/pathway-driverless-cars-summary.pdf,
[67] It is also to be noted that the UK did not sign onto the VC agreement

published in **Italy to authorize tests of driverless cars on the country's roads. A key point is that during testing, human on board, who will be able to take control of the vehicle is still required**[68].

The Netherlands: The Netherlands has actively supported the development of an infrastructure to initiate testing of connected and automated vehicles. In 2017, the Dutch Cabinet approved legislation that makes it possible for **manufacturers to carry out much more extensive testing of self-driving vehicles, with remote drivers.** A Task Force supporting the Dutch road authorities by developing knowledge and sharing experiences of tests with self-driving vehicles has also been established. The Dutch Vehicle Authority (RDW) has also initiated a "Digital Driving License Project".

Spain: Spain has introduced regulations from November 2015 that establish a legal framework allowing for tests to be conducted with autonomous driving vehicles on public roads. When testing CAD, any issue or incident must be immediately communicated to the Spanish Directorate General of Traffic (DGT). DGT intends to work on a so-called '21st century Traffic Act' which will regulate the driverless cars regime in detail.

Finland: in the strategic document "Road Transport Automation Road Map and Action Plan 2016–2020", foresees the opportunity of having on-road testing allowed through test plate certificates (SAE 0-5), with driver either inside or outside vehicle. Even if Finland has signed onto the VC, this is possible thanks to the national interpretation of its provisions.

5.3. Policy initiatives and strategic orientations

At **international level**, UNECE continues to address the topic trough WP.1 group, which reflects on testing of CAD on public roads. In addition, there is an ongoing draft resolution on the deployment of highly and fully automated vehicles in road traffic[69].

At **European level**, large scale and cross-boarder testing is supported these activities through research funding programmes and deployment projects. As summarised in the 3rd Mobility Package, "For the period 2014-2020, a total budget of around EUR 300 million from the EU's framework programme for research and innovation "Horizon 2020" has been allocated to support research and innovation on automated vehicles"[70]. Concretely, the Commission undertook the initiatives to[71]:

- Create a priority list of transport use cases for testing with the support of MS;
- Identify possible synergies between connectivity and automation use cases;
- Establish one single EU wide platform grouping all relevant stakeholders to coordinate open road testing.

At **national** level, aside the abovementioned activities to authorise testing, different Member States are currently working, or are planning to work, on documents clarifying the

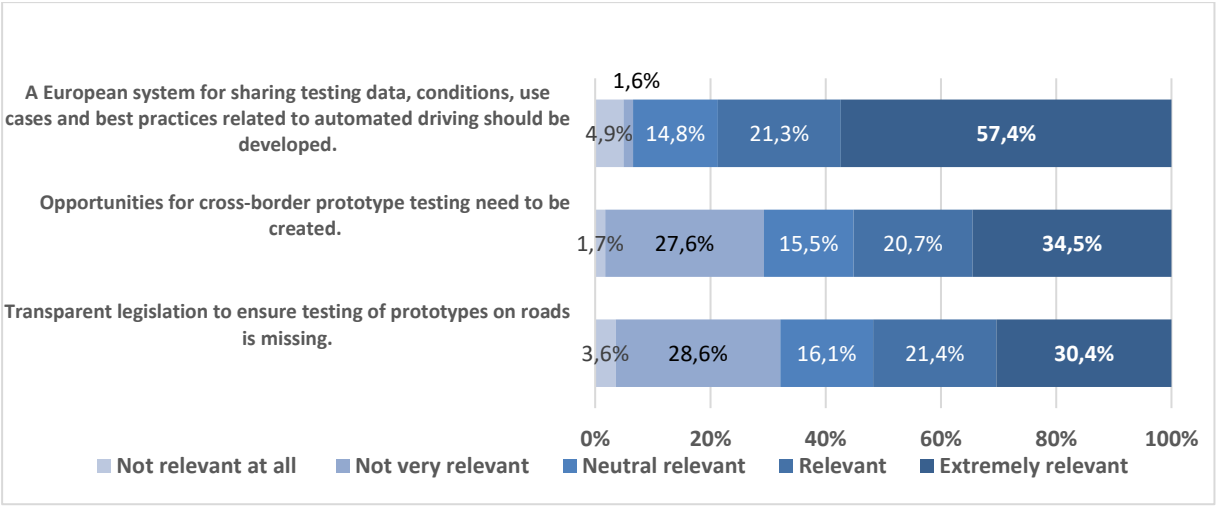
[68] https://www.thelocal.it/20180420/italian-parliament-driverless-cars-road-tests
[69] Available at: http://www.unece.org/trans/themes/transtheme-its/selfdriving/next-steps.html
[70] Available at: https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf , page 6
[71] Available at: https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf , page 8

testing requirements at national level. For example, Germany Federal Ministry of Transport and Digital Infrastructure, advocates for the need to close gaps in the field of testing to be potentially concluded by mid-2019[72].

5.4. Mapping of stakeholders' views

The survey conducted in the frame of the study asked stakeholders to identify the potential challenges related to automated vehicles on road. One of the results is that **79% of respondents believe that a European system for sharing testing data, conditions, use cases and best practices should be developed.**

Figure 5 Challenges related to automated vehicles testing on road



Another relevant point is that 55.2% of the respondents support the idea of cross-border prototype testing being a relevant or extremely relevant opportunity. Respondents also provided a feedback that is matching the direction of work ongoing at European level regarding initiatives for cross-border testing operations to ensure interoperability and connectivity between Member States. This was further confirmed by the stakeholder consultation, where stakeholders stressed the importance of cross-border testing, considering the fact that mobility itself is cross border and considering the goal to achieve a single market in EU, cooperation between Member States is vital.

Moreover, 51.8% of the respondents believe that transparent legislation to ensure testing of prototypes on road is missing. This outcomes relates to the fact that in some countries it is challenging for stakeholders interested in testing on roads, to understand the conditions and rules to receive testing authorisation.

In addition, the study asked stakeholders to indicate, for the issues above, whether the legislative framework would need to be adapted at the European level, National level, both above or none for all the issues above, European action and/or combined European and National action was indicated as the optimal way forward.

[72] German Federal Ministry of Transport and Digital Infrastructure "Action plan automated and connected driving"

5.5. Impact of the issue and possible solutions on business models

The level of interest on allowing testing of automated vehicles can be different across Member States. The most proactive countries are the ones that retain strong industrial competences in automated driving, wish to attract investments from the automotive industry and/or wish to benefit from faster CCAM uptake.

Given the level of interest in allowing testing of automated driving and provided that the interpretation of the VC and national road codes enable testing, a source of competitive advantage for MS is the presence of transparent rules and processes to obtain the authorisation. Multiple, unclear or non-transparent pre-testing requirements could discourage OEMs and other relevant players in the CAD testing to perform testing activities in a given country.

Finally, and relevant in particular for the connected and cooperative functions, strong fragmentation of the market uptake across Member States and lack of cross-border testing to ensure interoperability could discourage consumers in the future to invest in automated vehicles, since this could prevent the optimal usage of the vehicle across borders.

5.6. Conclusions and recommendations

In terms of recommendations, the analysis conducted in the framework of this project, has concluded that:

a) It is a priority for the Commission to encourage Member States to provide transparency of testing requirements/principles/guidelines. The European Commission could support achieving this goal by means of recommendations, by monitoring and analysing the different interpretations of testing requirements, and by cross-fertilisation actions aimed at driving Member States towards a more homogeneous approach.

b) The EC should establish stronger cooperation on testing across Europe. Aside from the already ongoing support to cross-border and large scale testing, the Commission could support the implementation of European system for sharing testing data, conditions, use cases and best practices related to automated driving. As a complementary action, the EC could provide to SMEs possibility to perform consortium testing and participate in cross-border testing initiatives.

6. CERTIFICATION

6.1. Issue definition

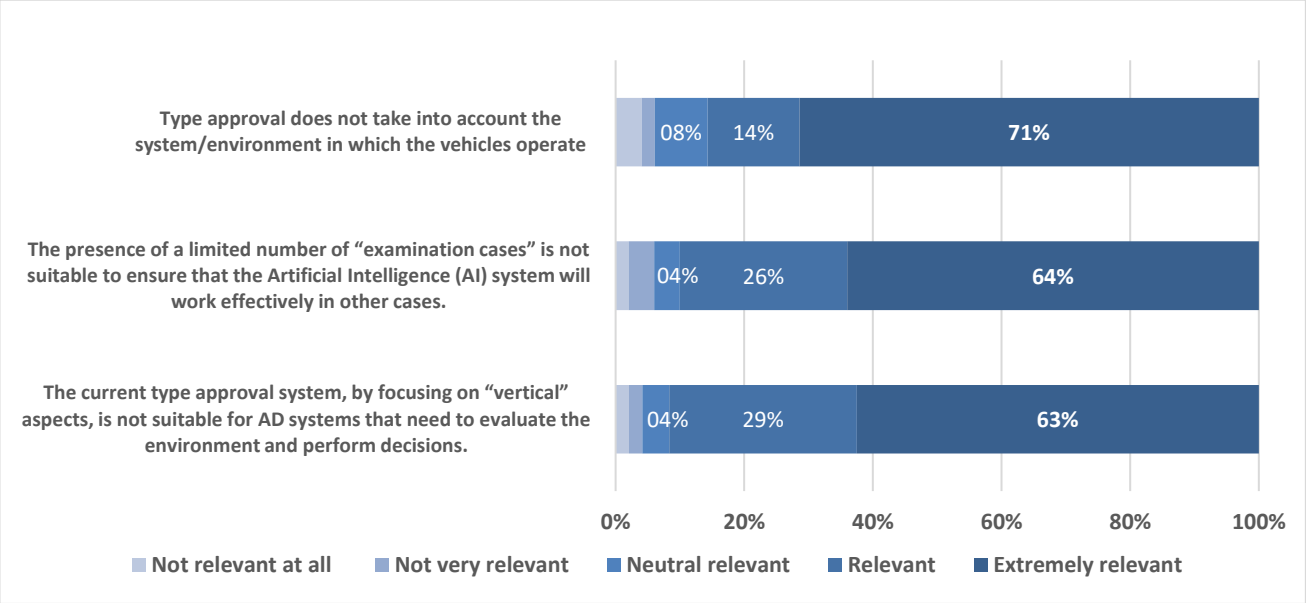
There is wide agreement among industry players and other stakeholders that the regulatory regime on certification, defined in UNECE regulations at international level and referred to under the EU type-approval system, should evolve to accommodate the specificities of automated driving.

In great summary, the current regulatory approach describes what to test and how. Approval is based on a certain number of "type cases", taking into account the vehicle and its components. Overall, approval is guaranteed once and then periodical technical inspections are foreseen. As confirmed by the wide majority of stakeholders, this approach, which works for traditional vehicles, poses a series of challenges for automated driving systems that monitor the environment, evaluate the situation and take decisions. This includes the following:

- Automated operation cannot be tested as combination of "vertical" components, which individually might meet requirements;
- The definition of a limited number of test cases is not suitable to ensure safety of an artificial intelligence based system, which needs to take decisions in the real world taking into account an endless number of possible situations and scenario;
- Also, in the current framework there is a limited possibility to consider the actual environment in which the vehicle operates;
- It would be challenging to ensure the validity of certification over time, as new threats and issues are likely to emerge over the lifetime of the vehicle and it is expected that these would be addressed through important update of the software.

Such view is fully confirmed by the survey conducted in the study. Respondents were asked to specify, for each potential challenges related to certification and type approval in the frame of the automated vehicles, the relevance of the issue from 1 to 5, where 1 is not relevant at all and 5 is extremely important/relevant. The outcomes of the survey are reported in the figure below.

Figure 6 Stakeholder survey - Issues related to certification and type approval



The three main challenges related to certification and type approval proposed to stakeholders all were suggested to be extremely relevant and important bottlenecks.

- 85% of respondents considers a relevant or extremely relevant challenge the fact that the type approval does not consider the system/environment in which the vehicles operate.
- Around 90% of respondents believe that it is a relevant or extremely relevant issue the fact that there is limited number of "examination cases", not sufficient to ensure that AI will work effectively in other cases.
- Finally, 92% of respondents believe (issue judged relevant or extremely relevant) that the current type approval system is not suitable for automated driving systems because of its focus on "vertical" elements.

6.2. Key market and industry trends

Being certification and type approval a regulatory and technical aspect, market and industry trends are at the core issue. However, the current need to uptake the certification framework arises from and needs to take into account the combination of a range of trends[73]:

- Increasing importance of data as well as cyber security;
- Increasing relevance of software and simulation, with regular over-the-air (OTA) updates making one-time homologation insufficient, as essential safety features can be subject to change through software updates;
- Increasing power of Tier 1 and Tier 0.5 suppliers, due to deep technological knowledge and a shift to construction in modules;

[73] VD Tuev, Achieving lifelong security and safety of tomorrow's cars via continuos testing and certification, presented during the project Stakeholder Workshop report of June 2018

- V2X interactions becoming more important in a connected world, implying also a larger ecosystem of involved parties;
- Highly automated driving specificities being incompatible with current homologation and testing approaches;

It is important to stress that the industry acknowledges the issue and has been taking an active role in addressing it, as proven by the fact that the current work ungoing at UNECE level under WP.29 is based on the proposal developed by OICA[74].

6.3. State of the art – legislative frameworks

Focusing on **type approval**, the current regulatory framework on certification applicable in Europe is centered on the Framework Directive 2007/46/EC, establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles) rules the approval schemes of the new motor vehicles and their trailers in the European Union[75].

Considering the requirements, **UNECE Regulation plays a central role**. The actual technical requirements against which vehicles have to be tested are covered in the legislation listed in Annex IV to the directive. Here the approach, further complemented and amended by subsequent pieces of legislation (notably Regulation (EC) No 661/2009), considered appropriate to refer, where relevant, to the corresponding UNECE Regulation annexed to the 1958 Agreement[76], as incorporated into Community law in accordance with Decision 97/836/EC.

This means that, the EU regulatory approach, considering the global scope of vehicle manufacturing and to reduce the administrative burden of the type-approval process, foresees that vehicle manufacturers can obtain type-approval, where appropriate, by means of obtaining approval in accordance with the relevant UNECE Regulation.

Within this framework, Directive 2007/46/EC includes provisions impacting administrative procedures at **national level** to be followed for the approval of vehicles. The EU type-approval system is based on the principles of third-party approvals* and mutual recognition* of such approvals. Under the type-approval regime, before being put on the market, the vehicle type is tested by a national technical service in accordance with the

---

[74] See UNECE Wiki – OICA, Initial ideas for a new certification system to accommodate AV. / software functionalities, June 2017

[75] It provides EU countries with a common set of rules for the approval of motor vehicles and their trailers and of systems, components and separate technical units intended for these vehicles. It makes type approval compulsory for all categories of whole vehicles, including those built in several stages. It lays down: i) a harmonized framework with general technical requirements for the type approval of new vehicles and of systems, components and technical units designed for such vehicles, so as to facilitate their registration, sale and entry into service in the EU; ii) rules regarding the sale and entry into service of vehicle parts and equipment. The directive applies to cars, vans, trucks, buses and coaches, which are now covered by fully harmonised EU requirements.

[76] Agreement concerning the adoption of uniform technical prescriptions for wheeled vehicles, equipment and parts which can be fitted and/or be used on wheeled vehicles and the conditions for reciprocal recognition of approvals granted on the basis of these prescriptions

legislation. The national approval authority then delivers the approval ('CE certificate') on the basis of these tests. The manufacturer may make an application for approval in any EU country. It is sufficient that the vehicle is approved in one EU country for all vehicles of its type to be registered with no further checks throughout the EU on the basis of their certificate of conformity.

Within this regulatory framework, relevant steps have been taken to deal with the challenges posed by automated driving in a certification perspective. With a focus on legislation in place (current initiatives are covered in Section 6.5), at **international** level UNECE WP.29 adopted an amendment to **UN Regulation No. 79** in March 2017. This amendment targeted the Automatically commanded steering function (ACSF) and corrective steering function (CSF). In the update, six new "categories" of ACSF were defined and the necessary elements to enable type approval of the first categories (Category A, park assist systems and Category B1, lane keep assist systems) were introduced[77].

At **European level**, different pieces of legislation that, although not addressing directly automated driving, updated Directive 2007/46/EC in light of the pace of technological progress and the related challenges related to type approval. As an example, Regulation (EU) 2015/166 takes stock of the need to set out specific procedures for type-approval[78] concerning new technologies or concepts incompatible with the existing measures implementing Regulation (EC) No 661/2009 covered by UNECE regulations. This "exemption" means that technologies not foreseen by EU or UNECE rules can be approved on the basis of a national ad-hoc safety assessment.

6.4. Policy initiatives and strategic orientations

At **international level**, driven by the initiative taken by OICA[79] a Task Force on Automated Vehicle Testing (*AutoVeh*) was set up within the ITS/AD informal working group under the UNECE World Forum for Harmonization of Vehicle Regulations (WP.29). The objective of this task force is to develop an extension of the certification framework to accommodate automated driving requirements.

More into details, the task force has been established to investigate testing/assessing the functionality of automated driving systems. It includes many CP and affiliated bodies, presenting a widest approach to the regulatory solutions and outcomes, with a 2-3-year time frame (draft regulatory proposals should be submitted to the June 2020/181st Session of WP29). The expected outcome of the Task Force is a regulatory test regime with adoption and lead times that could be implemented for new registration by 2022-2023. The initial structure of the draft regulation includes, as initally proposed by OICA, three elements:

[77] The Informal Working Group on ACSF is currently is now working on the development of requirements to cover the other Categories of ACSF for introduction into ECE 79 at a future date

[78] according to Article 20 of Directive 2007/46/EC

[79] OICA, the Organisation Internationale des Constructeurs d'Automobile, has produced, in the document "certification of automated vehicles, Document No. ITS/AD-12-11" ,a set of recommendations that includes the proposal to augment existing certification process to accommodate AV software functionalities as well as introducing the concept of multiple systems and technologies (horizontal) and the approval system to account for traffic scenarios beyond the scope of traditional testing.

- Classical physical certification tests,
- Real-world driving tests,
- and audits of manufacturer compliance with industry standards, best practices, and methods to ensure software integrity and cybersecurity, based on self declarations leveraging on internal testing, including simulations and virtual testing.

The logic of this certification framework is to be **additive** to the current one, which focuses on the certification systems of components, whereas he new framework will focus on automated driving software and functionalities.

In this perspective, it is important to stress that while the main focus of the current framework is safety, both safety and security will be relevant for certification regarding automated driving and software. In this frame, relevant activities are ongoing at standardisation level:

- ISO is currently conducting a revision of Revision of ISO 26262 and SOTIF autonomous driving standard, that will complement the ISO 26262 (Safety of the Intended Functionality) with ISO/PAS 21448, explicitly addressing autonomous vehicles by defining a minimum set of requirements for automation software.
- Work is ongoing on the drafting of standard ISO SAE 21434 - Automotive Cybersecurity Standard, to fill in a gap in the current cybersecurity framework not addressing automotive cybersecurity[80].

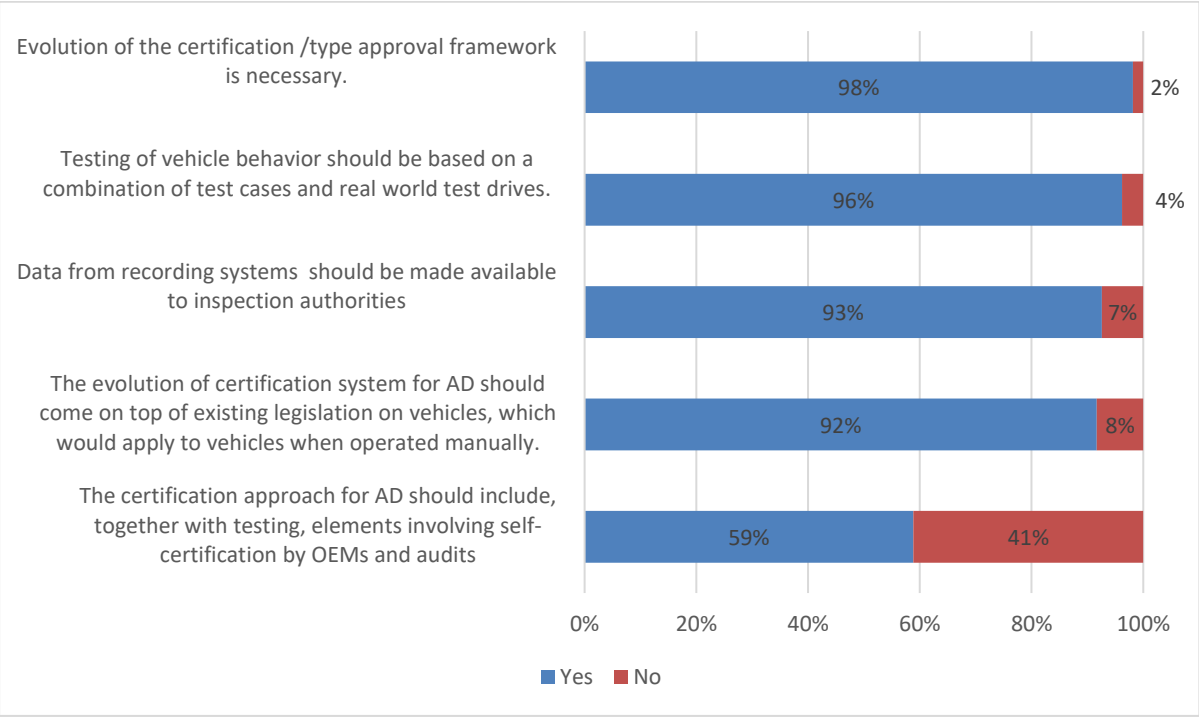
At **European level**, the European Commission declared in the 3rd Mobility Package[81] that it will work with Member States on guidelines to ensure a harmonised approach for national ad-hoc vehicle safety assessments of automated vehicles. Furthermore, the European Commission has expressed its interest in initiating activities with the Member States and stakeholders in order to develop a new approach for vehicle safety certification for automated vehicles.

6.5. Mapping of stakeholders' views

There is almost unanimous consensus among stakeholders that the certification and type approval framework should evolve, in light of the changes brought by automated driving. The survey conducted in the frame of the study asked whether respondents agree or not with a series of statements on certification related to automated driving. One of the results is that 98% of respondents believe that the evolution of the certification type approval framework is necessary.

[80] Work started in October 2016. A Working Draft was issued in April 2018, and release is expected in late 2019 or early 2020.
[81] Brussels, 17.5.2018 COM(2018) 283 final

Figure 7 Stakeholder survey – Need for evolution of the certification framework



Respondents also provided a feedback that is matching the direction of work ongoing at UNECE level. They agreed (92%) that the evolution of certification system for AD should come on top of existing legislation on vehicles, which would still apply to vehicles when operated manually. The logic of having testing based on a combination of test cases and real-world test drives was widely agreed (96%); however, there is less consensus (59%) on introducing in the certification approach, together with testing, elements involving self-certification by OEMs and audits to provide a comprehensive assessment while containing costs. This diversity of views reflects a key trade-off between the requirement on the one hand to ensure safety (and security) of automated vehicles and on the other hand the need for the industry to maintain testing and certification costs to an acceptable level.

Another relevant outcome of the survey, reflecting the importance to ensure that type approved vehicles remain safe over time, is that of 93% of the stakeholders think that data from recording systems (e.g. Electronic Data Recorders, Data Storage System for Automated Driving) should be made available to inspection authorities to identify safety challenges during the lifetime of the vehicle.

Finally, it is important mentioning that, while certification and type approval are mostly focused on the safety dimension, several stakeholders have been stressing the increasing importance of security. This regards both:

- Vehicles and components, with FIA – in a position paper of 2016 – requesting "the inclusion of a provision granting type approval only for tamper-proof systems, components and separate technical units for vehicles."
- More importantly, software and its update. Inspection companies and organisation contacted in the study stress on the one hand that given that technical certification for cybersecurity is just a snapshot in time, certification must focus on processes and not on technical specifications. This perspective is echoed by a position paper issued by BEUC, stating that "Manufacturers shall make sure that when they first put a product on the market, the software that runs on the product is as secure and

up-to-date as it can be. In addition, manufacturers should also be required to ensure that the software is updated during the entire lifecycle of the product whenever this is needed to guarantee that it remains secure."

6.6. Impact of the issue and possible solutions on business models

As stressed above, although this topic is mostly regulatory and technical, market and industry trends are not fully relevant to this issue, and the same applies to business models; however, the need to extend certification for automated driving implies a trade-off between the creation of additional requirements on the one hand to ensure safety (and security) of automated vehicles and on the other hand the need for the industry to maintain testing and certification costs to an acceptable level.

6.7. Conclusions and recommendations

Extension of the certification and type approval framework as to encompass automated driving is necessary. By ensuring safety and contributing to public acceptance, it is of key importance to support the uptake of the market.

At the present stage, the challenge consists in defining and implementing a suitable framework, capable to identify a set of test methods and criteria to be satisfied for automated vehicles of level 3 or higher. This challenge is already being addressed at UNECE level by a specific Task Force under the ITS/AD Informal Group within WP.29.

Also, activities at UNECE level are progressing on the update of UNECE Regulation 79.

In this frame, as the European approach to type approval refers to UNECE Regulation it is sensible to leverage on this activity, as well as to steer it by participating to the work in order to ensure that:

- An optimal balance is achieved between the extension, approach and stringency of the testing (and associated levels of safety and security), and the administrative burder on the industry;
- The process is taken advantage in case certification is relevant for European programmatic priorities related to certification – such as ensuring that European GNSS features related to safety (e.g. integrity) and security (e.g. authentication) are properly taken into account;
- Activities progress in due time and without blockages or delays.

The last point is particularly relevant because countries that have not ratified UNECE treaties and adopt a "leaner" approach are not bound to finalisation of the work to progress on automated driving adoption roadmaps. This in turn means possibility not only to ensure automated driving uptake faster, but also to roll out the services enabled by automated driving itself. In this perspective, the pace of progress of UNECE activity should be monitored, and available instruments under the EU framework (e.g. the exemption for technological innovation under Article 20 of Directive 2007/46/EC) could be used as possible issue mitigation instruments.

7. CYBERSECURITY

7.1. Issue definition

Main issue

Cybersecurity (CS) both at vehicle level and infrastructure level is defined as the full protection from unauthorised access to in-vehicle and system-level data and functionalities, including safety related applications.

Traditionally, vehicles were generally treated as being the product of the car manufacturer responsible to ensure conformity with safety standards. Until recently, this framework has proved to be efficient for for non-connected, non-autonomous vehicles as manufacturers can ensure conformity of production and subject vehicles to fault-testing under real-world operating conditions.

Cybersecurity represents an important risk in the context of CCAM. Vehicles can be connected to the internet to access real-time infotainment, navigation and customer services. Furthermore, the majority of the vehicles can already record and store technical and personal data, including location, details of the start and end points, the travel route, time and date of travel, and many other information.

In addition to this, in line with the evolution of future AVs, higher level of autonomation will imply that software is installed not only on secondary systems as infotainment and navigation systems, but also on hardware component managing the primary aspects of the vehicle, including breaking, steering and acceleration. For this reason, a cybersecurity threat may have relevant consequences as hackers may access and control the car remotely.

In particular, different types of risks are associated with a break of cybersecurity: on one side, the risk of intrusion (e.g. data or privacy related), and, on the other, risk related to the effects of malware (i.e. traffic safety related).

The level of traffic safety (TS) risk increases according to the role of the software in the critical functions of the vehicle, also considering that adding connectivity channels increase the number and variety of potential threats – notably cooperative approaches are deemed to entail cybersecurity risks as communication data can affect the critical functions of the vehicle.

In terms of defining solution to the issue, divergent cybersecurity approaches exist, as it has emerged during the different interactions with the automotive sector stakeholders.

OEMs would like to opt for a security-by-design and customised CS strategy, whereas other stakeholders suggest that a standardised approach following European CS principles would be optimal. Suppliers and other stakeholders have views in the middle, suggesting broad standards and minimum requirements – OEMs would then be free to develop their strategy to meet these.

Cross issues

In addition to the question of ensuring adequate level of cybersecurity at vehicle and system level from a technical point of view, an additional set of elements need to be considered when evaluating the overal question of Avs' cybersecurity.

One first aspect is related to the question of certification: as security will need to be ensured across the overall lifetime of the vehicle, periodical updates will be necessary. In order to ensure protection from CS threats over time, current certification frameworks will need to be updated accordingly, as in the current form they are not suitable to incorporate and certify software's changes over time.

One second aspect related to overall debate on access to data, which is analysed in depth under Section 8. Ccybersecurity strategies have significant implications for development of downstream business models, because strategies that limit the access to data as means to ensure security also limit the potential to develop services based on that data.

7.2. Key market and industry trends

With the emergence of AVs, OEMs are faced with a complex supply chain of sensor producers, software developers and operating system providers. Ensuring that best practices for cybersecurity are met by all suppliers, if to remain a responsibility of OEMs, could become a challenging issue. Furthermore, once considered the context of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) interactions, the risk of a cybersecurity attack will not only involve the vehicle system, but the communication one as well.

With the complex change in the value chain, OEMs should take into consideration cybersecurity strategy not only at the final product, but also within the value chain itself. The shift from hardware to software with the introduction of technology and digital companies in the value chain requires a completely new approach to cyber security.

However, according to a recent study, less than half of the OEMs possess operational cyber security units. Study of security operations and security monitoring should become part of the very beginning of the value chain. Once a vehicle leaves the factory floor and the direct control of the manufacturer, it is important that the car can be monitored for security anomalies and that it is possible to remotely update its security status via, for example, over-the-air (OTA) software updates.

On the other hand, cybersecurity could represent a real opportunity for the deployment of AI algorithms, since attacks are constantly-evolving, and defences frequently face previously-unknown types of malware. Presumably, AI would have an edge here given its ability to operate at scale and sift through millions of incidents to identify anomalies, risks, and signals of future threats.

Finally, it can also not be forgotten that end users themselves are a key link in the cybersecurity chain.

7.3. State of the art – legislative frameworks

When it comes to cybersecurity, the Directive on security of network and information systems (the NIS Directive) addresses cybersecurity and proposes measures '*with a view to achieving a high common level of security of network and information systems'*. The Directive will require, among others, fMember States to adopt national strategies on security of NIS, creation of computer security incident response teams and network; and sets security and notification requirements for operators of essential services and for digital service providers.

3.7.1. EU framework

Regarding cybersecurity, on January 13, 2017 the EU Agency for Network and Information Security (ENISA) released the study "Cybersecurity and Resilience of smart cars" ("ENISA Guidance"), which identifies good practices and recommendations to ensure security of smart cars against cyber threats[82].

Importantly, the recommendations apply not only to car manufacturers but also Tier 1 and Tier 2 suppliers, aftermarket suppliers, insurance providers and other auto industry stakeholders.

The good practice recommended under the ENISA guidance is categorized under three main categories: policy and standards, including best practices industry actors should follow in terms of industry coordination; Organisational measures, including provisions at management level to ensure the correct assessment of threat model and use cases, provide security and privacy by design and implement and test the security functions.

Furthermore, the ENISA guidance document provides an overview of technical recommendation that should be follow to ensure AVs from potential cyber-attacks.

This includes best practices and recommendations, including on

- storage and access to security events logs;
- use of cryptography experts;
- definition of access control mechanisms;
- denial of service threat to communication infrastructures, with the suggestion of unot using proprietary cryptographic schemes but rather use state-of- the-art standards instead;
- use mutual authentication for remote communication.

In addition to this document, the European Union has taken a number of actions to increase resilience and enhance its cybersecurity preparedness. The first EU Cybersecurity Strategy adopted in 2013 set out strategic objectives and concrete actions to achieve resilience, reduce cybercrime, develop policy and capabilities, develop industrial and technological resources and establish a coherent international cyberspace policy for the EU. Furthermore, in 2016 the European Commission adopted a Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, in which further measures were announced to step-up cooperation, information and knowledge sharing and to increase the EU's resilience and preparedness.

Today all new cars must be approved in accordance with UN Regulation 116 (Protection of motor vehicles against unauthorised use), which requires both a mechanical anti-theft device (in practice normally a steering lock and an electronic immobiliser. UN Regulation 116 is formulated to ensure that vehicle manufacturers put in place measures to prevent unauthorised use).

On the question of cybersecurity in the framework of V2X communication, the European Commission's C-ITS Platform has defined a trust model and certificate policy for the corresponding PKI (i.e. a system for issuing digital certificates to trusted devices through

[82] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/

a hierarchy of entities, the authorisation entity and the enrolment authorities respectively) for C-ITS in Europe[83].

On this issue, the Institute of Electrical and Electronics Engineers has published a standard that defines the formats and processes to build and verify signature and certificates that are specifically suitable for implementation on high performance and mobile embedded platforms. This standard - *Wireless Access in Vehicular Environment - Security Services for Applications and Management Messages* - IEEE 1609.2 - allows the processing of messages from hundreds or even thousands of vehicle per second.

IEEE 1609.2 has been adopted by the European Commission's C-ITS Platform through its sister standard, ETSI TS 103 097, which is fully based on IEEE 1609.2.

3.7.1. National frameworks

Different actions are currently ongoing at national level. France, for example, is currently setting up a working group for threat analysis with various stakeholders as well as working on issuing guidelines and principles for public actor. Similarly, the UK government has recently presented a document, "*The Key Principles of Cyber Security for Connected and Automated Vehicles",* introducing a series of 8 principles out how the automotive sector can make sure cyber security is properly considered at every level.

7.4. Policy initiatives and strategic orientations

At international level, a UN Task Force on Cyber security and OTA issues (CS/OTA), in the context of the World Forum for Harmonization of Vehicle Regulations (WP.29), a working party of the Sustainable Transport Division of the United Nations Economic Commission for Europe (UNECE), is currently investigating the best solutions to best address the issue of cybersecurity in the context of autonomous vehicles.

At European level, the European Commission is proposing to regulate the protection of vehicles against cyber-attacks as part of the revision of the General Safety Regulation for motor vehicles,as presented in the Communication "On the road to automated mobility: An EU strategy for mobility of the future" published in May 2018.

Finally, during a recent public event that saw the participation of Ms. Spanou, Director for Digital Society, Trust & Cybersecurity at the European Commission, it has been announced that the Commission will publish a Recommendation by the end of 2018 to tackle the issues of cybersecurity, access to data and connectivity[84].

7.5. Mapping of stakeholders' views

Cybersecurity, both at vehicle system level and at infrastructure system level (e.g. OEMs network security) has been indicated as one of the key concerns that could affect future autonomous vehicles. While part of the industry supports a standardized – and potentially

---

[83] European Commission (2017), "Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) - Release 1." Brussels: C-ITS Platform chaired by the European Commission, June.

[84] http://www.debatingmobility.eu/past-events/2018/6/19/breakfast-event-connected-and-automated-mobility-is-europe-going-in-the-right-direction

certified – universal standard of security, others advocate a heterogenous system represented by proprietary standards.

In addition to this, suppliers emphasize the importance of information sharing and are more inclined towards an "in-between the two solutions": while it is true that heterogeneous proprietary standards are supposed to be a harder target for cyber-attackers, stakeholders mostly agreed on the fact that some minimal/generic standards should be set in place.

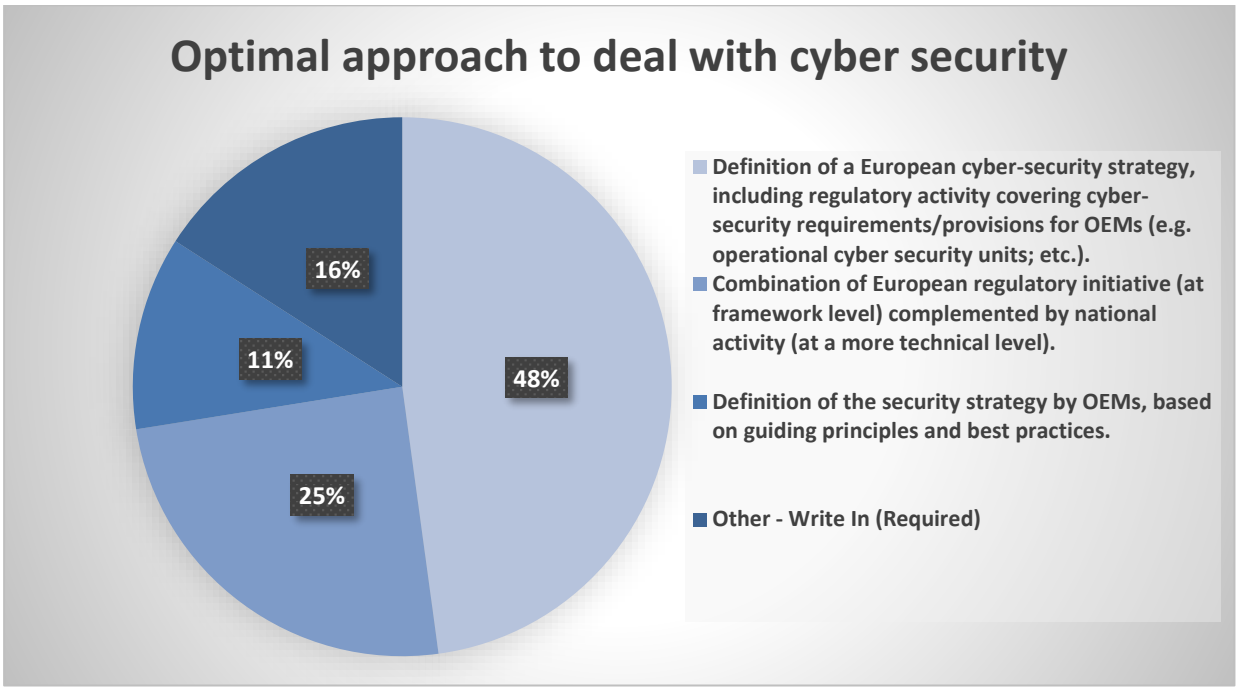
On the same topic, OEMs warn against standardization which may potentially disincentivize manufacturers and opt for some limited standardized requirements (e.g. security by design in development phase) and best practice sharing platforms.

In contrast the aftermarket advocates one or more standardized solutions, publicly certified systems with a possibility for independent certification once again stressing the importance of "a common language" i.e. interoperability.

When asked about how cyber-security should be managed, a majority of the stakeholders believe that complete public cyber-security regulatory framework is needed, with the remaining expressing their support toward a solution in which cybersecurity will be ensured by design and where OEMs will have the freedom of choosing different solutions and define their own cyber-security processes and strategies.

In particular, Almost 50% of the stakeholders welcome the definition of a European cyber-security strategy, including regulatory activity covering cyber-security requirements/provisions for OEMs (e.g. operational cyber security units; etc.). 25% support the combination of European regulatory initiative (at framework level) complemented by national activity (at a more technical level) and only 11% are for a definition of the security strategy by OEMs, based on guiding principles and best practices. Under "other", respondents shared that a minimum level of security should be ensured by legislation. However, the regulatory framework should not be an element of delay for the deployment of CCAM. Some stakeholders also believe that any effective approach to cybersecurity in CCAM should have (at least) a European dimension. The relation between EU and national domains is difficult to pre-specify but agreement and collaboration is necessary to avoid inconsistencies.

One respondent noted that Cyber-security is a subject that needs to be addressed at the global level (UNECE) and over the entire life (cradle to grave) of the vehicle. Another one suggested the setting up of a "European AUTO-ISAC": this body would provide cyber security analysis and share cybersecurity risks with the automotive sector in order to raise stakeholders awareness and exchange on ways to strengthens cars cybersecurity. This body should liaise with other AUTO-ISAC in the world to create synergies.

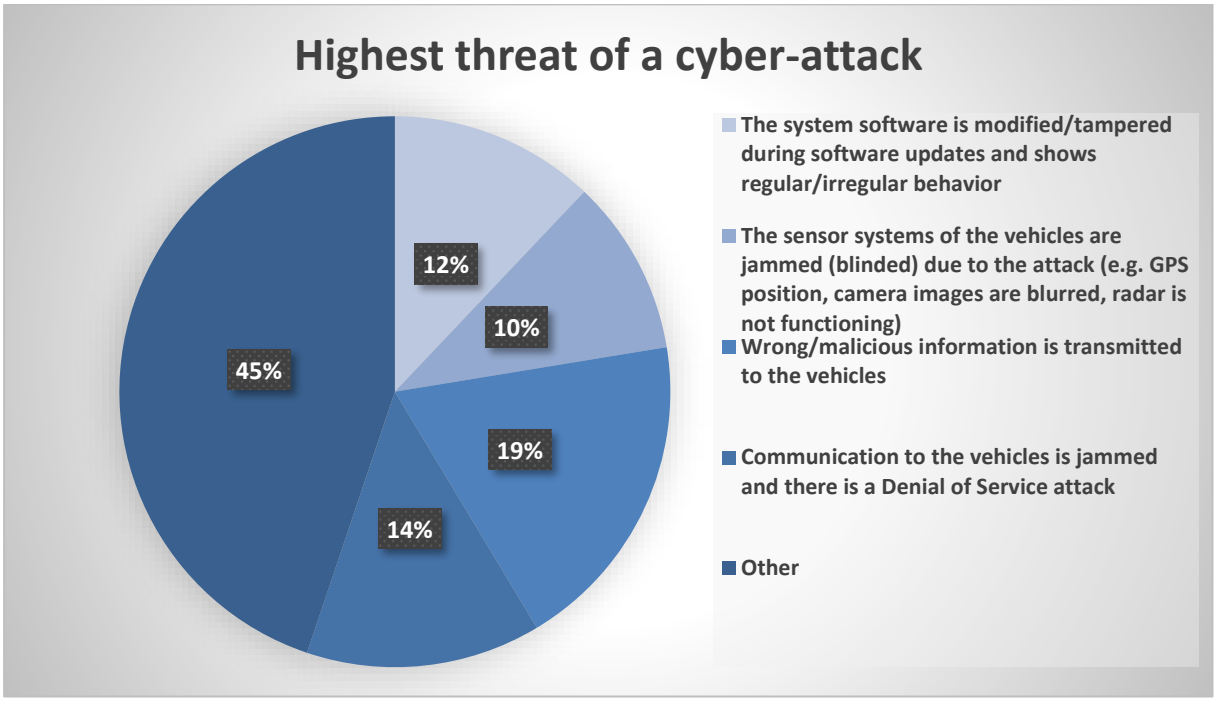


On the one hand, stakeholders agreed on a common position concerning the fact that OEMs should not be the only ones defining the security by design and this process should be shared across the value chain. Furthermore, ISO 21434 was indicated as the most adequate reference standard on which OEMs should base their security management.

When asked about the risks related to cybersecurity, the impact on safety and mass manipulation of vehicles leading to traffic security and safety of passengers was indicated as a major source of risk, together with privacy related stolen data.

In particular, All the threats listed as potential options (see below) are equally high for most of the stakeholder. This statement was shared by several respondents under "others" since the survey does not provide a choice of "all of them". In addition, other treats are identified to be the combined SAE/ISO standardisation and Autoisac[85]. A reference was provided to the list of threads developed by UNECE cybersecurity Working Group.

[85] (https://www.iso.org/standard/70918.html and https://www.automotiveisac.com/)



7.6. Impact of the issue and possible solutions on business models

In the case OEMs and the overall automotive sector will prove to be capable to design secure in-vehicle system capable of protecting data and functionality from unauthorised access, it will positively impact the perception of automated vehicles among the customers, with a positive impact on the uptake. (It is however unavoidable that security breaches will occur.) On the contrary, if OEMs will prove not to be capable to design secure in-vehicle system capable of protecting data and functionality from unauthorised access. Public opinion and customers to opt for normal vehicles or with limited automated functions. Uptake of advanced level of automation (above SAE level 3) to be heavily affected.

Furthermore, it can be expected that OEMs will move from their traditional role of hardware providers to all around vehicle system provider, expanding their role across the value chain including service providers players as security software companies. Partnerships and specific collaborations can be expected in this field.

In terms of cybersecurity at system level, defined as the full protection from unauthorised access to data stored on servers and other infrastructures, OEMs, telecommunication companies and service providers will need to prove to be capable to design secure in-vehicle system capable of protecting data and functionality from unauthorised access. This will positively impact the perception of automated vehicles among the customers, with a positive impact on the uptake. On the contrary, if OEMs, telecommunication companies and service providers will prove not to be capable to design secure in-vehicle system capable of protecting data and functionality from unauthorised access, public opinion and customers will opt for normal vehicles or with limited automated functions, with the consequence that uptake of advanced level of automation (above SAE level 3) to be heavily affected.

7.7. Conclusions and recommendations

Based on the different inputs and analysis conducted under this project, the following recommendations have been developed. In particular, the conclusions of this report support and welcome the latest decision of the Commission of publishing a Recommendation by the end of 2018 to tackle the issues of cybersecurity, access to data and connectivity, as declared in a recent public event by Ms. Spanou. In particular, Institutional bodies as ENISA should, based on the finalized UNECE WP.29 guidelines on cybersecurity, develop an implementation plan for an EU-wide certification scheme. (cf. EU Cybersecurity Act).

Furthermore, initiative as the European Cybersecurity Research and Competence Centre, aimed at supporting the development of respective tools and technologies necessary to ensure a continuous monitoring and evaluation of cyber-threats, should continue and the opportunity to expand their scope should be evaluated.

Finally, major efforts should be put at European and national level to increase citizens awareness concerning cybersecurity threats and risks.

In addition to that, the present report, based on the analysis and the feedback received during the stakeholders consultation, conclude that specific guidelines on technical aspects related to cybersecurity should we followed in the development of future automated vehicles. These recommendations, in line with the ENISA cybersecurity guidance, foresee:

- Safe storage and controlled access to security events logs, to ensure protection of customers' data and privacy.
- use of cryptography experts and independent audit bodies, to increase the level of complexity of security measures while preserving a minimum recognised standard.
- definition of access control mechanisms, to ensure a hierarchy of actors and reduce the risk of unauthorised access to in-vehicle and customers' data.
- use mutual authentication for remote communication, to reduce the risk of cyber-attack.

8. ACCESS TO DATA

8.1. Issue definition

The data generated by the automated cars is, and will increasingly be, a key source of value. Automated cars will generate a significant amount of data, which will then be stored, analysed, shared and most importantly monetised through a range of different services targeting end users, industry players and other sectors. Services leveraging on data generated by the vehicles could be offered in principle by all kind of stakeholders (suppliers, R&D, automakers, national authorities, local traffic controllers, aftermarket services), provided that they have access to the data.

In this frame, OEMs and partially suppliers have *de facto* control over most of the data generated by the vehicles. These players have different strategies. Most of the OEMs plan to or are exchanging the data generated by the vehicles with aftermarket services through a subscription business model[86]; Others, such as Tesla[87] prefer not to share the data generated by their vehicles and use it only for their purpose of updating the car performance.

From the policy standpoint, the key challenge is maximising the socio-economic benefits that can be generated by the access and use of vehicle data. The access to in-vehicle data will represent a vital element to ensure the provision of new services by many categories of current and potential service providers. OEMs, as the providers of the in-vehicle data architectures, do enjoy a preferential access to in-vehicle data, and on the ground of commercial and business opportunities, it is not in their best interest to make access to these data fully available to third parties.

In the frame of this issue, there are several other challenges that need to be addressed:

- **Cybersecurity:** Ensure that solutions for access to data are capable to ensure protection from intentional threats (almost the totality of the participants to the survey agreed on this point);
- **Need to allow fair data access to third parties.** 80% of respondents to our survey consider as relevant or extremely relevant the fair data access to third parties (i.e. access to in-vehicle data for commercial purposes). The study links some stakeholders' requirements towards data access (such a data being free of charge, as well as complete, real time, and secure) to the conditions under which data should be shared and managed. These conditions can be used to determine the possible solutions for data sharing and create a consensus around the main aspects. As mentioned above, security was quoted as the main concern with regard to the conditions for data access (90% of respondents). Furthermore, access to real-time data is as important as having access to complete datasets.
- **Data categorisation.** The categorisation of data will serve the market by enabling an overall understanding of the data itself, but the definition and categorisation of data does not need to be supported by a specific regulation. Different types of data can be distinguished, such as data generated by individuals as opposed to data generated by a machine. However, in practice, this distinction could be difficult. In

[86] https://www.acea.be/publications/article/position-paper-access-to-vehicle-data-for-third-party-services
[87] Stakeholder consultation

the current situation, data can be divided according to different categories, e.g. (from the perspective of OEMs)[88]:

m. Data triggered by the vehicle. Non-differentiating vehicle data (e.g. ambient temperature, traffic flows, road sign recognition, street parking) for services available across OEMs.

n. Vehicle-specific technical data (e.g. ECU monitoring, chassis sensor data) for OEM-specific services & component analysis/product improvement.

o. Data triggered by driver (e.g. vehicle position, speed, insurance, fleet, roadside assistance, diagnostic) for B2B and personalised services.

Defining the categorisation of data, was deemed as a reasonable starting point to be in the condition of taking decision on the access (possibly changing the situation depicted above), as agreed by almost all the stakeholders.

In summary, access to these data is a very controversial topic. Throughout the study it was shown that data access is one of the most difficult issues to solve in with regard to CCAM, due to the very different positions among the various stakeholders, which have raised a range of arguments.

8.2. Key market and industry trends

2.8.1. Current market situation and challenges

Vehicle data such as speed, position, engine and vehicle technical status, and many other parameters are already extensively collected and analysed by the OEMs. For example, GM has developed Onstar, a data analytics tool, collecting data in order to improve vehicle infrastructure. GM also partners with Apple and Google to introduce their infotainment interfaces to its cars. Another example is BMW CarData, enabling customised service options based on data from the vehicle[89]. With the upgrading of level automation, the data generation will increase heavily. **As data recording capabilities improve, connected cars are producing up to 25GB of data every hour[90].** Currently OEMs prefer to manage these data autonomously and/or to sell a subset of to third parties (in the form of either fees or free subscription).

Sensors on board of future vehicles will record an even more extensive amount of data. **These data will represent a vital element to ensure the provision of traditional services, such as repair and maintenance, and new services, including new mobility services.**

---

[88] http://www.cedr.eu/download/other_public_files/events/2018_open_data_workshop/2.0-20180417-CEDR-workshop-Open-Data-ACEA-presentation-Joost-Vantomme.pdf

[89] https://www.press.bmwgroup.com/global/article/detail/T0271366EN/bmw-group-launches-bmw-cardata:-new-and-innovative-services-for-customers-safely-and-transparently?language=en

[90] https://qz.com/344466/connected-cars-will-send-25-gigabytes-of-data-to-the-cloud-every-hour/

Under normal market conditions OEMs (and partially tier 1 suppliers), as providers of the in-vehicle data architectures, will enjoy a preferential access to in-vehicle data: if the business and/or regulatory stakeholders do not alter this trend, OEMs will likely be able to limit direct third-party access to such data. Subsets of these data could be accessed through solutions such as extended servers, where data sets will be available via a paid subscription.

As already mentioned, data is a major economic driver of future economy, impacting the definition, and the role, of current and future players of the automotive industry. Possibility of **access to data** collected from the connected and automated vehicle in a safe, and unfiltered way **is an enabler for new profit to all the actors active in the sector** as well as potentially enable new data-based service ecosystem (in the downstream automotive value chain). Depending on how data access will be available (to different players across the value chain), **actors of the automotive supply chain will exploit different profit pools** (derived e.g. from data connectivity services e.g. apps, navigation, entertainment, remote services and software updates). Possible options to data access are expected to impact both the size and distribution of revenues across the value chain.

2.8.1. Data access solutions

Overall there are three general possible solutions: the current in-vehicle interface, the onboard direct in-vehicle access or the off-board vehicle access through an extended server. The last solution offers different variations between privately owned by car manufacturer, neutral or managed via third party or public/non-profit body. The list below explains these solutions more into detail:

- **In-vehicle interface**: **This solution is the current OBD interface.** This interface allows connection to devices outside the vehicle. The OBD interface allows access to a standardized set of data such as emissions, fault codes etc Independent and authorized repairers and workshops use the current interface using an OBD connector.
- **Direct in-vehicle access** (in the on-board application platform and in-vehicle interface): This platform creates opportunity for all stakeholders to access data from the vehicle itself and to create a wide range of applications.
- **Off-board (server based) vehicle access**:
    p. ***Access to data through privately owned extended server*** (ISO standard (20077-1))***:*** The extended vehicle is a concept developed by OEMs where data generated by vehicle is sent over a secure and encrypted communication channel to a dedicated OEM server. Data made available at the OEM back-end server using a standardized interface will standardise sets of data that can be used by vehicle manufacturers or third-party participants for post processing and development of applications for vehicle users. An example of such solution is the **BMWCarData**[91].
    q. ***Access to Data Server-Shared Server:*** The shared server is neither financed nor operated by an OEM. The OEM plays a role of a system administrator for the transfer of data between the vehicle and the shared server. Data available at the standardized interfaces should be of the same quality as the data of OEM back-end.

[91] https://www.press.bmwgroup.com/global/article/detail/T0271366EN/bmw-group-launches-bmw-cardata:-new-and-innovative-services-for-customers-safely-and-transparently?language=en

r. ***Access to data Server-B2B Marketplace****:* B2B marketplace technical solution is again similar to the other data server solutions, but the 'marketplace' allows an independent third party to service and operate access to the vehicle manufacturer server.

s. ***Extended vehicle/ Neutral Server*****:** Extended Vehicle solution with the addition of a 'neutral server'. The neutral server operator can negotiate with the vehicle manufacturers for additional data fields to be included on their servers without revealing by whom and how this data will be used. As an example, VdTÜV proposes a concept called the **"Automotive Platform"** supporting data access and security standard for connected cars. The platform connects the cars with external services. It is a neutral server with secure, impartial and data protection-compliant cloud-based solution. In accordance with the principles of "Compliance by Design" and data neutrality, the TrustCenter creates technical precautions to prevent competition barriers via a coordinated web-based application for auto manufacturers and third parties. The consumer is able to control privacy and choose between services.

8.3. State of the art – legislative frameworks

In Europe, the data management for CCAM should take into consideration the principles from the Communication on Building a European Data Economy and the guiding principles set by European regulators. Data management should cover aspects such as data provision, fair data competition, privacy and protection. According to the GEAR 2030 report, access to data from vehicles will change the way services are provided to customers. Bearing in mind GDPR, access to data will enable all actors of the value chain to develop new services and business models and to create additional value for users.

Each of the three options offered by the WG6 of the C-ITS platform (using Data Server Platform, In-vehicle Interface, or On-board Application Platform) is likely to give rise to a range of "legal obstacles that will need to be navigated by market participants and there is a risk that the current legal framework may allow the market to develop in a way that is inconsistent with the five guiding principles agreed by WG6 and with relevant European legislation in general (e.g. competition legislation)[92]."

3.8.1. EU framework

There is no legal element that regulates how the access to vehicle data should be managed. However, there are relevant legislation which plays a role in the topic of CCAM data access:

- **The new General Data Protection Regulation (GDPR) is an enabler for CCAM.** An important issue with regard to CCAM is that there is a risk of breaches regarding customer privacy. This risk was managed by the European GDPR regulation, reinforcing **data responsibility** and engaging organisations to be stricter with and protective of the private data of their customers. Data protection authorities have also started to develop guidelines on how the data protection legislation (GDPR and national rules) is applicable in the framework of connected cars. All in all, **car manufacturer will no longer have to ensure compliance**

[92] TRL Report data sharing and connected vehicles

with 28 different national data protection laws. The GDPR does not solve the issue of data access but it provides a framework for customer privacy and protection of personal. Customers would expect to have a rich choice of services, share data and feel secure in the same time.

- EU **ePrivacy Regulation**[93] extends confidentiality rules for traditional telecommunications players to internet-based services. A connected car being an IoT use case, this regulation will also apply. The aim of the draft regulation is to break down data localization restrictions and help free data flow across EU borders.
- **Regulation (EC) No 715/2007 Article 6** provides access to vehicle repair and maintenance information. It states that "manufacturers shall provide unrestricted and standardised access to vehicle repair and maintenance information to independent operators through websites using a standardised format in a readily accessible and prompt manner, and in a manner, which is non-discriminatory compared to the provision given or access granted to authorised dealers and repairers." Manufacturers may charge reasonable and proportionate fees for access to vehicle repair and maintenance information covered by this Regulation".

3.8.1. National frameworks

An overview for a selection of Member States is reported below.

France: In relation to data access and connected vehicles, a recent report was published by CNIL – the French Data Protection Authority – on access to data and connected vehicles[94]. The authority looked into three use cases of connected cars and based on these developed a compliance package describing the rules on processing of personal data collected via vehicle sensors, telematics boxes, or mobile applications. The compliance package provides an overview of the French Data Protection Legislation and the GDPR and outlines a list of questions that should be asked prior to the processing of personal data.

Germany: Data management recommendations have also been researched and published, with the recommendations pointing to the importance of data minimization and transparency, developing products following privacy-by-design and default principles, reliable online communication component providing protection against attacks[95].

8.4. Policy initiatives and strategic orientations

4.8.1. International and European level

At international level, no action has been taken, at the best of authors' knowledge, on the issue of access to in-vehicle data. One of the potential explanation for this can be found in the high degree of heterogeneity that characterises the data and privacy legislative framework among single States.

---

93 https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

94 CNIL(2017), Connected Vehicles and personal data: Compliance Package, October 2017 Edition

95 Alex van der Wolk, Philip Radlanski, and Jens Wollesen (July 2017), "Germany's Federal Commissioner for Data Protection Issues Recommendations for Self-Driving Cars; MoFo Privacy Minute", available at https://www.mofo.com/resources/publications/170720-germany-data-protection-self-driving-cars.html and "Datenschutzrechtliche Empfehlungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum automatisierten und vernetzten Fahren"

The European Commission will continue monitoring the situation on access to in-vehicle data and resources and will consider further options for an enabling framework for vehicle data sharing to enable fair competition in the provision of services in the digital single market, while ensuring compliance with the legislation on the protection of data.

The European Parliament, in its "Draft Report on a European strategy on Cooperative Intelligent Transport Systems", urged the European Commission to take legislative action on access to in-vehicle data and resources before the end of 2018. Nevertheless, the Commission has clarified that it does not intend to provide, at least for the year 2018[96], any mandatory requirement for car makers on the issue of access to in-vehicle data. The Commission postponed the discussion on 2019, when it plans to issue a governance framework setting out its recommendations for data sharing, following further discussions.

4.8.1. National/regional level

As clarified in the section 8.3.2, France and Germany are the Member states, that undertook initiatives on data access.

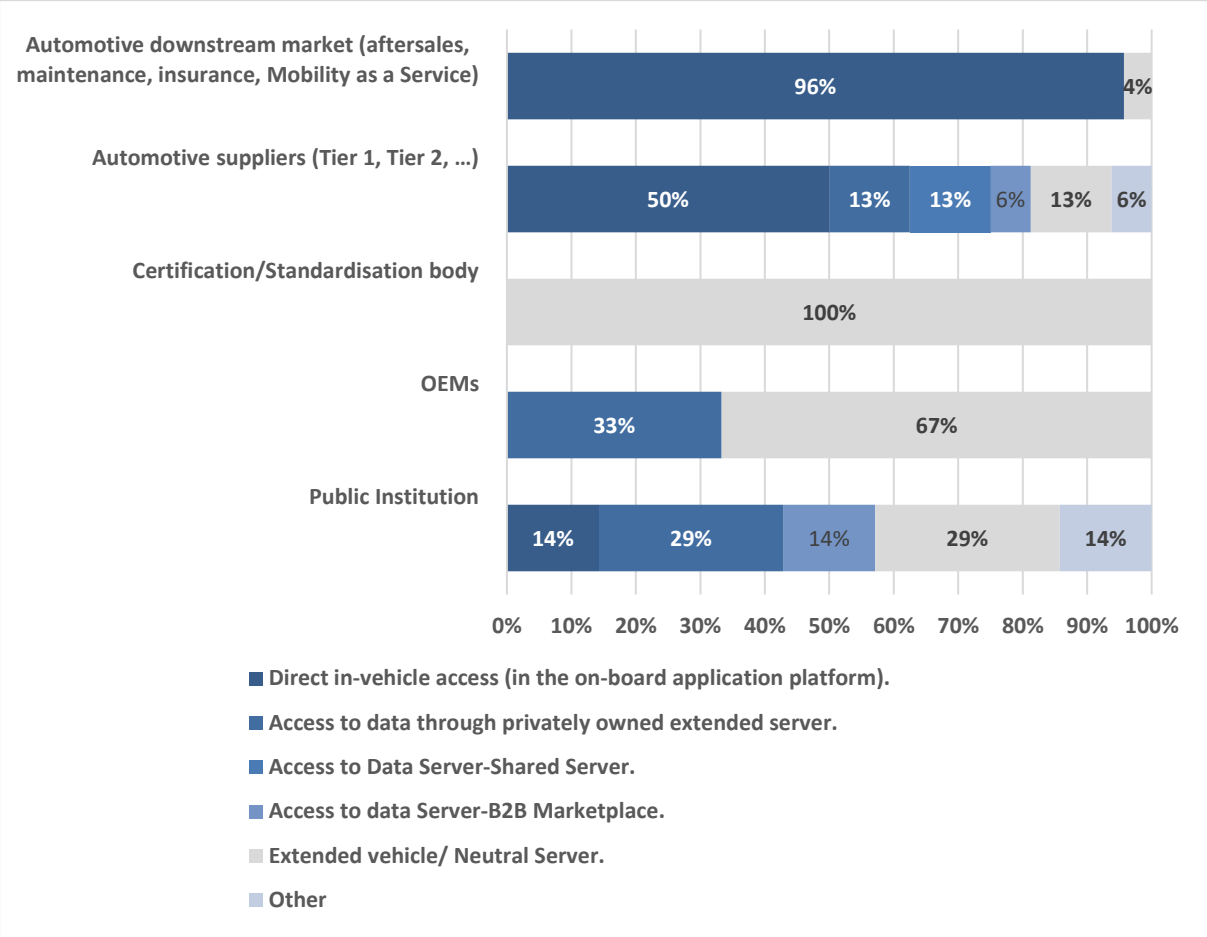
8.5. Mapping of stakeholders' views

The positions on access to data are very different across stakeholders. The surveyconducted in the study showed that direct in-vehicle access in the on-board application platform is overall the preferred solution with 59.3% of the votes – however this outcome is influenced by the higher number of participants representing the downstream sectors as compared to to the number of participants representing OEMs. The rest of the responses are split between the different options that exists for access to data through an extended server. This server could be neutral (18,6% consider this solution as the best one), it could be private (11,9% consider this solution as the optimal one), it could be shared or represent a B2B Market place (equally 5.1% each). Most stakeholders are sceptical about the existence of a solution, which is able to address the two concerns: the monopolization of data by manufacturers on the one hand (to the detriment of the aftermarket) and the vehicles potentially compromised (cyber-)security. While some stakeholders see the neutral server solution as promising, others question the possibility of real neutrality of a for-profit entity.

The received answers reflect a very strong polarisation according to the stakeholder categories, as evident from the figure below.

[96] POLITICO, "Commission shuts down push for law on connected car data", July 2018

Figure 8 Survey results: preferred access to data solution according to stakeholder type



Since there is a strong division and polarisation between the stakeholders'view, it is important to separate their views and present them separetly.

8.5.1.1 Automotive Suppliers' view

Automotive supplier's views are fragmented. On the one hand, associations such as CLEPA supports an *interoperable standardized and secure in-vehicle open telematics Platform*[97]. On the other hand, associations such as the VDA (German Association of the Automotive Industry) believes that the B2B OEM interface is a good intermediate solution and that there is no direct access to the vehicle by third parties to avoid risks to customer and public safety[98].

8.5.1.2 OEMs' view

Some of the OEMs provide a subscription-based platform that allows third party to use the data generated by the vehicle. The OEMs are against in-vehicle data access and their justification is the vehicle integrity and security. In response to the issues and need highlighted by stakeholders, OEMs propose intermediate solutions under the justification

[97] https://clepa.eu/wp-content/uploads/2015/08/20150722_CLEPA_PP_Open_Telematics_Platform.pdf
[98] https://www.vda.de/en/topics/innovation-and-technology/network/access-to-the-vehicle.html

that unrestricted direct in-vehicle data access could increase the likelihood of security issues. Such solutions include neutral players, from whom data could be retrieved.

Instead of direct third-party in-vehicle access to data, vehicle manufacturers prefer to communicate the relevant vehicle data in a secure manner to an off-board facility from where third parties can access it. To promote competition, service providers should have the choice between accessing data directly through the vehicle manufacturer's server or via 'neutral' servers that would gather the data from the servers of vehicle manufacturers[99].

8.5.1.3 Aftermarket, 3rd parties views:

According to the aftermarket players, access to in-vehicle data and resources can be granted through a secured, open and standardized technical solution. There are aftermarket services which demand full, unrestricted, real-time access to in-vehicle data, to generate new business opportunities.

According to aftermarket and more precisely FIGIEFA, the OEMs solution of extended server prevents equal access by independent operators and service providers and limits their ability to innovate and compete online on an equal basis[100].

CECRA association believes that there is a need of a framework granting standardised and direct unrestricted access to vehicle generated data for all market players[101]

Aftermarket service providers such as insurance companies, support the idea of legislative action on access to in-vehicle data and resources, enabling service providers to offer their products to drivers inside the vehicle, free from any interference by vehicle manufacturers[102]. They insist that EU policymakers must take legislative action to ensure that any technological solution to access in-vehicle data lets drivers decide with whom they share their data[103].

8.5.1.4 Users 'view

End users represented by BEUC, believe that third parties should have access to data to develop new products and services for the customer. They expect this access to follow a regulated approach with trusted third parties. They expect the "Commission to ensure neutrality by design for telematics platforms by mandating an open and secured approach allowing consumers to freely choose safe applications."[104]. Legal certainty is also needed, to ensure that the customer is in the centre of the agreed solution and all his rights are preserved[105].

8.6. Impact of the issue and possible solutions on business models

There are several possible scenarios related to data-related services their pricing, as mentioned in Section 8.2.2 and as outlined in one of the presentations discussed in the stakeholder workshop[106]. **The different approaches have significant impacts on the**

---

[99] https://www.acea.be/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf
[100] https://www.figiefa.eu/wp-content/uploads/Free-Flow-of-Data-FIGIEFA-Input-2016_12_23.pdf
[101] http://www.cecra.eu/statements/2016CECRAPPconnectivity03102016.pdf
[102] https://www.insuranceeurope.eu/european-parliament-approach-access-vehicle-data-welcomed
[103] https://www.insuranceeurope.eu/data4drivers-eu-rules-needed-give-drivers-control-their-vehicle-data
[104] https://www.fiaregion1.com/policy-position-on-car-connectivity/,
[105] http://www.beuc.eu/publications/beuc-x-2017-138_dve_beuc_connected_autonomous_cars.pdf
[106] by Mr. Bertin Martens, Senior Economist, Joint Research Centre of the European Commission during the Workshop on "Legal, economic, and business issues related to Cooperative, Connected and Automated Mobility (CCAM)" June 2018

business of downstream service providers. Examples of the impact of the issue by type of stakeholders are presented in the table below:

Table 4 Impact of the data access issue by type of stakeholders

Impact on data access by stakeholders category
Impact on data access for OEMs In the scenario of off-board access managed by OEMs, OEMs will be able to instaure "access price" which will give them the opportunity to create new profit by selling vehicle data. In addition, they could develop new services to offer directly to their customers rather than outsourcing such services or create strong partnerships with specific third parties. If the off-board access is managed by a neutral party, namely a data service provider entity, the OEMs will see their liability up to risk, which could have an impact on the uptake of CCAM. An alternative scenario could be generated by the entry into force of regulatory measures on data sharing that could eventually oblige OEMs to give full access to interested parties to vehicles' data. In such scenario, OEMs would enter in direct competition with data-based service providers. Again, this could impact the wiligness of OEMs to innovate and create new vehicle models.
Maintenance and Diagnostics Maintenance and Diagnostics is a Vehicle service with high evolution potential. In the future, maintenance will change by being mostly preventive and predictive maintenance. Most of the maintenance will be performed remotely (e.g. updates of the software). CAD enables the access to information provided by wide range of sensors and network data that provides a detailed picture of the car, which is then analysed and offers them the possibility to interact smoothly with humans or call for maintenance in advance. If data access is not available or limited, remote updates and data diagnostic of the cars will possibly be covered by the OEMs rather than the independent maintenance auto services. Regulations making the OEMs responsible for product functioning, creating incentives for car manufacturer to provide by themselves the maintenance and diagnostic service. This will represent an opportunity for OEMs to increase end user loyalty and keep the end user close to them even after the warranty provided. Finally, looking to users/drivers, access to the data generated by the vehicle could increase transparency regarding the necessary repairs activity and allow them to calibrate preventive maintenance and avoid more expensive repairs.
Insurance Digital diagnostic ports, have resulted in the availability of significant amount of data, covering various aspects of a car's health such as mileage, oil temperature, tire pressure and the driver's behaviour and handling of the car. These data, combined with GNSS and accelerometer data from black boxes and/or agreements with OEMs, not only helps insurers offer accurate and personalized insurance to consumers but has also resulted in new business models such as usage-based insurance (UBI). "*Pays as you drive"* and "*Pay when you drive"* are two recent approaches in the insurance sector, regarding connected cars, enabling better risk assessment and the provision of optimised insurance policies. Further business opportunities will depend on the data type and access. This is why, as mentioned above, several vendors already partnered with OEMs to enable UBI as an embedded service (e.g. Progressive with GM, State Farm with Ford and Allianz with BMW)[107] .
Infotainment services Infotainment services are a large market within CCAM. They services include advanced navigation, entertainment services and Comfort Services. Europe was the second biggest region in 2016 with a revenue of US$336.3m and 4.6 million from service subscriptions. The largest segment in infotainment services is Advanced Navigation with 2.6 million subscriptions and a revenue of US$200.0m[108]. Focusing as navigation as core application, advanced navigation is enabled by real-time data, which can increase the quality of the navigation and can potentially offer new services. As vehicles will increasingly collect data on the roads, this will improve the accuracy and informative power of the maps and improve in turn the navigation itself. Access to data will therefore have an impact on the provision of infotainment services and their quality.

During the study and within the validation workshop, the topic of **pricing** of data was discussed. Said that most stakeholders agree that free access to data is unrealistic, the topic of price discrimination by users was discussed. On the one hand some stakeholders suggested that a fully non-discriminatory access in economic view is not necessarily the

[107] http://telematicswire.net/automated-cars-driving-the-market-for-new-insurance-services-in-ubi/#UIDXaeL4E1b1OhpS.99
[108] *Statista Report "Connected car Outlook", 2018*

optimal one, suggesting that pricing and access conditions can be designed in such a way as to enable flexible business models built around experimentation and differentiation on quality. Other stakeholders suggested that price discrimination is contrary to the principle of fair access to data and suggested, as counter-argument to the push that price discrimination can have on fostering innovation through differentiation on quality, that in the navigation sector, often the most performant service is the one provided to end users for free.

8.7. Conclusions and recommendations

It is an evidence that future vehicles will allow the generation and collection of an extensive mass of data, therefore the management as well as the access and control of it will need to be clarified, since:

- As of today, **there is no a consolidated approach on data access**.
- The options and choices on access to data have a **significant impact** on the **distribution of profit pools** by players and on the **overall magnitude of potential socio-economic benefits**.

In a debate with completely different positions backed up by specific technical, political and economic arguments, it will probably take more time to let the technology and the market evolve before all the necessary elements for establishing clear rules and regulation. In this frame, it is essential to monitor the situation from a very close angle. Based on the different inputs and analysis conducted under this project, the following recommendations have been developed:

a) **European authorities should work to establish clear, full, transparent data-sets categorisation.** It is of prior importance to create a categorisation of all the data generated by the connected cooperative and automated mobility. There are already some initiatives in place to categorise data, but the effort should continue. The definition and categorisation of data will improve transparency and make it easier to take decisions. Also, it will create a framework in which it will be possible to take different decisions and consensus initiative depending on the type of data.

b) **Within the Recommendation planned to be issued at the end of 2018, stress the importance of ensuring that data access solutions developed and made available by OEMs** enable the generation of innovative downstream services while guaranteeing a level playing field for players competing in their provision.

c) In a situation where downstream services explicitly advocate for higher access to data and OEMs stress that the solutions they propose will satisfy their need, the European Commission should continue **analysing the service market of vehicle data.** One or two years after the Recommendation is issued, the EC should monitor the evolution of the market regarding services generated by vehicle data, to understand to what extent:
    a. OEMs have been able to enter into and compete in downstream service markets;
    b. The access to data has enabled downstream players to generate new services;

    Should the monitoring activity identify that downstream competition is impacted by asymmetric data access and that development of new data-based services is limited, a regulatory approach on data access should be pursued.

9. ROAD INFRASTRUCTURE EVOLUTION

9.1. Issue definition

The emergence of automated driving will eventually require public Institutions and national bodies to upgrade the current road network physical and communication infrastructure, so to provide a solid, fit-for-purpose road environment in which future vehicles will be capable of driving themselves autonomously, in a safe and efficient way, communicating and cooperating with each other. Furthermore, current commercial and legal practices may impede communication providers to access the physical infrastructure, *de facto* preventing the investments required to implement communication capabilities on already existing infrastructure.

9.2. Key market and industry trends

Future automated vehicles (AVs) will require two different type of infrastructure to fully operate at the highest level of autonomy: the physical road infrastructure, with clear and homogenous marking and signalling across different Member States, to ensure compatibility of different national road codes. The digital communication infrastructure, necessary to allow vehicles to communicate among themselves and road-side, with minimized delays and little interference with other actors.

In terms of physical infrastructure, signalling and marking across the road will represent a fundamental input for AVs. A multitude of sensors will help a vehicle to understand and move across the road having line marking and signalling to provide the primary sensor input. The sensor input will be compared with information deriving from HD maps and positioning sensors. Integral and well maintained marking across the roads will be a fundamental element to ensure full operability of AVs across the overall road infrastructure. In addition to this, road sign alignment, in terms of colours, size and symbols will be crucial to ensure AVs functionalities across different Member States.

The evolution of these two different types of infrastructure will be driven, in most of the cases, by different actors: while for physical road infrastructure the necessary updates will mostly be the result of a public policy and road operators' intervention, for the communication infrastructure different scenarios are possible.

Depending on which type of communication standard will prevail (Dedicated Short Range Communication, DSRC vs Cellular), different actors will be involved in the development and investment for the infrastructure: for the DSRC type road operators will be the main actors responsible for such deployment, while telecommunication companies will have a primary role in the deployment of cellular base infrastructure.

It will be of crucial importance that telecommunication providers obtain the right to access the physical infrastructure on which communication coverage should be provided. This is particularly relevant for situation in which network operators may legally impede, for commercial nature, to access the road infrastructure, *de facto* foreclosing the market to new telecommunication players.

Initiatives at European and National level

The European Union has identified in modern and connected infrastructure a driver for growth and development, as described in the European Commission "*On the road to automated mobility: An EU strategy for mobility of the future".*

In particular, through the Connecting European Facility, a fund of a total EUR 443 million triggering EUR 1.173 million of total investment, the European Commission aims at incentivising public/private partnerships with the goal of bringing new investments into current road infrastructure.

More than 40 European projects and European filed trials are today ongoing, including:

- The C-Roads platform, which aim is to is to develop harmonised specifications taking the EU-C-ITS platform recommendations into account, linking all C-ITS deployments and planning intensive cross-testing.
- The CONCORDA (Connected Corridor for Driving Automation) project, which objective is to contribute to the preparation of European motorways for automated driving and high density truck platooning. The main purporse of the project is to assess the performance of hybrid communication systems, combining 802.11p and LTE connectivity, under real traffic situations.
- L3Pilot, a large scale field testing focuses on large-scale piloting of SAE Level 3.

On a national perspective, different governments are currently investing in new road infrastructure, on in updating old ones with new technologies including communication capabilities. Notably France, in its document "Développement Des Véhicules Autonomes Orientations stratégiques pour l'action publique" stresses the role good and fit-for-purpose infrastructure will play in fostering the uptake of AVs.

9.3. Mapping of stakeholders' view

Across the study, stakeholders related to the automotive sector, as well as to the mobility services in general, have been contacted and interviewed through different stages of interaction. On the point of infrastructure evolution, stakeholders expressed a similar opinion in terms of necessity to increase public investment to:

a) improve current road condition, including signalling and road marking

b) foster public investment in connectivity features for new and old infrastructure, including developing *ad-hoc* partnership to foster public-private investments

c) monitor the commercial/legal conditions of access offered to communication services providers, in order to ensure a fair access to the road infrastructure.

9.4. Impact of the issue and possible solutions on business models

Public investments, private/public partnerships or privation of public infrastructure will bring the necessary investments to adapt road and communication infrastructure to future

automated vehicles. Partial/limited investments will be made on existing infrastructure to adapt them to automated vehicles.

New business opportunities will arise for players active in the communication sector: in particular, in case a standard based on cellular V2X communication will prevail, telecommunication companies will access a new important profit pool, adding vehicle-data communication to their business offer. On the contrary, in case a DSRC approach will be selected by the competent authorities, automotive industry players, including OEMs, could benefit from a new and relevant profit pool.

Furthermore, considered the heterogeneous situation in terms of public investment in Europe, a situation characterised by a differentiation between geographical areas of adequate and poor infrastructures may arise. This will inevitably fragment the market, with automated vehicles able to fully function only in areas with well equipped infrastructures. This might reduce the interest of consumers and could limit the uptake of CCAM in some areas. On the contrary, an EU-wide upgrade of road infrastructures will ensure a more solid uptake of all levels of CCAM.

Finally, many of the physical road infrastructures, especially among the ones of most recent construction, have integrated high-speed broadband cables for technical and non-commercial communication. To foster cellular coverage of these areas, mobile operators would need to "access" the road infrastructure to ensure that the necessary communcation network can be deployed at minimal cost to support connected and automated vehicles. Furthermore, a business case capable of putting together the interest of key stakeholders, including automotive industry, public authorities and consumers, as in terms of safety and quality of the infrastructures, as well as the interest of market investors will need to be developed.

9.5. Conclusions and recommendations

In terms of recommendations, the analysis conducted in the framework of this project, has concluded that:

b) Priority, in terms of policy action and public fund allocation, should be given to maintenance and refurbishment of signalling across EU roads, as well as to the alignment of signalling across the Member States. On this point, the stakeholders interviewed expressed positive feedback on the current directions projects as the ones financed thourgh the Connecting European Facility.

c) The Commission should recommend national institutions to investigate the opportunity to regulate how road network and road infrastructure operators grant access to third parties including telecommunication operators, so to ensure fair access to road infrastructure to these actors.

10. TECHNICAL CHALLENGES

10.1. Artificial intelligence

Artificial intelligence (AI) is expected to influence almost any kind of sector and industry, including the automotive industry. Technologies inside the automated car such as LIDAR, cameras, radars that collect scenario information are processed and used by the AI to take precise, immediate decisions. AI will find its application in scenario assessment and decision making, which both are safety related. As a consequence, the development of artificial intelligence technology, including both hardware capabilities and software programs, will represent an essential step in the development of highly automated vehicles. Finally, the use of AI will eventually raise ethical questions, as decisions involving life-threating situation will be taken by the vehicle and, not anymore, by the driver.

10.1.1 Key technical, market and industry trends

Artificial Intelligence for self-driving vehicles, depending on the level of automation, will go from improving driving experience, where the vehicle will anticipate drivers' needs and acts accordingly, to door-to-door transportation task for true L5 self-driving. While functionalities like line assist are already present in top-tier vehicles, full automated vehicle are not yet a reality, also due to the fact that the entire system is expected to be integrated and supervised by AI.

In the real world, AI is a critical component for two fundamental requirements: recognition of the world around the car and navigating safely in all traffic conditions.

AI for detection and recognition

The first step with AI technology in automobiles is detection and recognition. As with anything involving machine learning, the AI must be trained to put context and meaning behind detections in various scenarios the vehicle might encounter. This is commonly referred as the "recognition layer", a necessary precursor to decision-making.

While it is relatively easy to teach AI the difference between another vehicle, or pedestrian, or bicycle or building, there is much greater difficulty in training AI for the very real possibility of inclement weather, adverse driving conditions, unexpected obstacles or car accidents.

In addition to that, a significant challenge lies in the acquisition of quality, representative, diverse and well-labelled data, and since most of these situations happen randomly, it is nearly impossible to find real-world ways of exposing AI to the types of road scenarios that drivers encounter every day.

AI for driving functions

As sophisticated as AI training has become, the truly advanced part of using AI in autonomous driving will be in the motion. Far beyond simply helping the car to drive, motion includes using AI to manoeuvre and function in the real world and solve the dynamic driving task.

This represents a key challenge for autonomous driving: beyond the ability to simply see and recognize various traffic scenarios and issues on the road, in order to be truly automated vehicles will also need to immediately decide and react, much like a human would, or even with greater precision and enhanced agility.

Hardware issue

In the world of autonomous driving technology, the software solution is only one part of an issue. Besides the development of adequately complex algorithms, a key challenge is represented by the need of finding a way to incorporate the kind of hardware needed to run such massive computing applications while fitting in the form factor of a passenger car.

For driving solutions in particular, energy efficiency is a necessity, but there has traditionally been a trade-off between high performance and low power consumption. The current model has been focused on trying to solve operations for Neural Networks (NN) using Graphics Processing Unit (GPUs), although they have proved to be often under-performing, due to the unique nature of advanced NN operations.

Finally, a last issue concerns the non-compatibility of different software tools that are currently developed by the different OEMs and technology players, that calls for an industry standard, where an entire framework can be designed and built for any hardware supporting the standard.

10.1.1 Policy initiatives and strategic orientations

Artificial intelligence is at the core of European and national strategies to improve and boost European economies as well as increasing standard of life of European citizens.

In the recent Communication on Artificial Intelligence in Europe, published at the end of April 2018, the European Commission identifies such technology as a key enabler of automated driving vehicles, stressing the importance of public actions and coordination to support research and innovation across Europe, bringing AI to small business and potential users.

Furthermore, in a second document the European Commission has recently published, "Declaration of cooperation on Artificial Intelligence (AI)", Member States agreed to work together on the most important issues raised by Artificial Intelligence, from ensuring Europe's competitiveness in the research and deployment of AI, to dealing with social, economic, ethical and legal questions.

At national level, different Member States have identified the crucial role Artificial Intelligence will play with respect to automated driving, advocating for public action on the topic.

Furthermore, it is important to underline the activities that some Member States, as Germany, are currently supporting to address cross-related issues related to AI, as the question of ethics. For example, in June 2017, the Federal Minister of Transport and Digital Infrastructure has published a set of guidelines[109] focusing on level 4 and 5 VDA (=SEA) scale of automation.

[109] Available at https://www.bmvi.de/SharedDocs/EN/Documents/G/ethic-commission-report.pdf?__blob=publicationFile.

10.1.2 Mapping of stakeholders' views

Artificial intelligence was widely regarded by most of the stakeholders as one of the main technical and technological issues, mostly for the aspects that have been considered above. In addition to that, different stakeholders stressed the role ethics will play in future automated vehicles context.

10.1.3 Impact of the issue and possible solutions on business models

AI has a fundamental role in enabling the development of advanced level of autonomation, as above SAE level 3. Conversely, issues like social acceptance and legislation could heavily impact on the diffusion of AI in vehicle, endangering the development, and entry into the market, of highly automated vehicles.

If Artificial Intelligence development will not be halted by the issues presented above, it can be expected that a large investment in such technology will be made by all players of the value chain. In particular, it can be expected OEMs to start – and continue – investing AI related applications, potentially with the creation of new partnerships with non-traditional actors in the automotive sector.

The growing importance of AI in the future vehicles could create two different scenarios, with on side OEMs and high-tech suppliers to integrate AI capabilities and enlarge their role in the value chain, and on the other side new technology players with expertise in AI to become important actors in the automotive sector.

10.1.4 Conclusions and recommendations

Based on the analysis and the feedbacks received from the stakeholders across different interactions, the following recommendations are being developed:

- Endorse initiative to create a multi-stakeholder communication platform (cf. AI Alliance) to guarantee competitiveness and creation of ethical guidelines. (continuation of a social dialogue on automation)
- Continue coordination of research and investments at EU level, as the European Commission is currently working with Member States on developing a coordinated AI plan by end of 2018.
- Creation of a "a support centre for data sharing, which will be closely linked with the AI-on-demand platform to facilitate development of business and public-sector applications." (cf. Communication on Artificial Intelligence, actions beyond 2020).

10.2 Improvement of positioning technology

10.2.1 Issue definition

Automated cars require very stringent positioning performance. The first applications now being tested on the roads, albeit being technically simpler than future ones foreseeing a higher level of automation, require high performances in terms of positioning (and timing).

As automated cars will be mainly operated in urban environment, together with accuracy requirements also availability and robustness of positioning will become increasingly important, in particular because in urban environment, it is a real challenge to mitigate the limitations of globally avaliable positioning solutions (such as GNSS) in terms of availability. The following table provides a high-level summary of the user requirements regarding positioning.

Table 5 Automated driving: user requirements relevant for positioning

User requirement	Level
Availability	> 99.9%
Horizontal accuracy (95%)	Decimetre level
Time to convergence	Seconds
Robustness of the positioning information	High
Continuity	High
Position fix rate	over 10Hz

At the present stage, the achievement of a positioning solution combining the required level of performance with the cost-effectiveness requirements of the automotive market is still a challenge.

The relevance of the issue derives from the fact that no single positioning and/or perception/navigation technology meets all the requirements of automated driving. To overcome the shortcomings of individual positioning technologies, **sensor** and **data fusion** are considered by OEMs and suppliers as the go-to-solution for the development of fully automated driving technology. In this frame:

- GNSS is foreseen as an essential element to provide absolute positioning with global coverage;
- Once the vehicle is positioned on the road, a wide range of perception-based technologies, including LiDARs/Radars, Inertial sensors and cameras, will be used in a sensor fusion perspective to support navigation.

In this frame, the key challenge for the industry is to improve the performance of the single technologies while ensuring cost effectiveness, as well as advancing on sensor and data fusion and processing capabilities to feed then the decision to be taken by the artificial intelligence.

10.2.2 Key technical, market and industry trends

Looking strictly to positioning technology, automated driving represents a challenge for GNSS receivers, with positioning accuracy that needs to be improved to decimetre level, better continuity required in urban canyons, and requirements for better reliability and possibly authentication to prevent malicious attacks.

The industry, including both OEMs, Tier 1 suppliers and suppliers of positioning solutions has been recently very active on advancing in the field of positioning technology. A selection of recent developments is provided below:

- In the press release announcing the joint venture Sapcorda Services in 2017[110], the companies involved (Bosch, Geo++, Mitsubishi Electric and u-Blox), "*recognized that existing solutions for GNSS positioning services do not meet the needs of emerging high precision GNSS mass markets* […] *Sapcorda will offer globally available GNSS positioning services via internet and satellite broadcast and will enable accurate GNSS positioning at centimeter level. The services are designed to serve high volume automotive, industrial and consumer markets[111].*
- GNSS Receivers manufacturers are working to evolve their products from multi-constellation, single-frequency to a dual-frequency units (L1/E1 and L5/E5), triggering the birth of a new class of "dual-frequency, mass market" receivers.
- Major positioning service providers have been extending the scope of their high-accuracy correction services, targeting traditionally professional applications, so to address also automated driving applications[112].
- Tier one suppliers are competing, partnering and/or merging with technology companies, in order to provide platforms capable of meeting the requirements of automakers[113].

10.2.3 Policy initiatives and strategic orientations

The most relevant policy initiatives and commitments are identified at European level, with the commitment of further developing the Galileo services and related vehicle navigation technologies for driverless mobility[114].

In this frame, the European Commission, will by 2019 offer Galileo's initial high-accuracy services for free, being the first to be able to offer such navigation service on a worldwide base. Such decision, adopted on March 2018[115], specifically considers the requirements of automated driving as a driver for updating the service provision scheme and target performance of Commercial Services.

Furthermore, the European Commission is expected to prepare guidelines for the optimised use of advanced services, as high-accuracy, robustness and authentication of position, which will be offered by the Galileo system, and to provide guidance on their inclusion in vehicle navigation systems, to address liability and safety issues.

Positioning technology improvement In terms of positioning information technology, the European GNSS Agency is regularly monitoring the evolution of user requirements of automated vehicles related to positioning, in order to ensure a coherent development of EGNSS (European GNSS Systems) and to fill in existing gaps at the level of EU industry[116].

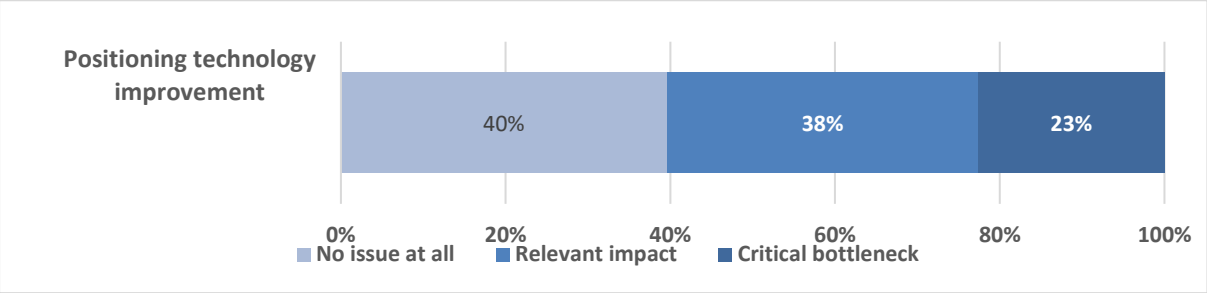
---

[110] https://www.u-blox.com/en/investor-news/bosch-geo-mitsubishi-electric-and-u-blox-establish-joint-venture-sapcorda-services
[111] https://www.bosch-presse.de/pressportal/de/en/bosch-geo-mitsubishi-electric-and-u-blox-to-establish-joint-venture-sapcorda-services-119616.html
[112] https://www.trimble.com/news/release.aspx?id=022218a
[113] https://automotive.electronicspecifier.com/driver-assistance-systems/the-arrival-of-self-driving-cars-with-sensor-fusion-and-processing
[114] As stated in the 3rd Mobility Package.
[115] Commission Implementing Decision (Eu) 2018/321 of 2 March 2018
[116] Automated driving is covered in the H2020 Programme, as example in the Topic *EGNSS applications fostering green, safe and smart mobility* under the EGNSS calls of the Space Programme. As additional selected example , the ESCAPE project, funded under the Fundamental Elements Programme, foresees Development of E-GNSS engine for safety-critical multi-applications in road transport call, aims at overcoming multiple challenges related

10.2.4 Mapping of stakeholders' views

The relevance of the issue is generally confirmed by the stakeholders answering our survey, with 61% of participants indicating that improvement of positioning technology represents either a challenge with relevant impact on the timeframe for the uptake of CCAM or a critical bottleneck.

Figure 9 Survey feedback on the relevance of positioning technology improvement as a challenge



Being the issue mainly technical, no significant disagreements have been identified among the different stakeholders.

10.2.5 Impact of the issue and possible solutions on business models

As mentioned above, automated vehicles require high accuracy, robust and trustable positioning information to allow a safe and reliable deployment. Highly accurate and reliable positioning information can be provided by high precision satellite information combined with sensors installed on the vehicle (and data obtained from V2X technologies) through sensor and data fusion approaches.

Investments and progress in the necessary technology will allow the future automated vehicles to receive high precision and reliable positioning information. At the present stage, the major challenge is not the definition of a solution meeting the technical requirements, but rather the combination of the required performance with the cost constraints that are of key importance in the automotive industry, in particular in the "volume" market segment of passenger cars.

The extent to which this objective will be achieved (and the timeframe required) will have an impact on the level of uptake of automated driving in the different market segment.

At the same time, the need of reliable and high precision positioning and navigation sensors and information represents a new profit pool for specialised technology companies, positioning service providers and other data services. This trend has been facilitating the entrance of various technology players in the automotive value chain.

10.2.6 Conclusions and recommendations

Based on the analysis performed, being this issue of technical nature it does not need any "direct" regulatory intervention.

---

to the use of GNSS technology in automotive safety-critical applications by developing a dedicated, reliable and. The project will last three years, until autumn 2019.

Policy and programme (concerning both the Galileo Programme and support to R&I through Horizon 2020 and Fundamenta Elements) actions are already ongoing to ensure that EU satellite systems are developed and evolve taking also into account the requirements of automated driving, based on a regular activities of consultation with industry players. Finally, the European Commission and the European GNSS Agency are also active to ensure that EGNSS is adopted in the positioning solutions developed by the industry.

In this frame, our recommendations are, as technology progressively achieves maturity, to closely monitor the ongoing activities on standardisation and certification (as example the. ongoing activities under the newly established Task Force on Automated Vehicles "TF AutoVeh" of WP.29). Potential actions to ensure the adoption of European GNSS include:

- Participating in international and European standardisation fora to ensure that specific differentiators of Europan systems and solutions (e.g. the unique authentication feature of Galileo) are properly considered in standards;
- Verifying the opportunity to consider positioning and GNSS related requirements and aspects in the ongoing process of update of certification and type approval covered by the Task Force "AutoVeh", which has been started to accommodate the specificities of automated driving.

10.3 Availability of HD maps

10.3.1 Issue definition

A high definition (HD) maps is what digital cartographers define as three-dimensional model of a vehicle's physical road infrastructure, with a target accuracy less than 10 cm. It represents an essential input for automated driving, and their development requires significant investments and continuous updates. Furthermore, to ensure automated driving across all environments, their coverage should be extended across all territory, and not only on densely populated areas, where usage – and profits deriving from it – would be higher. Finally, common technical formats are currently missing, with HD Maps database currently limited in terms of interoperability across automotive players.

10.3.2 Key technical, market and industry trends

Automated vehicles sensors, including the ones already installed in some top—tier vehicles with level 1 and level 2 automation functions, are capable of recognising road marking and signalling, so to be able to assist the driver in line assistance, emergency brake and other safety features.

Nevertheless, issues arise when road markings can wear away or disappear, for example under snow, or simply for bad/inadequate maintenance of road infrastructure. As it has been described in Section 9, this is a crucial aspect that needs to be addressed by road operators.

However, also in case of good road conditions, data deriving from road marking is associated, in case of higher level of automation, typically with data deriving from modern laser-surveying sensor systems as LIDARs, (Light Detection and Ranging).

LIDARS calculate distances by illuminating a target with laser light and measuring the time it takes for the light to bounce back to the source, in a similar manner to what radar equipment does with radio waves.

In the most recent AVs models, LIDARS and radars have an effective range up to 150-300 metres (depending on the configuration, typicall clusters of radars are used), but that can shrink significantly in heavy peticipation or when objects are obscured by vehicles ahead. As a matter of fact, also the most performant vehicle travelling at motorway speeds can "see" and understand the environment around itself only a very short periodahead.

For this reason, HD Maps are essential for the future development of AVs and their mass-market uptake as it provides information beyond the range of sensors. HD maps enable self-driving cars with two fundamental features:

- They provide the AV with the ability to anticipate turns and junctions far beyond sensors' horizons, increasing the overall safety, efficiency and comfort during the trip.
- They allow the car to position itself in complex environment within 10 cm accuracy, as the one represented by multi-lane road.

As stressed under Section 10.2, AVs will require improved positioning performances, capable of reaching cm level accuracy. HD maps, as they will include a so-called localisation layer, that through an analysis of different inputs deriving from a variety of sensors, will be capable of positioning the car within centimetres.

10.3.3 Policy initiatives and strategic orientations

The topic is currently being at the heart of different policies that and strategies that both the European Commission and national bodies are currently developing.

At European level, the topic of HD Maps is largely connected with the European Commission aim at improving Galileo services, positively impacting the integrity and reliability of digital maps.

At national level, different governments are encouraging public/private partnership to foster the development of HD Maps and road infrastructure. This is for example happening in Spain, where a recent document published by its Directorate General of Traffic, foresees a collaboration with Mobileye that will enable Spanish cities to become "Automation-ready" including through Mapping Data Generation, as well as in many other different countries.

10.3.4 Mapping of stakeholders' views

The issue of HD maps was investigated during the different round of interactions with automotive sector stakeholders as part of a wider category of issues involving technical/technological challenges.

Stakeholders largely agreed on the importance of issue, with almost 95% of the respondents of our survey evaluating the availability of HD maps either a challenge with relevant impact on the timeframe for the uptake of CCAM or a critical bottleneck. Stakeholders also stressed the need for further public/private collaboration to ensure all territory will be covered.

10.3.5 Impact of the issue and possible solutions on business models

The issue has an extremely important commercial aspect that, if not correctly addressed, may affect uptake of AVs across Europe.

As it has been underlined above, HD Mapping is an expensive activity, which involves important sunk costs – including the development of specific hardware and software environment – as well as high fixed costs, including constant updates and database maintenance. This explains why only few companies are currently active in this domain, with companies like HERE, TomTom, Google, ZF and Baidu being investing in this technology.

Furthermore, their use is mostly concentrated on those areas that are characterised by a high degree of population density: rural and low-density population areas do not represent an area of primary interest for private companies involved in the mapping business, as their profits, directly related to the number of users, will eventually be scarce.

For this reason, a situation in which portions of national/European are covered, mostly in correspondence with urban areas, and other portions are not, for example, rural and mountainous areas, is not unrealistic.

As it appears clear, this will have a fragmentation effect on the potential use of higher level of automation of future AVs, that may hinder the interest of consumers which could only benefit from complex automated functions in areas covered by HD maps.

10.3.6 Conclusions and recommendations

Given the commercial nature of the issue, the present report considers that only actions aimed at reducing the market failure represented by scarcely populated areas should be taken into consideration. In particular, the development of policies at European and National level should:

- Promote public/private partnerships to cover market failures as the one represented by scarcely populated/ rural areas.
- Help the coordination between international business players in order to develop a single format for HD maps, to increase the compatibility across different OEMs and potentially enable economies of scale.

10.4 Absence of a dominant standard for V2X communication

10.4.1 Issue definition

While a vehicle could implement automated features independently to its capability to communicate and cooperate with the external world, it is undisputable that connectivity will expand the potential of AVs, integrating them in a complex mobility ecosystem characterised by cooperative behaviour among vehicles and infrastructures.

Today, the market offers different technologies capable of offering connectivity and cooperative features, namely ITS-G5 and future cellular based 5G (although 5G is not available, testing has already started using the already available LTE-V2X). As the two technologies are currently non-compatible, an approach of "technology neutrality" could result counter-productive for the industry willing to invest in connected and automated vehicles and even represent a risk for the safety of consumers.

10.4.2 Key technical, market and industry trends

Among the many aspects that will characterise the future road mobility, a) cooperative safety, consisting of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) applications which exchange information, and b) automated vehicles, which utilize V2X

consisting of vehicle-to-vehicle, vehicle-to-infrastructure, vehicle-to-pedestrian (V2P), and vehicle-to-network applications (V2N) are expected to represent two milestones in terms of increased safety and efficiency.

In order to implement V2X features, vehicles will require communications networks that are capable of quickly (i.e. with minimal latency), securely and reliably exchanging information. As today, there is a debate on what form this will take, with two potentials main competitors: on one side, the early frontrunner represented by ITS G5, which operates in the 5GHz range, and is an adaptation of the widely-used IEEE 802.11 standard for Wi-Fi to incorporate Wireless Access in Vehicular Environments (WAVE). On the other side, the cellular based 5G, the fifth generation of mobile networks and evolution of 4G LTE.

More into details, the European C-ITS spectrum is subdivided into seven 10 MHz channels ranging from 5.855 to 5.925 GHz and is allocated in four sub-bands, depending on the kind of application and on the different requirements defined in ITS-G5. On the contrary, Low 5G frequency band in Europe are allocated at Member States level with low frequency band ranging from 3.4 to 3.8 GHz and high frequency band from 26.0 to 27.5 GHz.

The analysis of future spectrum allocation has been considered out of scope of the present report. Nevertheless, it should be kept in mind that spectrum allocation directly affect technology performances, and therefore the future decision on this matter will also have a role in determining which of the two standards will prevail.

The decisions will affect the two significant options in the V2X market; ITS-G5 (IEEE 802.11p-based Dedicated Short Range Communication, DSRC) is currently backed by important actors of the automotive and teleccomunication sector, including, among many, NXP, Denso, VW, Toyota, AutoTalks and Commsigmia, while the 5G variant (C-V2X) is supported by Qualcomm, Nokia. More generally, C-V2X technology supporters can be identified by those that are members of the 5G Automotive Association (5GAA), although no automakers have yet committed to a C-V2X deployment in their vehicles. Regarding ITS-G5 various pilot are executed on Truck Platooning with all main European truck OEM involved.

As it currently stands, these two V2X technologies are not interoperable, and even could interfere with each other within the available frequency band, an element of risk that would not benefit neither one of the two competitors.

In terms of market adoption, the IEEE standard technology has a competitive advantage related to timing, as a number of ITS-5G vehicle-to-infrastructure (V2I) pilots have already become active in Europe, involving ITS-G5 road-side systems that have been deployed over the last decade, mainly as a result of (EU-funded) research projects. On the other side, C-V2X test bed are being developed, as on Germany's A9 motorway.

The European Union committed to a deployment of 802.11p-based ITS-G5 infrastructure in 2016, by announcing seven C-ROADS projects, in Austria, Belgium, the Czech Republic, Germany, France, Netherlands, Slovenia and UK. Furthermore, at international level, deployments of 802.11p-based DSRC for safety applications has already begun in Japan by Hyundai, Kia and Toyota and the US by GM.

Both technologies present pros and cons, with the main ones being described below.

- **Availability**: ITS-G5 is a readily-available, internationally-recognized standard. On the contrary, Qualcomm has announced its first C-V2X chipset for availability in the second half of 2018, but further refinement and certification could take additional

iterations of the chip. Considering that large-scale field tests took 2 years to complete for ITS-G5, and when combined with the automotive development cycle of around 3 years, it could take until 2023-2024 for C-V2X to be tested and introduced into vehicles at scale.

- **Infrastructure requirement:** In terms of infrastructure needs, no network architecture (other than the one of the road itself for V2I) is needed to provide peer-to-peer communications (i.e. DSRC), as is the case for ITS-G5, between vehicles and road infrastructure, meaning that it could be deployed on any road, and even in rural areas where there is limited telecoms infrastructure. On the contrary, the deployment of C-V2X will require dedicated infrastructures, investments need to be made especially in those areas that are today scarcely covered by such infrastructure, i.e. highways, as the the low population density.
- **Security:** Different security concepts are used for ITS-G5 and C-V2X respectively ITS-G5, being a peer-to-peer infrastructure has built-in mechanisms for encryption, anomization to secure ad-hoc networking and data exchange. C-V2X can benefit from a global networking infrastructure and an end-to-end operational supervision and monitoring, to control which user equipment is connected. This is particularly relevant in terms of cybersecurity, as the risk of cyber-threat may increase exponentially by the number of connected devices.

10.4.3 Legal and Technical framework

European ITS Spectrum – current harmonised allocations

Spectrum allocation for ITS purposes is mostly regulated by EC Decision (2008/671/EC [7]) on harmonised use of 5 875-5 905 MHz (aka 5.9 GHz) band for safety related ITS applications. In addition, an ECC decision (ECC/DEC/(08)01 [8]) addresses other ITS uses in the 5 905-5 925 MHz band, where there are usage restrictions which may limit usability in the near future. Vehicle devices are licence-exempt because of safety aspects, whilst licensing for roadside devices are defined at national level.

Other main ITS allocations are reported in in EC Decision 2006/771/EC on short-range devices and in EC Decisions 2004/545/EC and 2005/50/EC on automotive Short-range Radars, including Road Transport and Traffic Telematics (RTTT), are as follows:

- 5 795-5 815 MHz (aka 5.8 GHz). Primarily used for road-tolling devices, although proximity to the 5.8 GHz band may lead to interference problems.
- 63-64 GHz. Needed for low latency / high reliability vehicle-vehicle control loops, as for platooning and automated driving. Currently only used on test systems;
- 24 GHz spectrum range is currently allocated to automotive short-range radars, but with a requirement to move to 79 GHz as a long-term solution.
- EC Decision (2008/671/EC) on harmonised use of 5 875-5 905 MHz (aka 5.9 GHz) band.

10.4.4 Policy initiatives and strategic orientations

Different initiatives, both public and private, have been launched recently to try and reach a common solution to the problem.

The most recent initiative concerns the Open Public Consultation the EC – DG Connect has launched at the beginning of 2018 for the support study for Impact Assessment of

Cooperative Intelligent Transport Systems. Among the different topics investigated, V2X communication standards hold a primary role.

The European Commission has also organised different working tables and workshops, together with industry representatives as well as consumers' associations, to provide a discussion floor where to discuss eventual solutions. For example, on September 2017 the Commission held a workshop on ITS short-range communications in the 5.9GHz band (5875-5905 MHz). The workshop was attended by about 90 participants from the car and telecom industries, national administrations, sectorial organisations. It was organised with the aim of facilitating a common understanding of the problem of non-coexistence in the 5.9 GHz band of two different technologies to be used for safety related ITS applications: ETSI-ITS-G5 (based on the IEEE 802.11p standard; and LTE-V2X (based on the 3GPP Release 14 standard). The aim of the workshop was also to find elements of agreement among the stakeholders.

Furthermore, on 13 March 2018 the European Parliament adopted its opinion on cooperative intelligent transport systems. In the document's conclusions, European Parliament is pushing for the swift introduction of connectivity to reduce casualties on Europe's roads. The report highlights the regulatory framework the introduction requires and sets out an ambitious time-frame. It conveys the vision of a single interoperable communication eco-system for C-ITS by 2019 and gives full support to the speedy launch of existing technology, whilst keeping C-ITS open to future and compatible technologies. The report highlights the need for a singular security system to assure the authenticity of messages and argues for strong data protection measures to protect the privacy of motorists.

10.4.5 Mapping of stakeholders' views

Interaction with stakeholders and experts from the automotive industry have confirmed that connectivity is seen as a central element in the context of CCAM. Interoperability between systems has been put forward as an essential element to ensure cross border operation, with regards to, for instance, data format.

As the question of interoperability directly relates to the need for a common communication standard to be used in V2X communication, a clear pattern emerges in terms of stakeholders' points of view: while OEMs (and some TIER1) clearly state that it is too early to think about acting when it comes to standardizing one technology or the other (to ensure interoperability in the future); the aftermarket urges regulators to advance in this respect (with the same endpoint/goal: interoperability).

Finally, when asked about policy initiatives, including the European driven C-Roads initiative, few converged on the fact that the platform should be more technology neutral (i.e. with regards to communication technology, as its current preference seems to be ITS G5 over cellular networks).

10.4.6 Impact of the issue and possible solutions on business models

Depending on the type of standard that will prevail, new profit pools for actors active in 802.11p-based or cellular technology could emerge. In both case, new infrastructure investment will be needed. Depending on which of the two, public/private partnership could take place.

The emergence of a dominant technology, by legislative actions or as an effect of market forces, will avoid the creation of a situation in which uncertainty on the opportunity to use and commercialised automated vehicles will heavily impact the uptake of automated

vehicles. Eventually, future vehicles might develop automated capabilities but only with limited/ basic connectivity-related capabilities. As a consequence, automated functions could be used mainly in "protected environment", e.g. highways (i.e. SAE level 4). This might reduce the interest of consumers for CCAM technology, as they might expect full autonomy of vehicles under all conditions (i.e. SAE level 5).

The Automotive value chain will be heavily affected depending on which communication technology will become the standard for V2X communication. On one side, if 5G mobile technology will be used, telecommunication companies will have access to a new source of profit represented by CAD market. In this scenario, Telecommunication companies are foreseen to become a relevant player in the future automated supply chain. On the other side, if ITS-G5, is (to become) the deployed standard of communication for V2V and V2I, OEMs will have a chance to gain a greater role and share in the value chain. Finally, if both technologies will become the standard for V2X communication, based for example on a redundancy ground, both players are expected to start cooperating, developing ad hoc, long-lasting partnerships.

Furthermore, on aspects that should be considered is the negative impact the current situation of uncertainty is having on the development of new technologies in the field of AVs: as two different technologies are competing, OEMs and upstream suppliers have *de facto* implemented a "wait-and-see" strategy, looking for clear indications from the European Commission on the topic. As a consequence, the European firms risk losing their competitive advantage in the sector, a situation that could have important consequences in a competitive environment as the ones of automotive.

10.4.7 Conclusions and recommendations

Based on the result of analysis conducted in the report, it has emerged how the current situation is an *empasse* for the technological development of V2X capabilities, affecting the European companies as they risk losing their competitiveness on the matter. For this reason, the following recommendation should be taken into consideration by the European Commission:

- European Commission-DG Connect should not delay a decision on the standard of communication that should be followed or at least recommended in Europe for V2X communication. A step in this direction could already be taken in the recommendation that will be issued by the end of 2018 to tackle the issues of cybersecurity, access to data and connectivity.

11 CONCLUSIONS

Automated vehicles will revolutionise the way European citizens move, increasing safety and security of both the passengers and pedestrians. In the recent years, automated technology has seen a drastic improvement in terms of performances, reliability and security, with first steps of automation being already on the market, SAE vehicles of SAE levels 3 and 4 being tested on standard roads and potentially on the market in the upcoming years.

Nevertheless, a set of issues of legal, technical and commercial nature are today present, and if not positively addressed, they will affect significantly the uptake of AVs in Europe. Across the study, an extensive activity of desk research, business intelligence and stakeholders consultation have allowed to define a set of issues that are, today, the ones capable of affecting this technology the most in the near future.

More in details, the following thematic areas were analysed:

- Liability, and the impact future AVs will have on current liability framework;
- Cybersecurity, which encompasses legal, commercial and technical aspects;
- Access to data, and its impacts on the uptake of data-enabled services;
- Testing and certification;
- The necessary evolution of Road infrastructure; and
- A set of issues of technical/technological nature, including Artificial Intelligence, HD Maps, Positioning technology and V2X Communication.

Based on the outcome of the analysis and the feedback of experts from the industry, the following recommendation have been developed.

Concerning the issue of **liability**, the present study advocates for a revision of the PLD and its scope of application by the relevant authorities. Furthermore, autonomous regulation could use compulsory insurance schemes, no-fault plans, as well as a risk-management approach.

In terms of **testing on public roads**, the Commission could encourage Member States to improve the transparency of testing requirements/principles/guidelines, by means of recommendations, by monitoring and analysing the different interpretations of testing requirements, and by cross-fertilisation actions aimed at driving Member States towards a more homogeneous approach where nessary. The Commission should also establish stronger cooperation on testing across Europe, through the implementation of a European system for sharing testing data, conditions, use cases and best practices related to automated driving.

When evaluating the question of AVs **certification**, the present report welcomes and supports the activity that is currently ongoing on this topic at UNECE level by the specific Task Force under the ITS/AD Informal Group within WP.29. Based on the outcome of this activity, European Commission should actively participate in this work, so to obtain in the final certification scheme an optimal balance between the extension, approach and stringency of the testing (and associated levels of safety and security), and the administrative burden on the industry. In case of delays in the process, available instruments and options under the EU legal framework could be used as possible mitigation instruments.

In terms of **cybersecurity**, the report indicates a potential mandate for ENISA to use the finalized UNECE WP.29 guidelines on cybersecurity to implement an EU-wide certification scheme. Furthermore, the report welcomes the initiative to create a network of competence centres across Member States as well as a European Cybersecurity Research and Competence Centre to aid the development of respective tools and technologies necessary to ensure a continuous monitoring and evaluation of cyber-threats.

Analysing the overall question of **access to data** from a legal, technical and commercial point of view, the feedback received across different interactions with industry and users representatives, together with experts' opinion, indicate as a priority the establishment of a clear, full, transparent data-sets categorisation. Within the Recommendation planned to be issued at the end of 2018, the Commission should stress the importance of ensuring that data access solutions developed and made available by OEMs enable the generation of innovative downstream services, while guaranteeing a level playing field for players competing in their provision. The Commission should then continue analysing the service market enabled by vehicle data. Should the monitoring activity identify, within 1 or 2 years, that downstream competition is impacted by asymmetric data access and that development of new data-based services is limited by the dominant position of OEMs, a regulatory approach on data access should be pursued.

Regarding **infrastructure evolution** to comply with the needs of future AVs, priority, in terms of policy action and public fund allocation, should be given to maintenance and refurbishment of signalling across EU roads, as well as to the alignment of signalling across the Member States. Furthermore, the Commission should recommend national Institutions to investigate the opportunity to regulate how road network and road infrastructure operators grant access to third parties including telecommunication operators, so to ensure fair access to road infrastructure to these actors.

In terms of **technical/technological challenges**, the following conclusions were reached:

- Concerning **artificial intelligence**, the present report advocates for initiative to create a multi-stakeholder communication platform to guarantee competitiveness and creation of ethical guidelines, as well as continuing the coordination of research and investments at EU level.

- On the issue of **positioning technology**, we suggest participating in international and European standardisation fora to ensure that specific differentiators of European systems (E.g. European GNSS). Furthermore, the opportunity to consider positioning and GNSS related requirements and aspects in the ongoing process of update of certification at UNECE level[117] should be strongly considered by European Institutions, as UNECE has started regulatory drafting activities on certification to accommodate the specificities of automated driving.
- On the issue of **HD maps**, the conclusions of this study indicate the promotion of public/private partnerships to cover market failures resulting from scarcely populated/ rural areas as the best approach to solve the commercial issue underlying the creation of HD maps. Furthermore, focus should also put on helping the coordination between international business players in developing a single format for HD maps, to increase the compatibility across different OEMs and potentially enable economies of scale.

[117] Activities are covered by the Task Force "AutoVeh" under the ITS/AD informal working group of UNECE WP.29

- Finally, on the issue of the **absence of a dominant V2X communication standard**, the present report calls the European Commission not to delay a decision on the standard of communication that should be followed in Europe for V2X communication. As the current situation is restraining technological development in the field, a clarification on the issue from the Institution will provide a strong signal to the automotive industry.

To conclude, the present report provides indications on the path Institutions and private actors should follow to ensure a rapid and solid uptake of automated vehicles. Considered the undiscussed benefits that could derive from this new technology in the everyday life of European citizens, the European Commission should make this a priority in the agenda for the upcoming years.

12 ANNEXES

12.1 Annex A: Bibliography

(n.d.). Retrieved from PEGASUS RESEARCH PROJECT: https://www.pegasusprojekt.de/en/about-PEGASUS

(n.d.). Retrieved from nuTonomy: https://www.nutonomy.com

Germany's Federal Minister of Transport and Digital Infrastructure. (n.d.). *Automated and Connected Driving*. Retrieved from https://www.bmvi.de/EN/Topics/Digital-Matters/Automated-Connected-Driving/automated-and-connected-driving.html

(FIGIEFA), N. P. (n.d.). Access to the vehicle,its data and resources. *Telematics workshop-Vehicle Data & Connected Cars.*

ACEA. (December 2016). *Position Paper: Access to vehicle data for third-party services.*

AFCAR. (April 2018). *Press Release: Broad industry coalition calls upon EU decision-makers to ACT NOW for equal access to in-vehicle data and functions.*

AI Poses a Tough Road Ahead for Autonomous Car Makers. (2018, June 7). Retrieved from ElectronicDesign: https://www.electronicdesign.com/automotive/ai-poses-tough-road-ahead-autonomous-car-makers

Allen & Overy. (2017). *Autonomous and connected vehicles: navigating the legal issues.*

An Overview of National AI Strategies. (2018, June 28). Retrieved from Medium: https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd

ANEC and BEUC. (2018). *Cybersecurity for Connected Products.*

Artificial Intelligence and Autonomous Vehicles. (2018, April 19). Retrieved from Medium: https://medium.com/datadriveninvestor/artificial-intelligence-and-autonomous-vehicles-ae877feb6cd2

Australia's National Transport Commission. (November 2016). *Regulatory reforms for automated road vehicles.*

Austrian Ministry for Transport, Innovation and Technology. (2016). *Automated - Connected - Mobile .*

Automotive HMI design: How AI can save the identity of car brands. (2018, January 8). Retrieved from Nuance: https://whatsnext.nuance.com/connected-living/automotive-hmi-design-can-save-identity-car-brands/

Automotive News. (2017, April 17). *Hyundai Mobis: Level 3 self-driving by '22*. Retrieved from http://www.autonews.com/article/20170417/OEM10/304179938/hyundai-mobis:-level-3-self-driving-by-22

Automotive News. (2017, June 28). *PSA plans 'hands off' self-driving cars after 2020*. Retrieved from http://www.autonews.com/article/20170628/COPY01/306289965/psa-plans-hands-off-self-driving-cars-after-2020

Autonomous cars driving the market for new insurance services in UBI. (2016, July 14). Retrieved from Telematic Wire: http://telematicswire.net/autonomous-cars-driving-the-market-for-new-insurance-services-in-ubi/

BEUC. (June 2018). *Automated decision making and artificial intelligence.*

BEUC. (November 2017). *Protecting European consumers with connected and autonomous cars.*

BEUC. (November 2017). *Review of Product liability rules.*

Bloomberg. (2017, December 6). *Nissan Plans to Introduce Fully Autonomous Driving Cars in 2022*. Retrieved from https://www.bloomberg.com/news/articles/2017-12-06/nissan-plans-to-introduce-fully-autonomous-driving-cars-in-2022

Boston Consulting Group. (February 2016). *What's Ahead for Car Sharing? The New Mobility and Its Impact on Vehicle Sales.*

CarAndBike Team. (2017, November 20). *Toyota And Suzuki Officially Confirm Technology Partnership Agreement*. Retrieved from https://auto.ndtv.com/news/toyota-and-suzuki-officially-confirm-technology-partnership-agreement-1656899

CECRA. (October 2016). *Position Paper on Connectivity'.*

Centre for Connected and Autonomous Vehicles (UK). (July 2017). *Market Forecast for Connected and Autonomous Vehicles.*

CLEPA. (2014). *Position Paper: Automated Driving.*

CLEPA. (2017). *Truck platooning: Smart mobility through intelligent transport systems and automated & connected driving.*

CLEPA. (July 2015). *Position Paper Open Telematics Platform .*

CONNECTED AUTOMATED DRIVING EUROPE. (n.d.). *Cloud-LSVA*. Retrieved from https://connectedautomateddriving.eu/project/cloud-lsva/

COST (European Cooperation in Science and Technology). (2018). *SaPPAR Guidelines: Performance assessment of positioning terminals.*

Deloitte. (2017). *The future of the automotive value chain: 2025 and beyond.*

Department for Transport (UK). (2018). *Automated and Electric Vehicles Act.*

DG GROW. (2017). *GEAR 2030 High Level Group on the Competitiveness and Sustainable Growth of the Automotive Industry in the EU- Final report.*

Dr. Christian Knobloch, D. J. (n.d.). A systematic approach from today‘s situation up to the fully automated mobility network and mobility ecosystem. *Webinar: Liability in ‘connected cars‘.*

Dr. Martin Burgmer, D.-I. C.-I. (n.d.). *Security Concept for an Interoperable Telematics Platform.*

(2018). *Draft Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD.* UN Task Force on Cyber security and OTA issues (CS/OTA).

Drive.ai. (n.d.). Retrieved from https://www.drive.ai

Economic Commission for Europe (Inland Transport Committee: submitted by Germany,Japan,Spain,the Netherlands,the UK). (2017). Automated Vehicles: Policy and Principles Discussion Document. *Global Forum for Road Traffic Safety.*

EU Member States representatives. (2018, April 10). *Declaration of cooperation on Artificial Intelligence.* Retrieved from https://ec.europa.eu/jrc/communities/digitranscope/document/eu-declaration-cooperation-artificial-intelligence

European Automotive and Telecom Alliance. (June 2018). *Regulatory Briefing paper: Cybersecurity.*

European Commission . (2018). *Press release: Commission publishes guidance on upcoming new data protection rules.*

European Commission - Joint Research Centre Directorate Growth and Innovation. (2017). *EU Industrial R&D Investment Scoreboard.*

European Commission. (April 2018). *Communication Artificial Intelligence for Europe.*

European Commission. (January 2017). *Communication from the Commission to the European Parliament,the Council,the European Social and Economic Committee and the Committee of the Regions: Building a Data Economy.*

European Parliamentary Research Service, Impact Assessment and European Added Value. (2018). *A common EU approach to liability rules and insurance for connected and autonomous vehicles.*

FIA Region 1. (2016). *Policy Position on Vehicle Type Approval.*

FIA Region 1. (2017, May). *My Car My Data campaign*. Retrieved from https://www.fiaregion1.com/my-car-my-data/

FIA Region 1. (February 2017). *Policy Position on Event Data Recorders.*

FIA Region 1. (June 2017). *BMW Car Data: General Analysis.*

FIA Region 1. (May 2017). *Policy position on car connectivity.*

FIA Region 1. (May 2017). *Policy Position on the Motor Insurance Directive.*

FIGIEFA. (December 2016). *Free Flow of Data – Commission Communication –Input from the Independent Automotive Aftermarket.*

Finnish Transport Agency. (2016). *Road Transport Automation Road Map and Action Plan 2016-2020.* Helsinki.

Ford and Autonomic are building a smart city cloud platform. (2018, January 9). Retrieved from Techcrunch: https://techcrunch.com/2018/01/09/ford-and-autonomic-are-building-a-smart-city-cloud-platform/?guccounter=1

Fortune (Magazine). (2017, August 16). *Fiat Chrysler Joins BMW and Intel's Autonomous Car Alliance*. Retrieved from http://fortune.com/2017/08/16/fiat-chrysler-bmw-intel-mobileye-autonomous-car/

Fortune. (2017, April 4). Daimler And Bosch Plan to Bring Self-Driving Taxis to Cities. Retrieved from http://fortune.com/2017/04/04/daimler-bosch-self-driving-taxis/

Fortune. (2017, November 30). *GM Wants to Bring an Uber-Like Self-Driving Car Service to Big Cities in 2019. Will It Work?* Retrieved from http://fortune.com/2017/11/30/gm-autonomous-ride-share-2019/

Fortune. (2017, February 27). *How Renault-Nissan Is Going to Get You in an Electric Driverless Car*. Retrieved from http://fortune.com/2017/02/27/renault-nissan-driverless-vehicles/

Fortune. (2017, March 7). *Meet Sedric, Volkswagen's Vision for Self-Driving Cars*. Retrieved from http://fortune.com/2017/03/07/volkswagen-self-driving-car-sedric/

Fortune. (2017, September 27). *Toyota Is Betting On This Startup To Drive Its Self-Driving Car Plans Forward*. Retrieved from http://fortune.com/2017/09/27/toyota-self-driving-car-luminar/

Fortune. (2017, November 20). *Volvo Cars Will Supply Uber With Up to 24,000 Self-Driving Cars*. Retrieved from http://fortune.com/2017/11/20/uber-volvo-self-driving-cars/

Fortune. (2017, December 6). *Why Ford Won't Rush An Autonomous Car To Market*. Retrieved from http://fortune.com/2017/12/06/ford-autonomous-cars/

France Ministry of Sustainable Development. (2017). *Développement des véhicules autonomes - Orientations stratégiques pour l'action publique .*

German Association of the Automotive Industry (VDA). (September 2016). *Access to the vehicle and vehicle generated data.*

Germany's Federal Government. (2017). *Action plan automated and connected driving.*

Germany's Federal Ministry of Transport and Digital Infrastructure. (2017). *Ethics Comission: Automated and Connected Driving Report.*

Giammarco Cecchini, A. B. (n.d.). Performance Comparison Between IEEE 802.11p and LTE-V2V In-coverage and Out-of-coverage for Cooperative Awareness.

Global Survey of Autonomous Vehicle Regulations. (2018, March 15). Retrieved from Medium: https://medium.com/syncedreview/global-survey-of-autonomous-vehicle-regulations-6b8608f205f9

GSA. (2017). *Central role for robust GNSS in autonomous driving.* Retrieved from https://www.gsa.europa.eu/newsroom/news/central-role-robust-gnss-autonomous-driving

GSMA. (September 2017). *Safe and Smarter Driving: the Rollout of Cellular V2X Services in Europe.*

Häckel, D. M., & Steiger, D. E. (November 2017). *Smart Funding: A coherent Approach for Connected & Automated Driving.*

HERE Technologies. (2017). HERE HD Live Map: Technical Paper.

Hogan Lovells. (2014, October 17). *German Data Protection Authorities Issue Resolution on Connected Cars*. Retrieved from Chronicle of Data Protection: https://www.hldataprotection.com/2014/10/articles/international-eu-privacy/german-data-protection-authorities-issue-resolution-on-connected-cars/

How Spectrum and Spectrum Policy Drive the Connected Car and Autonomous Vehicles. (2016, November 29). Retrieved from Hogan Lovells: http://www.hoganlovells.com/en/publications/spectrum-and-spectrum-policy-connected-car-and-autonomous-vehicles

IBM. (2013, June 25). *What is mobile cloud computing?* Retrieved from https://www.ibm.com/blogs/cloud-computing/2013/06/25/mobile-cloud-computing/

Insurance Europe. (2017, November). *#Data4Drivers petition*. Retrieved from , https://www.insuranceeurope.eu/data4drivers-eu-rules-needed-give-drivers-control-their-vehicle-data

Insurance Europe. (February 2018). *Press Statement European Parliament approach on access to in-vehicle data welcomed.*

Insurance Europe. (May 2017). *No need for new liability rules for new technologies.*

Insurance Europe. (May 2017). *Position Paper on liability insurance and emerging technologies.*

Intel. (n.d.). Retrieved from https://www.intel.co.uk/content/www/uk/en/automotive/automotive-overview.html

ISO. (n.d.). *ISO/DPAS 21448: Road vehicles -- Safety of the intended functionality*. Retrieved from International Organization for Standardization: https://www.iso.org/standard/70939.html

Journey. (n.d.). Retrieved from Waymo: https://waymo.com/journey/

McKinsey & Company. (2018, February). *Rethinking car software and electronics architecture*. Retrieved from https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/rethinking-car-software-and-electronics-architecture

McKinsey & Company. (2014). *Connected car, automotive value chain unbound.*

McKinsey & Company. (February 2017). *Shifting gears in cyber security for connected cars.*

McKinsey & Company. (January 2016). *Automotive revolution –perspective towards 2030.*

McKinsey & Company. (January 2018). *Artificial Intelligence-Automotive's New Value-Creating Engine.*

Ministry of Industry, B. a. (2018). *Strategy for Denmarks digital growth.* Retrieved from https://em.dk/english/publications/2018/strategy-for-denmarks-digital-growth

Nasr, A. (24 January 2018). *Data Sharing and Security.* HERE Technologies.

National Academy of Sciences (US). (2017). *Briefing Document: NCHRP Research Report 845:Advancing Automated and Connected Vehicles: Policy and Planning Strategies for State and Local Transportation Agencies.*

NHTSA. (September 2016). *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety.* U.S. Department of Transportation.

OICA. (2017). Certification of Automated Vehicles.

OICA. (2018). Structure of a future Regulation automated and autonomous driving systems. *SG-2 Real World Test Drive.* Hague: UN Task Force on Automated Vehicle Testing (TVAF).
Oliver Wyman analysis. (2015). *Automotive Manager.*
Osborne Clarke LLP. (2016). *Legal study on Ownership and Data Access.* DG Communications Networks, Content & Technology.
Pinsent Masons. (April 2016). *Connected and Autonomous Vehicles: the emerging legal challenges.*
Prof. Dr. Stijn Kelchtermans, P. D. (October 2015). *Economic Analysis of the Introduction of a Telematics Platform in the Motor Vehicle Industry.*
Ptolemus Consulting Group. (2016). *Usage-Based Insurance: Global Study.*
PWC. (2016). *Connected car report .*
PWC. (2016). *Global Innovation 1000 Study.*
Roland Berger . (January 2018). *Auromated Vehicles Index: Q4 2017.*
Roland Berger. (November 2014). *Autonomous driving: Disruptive innovation that promises to change the automotive industry.*
SG Analytics. (n.d.). *Data analytics in the automotive industry – Shifting gears, steering disruption*. Retrieved from http://www.sganalytics.com/blog/data-analytics-automotive-industry/
SMMT. (February 2017). *Position paper: Connected and Autonomous Vehicles.*
Spain's Subdirectorate-General for Mobility Management. (2016, March 10). *Instruction 15/V-113: Authorization to conduct tests or research trials of automated vehicles on roads open to general Traffic.* Retrieved from UNECE: https://www.unece.org/fileadmin/DAM/trans/doc/2016/wp1/ECE-TRANS-WP1-2016-INF-8e.pdf
SPI,VTT & ECORYS. (May 2017). *Public support measures for connected and automated driving: Final Report.*
Statista. (March 2017). *Connected Car: Market Report.*
Steer Davies Gleave; 4icom. (October 2015). *State of the Art of Electronic Road Tolling.* DG MOVE.
Telecoms versus carmakers in race to get connected. (2017, November 13). Retrieved from Financial Times: https://www.ft.com/content/6c1b7f60-a9d3-11e7-93c5-648314d2c72c
TEPR. (March 2018). *Support study for Impact Assessment of Cooperative Intelligent Transport Systems: Analysis of responses to the Open Public Consultation .*
The driverless, car-sharing road ahead . (2016). *The Economist*.
Toyota will offer Alexa in its cars starting later this year. (2018, January 9). Retrieved from Techcrunch: https://techcrunch.com/2018/01/09/toyota-will-offer-alexa-in-its-cars-starting-later-this-year/
TRL. (2016). *Study on the assessment and certification of automated vehicles: Final Report.* Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (EC).
UK's Centre for Connected and Autonomous Vehicles. (2017). *The Key Principles of Cyber Security for Connected and Automated Vehicles.*
United States Patent and Trademark Office. (2017, December 21). Retrieved from United States Patent Publication: Autonomous Navigation System: http://pdfaiw.uspto.gov/.aiw?PageNum=0&docid=20170363430&IDKey=E2ED13A76A17&HomeUrl=http%3A%2F%2Fappft.uspto.gov%2Fnetacgi%2Fnph-Parser%3FSect1%3DPTO1%2526Sect2%3DHITOFF%2526d%3DPG01%2526p%3D1%2526u%3D%2Fnetahtml%2FPTO%2Fsrchnum.html%2526r%3D1%2526f%3DG%2
VdTÜV. (January 2017). *Position: Requirements for the telematics interface in vehicles.*
VI-grade. (n.d.). *Human Centric Vehicle development using Advance Real-Time All-In-The -Loop Simulators.*
Volvo Cars to supply tens of thousands of autonomous drive compatible cars to Uber. (2017, November 20). Retrieved from Volvo Car Group: Global Newsroom: https://www.media.volvocars.com/global/en-gb/media/pressreleases/216738/volvo-cars-to-supply-tens-of-thousands-of-autonomous-drive-compatible-cars-to-uber
WP.29 GRRF. (2015). Working Paper: Guidance to GRs concerning Automated Driving Technology. UNECE.

12.2 Annex B: Stakeholder consultation report

12.2.1 Introduction

In this section we summarize the consulted stakeholders' views (c.f. tables below) from two phases of consultation via interview.

- The first consultation focuses on various aspects including key trends, business models' evolution, as well as technical, commercial, legal and policy-related elements concerning CCAM. In addition to the discussion itself, the consultation process involved a post-interview validation procedure whereby stakeholders had the opportunity to add or adjust the inputs provided. In the period from February to March 2018, VVA interviewed more than 30 stakeholders representing the upstream automotive value chain - traditional and new-technology suppliers –, OEMs, both "traditional" and newly emerged, and downstream automotive value chain, including service providers – as well as mobility providers - and aftermarket players.
- The second phase engaged a smaller number of stakeholders (15). The aim was to validate the conclusions taken after the first consultation together with the desk research phase, as well as to investigate more in depth the issues impacting the uptake of CCAM.

The input of the stakeholder's consultations served the elaboration of the workshop structure and as an overall contribution to the final report.

Table 6 1st Phase Consultation participant

	Value chain segment	Entity
1	Tier 2 Supplier	Qualcomm
2	Tier 1 Supplier	Denso
3	Tier 1 Supplier	Bosch
4	Association - Tier 1 Supplier	CLEPA
5	Tier 0,5 Supplier	Kapsch
6	Tier 0,5 Supplier	VI-Grade
7	Tier 0,5 Supplier	Valeo
8	Tier 0,5 Supplier	TraceTronic GmbH
9	Tier 0,5 Supplier	FICOSA
10	Tier 0,5 Supplier	Nutonomy
11	OEM	BMW
12	OEM	Tesla
13	OEM	Volvo Group Headquarters
14	Association - OEM	European Automobile Manufacturers' Association (ACEA)
15	Service provider	MaaS Global
16	Service provider	FleetComplete
17	Service provider	Uber

	Value chain segment	Entity
18	Aftermarket	CITA
19	Aftermarket	VdTÜV
20	Association - Aftermarket	Insurance Europe
21	Association - Aftermarket	FIGIEFA
22	Aftermarket	MOBIVIA
23	Associations - aftermarket	CECRA
24	Telecommunication service provider	Vodafone
25	Association - Telecommunication service provider	GSMA
26	Research institution	University of Marburg
27	Research institution	University of Derby,
28	Infrastructure operators/Service provider	I-SENSE
29	Solution providers	FDC
30	Consulting firm	LS Telcom
31	Associations – end users	FIA
32	Associations – end users	BEUC

Table 7 Stakeholder list of second consultation

Number	VC representative	Company
1	Tier 2	Qualcomm
2	Tier 1	Valeo
3	Tier 1	Bosch
4	Tier 0,5	Nutonomy
5	Service provider	Uber
6	Others	ATEC-ITS France (FDC)
7	Others	University of Derby
8	OEMs	BMW
9	OEMs	Tesla
10	Aftermarket	I-SENSE
11	Aftermarket	Insurance Europe
12	Aftermarket	VdTÜV

12.2.2 First stakeholder consultation

12.2.2.1 Key trends

Would you agree with the estimates for the uptake of automated driving in EU provided in the tables? Why or why not? Which are the key preconditions and drivers to achieve a fast uptake? What are the main challenges that can slow it down?

Table 8 Forecasted share of new vehicle sales for level 1 and level 2 SAE, by region

	2030	2040	2050
Europe	*41%*	*0%*	*0%*
North America	*41%*	*0%*	*0%*
Asia Pacific (ex - Japan)	*75%*	*13%*	*0%*

Source: Goldman Sachs Global Investment Research

Table 9 Forecasted share of new vehicle sales for level 3 SAE, by region

	2030	2040	2050
Europe	*34%*	*6%*	*0%*
North America	*42%*	*0%*	*0%*
Asia Pacific (ex - Japan)	*24%*	*39%*	*13%*

Source: Goldman Sachs Global Investment Research

Table 10 Forecasted share of new vehicle sales for level 4 SAE, by region

	2030	2040	2050
Europe	*25%*	*94%*	*100%*
North America	*17%*	*90%*	*100%*
Asia Pacific (ex - Japan)	*1%*	*48%*	*87%*

Source: Goldman Sachs Global Investment Research

The general uptake trend (and timeframe) is largely confirmed by interviewees, despite recurring observations regarding the (slightly) optimistic magnitudes. Level 3 is not expected by some stakeholders to ever rise above 0, given the complexity associated with it: the possibility of switching control between the automated vehicle and driver raises a series ethical and liability concerns. In this respect, a direct transition to Level 4 is suggested. Legislation or the presence of the relevant regulatory framework is often seen as both: a potential main driver as well as potential impediment to the development of AV technology. Although the majority agree that higher levels of automation are difficult to predict, one stakeholder suggests that the uptake levels for Levels 3-4 may depend, for instance, on the way CCAM is delivered. In case of private provision (i.e. a launch on the mass-market with convenience as the main rationale behind the purchase) regions with more favourable conditions e.g. more freeway driving, will have higher deployment rates. Another stakeholder suggests a reversed relationship in case of delivery as a service, namely that shared mobility services will encourage urbanization.

On a comparative base, which are the key reasons underlying possible different uptakes of CCAM in EU vis-a-vis other international markets, as shown in for the North America and for the Asia – Pacific market area?

Gaps between regions (Europe, North America, Asia Pacific), in case identified by some, are at the same time questioned by other stakeholders. The main recurring element enabling different uptake levels concerns the (presence of a) regulatory framework on CCAM. In this sense, disaggregated parts of Asia (China and Singapore) as well as North America which already allow AVs on public roads, are expected to have a head start. Ensuring safety (as a part of social acceptance in general) is the next major identified element to foster uptake. One suggestion is that proving automation/technology as safer compared to human beings will be pivotal when it comes to society embracing technological developments at large. Again, differences in infrastructure, available network connectivity (more generally: favourable conditions e.g. weather, driving behaviour) will potentially fuel differences between regions. One stakeholder views the associated high cost with this technology may underline the heterogeneity, given the variances in purchasing power across the globe.

Even though many interviewees hint that North America may have a head start (as opposed to the table which places the emphasis on Europe for LVLs1/2 and LVL4), given cultural and legal aspects, some TIER 0,5 stakeholders consider these regional differences may even out in the long-term. This conclusion can be generalized based on the abovementioned elements (either facilitating or slowing down uptake), which can be said to be roughly evenly scattered across regions, and the fact that competition will ensure that technology deployment in one region is caught up with. In addition to that, it has been stressed during the consultation that the issue's complexity will require a global/unified approach, for example with regards to homologation.

What are in your opinion the main factors behind newly formed partnerships in automotive? Do you believe this is the start of a new business model for the automotive sector, or rather a temporary solution OEMs are leveraging on to develop their own knowledge? Can you identify new areas that will originate partnerships and alliances in the upcoming years?

Technological developments certainly affect the "traditional" automotive ecosystem. Most interviewees claim to have witnessed at least one of the various configurations: automakers partnering with technology providers; collaborations between automakers; car manufacturers ride-sharing firms; academic or government institutions; suppliers of automakers and technology providers.

The majority also believe that collaboration models across as well as within the automotive industry, will become more common, as it moves into the direction of a mobility sector. One stakeholder attributes this evolution to 3 specific factors: connectivity, electrification, automated driving, which unlike previously, today need to be managed at the same time. This evolution is also linked to the entrance of new players. The so-called 'tech giants' and players from different industries have the potential skills to complement the current challenges faced by established actors. Nevertheless, a few stakeholders suggest these new entrants will still require experience with e.g. 'traditional elements' such as hardware.

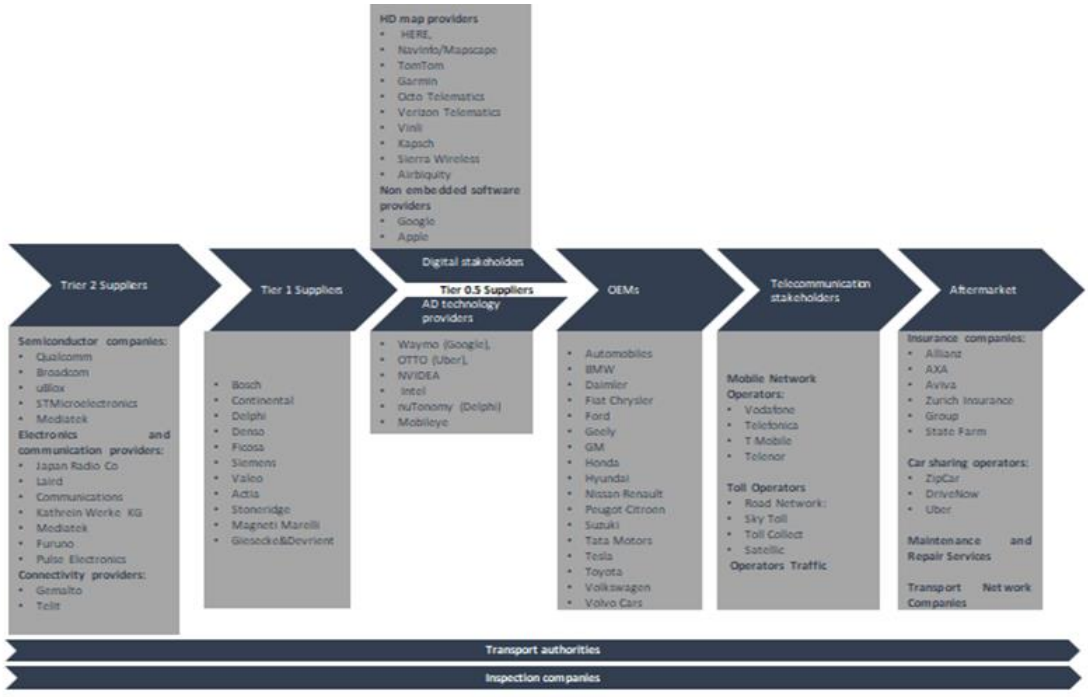
It is widely agreed that individual market players will associate to complement each other's skills (accumulate knowledge) and develop complete solutions. An emerging concept to describe this evolution from a purely economic rationale is "frenemy" (coopetition): referring to alliances aiming to achieve efficiencies inaccessible otherwise. One automotive supplier views the nature of newly formed structures as short-lived: these will shift back to long-standing, traditional partnerships once commoditized; vice versa, most stakeholders view additional capability development as necessary to face the changes in

traditional ecosystems, making partnerships/collaborations a norm in the future. Further consolidation in the market is expected to the extent that these cooperations deliver added value. One stakeholder perceives intra-industry collaborations as essential in the context of higher automation levels, given the corresponding intertwined liability as well as ethical concerns between different actors; however, the same source suggests their rate might decrease in the future.

12.2.2.2 CAD Service and business models' evolution

5.Do you agree with the value chain below? If not, which elements would you suggest modifying?

Table 11 Automotive value chain



All Tier 0.5 and some OEMs mostly agree with and view the value chain illustration as offering a good perspective on the market. Other players claim that there is a need to move away from the linear representation: as the complexity in the current VC is beyond the "classical layout".

A few interviewees suggest that an improved or more comprehensive representation needs to capture selective competition and direct collaborations amongst different actors, for instance the attempt of various actors (starting with TIER1) to reach out directly to the customer mobility ecosystem; although there has been a range of suggestions, broad agreement is to replace telecommunication stakeholders by "data market providers" by including public transport authorities; further, a split in the aftermarket section to encompass service providers and services for mobility, has been a prevalent suggestion. Some stakeholders also stress the difficulty of attributing certain market players to a single part of the value chain (e.g. a company that could equally be classified as TIER 1 and Aftermarket).

6.How will the value chain evolve in the next 10-15 years, in terms of roles, new entrants, bargaining and decision-making power?

There is an underlying, common agreement among interviewees on the fact that future evolutions in the automotive sector are hard to predict, which results in divided views regarding forecasted developments: on the one hand some stakeholders believe that no major changes will occur, others anticipate more fluidification among diverse actors' roles while few envisage (specific) radical transformations.

In line with emerging new services and business models for providing customer value. e.g. mobility services such as ride/car sharing; infotainment and entertainment services, several stakeholders point at the increased interaction between different players across the value chain. At one extreme these higher rates of interactions may result in a more dynamic/circular/network value chain, according to some interviewees. A less transformative interpretation would result in a cross-fertilization between different segments. Nevertheless, a small group of stakeholders adhere to the old value chain's persistence despite acknowledged evolutions.

A few stakeholders point out that the current trend concerning cooperation across the value chain as well as market consolidation will persist and reflect in the value chain. This evolution is sustained by the increasing complexity of, for instance, car's design; Some specifically attribute the transformed layout to future developments with regards to connectivity: the growing importance of communication (information exchange) between cars as well as external environment e.g. smart infrastructure would also have an impact in terms of a vehicle's design and entail associations amongst different actors.

(e.g. development of complete solutions could result in fusions between digital stakeholders and AD technology providers; synergies between V2V services; moreover, blurred liability/responsibility between actors e.g. on higher levels of automation as well as cybersecurity concerns, will require also closer collaboration).

While a part agrees that, main actors will remain in place, in various occasions, interviewees suggest their roles are to become more fluid with emerging opportunities for change. Tech giants' entry is highlighted by a few, but their future role and potential impact are difficult to predict. More 'transformative' views are shared amongst emerging mobility services (service and technology providers). One stakeholder suggests a complete shift away from the OEMs perspective (production of cars) given that the automotive industry moves towards production of services. Technology providers forecast a devaluation of car ownership to the extent that people do not own a car in the future.

An important observation shared by some stakeholders is that the outcome with regards to data access regulation (e.g. the distribution of roles) will be pivotal in terms of the value chain's future evolution.

Focusing on data ownership, which players in the value chain are expected to own most of the data? Do you think these players would be willing to share these data to support the provision of added value services offered by other players? Under what conditions?

One dominant approach among interviewees was to distinguish between the "ownership" and the actual possession or management of data. Consequently, the clear majority agrees to the fact that any data generated by AVs and related applications belongs to the consumer i.e. is owned by him/her. However, access to data is more important, and although related, could according to some, be solved independently of the "ownership question" which requires a legal solution (e.g. data protection regulation).

The status quo, whereby OEMs find themselves in a more advantaged position compared to the rest of the value-chain (especially with respect to the aftermarket) i.e. manage and control most of the data, is different from 'what should be the case' according to many interviewees; nevertheless, a large majority still expect OEMs to manage most of the data in the future.

ExVe (extended vehicle) is a solution created by vehicle manufacturers for granting access to third-parties. Although some OEMs themselves acknowledge the proposed systems' short-comings, among which, the restricted access to third parties e.g. via certificated access conditions, the majority view it as the only currently available, (pragmatic) market solution. Aftermarket (independent service providers) representatives openly reject it: given that many services depend upon direct access to in-vehicle data in real-time, the ExVe "cuts-off" service providers from offering key services and consequently operating own business models. For instance, independent diagnostic test routines/prognostics requires installation of embedded applications and suitable technical conditions (e.g. ultra-low levels of latency).

In this sense, "data ownership" remains a key open question in CCAM given the presence of two strongly conflicting views. Just like OEMs, which view a closed system as an essential setup for guaranteeing a vehicles' integrity and security, software makers/digital enablers will also be reluctant to share data, for instance due to concerns related to intellectual property infringements. On the other end, platform owners (service enablers) as well as the aftermarket in general will, in many cases, require access to in-vehicle data (which as a result, becomes synonymous with access to market). Consequently, reaching an agreement 'to create shared value' for all parties involved is seen by many stakeholders as a real challenge. At the same time, it has been hinted that a scenario with self-sufficient OEMs (i.e. a closed ecosystem) is unlikely, given the context in which delivering complete solutions will inevitably involve joined forces. It has also been suggested (aftermarket player) that an appropriate solution to the "access to data question" should be measured in terms of outcome i.e. if provision of services is possible (independently of who develops the concept/technology)

New mobility services can emerge from CCAM. Can you identify the main ones? Can you comment on their market potential in EU? Which would be the enabling conditions for the successful uptake of these services?

Most interviewees expect a wide range of mobility services to emerge from CCAM. Mobility related services are characterized by efficiency enhancing and socially beneficial properties. Among the primary benefits, according to most stakeholders, is that these will eventually lead to decongesting urban areas as well as a reduction in pollution levels. In addition, car/ride-sharing (e.g. Uber), carpooling and similar services imply lower costs and as a result more accessible transport to end users in addition to a more efficient car usage. In line with resource optimization (e.g. smarter mobility) are emerging services like platooning/cooperative driving trucks (which reduce fuel consumption). Better traffic management will be enabled by urban tolling, which according to a stakeholder will be among the first services to be deployed.

A commonly anticipated complementary evolution are infotainment or convenience-related services. Examples given by various stakeholders include information (e.g. traffic) services, driver assistance, real-time mapping, synchronization with personal devices— jointly aimed at enhancing individual users' experiences.

Among enabling conditions, some stakeholders point out that mobility as a service requires mobility data, since the availability of service depends on access to (relevant) data. In addition, another stakeholder believes the development of cooperative and intelligent

transport systems (C-ITS) will allow for additional services, for instance, vehicle to vehicle connectivity as well as vehicle to infrastructure interactions. Concerning infotainment services (as well as services for commercial purposes in general), a pair of interviewees jointly suggest that customer consent will constitute the main precondition for service deployment. In various occasions, interviewees point out specific consumer behaviour patterns that could potentially hinder this development. For example, despite evolution of the concept of car ownership, cars as a symbol of status could endanger uptake of MaaS. In a similar key, users enjoying driving experience will be reluctant to embrace these changes.

Is there a specific regulation on insurance schemes for CCAM in the member State/ States where your organization in established? If so, how does it work?

Where identified, two EU directives are classified as relevant regulation on insurance schemes for CCAM: the motor insurance and product liability directives. The motor insurance directive is described as ensuring mandatory third-party liability insurance, with victims eligible for compensation under any accident circumstances. While some stakeholders view AVs as within the directive's scope in its current formulation, others suggest it should be modified to explicitly address these vehicles. The other relevant directive, concerning product liability, is seen to harmonize or provide a set of general principles with regards to product liability at the European level.

Focusing on insurance services, please provide your view regarding:

> *a) What are the key challenges that the insurance sector faces in respect of driverless cars?*
> *b) How will the business model of insurance companies evolve? Can you give examples of new products?*
> *c) How would an insurance scheme for CCAM work in practice?*
> *d) How do you think the liability framework should best evolve to accommodate the uptake of automated driving, at both national and European level?*

A small group of stakeholders were able to provide an answer concerning the evolutions and challenges to be faced by the insurance sector in the context of CCAM.

An identified challenge for insurance services concerns (in-vehicle) access to data. Data will enable insurers to understand accidents' circumstances, locate liability level (resulting in faster claim validation) and simplify insurance claims. Data analysis will also allow insurers to understand risk and design appropriate/corresponding coverage.

A second underlying element, is the uncertainty associated with increased safety and corresponding risk reduction associated with CCAM deployment (i.e. once the driver is taken out of the loop). As an illustration one stakeholder foresees the introduction of CCAM as detrimental in terms of insurers' profits while other interviewees see the emergence of fleet (transportation service) providers as an opportunity (new business model) for insurers given that more intensive vehicle exploitation will lead to more risks.

One stakeholder envisages the evolution of insurers business model in terms of the evolving relationship between car and its owner/user, suggesting that car-sharing will shift the focus to the latter by, for instance, ensuring continuity of mobility. Another view is that since driverless cars will result in significant safety improvements (and a respective shift to product insurance), insurers will require additional elements to determine the appropriate volume of coverage. Depending on the evolution with respect to data access, this will enable insurance services to undertake unrelated diversification (e.g. traffic

management information) and enhance existing products such as e.g. usage-based insurance, driver coaching, advanced-breakdown services.

In practice, insurance and claim processes are suggested to be kept as simple as possible.

Repair & maintenance services; Please provide your view regarding:

> *a) What are the key challenges that these service providers currently face or could face in the future?*
> *b) How will the business model of maintenance and diagnostic companies evolve because of the uptake of CCAM? Can you give examples of new services?*
> *c) How would an efficient and effective diagnostic and maintenance service in respect of CCAM work in practice?*

Access to in-vehicle data is largely recognized as an important issue in the context of repair and maintenance services. A level-playing field is essential in terms of competition, more so, the future business of independent repair and maintenance services (aftermarket) itself. For instance, one stakeholder believes provision of maintenance/repair might shift to OEMs as well as their authorized service providers to the detriment of SMEs (i.e. independent maintenance service providers), if the liability framework whereby OEMs accept liability for controlled parts only is maintained. A couple of stakeholders emphasize the need to strike a balance between open access—understood as the ability of these services to directly interact with consumers—and respect of data privacy rules.

Increased vehicle exploitation is seen to affect demand for services in both directions, while another stakeholder sees the effect in terms of a necessary decrease in the downtime for repair. An additional consideration concerns electric vehicles deployment which one stakeholder believes will require less maintenance. A small group of stakeholders view new skills and competence acquisition as an additional challenge to be faced by RMIs (for instance with regards to data management).

Views regarding future developments in terms of business model evolution are fragmented. This can be explained by the uncertainty related to data regulation, which will largely influence the allocation of roles between various actors. One suggestion is that permanent online communication will result in more personalized services as well as direct customer interaction. Prognostics/diagnostics/remote monitoring can significantly shape the RMIs service provision given its properties to prevent costly breakdowns, enable better planning and enable more efficient service provision in general.

According to aftermarket representatives, efficient provision is synonymous with a competitive service, and requires remote/online/live access to in-vehicle data. In this case the aftermarket is expected key player in lifetime and predictive maintenance. On the other hand, a scenario whereby maintenance services are controlled by OEMs is envisaged by another interviewee.

Rental and car sharing; Please provide your view regarding:

> *a) What are the key challenges that car rental and car sharing companies currently face or could face in the future?*
> *b) How will the business model of car rental and car sharing companies evolve because of the uptake of CCAM? Can you give examples of new services? Who will be the main service providers?*

Once again stakeholders emphasize the importance of access to in-vehicle data for service provision; a couple highlight privacy concerns (e.g. erasing customer data after service provision). Others stress the importance of interoperability. (including for instance, incentives from local authorities in the form of dedicated park lanes). In the context of increased competition, cost and effective resource management (cf. fleet owners) will become increasingly important.

In terms of business model evolution because of the uptake of CCAM, a group of stakeholders suggests that strategically smart players will respond to the increasingly complex environment through additional capability development: by either partnering or building up internal knowledge. Another stakeholder foresees a shift towards more customer-centric business models.

In your opinion, to what extent these trends will impact the vehicle sales market? What will be your estimate impact on sales in ten years from now?

A group of stakeholders foresee some drop-in car sales. At the same time increased vehicles' exploitation may increase requirement of maintenance services as well as higher car substitution rates. Another interviewee believes that the long-term trend may result in an adaptation in terms of manufacturing requirements to allow for longer exploitation/extended car-lifecycles in the form of e.g. modular cars.

12.2.2.3 Technical questions

Which are the most relevant technical impediments to the diffusion of automated driving? Which are the possible solutions to overcome them?

Main challenges related to the diffusion of automated driving occur at higher levels of automation (Levels 3-4-5). Most interviewees stress the difficulty of dealing with complex environments, including urban driving (with unpredictable human drivers' behaviour, roadworks), abnormal weather conditions etc. To ensure safety many suggest testing whereby all possible situations should be covered. A few stakeholders highlight that this requires data as well as access to it in certain cases. Another stakeholder suggests a short-term solution in the form of a remote command centre, as part of a phased, step-wise transition to fully automated vehicles.

Among the explicitly mentioned technological impediments a few interviewees view currently available technologies for location-identification (high precision/accuracy geolocation; HD maps) as hindering development. Another group of stakeholders sees no specific impediments but rather a necessity of continuous technological improvements, in various occasions highlighting the importance of ongoing investments and research. Additionally suggested, complementary solutions include AI and machine learning: yet both require a stepwise development. With regards to HD maps, one stakeholder suggests that these would require collaboration/a common platform across the sector.

In addition to operational reliability, another important aspect referred to by many interviewees concerns proving conceptual reliability (as part of social acceptance) in terms of e.g. the safety, functionality and security of safety relevant electronic systems; specifically, the adoption and review of technical inspection of automated and connected vehicles was strongly recommended by an interviewee. This links to the definition of verification and validation procedures, given that a few stakeholders suggest that testing (against defined standards) may be a solution.

In this respect a group of stakeholders sees the absence of regulation/lack of standardisation concerning communication standards (e.g. V2X, V2V, V2I); unified

connectivity standards/solutions as well as testing methodology (physical system; virtual parts and database testing) as an additional impediment.

Which are the main technical impediments to the diffusion of potential services enabled by automated driving and the management of data generated to support it? Can you suggest possible solutions to overcome them?

Similarly, to the diffusion of automated driving, the lack of standardisation with regards to product validation (e.g. certification, and bottom layer compliance assessment) is seen as an important barrier to the diffusion of potential services enabled by automated driving. Some stakeholders also mention a common standard of communications/interoperability while others refer to the importance of developing corresponding infrastructure. With respect to data, in addition to the need to clarify control aspects, a few stakeholders also point at the importance of consumers' privacy protection.

Data authority management is another significant aspect addressed by many interviewees, given that regulation of access to data is essential for establishing a level playing-field. Aftermarket stakeholders claim that the ExVe solution proposed by OEMs represents a main threat to development of services. Hence the suggestion to have a more neutral solution; another stakeholder suggests an on-board application platform with open (and non-discriminatory) access to all actors.

Which are the missing elements in the standardisation domain that need to be developed and/or to be brought forward to support the uptake of automated driving?

Most interviewees believe that safety-related aspects should be standardized. This concerns testing, inspection procedures as well as expected standards of performance. Some even suggest an expansion of the European standards towards e.g. a worldwide ISO certification. Nevertheless, a few stakeholders stress that standardization should occur in terms of outcome rather than technology, so as not to limit the technical solution. A related element concerns information (cyber-) security. Some stakeholders expect a definition of a basic level of security, with respective specifications to assess whether this level was reached (also its certification.) A smaller group of stakeholders specifies that communication should be standardized where it enables interoperability, given that technology neutrality (e.g. hybrid options) is seen as an important element. Access to data may be a potential area of standardization (transparent, open and technology neutral standards (advocated by aftermarket players) in many cases is seen to border with privacy/information security concerns such as protection from unauthorized access (in addition to the earlier mentioned safety concerns).

Regarding digital and physical infrastructure another group of interviewees view this domain as important. One interviewee suggests introducing a classification scheme while others point out the importance of coordination between cities planning digital infrastructure roads. Another suggestion refers to standardizing maps.

What are in your opinion the most relevant aspects that will need to be addressed from a technical point of view to ensure a safe and reliable connection between the connected vehicles and the road environment?

Many stakeholders emphasize the importance of coverage/reliable communication e.g. a consistently operational (smart/digital) infrastructure; performing 5G network coverage; as well as (extremely) low latency levels. At the same time, a few interviewees suggest that operational reliability can be ensured by excluding a complete dependence on coverage, e.g. by foreseeing backups in case of dropouts, as well as hybrid communication. (incorporating short-range and long-range communication systems)

Security, including information security (concerning exposure to cyberthreats) is also highlighted. Direct access to in-vehicle data for third parties would involve a secure interface for ad hoc communication as part of a suggested comprehensive security model i.e. separation between critical (safety-related) and non-critical parts (e.g. convenience-related functions).

What type of risks connected to the safety of non-embedded software (apps) can you identify?

Risks connected to the safety of non-embedded software centre around two areas, namely cybersecurity (in terms of cyber-attacks/hacking) and privacy of data. Given that non-embedded software apps are often seen to have security gaps, they are regarded as potential means for carrying out cyber-attacks. Consequences include: vehicle's affected safe operation; disabled functions; modified software; breach of data integrity/safety; confidentiality concerns; loss/alteration of data.

How will CCAM data be managed and by which players? Can you comment on the role that cloud-based data platforms are expected to cover? How will the ownership of the data evolve? Which will be the challenges to be faced?

A few stakeholders are foreseeing CCAM data being managed by several actors with an emphasis on a user centred approach in data sharing. One specific suggestion is that in the future, the collection of data may shift to providers of mobility (e.g. fleet) services; a few others envisage a concentration of control by OEMs.

Vehicle manufacturers often view data-cloud systems as the only solution to third-party access to in-vehicle data in the context of the current (product) liability regime. On the other hand, aftermarket representatives are sceptical and would only accept neutral-server (independent data trustee) systems as an intermediary solution. In addition, some tend to view such a centralised system (single-access point) as dangerous in terms of cybersecurity. A few stakeholders emphasize that it is more important to regulate data access conditions and that the choice with respect to cloud-based technology is secondary.

In this sense in will be challenging to reach a consensus between the various actors, regulate and develop appropriate technical solutions regarding the issue: on the one extreme (more often aftermarket) services would like to ensure no data-flow blockages (i.e. competition) and there is a need to respect consumer privacy/rights at the same time; on the other hand regulation will have implications for the liability regime: given that OEMs are inclined to ensure product liability to the extent they are in control.

How will cybersecurity in automated vehicles be ensured? Are there practices and approaches you would like to suggest? Which are their pros and con? How can public and private sector work together to ensure cybersecurity?

Interviewees most often invoke the concept of 'security by design' i.e. a division between different layers/systems in the vehicles architecture. On the other hand, some stakeholders suggest that cybersecurity should involve an industry-wide solution given the dynamic nature of the field (which calls for a continuous evaluation of risks). Besides, a few stakeholders view open systems as more secure compared to single-entry point set-ups.

One suggestion regarding best-practices is that the automotive industry could apply existing ones in the IT domain. Another idea is to create information centres/platforms for sharing best practices (e.g. ISAC).

The public sector is expected to operate with aggregated data. Interviewees tend to agree that the outcome (in terms of legislation/regulation) should be the result of cooperation between public and different private actors (across the automotive ecosystem) using end-user's perspective.

12.2.2.4 Legal aspects of automated driving

Which are the most relevant legal impediments to the diffusion of automated driving in Europe? Which are the possible solutions to overcome them? Should these issues be addressed at national or at EU level?

Which are the main legal impediments to the diffusion of potential services enabled by automated driving and the data generated to support it? Can you suggest possible solutions to overcome them? Should these issues be addressed at national or at EU level?

How do you think the liability framework should best evolve to accommodate the uptake of automated driving, at both national and European level?

In case of damage or incident involving an automated vehicle, to which extent the responsibility should be given to the driver, the vehicle as "electronic person" or the car manufacturer? Which are pros and cons for each of the options? Which are the implications on users, insurance companies, OEMs and other stakeholders?

[The questions were generally answered in combination]

It was confirmed by most the stakeholders that the legal framework around liability is not clear and it is an urgent legal impediment. Responsibility should be defined and regulations such as the product liability should be revised. Normally the liability ends up with the driver. But when the driver is taken out, liability ends up with car itself. On the other hand, insurance companies are the future solver of accident disputes between the machine (the OEM) and the driver. Regulation is needed to keep insurance markets functioning with fatalities/accidents. The resolution of the issue of liability can become easier with the installation of black box in the car. Many of the stakeholders welcomed the idea, as a compulsory future legal rule. Proper cause clarification is a prerequisite for correct adjustment of claims.

Artificial intelligence and mainly algorithms should be taken into consideration when establishing the legal framework around CCAM. Notion such as ethical engineering should be addressed at EU level, following the example of Germany. European ethical rules on Artificial intelligence (in general, not only around automotive sector) was discussed.

Additionally, and probably one of the main points which displayed was the regulation of data management, meaning storage, analyse, sharing. transparent standards for the recorded data, (data formats) and regulated access to the data is stressed by many of the stakeholders. All the Member State should consider the requirements of data and privacy protection of the vehicle owner/driver.

It was stressed that we need common standard for common and secure exchange of data, defined at EU level: "Standard for secure data exchange".

Is there a legal framework specifically introduced to regulate CCAM in the member State/States where your organization is established? If so, what does it provide for? If not, what does general liability rules provide for in case of an accident involving CCAM?

Most of the stakeholders did not provide an answer to this question, but all of them stressed the fact that legal certainty and clarity is fundamental. The GDPR was given as an example.

The main point is that it will change how data will be handled, supportive of privacy (critical for consumers' trust).

How does the current liability framework/frameworks applicable to your organization impact the business of CCAM providers? What are the actions that industry players are taking to manage current legal allocation of liabilities?

The question was generally answered when stressing the liability as a main legal impediment, but concrete examples of framework established in EU member states was not given, except in the case of Germany where the insurers are covering both the OEM and the driver in case of accident.

Spectrum allocation

The table reports the allocated/ foreseen frequencies for automotive and transport system applications in the European Union.

Table 12 Allocated-foreseen frequencies, by region

Frequency Range	Usage	Category
13.56 MHz	Passive Keyless Entry	Safety/automated/ADAS
174 – 210 MHz	Digital Broadcasting System (with/without enhanced codec)	Telematics/infotainment/download of HD maps
312 – 315 MHz	Keyless car entry	Safety/automated/ADAS
Various between 400 – 1900 MHz	Commercial wireless services (cellular, GSM, 3G, 4G)	Telematics/infotainment/download of HD maps
433 MHz	Tyre Pressure technology	Safety/automated/ADAS
480-860 MHz	Terrestrial Digital Video Broadcasting (with / without enhanced codec)	Telematics/infotainment/download of HD maps
868 MHz	Key fobs	Safety/automated/ADAS
2 400 MHz	Wi-Fi for Vehicle to Vehicle Communication / maintenance	Safety/automated/ADAS
2 400 - 2 483 MHz	Bluetooth for Vehicle to Vehicle (V2V) Communication / maintenance	Safety/automated/ADAS
3 300 – 3 800 MHz	Vehicle to Network communication (e.g. streaming video, interactive maps)	Telematics/infotainment/download of HD maps
5725 - 5830 MHz	Transport and Traffic Telematics (TTT) applications	Telematics/infotainment/download of HD maps
5795 – 5815 MHz	Road tolling and Smart Tachographs	Safety/automated/ADAS
5 900 MHz	Digital Short-Range Communication	Safety/automated/ADAS
5 875 - 5 905 MHz	ITS safety related applications	Safety/automated/ADAS
5 905 - 5 925 MHz	Future ITS applications	Safety/automated/ADAS
5930 - 6400 MHz	ITS applications	LTE/5G
2405 - 24.25 GHz	Automotive radars	Radar

24.25 - 24.45 GHz	Automotive radars	Radar
24.45 - 24.5 GHz	Automotive radars	Radar
60 GHz	Vehicle to Vehicle communication	Safety/automated/ADAS
63 GHz	Car to roadside communication (e.g. Electronic Toll Collection)	Safety/automated/ADAS
76 - 77.5 GHz	Transport and Traffic Telematics (TTT) applications	Telematics/infotainment/download of HD maps
77.5 – 78 GHz	Ground based short range radar (incl. automotive radars)	Radar

In your opinion, is such allocation adequate to accommodate the needs of CCAM in Europe, including enabled services?

Which aspects of the current allocation do you consider the most problematic concerning CCAM and enabled services? If any, what would you suggest improving such allocation?

In your opinion, what are today the main issues in terms of harmonisation of frequencies allocation between different jurisdictions, considering both differences in terms of Member States and regional differences? How important do you consider spectrum harmonisation in terms of development of CCAM vehicles in the future? Why?

The three questions above were answered by few stakeholders and their input was mostly used to bring adjustments to our table.

ITS in harmonised spectrum allocation means ITS-specific bands, so the default value should be 5.9GHz and unlicensed ITS in 63-64 GHz (mmW) is not mature now. The difference between Member states administrations in CEPT level is that Germany, Austria and Sweden would like 802.11p based ITS-G5 (DSRC) to be default radio access in the 5.9GHz ITS band. However, cellular V2X community would like equal footing and let the market decide the choice of technology. PC5 side link can also be in licensed band. The risk is that this is not harmonized across Europe.

Is there a clearly defined regulation determining the conditions for testing, in real-life environments? Are those rules, if any, set at the European, national or international level? How do they, if any, interact among each other? Do they overlap or is there a clear-cut division of competence among different level of regulations?

As earlier mentioned, standards for testing these systems is crucial to ensure functioning throughout car's whole lifecycle.

Is it difficult to identify the competent authorities and relevant procedures to be authorised to test CCAM vehicles? Is it difficult to obtain such authorisation? If so, why, and how could the existent problems be solved? What kind of CCAM testing is allowed under the relevant regulation (or set of regulations) which is applicable to your organization?

The stakeholders think that testing should be cross border because mobility is cross border and the goal is to have one single market in EU. This would help to have more efficient mapping systems. It was outlined that testing is allowed in most of the Member States, which is seen as a very positive step forward, however a clear definition of the testing requirements is not yet presented Standardize levels of quality signalling and infrastructure should be introduced.

It was clearly stated that there are not testing regulation on EU level. Testing is allowed but no guidance or testing principles are defined, which is something identified as a risk from the stakeholders. Each Member state has its own testing requirements, but they should be standardized across Europe.

It was also stress the need to re-address the type approval directive (describing tests for AD; IT security; observance of data protection requirements) because all responsibilities and obligations related to technical services are provided by the type approval regulation. Information needs to be provided for the periodic technical inspection and market surveillance in a standardized way to ensure the safety of vehicles over the entire lifecycle.

According with data protection legislation, the transfer of personal data is restricted out of the EEA. How does the current legislation impact the data management of CCAM providers? What are the actions that industry players are taking to manage current requirements?

Most of the stakeholders think that this is not the most important issue and that in reality, this aspect will not face problems in terms of regulation.

According with the proposed Regulation for the free flow of non-personal data in the EU, data localisation requirements would be abolished while access rights to competent authorities for regulatory control would be granted. How would this regulation, if approved, impact the data management of CCAM providers, compared to the current legal framework? What is your interpretation of "non-personal data" in a CCAM context?

The question seemed to be difficult to understand and answer from most of the stakeholders was not provided. What was stressed however is the importance of definition regarding the personal vs non-personal data. The border between the two in the context of CCAM is very weak therefore we need a clear separation supported by legal text on EU level. Another point related to personal data is the so called "secondary use of data". The issue pointed out here is the use of data for statistical purposes for example, which are not for the specific need of the customer or does not require real time access.

12.2.2.5 Commercial aspects of automated driving

Are there any commercial impediments to the uptake of automated driving? Which are the possible solutions to overcome them?

Uncertainty with regards to current or future aspects is identified as the main shared impediment to the uptake of automated driving. This varies across different stakeholder groups ranging from vagueness regarding expected standards of performance; legislation: both regarding data provision and automated vehicles themselves (e.g. deployment of AVs on European roads); ROI; as well as the difficulty to estimate future demand. A couple of stakeholders suggest standardisation and adoption of legislation/clearly defined rules and guidelines as a potential solution to avoid delays in deployment of automated vehicles.

High-cost of technologies (and respective price) are frequently identified as a major barrier. One evolution is that these technologies may be perceived as pertaining to the luxury segment (i.e. niche market) thereby considerably downsizing/slowing down market launch. As an alternative to the assumed diffusion of technology across market segments over time, another stakeholder suggests introducing a tax incentive for automated vehicles, making a parallel between increased safety /and reduced emissions (in the case of green-vehicles); a more generic approach involves research and continuous investments. On the other hand, an interviewee suggests that 'patience' will be more problematic than high cost in the sense that market pressures may cause AV technology deployment before it is ready.

One stakeholder emphasizes the importance of ensuring competition/level-playing field regarding aspects such as equal access to data given that it is challenging to foster an evenly distributed/shared value across the value-chain. A couple of stakeholders hint towards shared infrastructure investments as a potential solution.

Can you identify commercial impediments to the uptake of the services enabled by automated driving? Which are the possible solutions to overcome them?

Commercial impediments to the uptake of services often overlap with those concerning the uptake of automated driving. A majority of actors view a favourable cost benefit ratio as a prerequisite for successful service deployment. Another important consideration refers to ensuring fair terms of competition to avoid a (partial) monopolization of the value chain; this will involve a clarification with regards to data access, which is two-fold: involving customer consent and technical solution. In this sense one stakeholder sees the ExVe solution advanced by vehicle manufacturers as the main impediment for service development in the aftermarket. Related to competition, collaboration between different actors is also seen as important by a few interviewees for instance in terms of investment and maintenance of infrastructure (given the high cost associated, will require coordination between public authorities and private actors).

CCAM is developing very fast but to be operational, depends also on the development of adequate road and IT infrastructure. Is this happening at the right pace in EU? Which are the best practices? To what extent automated vehicles will be able to operate outside main cities, where infrastructure is less developed?

This question has only been answered by a small group of stakeholders. One stakeholder points out a heterogeneous situation across (and within) individual member states suggesting that Level 5 automation scenario is unlikely to be achieved in the absence of full road network coverage.

Best practices would include a ubiquitous cellular coverage and as specified by another stakeholder an implementation of both Wi-Fi and cellular C-V2X. Another suggestion concerns road infrastructure measures to ensure efficient and sustainable management of digital and physical infrastructures; collaboration (public-private); as well as the definition of a shared protocol across regions which could be beneficial in terms of sharing/exchanging experience between different players.

Once the car is sold, who will bear the responsibility of protecting the vehicle against software vulnerabilities? Do you think regulation will be required to define roles and responsibilities? At which level?

Responsibility against software vulnerabilities is commonly identified with the OEM/vehicle seller; especially in the case whereby no direct access to in-vehicle data by third-parties is foreseen. Some stakeholders suggest liability should be shared with another party, for instance a digital provider to jointly deliver regular software updates. A majority view regulation as important to delineate roles and responsibilities between different actors and ensure fair competition; in addition, in terms of updates, a requirement for car users to install latest software versions is anticipated. (e.g. as part of a PTI inspection)

12.2.2.6 Discussion on policy actions

Which policy actions do you deem most important to support the uptake of automated driving? Would you see these actions best adopted on a European or on a national basis? Why? Are there aspects that you would instead suggest not to regulate and to leave to the market?

Before even the vehicle became a reality on the road and before to consider issues related to communications, data and consumer, a range of regulatory measurements should be undertaken for: certification, verification and validation of AD. Establishing a list of criteria a vehicle needs to satisfy to comply with the defined AD LV 3,4,5, especially in terms of safety standards, should be stated and harmonized.

Another point that was made is the Ethical engineering. This concept should be addressed at European level. Ethics could be solved through policy measures to clearly identify the AI role in CCAM. There are still open questions to be addressed such as human dignity, personal freedom and security requirements.

Discussion on testing was held, pointing out the positive actions taken by both the Europe and individual Member states to establish testing on the roads. However, work on testing principles, elaborating a set of procedures, (taking example from the braking system test) to ensure CCAM technology onboard of vehicles is tested thoroughly before being put on the consumers' market is the next step. Provide possibility to SMEs consortium testing solutions. Allow testing in real life situation, where it is still not the case, to foster the uptake.

There are different points of view regarding whether to share the data generated by CAD among all value chain stakeholders, aftermarket services and national/EU authorities. What is your opinion? Should the sharing of the data be regulated? What actions should be taken, if any, to guarantee the fair access and at the same time the control of personal data?

Data sharing and management of information was one of the main controversial part of the stakeholder consultation, however it was clearly stated by all the participants that Europe should reach a consensus and choose the right approach between on-board application platform with an open access for all actor or market driven approach by OEMs.

It was noted that if Europe wants to connect the future automated vehicles, European-wide communication standards will be needed. Standardisation of communication between V2V and V2I is crucial for connectivity but also interoperability.

Policy recommendations concerning the operation of the CAD vehicle was also made. Legislation adaptation still need to be done on Vienna Convention and national traffic rules. Stimulate WP 29 Working group for discussion to establish LV 3 and LV 4 on the market. The Highway Code (Behavioural Law) is the responsibility of the national authorities; however, the EU should play a coordinating role.

In terms of Liability a clear legislative rule on liability and redefinition on insurance companies' role was requested. Create guidelines for insurance companies is additional recommendation, that may facilitate the change of insurers business model in a smooth way.

Define cybersecurity principles is one of the main points stressed out during the consultation phase. Guidelines for effective security protocols will reassure the value chain but also the customer.

Policy actions should be undertaken in terms of Infrastructure. It was suggested that Europe should continue to improve infrastructure trough Galileo; 5G. We should also invest in basic road maintenance and good harmonization of road quality in Europe and consider Smart infrastructure only where critical and safety relevant. It was stressed that for the car to be automated, we need nothing else that good basic infrastructure. To introduce

connectivity and VtoI and VtoX, we will need a have investment in infrastructure, which could be a potential bottleneck for the uptake of CCAM.

Another policy recommendation is to create incentives on National level for innovation in mobility projects. As an example, it was given the tax incentive for mobility as a service. During the consultation, the customer was put ahead as a very important part of the CCAM, which is often discarded. The policy recommendation related to this is to develop principles and mechanisms (e.g. public awareness consultations, programs to foster public acceptance of Automated vehicles) to manage public response to potential (and probable) accidents involving CAD vehicles. Keeping the consumer in the eye of developments by ensuring consumer's rights, should be a priority. GDPR will help the consumer to gain control on his own data, privacy and choice of service (or not).

12.2.3 Second stakeholder consultation - validation

12.2.3.1 Taxonomy

It has emerged during the first round of interviews a certain lack of clarity in terms of definition of the terms that are nowadays widely used in the context of CCAM. For this reason, we considered appropriate to provide a concise definition of the major terms that will be used across the present interview guide and the subsequently report.

Please find below a synthetic definition of the concept of Cooperative, Connected, Automated vehicles, as well as of Mobility and Mobility as a Service.

Cooperative: The vehicle interacts directly with each other and with the road infrastructure referred to Cooperative Intelligent Transport Systems (C-ITS). This VtoV and VtoX communication is defined as the cooperative element of the CCAM. Vehicle cooperation is enabled by digital connectivity between vehicles and between vehicles and transport infrastructure.

Connected: The vehicles are already connected devices, meaning that they are connected to Smartphones, having infotainments services, internet and GNSS. A connected car is a car that is equipped with Internet access, and usually also with a wireless local area network. This allows the car to share internet access with other devices both inside as well as outside the vehicle.

Automated: Refers to self-driving cars, autonomous cars, vehicles that can guide themselves without human conduction. It is a vehicle that can sense its environment and navigating without human input. In terms of level of automation, the classification below corresponds to the one established by the SAE International

Automated Driving Standards in the standard SAE J 3016:

- *At level 0, the driver performs all operating tasks like steering, braking, accelerating or slowing down, and so forth.*
- *At level 1, the vehicle can assist with some functions, but the driver still handles all accelerating, braking, and monitoring of the surrounding environment.*
- *At level 2, the vehicle can assist with steering or acceleration functions and allow the driver to disengage from some of their tasks.*
- *At level 3, the vehicle itself controls all monitoring of the environment (using sensors like LiDAR). The driver's attention is still critical at this level, but, in safe conditions, technology allows the user to disengage from "safety critical" functions such as braking.*

- *At level 4, the vehicle is capable of steering, braking, accelerating, monitoring the vehicle and roadway as well as responding to events, determining when to change lanes, turn, and use signals.*
- *At level 5, there is no need for pedals, brakes, or a steering wheel, as the autonomous vehicle system controls all critical tasks, monitoring of the environment and identification of unique driving conditions like traffic jams.*

Mobility as a Service (MaaS): It is a mobility distribution model in which all a customer's major transportation needs are met via a single platform by a single service provider that orchestrates each individual transport service component to meet a customer's end-to-end service expectations. This is enabled by combining transportation services from public and private transportation providers through a unified gateway that creates and manages the trip, which users can pay for with a single account. Users can pay per trip or a monthly fee for a limited distance.

Do you agree and approve these definitions?

Interviewed stakeholders broadly agreed on the provided definitions, the SAE classification. Nevertheless, the reconsideration of SAE levels (current and future) was pointed out by a couple of stakeholders given safety-related concerns. A few emphasised the restrictive definition of MaaS: "alternative to the use of private car"; one interviewee had a remark with regards to the automation levels under autonomous definition, namely that automated cars start to be classified as such from level 3 onwards; a few commented on the definition of "connected": (restrictive definition in case only referring to infotainment; rather enabler of cooperative systems) and intersection/blurred lines with cooperative.

Testing of preliminary findings

12.2.3.2 Partnerships and long-term cooperation

Preliminary finding: *the current evolution in the automotive industry requires a complex set of specific skills which no single player may be in the position of fully cover in the future. This element makes partnerships a vital element to further increase knowledge and know-how across different players of the value chain.*

Investigating this business dynamic with stakeholders, it has emerged that those established partnerships are not a short-medium solution but rather a long-term strategy, developed to allow ultra-specialisation in specific domains.

2.Would you agree with this conclusion? Or, alternatively, do you think that under certain conditions, a specific player can become self-sufficient in the production of future autonomous vehicles?

A large majority of stakeholders interviewed agree with the outlined dynamics in the context of CCAM. Specific instances include collaborations between software and hardware developers, OEMs and TIER 1/2 with regards to developments such as for instance MaaS (mobility as a service), AI as well as integrated support throughout a vehicle's lifecycle. A couple of interviewees point out room for regulation with regards to a certain player becoming self-sufficient (OEMs, mapping and insurance companies). One comment was made regarding to the presence of a "lock-in effect" related to the use of a certain platform/interface, making these partnerships expensive and only worthwhile to be pursued in the long-run.

12.2.3.3 Personal transportation evolution

Preliminary finding: *The automotive industry is moving into the direction of providing mobility services. In this respect, automated driving can be seen as an enabler for mobility as a service. As the offer of new means of transportation increases with the expansion of ride-hailing applications as well as of car sharing services, the emergence of autonomous vehicles could eliminate the difference between the two.*

To what extent do you see this evolution from the current personal mobility offer in terms of transportation to MaaS, including the potential loss of private vehicle ownership happening in the next 10-15 years? In your opinion, what would be the impact on traditional industry players (OEMs)?

Fragmented views were presented. OEMs confirm the importance of this trend by exploring opportunities to engage in MaaS. A few stakeholders mention the differentiation within MaaS between rural and urban areas: on the one hand the popularity of long-distance ridesharing today confirms future trend (including the demographic ageing trend whereby people retire farther away from the urban areas) while on the other hand owning a car may remain a necessity in remote/low-density areas, given that it is harder to reach a critical mass for service providers. One stakeholder (TIER 1) explicitly categorizes contemporary developments of mobility services as urban centric. The role of policy-makers in promoting/incentivizing MaaS was once again emphasized in terms of potential uptake. (in the form of e.g. fiscal incentives, investments in terms of infrastructure). Most stakeholders would agree this the shift from private car ownership is a lengthy process involving social change.

12.2.3.4 Technology availability and mass-marketisation of CAD vehicles

Preliminary finding: *The high cost of the technologies currently needed to implement autonomous features in vehicles, as LiDar and sensor equipment, and the relatively high-price of cars offering autonomous capabilities, have been identified as a major commercial barrier to the diffusion of CCAM. Nevertheless, continuous investments and research (R&D) could potentially help decrease these costs, reducing the impact of this commercial impediment.*

Based on your expertise and knowledge, would you agree with the presented statement? In your opinion, are there any additional aspects which you do not expect to be overcome soon? And if yes, are there any specific aspects that would require (public) funding/support to be efficiently overcame?

Stakeholders' views broadly converge on the idea of a foreseeable democratisation of AD functions in the future. Nevertheless, automated vehicles (including the cost of certain technologies like LiDAR) are expected to remain expensive compared to traditional cars. OEMs as well as some suppliers highlight the importance of sales volumes with respect to this trend: higher market uptake will imply a more favourable cost-structure for manufacturers. An additional consideration is the deployment of CCAM in the form of MaaS ("democratic") or private ("niche/luxury"). Among the unsolved challenges safety regulations have been pointed out as an additional determinant for the cars' future prices.

12.2.3.5 Connectivity and Cooperative Technology

Preliminary finding: *Connectivity is seen as a central element in the context of CCAM. Interoperability between systems has been put forward as an essential element to ensure cross border operation, with regards to, for instance, data format. As a matter of fact, one of the specific policy recommendations that was suggested by different stakeholders included the possibility to harmonize V2I, V2V, V2X communication standards.*

In terms of cooperation among vehicles, C-roads, represents an existing initiative on the European level, which focuses on harmonising C-ITS related deployments. Relevant elements for CCAM include the promotion of hybrid communication technologies, namely ETSI ITS-G5 and existing cellular networks.

Do you believe C-Roads is sufficient as policy initiative or would you see room for improvement? (e.g. additional coverage in terms of member states; more explicit focus on automation rather than cooperation)

It is important to emphasize that almost half of the stakeholders had limited to no knowledge of the C-Roads initiative which led them to conclude more action has to be undertaken in terms of coverage and/or awareness. For the interviewees familiar with the initiative views were fragmented: a few converged on the fact that the platform should be more technology neutral (i.e. with regards to communication technology, as its current preference seems to be ITS G5 over cellular networks). Investing into a V2X protocol is seen as a "promising initiative" by one, and not seen as a priority by other actors: manufacturers will develop their own solutions instead and/or design cars in such a way as to rely less on external connectivity. In a similar vein a couple of stakeholders suggest more involvement/cooperation with industry players. One stakeholder suggests C-Roads should take form of a centralized approach like the air traffic centres/authorities in the aviation industry.

6.In your view, is there enough action undertaken in terms standardization of communication?

With regards to the question of standardization of communication technologies a clear pattern emerges in terms of stakeholders' points of view: while OEMs (and some TIER1) clearly state that it is too early to think about taking action when it comes to standardizing one technology or the other (to ensure interoperability in the future); the aftermarket urges regulators to advance in this respect (with the same endpoint/goal: interoperability).

12.2.3.6 Social Aspects related to CCAM

Preliminary finding: *It has been underlined during different interviews that social acceptance will play a major role in fostering – or reducing – the uptake of autonomous vehicles, depending on how customers will judge the reliability, safety and trustworthiness of future cars. [probe for social acceptance of accidents involving autonomous vehicles]*

7.Based on your expertise and knowledge, what is your opinion on this aspect? Would you agree that social acceptance is a necessary enabler for the uptake of high levels of automation?

Consumer trust and acceptance are unanimously seen as an enabler for the diffusion for automated driving technologies. Nonetheless, when it comes to discussing the implications, stakeholders' views are divergent: policy actions/regulation, informative/communication

campaign (government and private initiative) while a minority does not see social acceptance as a "real" barrier to uptake (at this stage). A few interviewees mention that guaranteeing safety (e.g. against stringent testing standards; addressing cybersecurity issues) will be critical while confidence in the technology itself will come over time.

Preliminary finding: *Consequently, customers may base their purchase choice considering social and personal beliefs rather than pure commercial and technical aspects of the vehicle.*

8.On this point, do you believe a policy action should be taken to create awareness on reliability, safety and trustworthiness of automated driving, once these will be demonstrated? Or do you think this activity should be left to the market?

Most agree support from public sector is required. Agreement on safety and standards needs to be reached between the industry and policymakers, and this will require at least guidelines (e.g. in the form of uniformly applied terminology) and a legal framework for regulating emerging CCAM related-concerns (e.g. ethical, responsibility aspects) at the other end of the spectrum.

Preliminary finding: *Cybersecurity, both at vehicle system level and at infrastructure system level (e.g. OEMs network security) has been indicated as one of the key concerns that could affect future autonomous vehicles. While part of the industry supports a standardized – and potentially certified – universal standard of security, others advocate a heterogenous system represented by proprietary standards.*

9.Which do you consider to be the most appropriate solution? Would you be able to identify the pros and cons of each proposed solution?

Suppliers emphasize the importance of information sharing and are more inclined towards an "in-between the two solutions": heterogeneous proprietary standards are supposed to be a harder target for cyber-attackers, but some minimal/generic standards must be set in place? OEMs warn against standardization which may potentially disincentivize manufacturers and opt for some limited standardized requirements (e.g. security by design in development phase) and best practice sharing platforms. In contrast the aftermarket advocates one or more standardized solutions, publicly certified systems with a possibility for independent certification once again stressing the importance of "a common language" i.e. interoperability.

12.2.3.7 Legislative framework

Preliminary finding: *The C-Roads Platform provides documents such as "Test infrastructure operational document", which presents testing detailed use-cases focused on C-ITS. On the other hand, during the initial consultation, it was highlighted that testing requirements and best practices at European level are still lacking in terms of testing and certification of CCAM.*

10.Based on your experience and knowledge, do you consider initiatives such as the C-Roads Platform inclusive enough in terms of information and data on testing provided? Do you think that additional effort should be made to focus not only on the cooperative aspect of CCAM, but also on the automated one?

OEMs emphasize the need to move to operation (on public roads) as opposed to mere testing. Others acknowledge the importance of standardized testing and the lack of certification. (clear regulatory pathways and comparability).

Preliminary finding: *The Vienna Convention on Road Traffic regulates the admission of vehicles in international traffic and harmonises traffic rules across countries. The amendment of the Vienna Convention (VC) was initiated in early 2014 by Austria, Belgium, France, Germany and Italy and currently allows testing since its latest update in March 2016. The introduced changes allow Member States to perform testing of automated vehicles and to adapt their national road regulations. However, the current version of the Convention does not remove all barriers to automated vehicles, since full operation is still not allowed.*

11.Based on your experience and knowledge, do you consider as a necessary condition for the mass-market use of CCAM a further amendment of the Convention? If yes, what should be ideal timeframe?

Further Vienna Convention amendment for testing and large-scale operation is required (it was remarked that it will be a time-consuming process that has to start as soon as possible). Harmonization amongst member states will be important to ensure cross-border operation. One stakeholder points out to the "paradox of VC" namely that non-signatory states have much more room for manoeuvre compared to current VC road-traffic regulating countries.

12.2.3.8 Ethics

Preliminary finding: *The German Ethics Commission Guidelines, released in June 2017, focused on higher levels of automation (LVLs 4 and 5). The document includes a list of 20 ethical rules covering issues related to human dignity, personal freedom and security requirements. It acknowledges that some dilemmas cannot be clearly standardized, but that technology should be designed in such a way as to avoid these critical cases from arising in the first place.*

12.Do you think that the German example should represent an example to follow at European level? To what extent do you see ethical engineering and the role of AI in CCAM addressed through policy measures, potentially at European level?

-
- Most stakeholders view ethical questions as an important aspect to be addressed in the context of CCAM. Stakeholders were only marginally aware of the guidelines issued by the German Commission. Among these interviewees the majority agreed it is a good starting point. One stakeholder points out that ethical questions can be stepped aside when the objective is to maximize functional safety.

12.2.3.9 Liability

Preliminary finding: *After the stakeholder consultation and additional academic research, the following conclusions were reached concerning liability issues related to CCAM:*

- *Up to SAE level 2, human drivers are required to monitor the systems and should remain liable (fault-based liability). However, systems should be designed to ensure the driver's sustained attention;*
- *From SAE level 5 onwards, drivers are not required to monitor their vehicles. They should be allowed to engage in other tasks if they are ready to take over again. In this case, the vehicle manufacturer or road operator could be considered liable for any accident (fault-based liability and product liability);*
- *From SAE automation level 3 onwards, liability in case of accident or infringement to the highway code needs to be redefined and clearly communicated to the users.*

Based on your expertise and knowledge, would you agree with this approach?

Level 3 is flagged as the most problematic one in terms of liability: one stakeholder views it as a "peak" rather than a progression. Some agree to a direct transition to Level 4. There is a broad agreement that higher levels of automation will at least involve additional actors (besides the human driver) if not involve a transfer of responsibility to the software/hardware manufacturer.

The EC intends to issue a guidance document on the interpretation of the Product Liability Directive by mid-2019. Based on your expertise and knowledge, do you think this would help the clarification on liability issue? Do you think that there are still gaps in the liability definition for CCAM?

The largest share of interviewees does not have an opinion/clear view on the subject. Others highlight the need for further clarification (since the guidelines are not yet available and/or may create additional confusion) e.g. in terms of liability corresponding to each level of automation. There is a split between aftermarket players: on the one hand, there is a call for revising the PLD to cover full lifecycle, while on the other, (IE) insists to preserve the status quo.

For SEA level 3 onwards, UK is opting for Automated and Electric Vehicle Bill, making it compulsory for users of automated vehicles to have insurance that covers the technical failure of the AV technology. It therefore places a first insurance liability on users including damages caused to the driver in AVs who are legitimately disengaged from the driving tasks. When an accident is caused by an automated vehicle when driving itself, an insured person or any other person suffers damage because of the accident, the insurer would be held liable.

Based on your expertise and knowledge, would you agree with this approach as a solution to be considered at EU level?

Divergent views were brought forward. While some stakeholders welcome the idea of compulsory insurance, with one stakeholder suggesting a European Insurance, others opt for a preservation of the heterogeneity of liability regimes.

12.2.3.10 Data – collection, management and use

***Preliminary finding**: As future vehicle will allow the generation and collection of an extensive mass of data, the management as well as the access and control of it will need to be clarified, as per today, there is no a consolidated approach on this topic. Depending on the type of data, different policies could be followed, corresponding to different degrees of privacy, security and commercial use.*

Consequently, some stakeholders highlighted the need to differentiate between technical/non-technical and personal/non-personal, and to categorise it by flow (in/in; in/out; out/in) and by type (emergency/infotainment/repair and maintenance).

Based on your knowledge and experience, do you agree that different categories/types of data should be clearly defined? Do you think that the ones mentioned above is the right sort of categorisation?

The importance of defining a categorisation was underlined, as a reasonable starting point. A couple of stakeholder's stress that a clear understanding of the data available is an essential step that must precede the categorization itself. Even though personal data is defined by the GDPR (according to most), one stakeholder points out that under WP29 categorization would be redundant as all data leaving the vehicle falls into this category. Additionally, suggested categories include public/critical relevance.

Based on your knowledge and experience, do you agree that there should be specific policies dealing with specific categories of data?

Amongst the minority of interviewees who expressed their view, positions are divided: some do not see room for additional legislation, while others admit there is a need for additional clarification, including definitions of categories.

Based on your knowledge and experience, where do you consider the main gaps in terms of data regulation? What could be the impact?

In addition to views presented above, some stakeholders chose to further elaborate on the complexities with regards to: categorization (which must account for various actors' business models) and transparency (questioning the scope of GDPR).

***Preliminary finding**: In terms of access to vehicle data, a bipolar situation has been described by the stakeholders: on the one hand aftermarket services demanding full, unrestricted, real-time access to in-vehicle data, to generate new business opportunities. On the other hand, OEMs, under the justification that unrestricted direct in-vehicle data access could increase the likelihood of security issues, proposing intermediate solutions, including neutral players, from where data could be retrieved.*

Based on your knowledge and experience, to which extent do you believe a third-party data provider as the one suggested by car manufactures would be appropriate in terms of type and amount of data?

Security concerns lie at the core of the debate concerning data access. Most stakeholders are sceptical about the existence of a solution able to bridge the two concerns: the monopolization of data by manufacturers on the one hand (to the detriment of the aftermarket) and the vehicles potentially compromised (cyber-)security. While a couple of stakeholders see the neutral server solution as a potential solution, others question the possibility of real neutrality in the case of a profit-driven entity's control.

If you do not agree with the proposed solution of an extended service, do you believe the security risk could be overcome, by players receiving full access to in-vehicle data (e.g. aftermarket players)?

Once again interviewees stress the cybersecurity and safety concerns related to third party access to in-vehicle data. Neutral server is a hinted "way forward" although stakeholders emphasize the technological limitations (optimistic scenario: to be resolved in long-term perspective) e.g. limited processing power and the respective need to focus on applications which directly contribute to the driving task.

***Preliminary finding**: In the first phase of the consultation, it was widely agreed that customers should have the choice and the possibility to decide which 3rd party entity can have access to a set of data. Customers should know for what their data is used, by who and for how long.*

However, some data sets are re-used for purposes others than commercial ones, such as studies on traffic management; aimed at improving the common social benefit. In this case, a legitimate interest cause is in place and customers consent is not required. In this frame, who and how decide the legitimacy of the use is today under discussion. While different stakeholders expressed the opinion that customers should be entitled to differentiate between legitimate and illegitimate reasons to access their data, others would delegate such a task to a neutral body.

21. Based on your experience and knowledge, what is your feedback on this issue? Do you think that a public consultation regarding the customer opinion on the matter could be useful? Do you think that an impact assessment will be useful to find a solution on data access and management?

A few stakeholders shared their views about on this matter. Half see room for impact assessment and to a limited extent public consultation to support regulation; the other half mention additional aspects such as competition to contribute to policy development.

- **Future business models' validation**

12.2.3.11 Scenario characterisation and issues identified

***Preliminary finding**: As part of the analysis conducted in the framework of the study, a set of potential scenarios covering the evolution both in terms of uptake and modification of the current value chain have been developed. Those are based both on the inputs provided by the stakeholders during the first round of interviews and through business intelligence and research activity.*

These scenarios have been built on the concept that a series of challenges, of technical, legal and commercial nature, will need to be overcome to ensure a full integration of autonomous and connected vehicles in the future society. The challenges were identified during the first round of interviews by the stakeholders, and they have been characterised in "enabler", meaning their solution is essential to ensure future development of CAD vehicles, and "differentiator", meaning that depending on how they will be solved, different players of the current automotive value chain will be affected. The following 4 scenarios were finally developed:

1.Scenario 1, unsolved technical issues. In this scenario, technical issues, considered an enabler for a solid uptake of CAD in the mass market, will not be overcome.

2.Scenario 2, technological progress in a low-regulated environment. In this scenario, although technical issues will be positively solved, legal issues, also considered an enabler for a solid uptake of CAD in the mass market, will not be overcome.

3.Scenario 3, technological progress, implementation enables and unregulated data access. In this scenario, both technical and legal issues will be resolved, although data access, a key issue in the evolution of the future business models of the automotive sector, will not be regulated.

4.Scenario 4, technological progress, implementation enables and regulated data access. In this last scenario, together with technical and legal issues, access to data will be regulated.

Table 13 Scenario characterisation

Type of issue	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Technical Issues ***Enabler***	✗	✓	✓	✓
Legal Issues ***Enabler***	✗	✗	✓	✓
Commercial issues ***Differentiator***	✗	✗	✗	✓

A short description of each issue is described below:

Table 14 Issues description and scenarios characterisation

Type of issue	Issues
Technical Issue ***Enabler***	**Artificial Intelligence** Artificial intelligence will represent an essential technology to achieve level of autonomy above level 3, in which the vehicle is responsible of taking independent decision based on real time data from sensors and previous knowledge acquired and analysed independently by vehicle itself. The challenge is to improve artificial intelligence algorithms enough to guarantee safe operation for automated vehicles.
Technical Issue ***Enabler***	**V2X communication technology** A safe, reliable and cost-effective vehicle to vehicle/ vehicle to infrastructure communication technology will be a fundamental condition to enable the uptake of autonomous vehicles, particularly for level 4 and level 5.
Technical Issue ***Enabler***	**Infrastructure upgrade** Future autonomous vehicles will require upgrades of the current road infrastructures. This will include road conditions (signalling, marking), communication infrastructures (broadband coverage) as well as satellite positioning technology.
Technical Issue ***Enabler***	**Positioning technology** Future Autonomous vehicles will require high performances positioning technology, capable of ensuring both high accuracy and reliability across different environment.
Technical Issue ***Enabler***	**Cybersecurity (at vehicle and network system level)** Cybersecurity both at vehicle level and infrastructure level is defined as the full protection from unauthorised access to in-vehicle data and functionalities, including safety related applications.
Legal Issue ***Enabler***	**Definition of a liability framework for automated driving** The more automated will be the vehicle, the less scope there is for negligence liability to be placed on the driver within existing legal frameworks.
Legal Issue ***Enabler***	**Case and Role for Event Data Recorders** Event data recorders could potentially help aftermarket players (e.g. insurances) in developing new business in relation with CCAM. Nevertheless, privacy and legal issues may arise.
Commercial issues ***Differentiator***	**Access to vehicle Data** Access to in vehicle data will represent a vital element to ensure the provision of new services. OEMs, as the current providers of the in-vehicle data architectures, will enjoy a preferential access to in-vehicle data, and on the ground of cybersecurity concerns, they could limit the access to this data to third parties.
Commercial issues ***Differentiator***	**Willingness to pay by end users** As the introduction of autonomous features could potentially increase the final price of vehicles, customers may, or may not, be inclined to spend more for CAD features.

Based on your experience and knowledge, would you agree with the issues identified and the proposed scenarios derived from them? Would you suggest any further issue to be investigated and included in the scenarios? Do you think that some of these issues require policy action at European level to overcome them?

Most stakeholders found the approach comprehensive in terms of issues identified. A few stakeholders have an optimistic outlook in terms of a transition from scenarios 3 to 4 within a timeframe of 10-15 years. (required policy action) One stakeholder strongly disagrees with the classification of V2X technology as an enabler to autonomous driving: according to them, (external) connectivity and automation are parallel tracks.

Preliminary finding: *We identified the positive overcoming of the technical challenges identified in Scenario 1, as very probable, considering the constant technological evolution that has always characterised the sector. In a similar way, we consider realistic a positive outcome of the legal challenges presented in Scenario 2, potentially in the next 5-10 years. Finally, we identified in the commercial barriers included in Scenario 3 and Scenario 4 the elements characterised by the highest level of uncertainty, in terms of which one would prevail.*

23.Whenever possible, would you be able to provide an estimation of which scenario do you consider the least/the most truthful one, based on your expertise? Do you consider there are additional factors, beside the ones identified, that could impact one or more scenarios? Would you be capable of providing an indicative timeline for each Scenario? And finally, do you believe that Scenario 2, 3 and 4 could realistically happen also without the support of the public sector, e.g. at European level?

A couple of stakeholder view scenario 3 as the most truthful. One sees scenario 2 and other agree that regulation (e.g. a European legal framework) will play an important role for instance by encouraging shared mobility; data regulation (potential to set-back technology); facilitating testing; public awareness/feedback with regards to technology. In terms of specific timeframes, a single stakeholder provided feedback: according to them, deployment will happen within 2-3 years through early adopter cities with a gradual expansion in the next decade.

Preliminary finding: *While Scenario 1 and Scenario 2 involve the overcoming of technical and legal issues, the element differentiating Scenario 3 and 4 reflect the different way in which data will be managed, providing the opportunity to exploit vehicle and road data also to service providers actors in Scenario 4. For this reason, while Scenario 1 and 2 mostly affect the forecasted uptake of CAD vehicles, Scenario 3 and 4 mostly differ in terms of value chain modification. Consequently, our conclusion is that in Scenario 4, a regulated access to data will allow the creation of an ecosystem of new / transformed companies oriented toward the exploitation of the data economy.*

24.Based on your expertise, would you agree with this preliminary conclusion? If not, what would be your major concerns on the presented conclusion?

No stakeholder was able to provide a specific answer to this question except for one comment which approved of the general approach.

12.2.3.12 Profit Pools and Forecasted Business Models

Preliminary finding: *In an effort to identify the future business models that will characterise the way of doing business of the players of the automotive sector, we analysed how the current major profit pools of automotive industry will evolve in the future, trying to identify which players of the supply chain will be in the best position to exploit them. Five main profit pools were analysed, namely:*

a.Hardware components
b.Software
c.Vehicles manufacturing
d.Service provision – aftermarket
e.Service provision – mobility providers.
We conducted our analysis taking in consideration 5 main categories of players, 3 "traditional" - Suppliers, OEMs and Aftermarket providers - and 2 "innovative", - Tech players and Mobility Providers-.

We observed that depending on the scenario analysed, different players of the value chain could benefit from the identified profit pools. We foresee that in Scenario 1 and Scenario 2, where technical and legal barriers are respectively solved, an increasing role will be played by high-tech companies, although no major changes will occur at downstream level. On the contrary, Scenario 3 and 4 could heavily affect the automotive value chain, depending on the degree of access to in-vehicle data that will be granted to downstream players, as mobility services providers and aftermarket.

We identified in Scenario 3 a strong role for OEMs, with their business moving from hardware and vehicle manufacturing to software and service provision, with the consequence loss of market power for aftermarket and software component players. On the contrary, we identified growing opportunities – and growing importance in the value chain – of aftermarket players, including mobility provider, in scenario 4, that foreseen a regulated access to vehicle data to all the players.

25.Would you agree with the identified profit pools? Do you consider any additional area of profits should be taken into consideration, due to its relevance for the future CAD sector? and do you agree with the suggested foreseen evolutions in terms of role of different actors in the value chain?

A few stakeholders have explicitly agreed to the statements put forward. There is no clear view with respect to OEMs engaging in provision of mobility services. The importance of data in terms of profit pools is emphasized by a couple of stakeholders. Another stakeholder stresses the difficulty of estimating the future, but from their perspective/position in the value chain: in the 10-15 years the market will become more B2B with data playing an important role in terms of profit-pools. (in addition to car selling and servicing)

26.It could be argued that as OEMs could potentially see a decrease in their market power in Scenario 4 in favour of aftermarket and service providers players, they could become less prone to invest in CAD technology, with an important impact in terms of CCAM development and consequent. What is your point of view on this aspect?

Many stakeholders were unable to provide specific feedback on this aspect. Remaining views are divided: while some foresee OEMs maintaining a strong position even in the context of their investments in CAD, another view acknowledges the possibility of a scenario whereby most profits are derived by various platforms.

12.3 Annex C: Mapping of strategic orientations

12.3.1 Introduction

The following Annex will present an overview of the most recent actions taken by national Governments, European and International Institutions with respect to CCAM. The goal of the next chapters is to identify the strategic orientations of the different actors on the issues identified, so to provide an up-to-date overview of the current and near-future legislative framework at national, European an international level.

12.3.2 Liability

12.3.2.1 International level

At international level, although liability and responsibility are beyond the remit of UNECE and WP1, guidance is provided on how a set of general provisions with regards to compliance with traffic rules and driver behaviour could be issued.

Relevant on this issue is the document "*Automated Vehicles: Policy and Principles Discussion Document*", prepared by the experts from Germany, Japan, Spain, the Netherlands and the United Kingdom of Great Britain and Northern Ireland and included in the United Nations Economic Commission for Europe Informal Documents for the 75th session of the global forum for road traffic safety (wp.1).

The document provides preliminary indications on how (although liability and responsibility is beyond the remit of UNECE and WP1), a set of general provisions with regards to compliance with traffic rules and driver behaviour could be issued stressing how CP can use their national traffic rules to provide details. Furthermore, it underlines how assigning criminal and civil liability in the event of a traffic violation or a collision involving an automated vehicle goes beyond the scope of the International Road Traffic Conventions. Finally, it underlines how CPs should, in accordance with their domestic circumstances, ensure that legal regimes are adapted/created to address civil & criminal liability issues in relation to incidents that involve the use of Self-Driving Systems.

12.3.2.2 European level

At European level, the European Commission has just evaluated the Product Liability Directive and as a follow-up, it will issue an interpretative guidance clarifying important concepts in the Directive including in the light of technological developments.

Furthermore, the Commission is proposing to regulate data recorders for automated vehicles as part of the revision of the General Safety Regulation for motor vehicles, to clarify who was driving (depending on the level of automation of the vehicle, the driver or the vehicle itself) in case of an accident.

Furthermore, on this issue, the study "*A common EU approach to liability rules and insurance for connected and autonomous vehicles*" produced by the European Parliamentary Research Service and published on February 2018, accompanying the European Parliament's legislative own-initiative report, provides a preliminary differentiation between the various type of risks related to CCAM.

The document distinguishes between 4 categories of risks: software failure, network failure, hacking/cybercrime and programming choice which the PLD and MID do not address. In terms of recommendations, the document recommends no amendment to PLD

but close collaboration between MSs liability regimes (to ensure timely victim compensation).

Concerning the use of event data recorder, the European Commission, in the document *"GEAR 2030 High Level Group on the Competitiveness and Sustainable Growth of the Automotive Industry in the EU- Final report",* foresees the inclusion of mandatory requirement for event data recorders in type-approval legislation.

12.3.2.3 National/regional level

At national level, different Member States are currently working on action plan to address the question of liability in the context of automated vehicles.

Austria, in its recent action plan "Automated - Connected – Mobile", also addresses, among other issues, the question of liability, through the development and prioritization of use cases.

France has addressed in its strategic document "Development Des Véhicules Autonomes Orientations stratégiques pour l'action publique" the question of liability, underlying the need to develop a legal framework to be completed before 2020/2022, capable of addressing the liability concerns that will emerge with the spreading of AVs.

Furthermore, in the document "*New France for industry",* different issues concerning automated vehicles, including the question of liability are evaluated, underlying the need for a reform/update of the liability framework.

Germany, as one of the most advanced countries in terms of adopting of CCAM-related legislation, has recently amended the Road Traffic Act, to recognise the automated driving systems in vehicles with high automation. In terms of liability, the allocation of fault and liability (i.e. whether the driver was vigilant to take control of the situation or the accident was caused based on failure of the system when the driver was relying on it properly) are to be ensured by the inclusion of a black box in automated driving systems vehicles, concluding that liability towards an accident victim would still be governed by the existing German car owner framework putting the liability with the vehicle owner.

In **Sweden**, as recognised by a study by European Parliament Research Service, a proposal for regulation for the testing of autonomous vehicles has evaluated that the laws on compensation for traffic accidents can be applied to all levels of automated vehicles.

Finally, in the **United Kingdom**, In the end of January 2018, the Automated and Electric Vehicles Bill has been scrutinized by the House of Commons and has been passed to the House of Lords. in situation in which a vehicle is driving itself, meaning that it "is not being controlled, and does not need to be monitored, by an individual, the liability of the insurer can be limited in case of an accident resulting from unauthorised software alterations or failure to update software.

12.3.3 Certification

12.3.3.1 International level

At **international level**, driven by the initiative taken by OICA[118] a Task Force on Automated Vehicle Testing (*AutoVeh*) was set up within the ITS/AD informal working group under the UNECE World Forum for Harmonization of Vehicle Regulations (WP.29). The objective of this task force is to develop an extension of the certification framework to accommodate automated driving requirements.

More into details, the task force has been established to investigate testing/assessing the functionality of automated driving systems. It includes many CP and affiliated bodies, presenting a widest approach to the regulatory solutions and outcomes, with a 2-3-year time frame (draft regulatory proposals should be submitted to the June 2020/181st Session of WP29). The expected outcome of the Task Force is a regulatory test regime with adoption and lead times that could be implemented for new registration by 2022-2023. The initial structure of the draft regulation includes, as initally proposed by OICA, three elements:

- Classical physical certification tests,
- Real-world driving tests,
- and audits of manufacturer compliance with industry standards, best practices, and methods to ensure software integrity and cybersecurity, based on self declarations leveraging on internal testing, including simulations and virtual testing.

The logic of this certification framework is to be **additive** to the current one, which focuses on the certification systems of components, whereas he new framework will focus on automated driving software and functionalities.

In this perspective, it is important to stress that while the main focus of the current framework is safety, both safety and security will be relevant for certification regarding automated driving and software. In this frame, relevant activities are ongoing at standardisation level:

- ISO is currently conducting a revision of Revision of ISO 26262 and SOTIF autonomous driving standard, that will complement the ISO 26262 (Safety of the Intended Functionality) with ISO/PAS 21448, explicitly addressing autonomous vehicles by defining a minimum set of requirements for automation software.

Work is ongoing on the drafting of standard ISO SAE 21434 - Automotive Cybersecurity Standard, to fill in a gap in the current cybersecurity framework not addressing automotive cybersecurity[119].

---

[118] OICA, the Organisation Internationale des Constructeurs d'Automobile, has produced, in the document "certification of automated vehicles, Document No. ITS/AD-12-11" ,a set of recommendations that includes the proposal to augment existing certification process to accommodate AV software functionalities as well as introducing the concept of multiple systems and technologies (horizontal) and the approval system to account for traffic scenarios beyond the scope of traditional testing.

[119] Work started in October 2016. A Working Draft was issued in April 2018, and release is expected in late 2019 or early 2020.

12.3.3.2 European level

At European level, the European Commission declared that it will work with Member States on guidelines to ensure a harmonised approach for national ad-hoc vehicle safety assessments of automated vehicles. Furthermore, the European Commission has expressed its interest in initiate activities with the Member States and stakeholders in order to develop a new approach for vehicle safety certification for automated vehicles.

In its communication on "the road of automated mobility: An EU strategy for mobility of the future" the European Commission has presented its new EU vehicle approval framework, that for the first time combine vehicle approval rules with market surveillance rules. The Commission aims to start working on a new approach for certifying the safety of automated vehicles starting from this new framework.

The European Commission, in its document "*Study on the assessment and certification of automated vehicles, final Report",* provides recommendations aimed at addressing the future assessment and certification of automated vehicles.

Firstly, the document advocates for support for amendments to UN Regulation 79 to allow the approval of Automatically Commanded Steering Functions (ACSF), in particular the Lane Change Assist (LCA) and enhanced Lane Keep Assist Systems (LKAS).

Secondly, concerning the interpretation of the existing assessment procedure for the safety of complex electronic systems (CEL annex), it proposes solutions that include involving Technical Services early in the development process. (audit and report template).

Third, to ensure operational safety of ACSF under all real-world driving conditions, it underlines how requirements similar to SAE L3 (driver monitoring system) should be imposed.

Fourth, it calls for requirement of comprehensive assessment (possibility to occur in ODD) to be either integrated into existing UN Regulation 79 or in a new horizontal regulation for AVs.

Finally, it reiterates how manufacturers should prevent foreseeable driver misuse, through a long-term strategy including the development of appropriate requirements and horizontal regulation for driver monitoring.

In addition to the point presented above, the European Commission document ""*Study on the assessment and certification of automated vehicles, final Report"* also provides indication to cover all safety-relevant scenarios, including the requirement for the collection of "*event, incident, and crash data, for the purposes of recording the occurrence of malfunctions, degradations, or failures in a way that can be used to establish the cause of any such issues*", under the concept of Data Storage Systems for Automated Driving.

Finally, the document gives an insight also on Over-the-air (OTA) software updates, stressing that responsibility regarding vehicle's compliance with legislation should be clarified. As well as underlying that OTA updates could be limited to non-critical functions given cybersecurity concerns. Finally, the document foresees that software checks could also be performed during PTI.

12.3.3.3 National/regional level

At national level, different Member States are currently working, or are planning to work, on documents clarifying the testing requirements and certification at national level.

Germany Federal Ministry of Transport and Digital Infrastructure, in its recently published document *"Action plan automated and connected driving",* advocates for the need of developing standards for automated driving, as well as to close gaps (i.e. standardised testing certification and procedures) in the field of testing to be potentially concluded by mid-2019.

12.3.4 Testing on Roads

12.3.4.1 International level

At international level, testing on road has not been covered in terms of legislative acts/strategic orientation, as it involves direct consequences on national / European legislation.

12.3.4.2 European level

In terms of testing on road, the European Commission will support demonstrations and large-scale testing currently ongoing in different Member States, through research funding programme, deployment projects and providing coordination of cross-border testing. From a budget perspective, for the period 2014-2020 a total budget of around EUR 300 million has been allocated for these activities. In addition to that, additional call for proposals for projects covering automated road transport are planned for the period 2018-2020, with a total budget of EUR 103 million.

12.3.4.3 National/regional level

At national level, different Member States are currently working, or are planning to work, on documents clarifying the national legislation to allow on-road testing.

The following list has therefore to be considered as non-exhaustive, aiming only at providing an overview of the major actions taken in the recent months by different member States.

France Ministry of Sustainable Development has recently published the document "Développement des véhicules autonomes - Orientations stratégiques pour l'action publique" that provides initial guidelines aimed at addressing the current French Legal framework to authorize on-road testing, as well as endorsing the "system-horizontal framework" UNECE approach to testing.

Spain Directorate General of Traffic has published, in April 2016, the document "*Instruction 15/V-113: Authorization to conduct tests or research trials of automated vehicles on roads open to general Traffic",* amending the current road traffic legislation to allow urban and interurban on-road AV testing.

Finland, in the strategic document "*Road Transport Automation Road Map and Action Plan 2016–2020",* foresees the opportunity of having on-road testing allowed through test plate certificates (SAE 0-5), with driver either inside or outside vehicle.

Finally, **Austria** Federal Ministry of Transport, Innovation and Technology (BMVIT) has recently presented the national action plan "*Automated - Connected - Mobile" Code of Practice,* foreseeing the development of a framework to ensure safe (gradual) on-road testing for Avs.

12.3.5 Cybersecurity

12.3.5.1 International level

At international level, UN Task Force on Cyber security and OTA issues (CS/OTA) is currently investigating the best solutions to best address the issue of cybersecurity in the context of autonomous vehicles.

A first set of guidelines introduced in the draft paper on "*Recommendations for Cyber Security"* has been published in May 2018, providing insights on how horizontal regulation should include requirements to produce a certificate of compliance for the cyber security management system of the vehicle manufacturer, as well as adopting a vehicle type approval procedure regarding cyber security.

12.3.5.2 European level

At European level, the European Commission is proposing to regulate the protection of vehicles against cyber-attacks as part of the revision of the General Safety Regulation for motor vehicles.

The European Commission aims to implement a pilot on common EU-wide cybersecurity infrastructures and processes needed for secure and trustful communication between vehicles and infrastructure for road safety and traffic management related messages, in accordance with the already published guidelines on certification and security policies.

12.3.5.3 National/regional level

At national level, different Member States are considering legislative actions and principle to address the issue of cybersecurity in current and future autonomous vehicles.

France Ministry of Sustainable Development, in its recently published document *"Développement des véhicules autonomes - Orientations stratégiques pour l'action publique"* illustrates different guidelines to ensure cybersecurity, as integrating technical regulation and developing threat analysis through a working group including national and international representatives of the automotive industry.

Similarly, the UK government has recently presented a document, "*The Key Principles of Cyber Security for Connected and Automated Vehicles",* introducing a series of 8 principles out how the automotive sector can make sure cyber security is properly considered at every level.

12.3.6 Access to data

12.3.6.1 International level

At international level, no action has been taken, at the best of authors' knowledge, on the issue of access to in-vehicle data. One of the potential explanation for this can be found in the high degree of heterogeneity that characterises the data and privacy legislative framework among single States.

12.3.6.2 European level

The European Commission will continue monitoring the situation on access to in-vehicle data and resources and will consider further options for an enabling framework for vehicle data sharing to enable fair competition in the provision of

services in the digital single market, while ensuring compliance with the legislation on the protection of data.

Nevertheless, the Commission has clarified that it does not intend to provide, at least for the year 2018, any mandatory requirement for car makers on the issue of access to in-vehicle data. The Commission postponed the discussion on 2019, when it plans to issue a governance framework setting out its recommendations for data sharing, following further discussions.

Furthermore, on the issue of access to data, the European Commission has presented, in its report *"Access to In-vehicle Data and Resources Final Report"*, three technical solutions for the access to in-vehicle data and resources, including the following technical architectures: Data Server Platform, In-vehicle Interface and On-board Application Platform.

Following this document, the European Parliament, in its "*Draft Report on a European strategy on Cooperative Intelligent Transport Systems",* urged the European Commission to take legislative action on access to in-vehicle data and resources before the end of 2018.

12.3.6.3 National/regional level

At national level, cybersecurity is being discussed as one of the many areas in which future legislative action may be required.

France Ministry of Sustainable Development presented in its document *"Développement des véhicules autonomes - Orientations stratégiques pour l'action publique"* the necessity of building a framework capable of ensuring on the one hand security, traffic management and other actions and on the other hand, the development of mobility services.

12.3.7 Infrastructure evolution

12.3.7.1 International level

Although different Organisations have agreed on the importance of modern, fit-for-purpose road infrastructures to ensure a rapid and solid uptake of CCAM across Europe and internationally, no relevant and specific strategic orientations have been provided on this topic, mostly due to the national and European dimension of the issue.

12.3.7.2 European level

At European Level, while most of the investment will come from the private sector, the EU provides significant stimulus for and innovation and for deployment of targeted infrastructures.

The Connecting Europe Facility (a total of EUR 443 million triggering EUR 1.173 million of total investments) has positively contributed to the digitalisation of road transport infrastructures across different Member States, supporting automation.

Furthermore, to allow the creation of partnerships and synergies between the transport, telecom and digital part of Connecting Europe Facility, the Commission has declared its interest in including a coordinated call for projects in its 2018 work programme for Connecting Europe Facility.

12.3.7.3 National/regional level

France Ministry of Sustainable Development presented in its document "Développement des véhicules autonomes - Orientations stratégiques pour l'action publique" the interest in developing a framework ensuring from one side the safety of road users and, on the other, the efficient traffic management. Furthermore, the document advocates for the development of a plan to ensure connectivity across the road infrastructure.

12.3.8 Technical challenges

12.3.8.1 Introduction

The following section will present the actions that national governments, European and International Institutions had, or will implement in the near future with respect to those elements that have been presented in the chapters above under the category "technical challenges".

This include four different macro themes, namely: Artificial Intelligence, High Definition maps, Position technology, V2x communication.

Finally, due to the extensive number of actives currently ongoing on these different focus, it has been decided to focus only on those orientations having a direct impact on European consumers, therefore focusing only on European and national level.

Artificial intelligence

12.3.8.2 European level

The Commission will support AI technologies both in basic and industrial research. This includes investments in projects in key applications, including connected and automated driving.

In the recent Communication on Artificial Intelligence in Europe, published at the end of April 2018, the European Commission identifies such technology as a key enabler of automated driving vehicles, stressing the importance of public actions and coordination to support research and innovation across Europe, bringing AI to small business and potential users.

Furthermore, in a second document the European Commission has recently published, "Declaration of cooperation on Artificial Intelligence (AI)", Member States agreed to work together on the most important issues raised by Artificial Intelligence, from ensuring Europe's competitiveness in the research and deployment of AI, to dealing with social, economic, ethical and legal questions.

12.3.8.3 National/regional level

At national level, different Member States have identified the crucial role Artificial Intelligence will play with respect to automated driving, advocating for public action on the topic.

France Ministry of Sustainable Development, in its document "Développement des véhicules autonomes - Orientations stratégiques pour l'action publique", quotes the recent speech of President Emmanuel Macron on the Artificial intelligence, underlying the extremely relevant role such technology will have in ensuring the development of autonomous vehicles. The document identifies 4 key areas, namely computer power,

cybersecurity, human-machine interfaces and education in which future policy actions should be oriented.

Denmark's Strategy for Denmark's Digital Growth (Ministry of Industry, 2018), released January 2018, aims to make Denmark a leader in the digital revolution and to create growth and wealth for all Danish people, investing in sectors where Artificial Intelligence could have a primary role, including IoT and automated driving.

Finland created a task force on Artificial Intelligence in May 2017, aimed at investigating potential opportunities of development for the country's economy. The first report, Finland's Age of Artificial Intelligence, surveyed Finland's strengths and weaknesses in AI and provided recommendations to turn Finland into a global leader in the application of AI.

Sweden released its strategy, National Approach for Artificial Intelligence, in May 2018. Although it does not include specific policy announcements, it provides guidance on the topic, outlining the strategic priorities for AI in Sweden, including its integration in the automotive sector.

High Definition maps

12.3.8.4 European level

At European level, the European Commission action, in parallel with the one on positioning technology, aims at improving Galileo services, positively impacting the integrity and reliability of digital maps.

In a recently published document by the Commission, "Communication on the road to automated mobility: An EU strategy for mobility of the future", the European Commission declares its intents to further develop the Galileo services and related vehicle navigation technologies for driverless mobility. As the document underlines, Galileo is a major asset for precise and secured positioning and for the integrity and reliability of digital maps. A study will be launched in 2018 to investigate the question of integrity and reliability of digital maps. National/regional level

12.3.8.5 National level

At national level, different Member States are encouraging public/private partnership to foster the development of HD Maps and road infrastructure.

In terms of **HD Maps**, a necessary element to ensure the rapid and solid development of CCAM, different Member States have produced, in the past months, document and studies aimed at addressing the issue.

- In **France**, the Ministry of Sustainable Development, in its document *"Développement des véhicules autonomes - Orientations stratégiques pour l'action publique",* Encourage and support development of HD maps in collaboration with IGN (Institut géographique national).
- In **Spain**, a recent document published by its Directorate General of Traffic, foresees a collaboration with Mobileye that will enable Spanish cities to become "Automation-ready" including through Mapping Data Generation.
- In **Germany,** the Federal Ministry of Transport and Digital Infrastructure, in its strategic document *"Implementing the Automated and Connected Driving Strategy (programme)",* identifies as a responsibility of the market the development of appropriate datasets, including mapping databases.

- Finally, **Finland**, in its *"Road Transport Automation Road Map and Action Plan 2016–2021"* urges the need of participating in international cooperative standardisation efforts so that difficult weather and road surface conditions will be taken into consideration during the development and testing of road markings and sensor technologies.

Positioning technology

12.3.8.6 European level

A European level, the European Commission will by 2019 offer Galileo's initial high-accuracy services for free, being the first to be able to offer such navigation service on a worldwide base.

Furthermore, the European Commission is expected to prepare guidelines for the optimised use of advanced services, as high-accuracy, robustness and authentication of position, that will be offered by the Galileo system, and to provide guidance on their inclusion in vehicle navigation systems, to address liability and safety issues.

In addition to this, the European Commission, in its document "Space Strategy for Europe" declared that "In the longer term, the Commission will encourage the uptake of space solutions through standardisation measures and roadmaps, and by integrating space into future strategies addressing, for example, autonomous and connected cars, railways, aviation and unmanned aerial vehicles (drones)".

Positioning technology improvement In terms of positioning information technology, the European GNSS Agency has recognised the role a modern, safe and reliable GNSS infrastructure will have in ensuring a rapid uptake of AVs in its report "Central role for robust GNSS in autonomous driving", that highlights how the suitability of the EU-GNSS solution for ITS and Automated Driving is pending on performances in terms of: accuracy, integrity, availability. The report underlines how inherent GNSS (satellite) signals' weaknesses can be addressed through hybridization with other positioning sensors and highly accurate digital maps.

Projects like ESCAPE, funded under the Fundamental Elements Development of E-GNSS engine for safety-critical multi-applications in road transport call, are currently ongoing, aiming to overcome multiple challenges related to the use of GNSS technology in automotive by developing a dedicated, reliable and accurate engine, specifically designed for automotive safety-critical applications. The project will last three years, from autumn 2016 to autumn 2019, and it has a 5.4 M€ budget.

COST, the European framework supporting trans-national cooperation among researchers, engineers and scholars across Europe, has presented as part of the SaPPART project the document "Guidelines Performance assessment of positioning terminals", providing an initial assessment of certification framework for positioning performance assessment, comparing three main approaches for testing the performance of positioning systems (field tests, laboratory tests and R&R tests).

12.3.8.7 National/regional level

Being a topic including supranational infrastructures, as Galileo system, Member States did not present specific orientation on this topic. Nevertheless, the need for a high performance, secure and independent navigation systems has been stressed numerous

times in different national strategic documents issue on topics like defence, environmental preservation and borders security.

12.3.8.8 National/regional level

Absence of a dominant standard for V2X communication

12.3.8.9 European level

The European Commission is currently investigating the question of V2X communication in Europe, through public consultation and *ad-hoc* committees.

In the working document published in October 2017 by the European Commission Radio Spectrum Committee, the Committee, although not officially representing the position of the European Commission, concludes that

"*Considering that the 5.9 GHz band is likely to be used by different technologies for safety-related transport systems (for road and rail such as ETSI ITS-G5, LTE-V2X and CBTC) each having its own merit, and observing the EU spectrum policy principle of technology neutrality, the Commission services take the view that there are sufficient grounds to study the possibility of expanding the 5 875-5 905 MHz band by 20 MHz upwards and pending the results and subsequent discussions in the RSC to amend Article 2(1) of Decision 2008/671/EC in order to expand the definition of safety-related ITS beyond road transportation based on the result of studies in response to this EC mandate."*[120]

Furthermore, the Commission launched in December 2017 a public consultation on the topic, with the goal to eventually clarified the issue with a legislative act in the next future.

Finally, The European Union committed to a deployment of 802.11p-based ITS-G5 infrastructure, in 2016, by announcing seven C-ROADS projects, in Austria, Belgium, the Czech Republic, Germany, France, Netherlands, Slovenia and UK. [121]

12.3.8.10 National/regional level

Being the question of spectrum dealt at European and International level, no specific position on this issue has been taken at national level. Nevertheless, in different occasion governments and national institutions have stress the need for clarification on the topic, in order to ensure the highest degree of compatibility among vehicles of different manufactures.

12.4 Annex D: Mapping of stakeholders' positions

12.4.1 Introduction

This section presents an attempt to "map" views held by key stakeholders occupying various roles in CCAM development across the automotive industry and beyond. In addition to incorporating the inputs from consulted stakeholders (presented in Annex B: Stakeholder Consultation report), the first "layer" of the mapping is substantiated by

[120] EUROPEAN COMMISSION Communications Networks Content & Technology, Directorate-General Electronic Communications Networks & Services Spectrum, RADIO SPECTRUM COMMITTEE, Working Document,https://circabc.europa.eu/d/d/workspace/SpacesStore/f182c247-a298-440e-97f4-4e3271399b00/RSCOM17-26rev2%20ITS%20Draft%20Mandate%20to%20CEPT.pdf
[121] https://rethinkresearch.biz/articles/eu-make-defining-decision-v2x-market/

official statements quoted from policy/position papers with regards to relevant issues published by associations representing the interests of various groups. (distinguished in italics, quotation marks). Secondly, the collection of stakeholders' position is based on the content of the CCAM Workshop[122]. Finally, following the workshop, additional contributions and inputs from willing stakeholders were collected for a completer perspective.

12.4.2 Overview of key stakeholders considered

Stakeholders' group	Description
Automotive Suppliers (upstream)	Upstream suppliers in the automotive industry supplying car components consist of the TIER 2, TIER 1 and TIER 0.5 Suppliers (digital and AD technology providers). The views of individual actors are complemented by the positions of relevant associations in the automotive industry: CLEPA and SSMT (The Society of Motor Manufacturers and Traders, UK).
OEMs	The role of vehicle manufacturers in the future automotive landscape may evolve beyond producing hardware. Here, the views of individual carmakers (e.g. BMW, Tesla) and the vision of the European Automobile Manufacturers' Association (ACEA) are presented.
Aftermarket repair, sales and maintenance providers	Independent wholesalers of vehicle components including repair and maintenance services and car dealers, will also be affected by the possibilities brought about by the digitized vehicle. Their views are represented by two associations: The Federation of Automotive Aftermarket Distributors (FIGIEFA) and the European Council for Motor Trades and Repairs (CECRA). The views of associations of inspection companies are highlighted for relevant aspects. (VdTÜV, CITA)
Aftermarket services providers (i.e. insurance, telecommunication)	This group consists of the views of aftersales services: insurance companies; as well as mobility providers: car sharing operators (e.g. Uber). Given that connected cars face a choice of communication technologies namely between shorter-range and cellular based connections, the position of mobile network operators is reflected by GSMA and the European Competitive Telecommunications Association (ECTA).
Users	Representatives of general consumers (i.e. BEUC) and automotive consumers (i.e. FIA).

The collection of stakeholders' positions is based on various sources:

- **Policy papers**: positions and relevant official public communications/documents associations were consulted, mostly online.
- **Stakeholder consultation 1, February to March 2018**: Conducted by VVA, with the participation of over 30 stakeholders, covering the whole automotive value chain, (upstream automotive value chain - traditional and new-technology suppliers, OEMs, both "traditional" and newly emerged, and downstream automotive value chain, including service providers – as well as mobility providers - and aftermarket players) the consultation addressed various aspects including key trends, business models' evolution, as well as technical, commercial, legal and policy-related elements concerning CCAM.

[122] Workshop organised in Brussels on 28/07/2018 by the consortium to discuss the study findings and key issues affecting CCAM.

- **Stakeholder consultation 2, May 2018**: engaging fewer stakeholders to validate the conclusions taken after the first consultation together with the desk research phase, as well as to investigate more in depth the issues impacting the uptake of CCAM.

- **CCAM Workshop, 28 June 2018**: Workshop organised in Brussels by the consortium to discuss the study findings and key issues affecting CCAM.
- **Post-workshop stakeholder additional contributions, July 2018**: additional stakeholders volunteered to provide additional clarifications and inputs following the CCAM workshop.

The positions and priorities of the grouped stakeholders are summarized per key issue

132 / 165

12.4.3 Liability - High-Level overview of stakeholders' positions

Stakeholders' group	Position– Statement	Source
Automotive Suppliers (upstream)	CLEPA emphasizes the need to expand the Product Liability Directive's scope to incorporate intangible elements, such as software. Various stakeholders stress the importance of defining responsibilities (e.g. a set of guidelines) to ensure predictability in terms of liability allocation.	Stakeholder consultation 1, February 2018
OEMs	According to ACEA, legislation should be put in place to define the driver's role across the different driving scenarios. A couple of stakeholders suggest inputs from Event Data Recorders should be used to determine liability allocation in higher levels of automation.	Stakeholder consultation 2, May 2018 Stakeholder consultation 1, February 2018 Post-workshop additional contributions from stakeholders, July 2018
Aftermarket, sales and maintenance providers	Some stakeholders belonging to this category suggest reviewing the Product Liability Directive to incorporate multiple actors in the process of liability identification.	Stakeholder consultation 2, May 2018
Aftermarket services providers (i.e. insurance, telecommunication)	*"Insurance Europe stresses that any proposal to amend the PLD should not be considered until:* *a thorough assessment of the current situation under the PLD has been conducted, taking both consumer and distributor/producer impact into account; pending completion of that assessment, a widespread and consistent problem with consumer access to compensation under the PLD has been clearly identified."* *"Insurance Europe believes that any intervention at EU level regarding liability regimes for new technologies would be premature, and that current liability legislation provides adequate protection for consumers while allowing enough time for insurers to develop the right insurance products for emerging risks."*	Insurance Europe, 'Position paper on liability insurance and emerging technologies', May 2017 https://www.insuranceeurope.eu/sites/default/files/attachments/Position%20paper%20on%20liability%20insurance%20and%20emerging%20technologies_0.pdf, Insurance Europe, 'No need for new liability rules for new technologies', https://www.insuranceeurope.eu/no-need-new-liability-rules-new-technologies, May 2017, (accessed 23 July 2018).
Users	*'The Motor Insurance Directive should be futureproof and ensure the victims' protection with the increasing automation of the driving task.'* *'DSSAs (Data Storage Systems for Automated Driving) should be considered for automated vehicles from SAE level 3 onwards and standards should be defined if they are fitted in vehicles.'* *"the [Product Liability] Directive needs to be reformed in order to build consumer confidence in C&A vehicles"; Extension of the scope to all types of products, digital content products, and (digital and*	FIA, 'Policy Position on the Motor Insurance Directive', https://www.fiaregion1.com/wp-content/uploads/2018/02/2018-01-24-FIA-Region-I-Policy-Position-on-Motor-Insurance-Directive_FINAL.pdf, January 2018,(accessed 23 July 2018)

133 / 165

Stakeholders' group	Position– Statement	Source
	other) services; Analyse the merits to introduce a mandatory insurance system, particularly for risk sectors.	FIA, 'Policy Position on Event Data Recorders', https://www.fiaregion1.com/policy-position-on-event-data-recorders/, February 2017, (accessed 23 July 2018) BEUC, 'Protecting European consumers with connected and autonomous cars', http://www.beuc.eu/publications/beuc-x-2017-138_dve_beuc_connected_autonomous_cars.pdf , November 2017, (accessed 23 July 2018). BEUC, 'Review of Product liability rules', http://www.beuc.eu/publications/beuc-x-2017-039_csc_review_of_product_liability_rules.pdf, November 2017.

12.4.4 Certification - High-Level overview of stakeholders' positions

Stakeholders' group	Position– Statements	Source
Automotive Suppliers (upstream)	CLEPA suggested the need for policy action in the form of European test beds to accelerate CCAM deployment, while a couple of stakeholders emphasize the need to develop a common testing methodology. (set of testing procedures or standards to be tested against)	Stakeholder consultation 1, February 2018
OEMs	Stakeholders belonging to the vehicle manufacturers category did not present a common view on the topic.	Stakeholder consultation 1, February 2018 Stakeholder consultation 2, May 2018
Aftermarket inspection, repair, sales and maintenance providers	Inspection companies suggest a continuous approach for safety related testing. Given that technical certification for cybersecurity is just a snapshot in time, certification must be done on processes and not on technical standards. There is a need for a mutual understanding of what (software) should be tested (and updated).	CCAM Workshop, 28 June 2018.
Users	*[concerning general vehicles] "FIA requests the inclusion of a provision granting type approval only for tamper-proof systems, components and separate technical units for vehicles."*	FIA, Policy Position on Vehicle Type Approval, https://www.fiaregion1.com/policy-position-

134 / 165

Stakeholders' group	Position– Statements	Source
	"Manufacturers shall make sure that when they first put a product on the market, the software that runs on the product is as secure and up-to-date as it can be. In addition, manufacturers should also be required to ensure that the software is updated during the entire lifecycle of the product whenever this is needed to guarantee that it remains secure."	on-vehicle-type-approval/, June 2016, (accessed 23 July 2018) ANEC and BEUC, 'Cybersecurity for Connected Products', http://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf, March 2018, (accessed 23 July 2018).

12.4.5 Testing on public roads – High-Level overview of stakeholders' positions

Stakeholders' group	Position– Statements	Source
Automotive Suppliers (upstream)	*"Increase the number of 'real-life traffic tests'"* Stakeholders from the automotive suppliers expressed their support for a regulatory framework capable of ensuring the increase of real-situation testing, stressing the fact that Vienna Convention in current formulation represents an impediment to real-life testing and that the updated legal framework should specifically address automated driving functions.	CLEPA, 'Truck platooning: Smart mobility through intelligent transport systems and automated & connected driving', https://clepa.eu/wp-content/uploads/2017/10/CLEPA-Platooning-Panel-A4-V4-HD.pdf, October 2017, (accessed 23 July 2018). Stakeholder consultation 1, February 2018 Stakeholder consultation 2, May 2018
OEMs	Stakeholders belonging to the vehicle manufacturers category did not present a common view on the topic.	Stakeholder consultation 1, February 2018

135 / 165

Stakeholders' group	Position– Statements	Source
Users	Road safety is a top priority: one user representative expects the EU, (at UN-ECE level), to adopt and implement concrete building block regulations to protect its citizens. User representatives stressed the need for more stringent legal framework with regards to pre-market launch product validation.	Stakeholder consultation 1, February 2018 CCAM Workshop,28 June 2018

12.4.6 Cybersecurity - High-Level overview of stakeholders' positions

Stakeholders' group	Position– Statements	Source
Automotive Suppliers (upstream)	*"SMMT supports the development of a set of guidelines for ensuring vehicle cyber security currently being developed under the auspices of the WP.29 at the UNECE"* A couple of stakeholders from the automotive supplier industry agreed on the importance of creating an environment for sharing best-practices. Furthermore, different actors stressed that standards should be put in place and achieved individually by industry players, to create a heterogenous cybersecurity environment.	SMMT, 'Position paper Connected and Autonomous Vehicles', https://www.smmt.co.uk/wp-content/uploads/sites/2/SMMT-CAV-position-paper-final.pdf, February 2017, (accessed 23 July 2018). Stakeholder consultation 1, February 2018 Stakeholder consultation 2, May 2018
OEMs	*"EATA considers that the establishment of an EU certification framework should build upon existing national and international certification standards and regulations such as the regulations on automotive cybersecurity and on over the air software updates, currently being drafted at the UN-ECE WP 29."* The automotive association (ACEA) as well as an OEM representative maintain that UNE-CE standards should be followed.	European Automotive and Telecom Alliance, 'Regulatory Briefing paper: Cybersecurity', June 2018, (accessed 24 July 2018). Stakeholder consultation 1, February 2018 Stakeholder additional inputs, July 2018
Aftermarket inspection, repair, sales and maintenance providers	Stakeholders belonging to this category underlined in different occasions that cybersecurity concerns should not be used as a caveat to prevent unrestricted free access to in-vehicle data.	Stakeholder consultation 1, February 2018 Stakeholder consultation 2, May 2018 Stakeholder additional inputs, July 2018

136 / 165

Stakeholders' group	Position– Statements	Source
Aftermarket services providers (i.e. insurance, telecommunication)	*"EATA considers that the establishment of an EU certification framework should build upon existing national and international certification standards and regulations such as the regulations on automotive cybersecurity and on over the air software updates, currently being drafted at the UN-ECE WP 29."* Stakeholders belonging to this category underlined in different occasions that cybersecurity concerns should not be a caveat to impede unrestricted free access to in-vehicle data. A suggestion from this group of stakeholders is to involve more players outside the automotive value chain, namely from the digital industry, to achieve innovative solutions.	European Automotive and Telecom Alliance, 'Regulatory Briefing paper: Cybersecurity', June 2018, (accessed 24 July 2018). Stakeholder consultation 1, February 2018 Stakeholder consultation 2, May 2018 Post-workshop additional contributions from stakeholders, July 2018 CCAM Workshop, 28 June 2018
Users	*"For high-risk-affected connected products (e.g. self-driving cars), the application of minimum security requirements should be complemented with mandatory cybersecurity certification"*	ANEC and BEUC, 'Cybersecurity for Connected Products', http://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf, March 2018, (accessed 23 July 2018).

12.4.7 Data Access - High-Level overview of stakeholders' positions

Stakeholders' group	Position on data access – Statements	Source
Automotive Suppliers (upstream)	*"CLEPA supports an interoperable standardized and secure in-vehicle open telematics Platform."* *"An intermediate solution should provide a competition neutral data access via a backend server together with a state of the art data access via an in-vehicle connector."* *"Access to vehicle data via the B2B OEM interface is based on B2B agreements."; "There is no direct access to the vehicle by third parties to avoid risks to customer and public safety"*	CLEPA, 'Position Paper Open Telematics Platform', https://clepa.eu/wp-content/uploads/2015/08/20150722_CLEPA_PP_Open_Telematics_Platform.pdf, July 2015 (accessed 23 July 2018). German Association of the Automotive Industry (VDA), 'Access to the vehicle and vehicle generated data', https://www.vda.de/en/topics/innovation-and-technology/network/access-to-the-vehicle.html, September 2016 (accessed 23 July 2018).
OEMs	*[…cybersecurity concerns...] "third parties shall not have direct in-vehicle access to data. Instead, vehicle manufacturers will communicate the relevant vehicle data in a secure manner to an off-board facility from where third parties can access the data."*	ACEA, 'Position Paper: Access to vehicle data for third-party services', https://www.acea.be/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf, December 2016(accessed 23 July 2018).

137 / 165

Stakeholders' group	Position on data access – Statements	Source
	"To promote competition, service providers should have the choice between accessing data directly through the vehicle manufacturer's server or via 'neutral' servers that would gather the data from vehicle manufacturers' servers." *"Access to vehicle data via the B2B OEM interface is based on B2B agreements."; "There is no direct access to the vehicle by third parties to avoid risks to customer and public safety".*	German Association of the Automotive Industry (VDA), 'Access to the vehicle and vehicle generated data', https://www.vda.de/en/topics/innovation-and-technology/network/access-to-the-vehicle.html, September 2016(accessed 23 July 2018)
Aftermarket inspection, repair, sales and maintenance providers	*"The proprietary design of the in-vehicle telematics applications (data plus algorithms) prevents equal access by independent operators and service providers and limits their ability to innovate and compete online on an equal footing. It ultimately limits consumers' freedom of choice between competitive repair, mobility and consumer convenience services."* *"There is an urgent need of a framework granting standardised and direct unrestricted access to vehicle generated data for all market players."* *"The VdTÜV approach of an automotive platform provides a reliable extended vehicle concept for all market players and consumers who engage in data protection as well as in both safety and security as an added value for future connected cars."*	FIGIEFA, Free Flow of Data – Commission Communication –Input from the Independent Automotive Aftermarket, https://www.figiefa.eu/wp-content/uploads/Free-Flow-of-Data-FIGIEFA-Input-2016_12_23.pdf, December 2016(accessed 23 July 2018). CECRA, 'Position Paper on Connectivity', http://www.cecra.eu/statements/2016CECRAPPconnectivity03102016.pdf, October 2016, (accessed 23 July 2018). VdTÜV, 'Position: Requirements for the telematics interface in vehicles', https://www.vdtuev.de/en/dok_view?oid=662438, January 2017(accessed 23 July 2018).
Aftermarket services providers	*"Insurance Europe welcomes the EP's draft report which calls the "European Commission to take legislative action on access to in-vehicle data and resources before the end of 2018, enabling service providers to offer their products to drivers inside the vehicle, free from any interference by vehicle manufacturers."* *"EU policymakers to take legislative action to ensure that any technological solution to access in-vehicle data lets drivers decide with whom they share their data."* *"A broad coalition comprising vehicle dealers, automotive aftermarket and mobility services operators, the European insurance industry, the European representations of both motorist consumers and SMEs, is urging EU decision-makers to act decisively to establish fair and equal access to in-vehicle data and resources."*	Insurance Europe, 'Press Statement European Parliament approach on access to in-vehicle data welcomed', https://www.insuranceeurope.eu/european-parliament-approach-access-vehicle-data-welcomed, 21 February 2018, (accessed 23 July 2018). Insurance Europe, '#Data4Drivers petition', https://www.insuranceeurope.eu/data4drivers-eu-rules-needed-give-drivers-control-their-vehicle-data, November 2017(accessed 23 July 2018). AFCAR,'Press Release: Broad industry coalition calls upon EU decision-makers to ACT NOW for equal access to in-vehicle data and functions', https://www.fiaregion1.com/wp-content/uploads/2018/04/AFCAR-Manifesto-for-equal-digitalisation-chances.pdf, April 2018 (accessed 25 July 2018).
Users	*"Legal certainty is needed to address the data control issues and ensure that ultimately it is the consumer who is in the driver seat when it comes to the usage of the data generated by his/her connected car."* *"A variety of service providers should have the right to develop products and functionalities for car data, ensuring fair competition in an open market place."; "A regulated approach to accessing car data for trusted third-party providers puts consumers at the centre"* *"The FIA calls on the Commission to ensure neutrality by design for telematics platforms by mandating an open and secured approach allowing consumers to freely choose safe applications."*	BEUC, 'Protecting European consumers with connected and autonomous cars', http://www.beuc.eu/publications/beuc-x-2017-138_dve_beuc_connected_autonomous_cars.pdf, November 2017, (accessed 23 July 2018). FIA, 'My Car My Data campaign', https://www.fiaregion1.com/my-car-my-data/, May 2017, (accessed 23 July 2018). FIA, 'Policy position on car connectivity', https://www.fiaregion1.com/policy-position-on-car-connectivity/, April 2016, (accessed 23 July 2018).

138 / 165

12.4.8 Infrastructure evolution - High-Level overview of stakeholders' positions

Stakeholders' group	Position on infrastructure– Statements	Source
Automotive Suppliers (upstream)	*[referring to the actions needed] "upgrade road infrastructure; further enhance different technologies to allow multi-brand platooning"* *"improved standards for road traffic signs and road markings and their durability will support better performance of Traffic Sign Recognition."*	CLEPA, 'Truck platooning: Smart mobility through intelligent transport systems and automated & connected driving', https://clepa.eu/wp-content/uploads/2017/10/CLEPA-Platooning-Panel-A4-V4-HD.pdf, October 2017, (accessed 23 July 2018). CLEPA, 'Position Paper Automated Driving', https://clepa.eu/wp-content/uploads/2017/10/CLEPA-Platooning-Panel-A4-V4-HD.pdf, October 2014, (accessed 23 July 2018).
OEMs	The association (ACEA) stressed how institutions should coordinate the deployment of digitalised infrastructures (e.g. among different cities) as well as between different actors.	Stakeholder consultation 1, February 2018
Aftermarket services providers (i.e. insurance, telecommunication)	ECTA stressed that public sector should provide access to facilities and infrastructures (i.e. antennas, cables). Furthermore, it was indicated that network coverage will influence deployment rate of CCAM, so public support will be required to Improve the cost and speed of deployment, (in the form of direct investments) as well as permits. Network interoperability and coverage was identified as very important, including the definition of a standard for V2V connection.	Post-workshop additional contributions from stakeholders, July 2018

12.4.9 Technical challenges - High-Level overview of stakeholders' positions

Stakeholders' group	Position on technical challenges– Statements	Source
Automotive Suppliers (upstream)	*"There ought to be network neutrality, in that data transmission for safety-critical services must be prioritised ahead of other services, with each category ascribed a defined quality of service."* *"CLEPA R&I roadmaps support this development with technological advancements in key innovation areas (i.e. safety and ITS). These include necessary progress and implementation of advanced safety technologies, communication, data handling, highly precise dynamic positioning, environmental recognition, human factors and human machine interaction, etc."* *"CLEPA supports activities accelerating deployment of vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication such as the development of an interoperable, open access, secured and standardized telematics platform."* "*it is critical to allocate sufficient radio frequency bandwidth for V2V and V2I communication."*	SMMT, 'Position paper Connected and Autonomous Vehicles', https://www.smmt.co.uk/wp-content/uploads/sites/2/SMMT-CAV-position-paper-final.pdf, February 2017, (accessed 23 July 2018). CLEPA, 'Position Paper Automated Driving', https://clepa.eu/wp-content/uploads/2017/10/CLEPA-Platooning-Panel-A4-V4-HD.pdf, October 2014, (accessed 23 July 2018). Stakeholder consultation 1, February 2018

139 / 165

Stakeholders' group	Position on technical challenges– Statements	Source
	A couple of TIERs (1 and 0,5) stakeholders suggest safety related aspects must be standardized.	
OEMs	ACEA calls for infrastructure improvements, and along with another OEM representative—stressed the importance of HD maps. VACEA also expressed concern on the standardisation of the HMI (Human Machine Interface), as this would block technological progress guaranteed by competition among OEMs. Furthermore, it has been raised in different occasion that it may be too early to evaluate the effectiveness of technologies.	Stakeholder consultation 1, February 2018 Stakeholder consultation 2, May 2018
Aftermarket repair, sales and maintenance providers	FIGIEFA points out that infrastructure-related costs could be burdensome for OEMs.	Stakeholder consultation 1, February 2018
Aftermarket services providers (i.e. insurance, telecommunication)	*"The GSMA urges the European Commission to adopt a technology-neutral approach in developing the EU's Cooperative Intelligent Transport Systems (C-ITS), notably on safety-related connectivity"*	GSMA,'Safe and Smarter Driving: the Rollout of Cellular V2X Services in Europe', https://www.gsma.com/gsmaeurope/resources/postions-reports-publications/eu-intelligent-transport-system/, September 2017, (accessed 23 July 2018).
Users	*"AI products and services must be consumer-friendly and legally compliant by default. They must be designed so as to avoid undue discrimination, invasive marketing, or loss of privacy. Public research and stakeholder discussions are necessary to address the question of ethics of AI. Guidance on AI and automated decision making should be developed, focusing on the repercussions of AI on fundamental rights, non-discrimination, consumer protection, and transparency."* *"Users should have a right to transparency: there should be a general information obligation for companies providing services to consumers that are based on automatized processes such as those based on algorithms."*	BEUC, 'Automated decision making and artificial intelligence', http://www.beuc.eu/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf , June 2018, (accessed 23 July 2018).

12.5 Annex E: Survey Report: Report for Survey for DG CONNECT Survey on legal, economic, and business issues related to Cooperative, Connected and Automated Mobility (CCAM)

In this annex we provide the outcomes of the survey for DG CONNECT Survey on legal, economic, and business issues related to Cooperative, Connected and Automated Mobility (CCAM).

12.5.1 Introduction aim and scope

As part of the assessment of legal, economic, and business issues related to Cooperative, Connected and Automated Mobility (CCAM), we designed a survey aimed at identifying the major bottlenecks of technical, legal and commercial nature that may affect the uptake of CCAM in Europe. The survey was open and addressed to all the stakeholders involved in the value chain of CCAM.

The survey had the objective to complement and validate the findings that result from the desk research and interviews. It focused on collecting the stakeholders' opinion on the following challenges associated with CCAM deployment:

- Liability framework for automated driving;
- Development of legal framework on testing and certification;
- Cybersecurity approach and role of regulation;
- Approaches to vehicle data access;
- Artificial intelligence algorithms;
- Upgrade of Road infrastructure;
- Improvement of positioning technology;
- Availability of HD maps;
- Emergence of a dominant standard for V2X communication;
- Willingness to pay by end users.

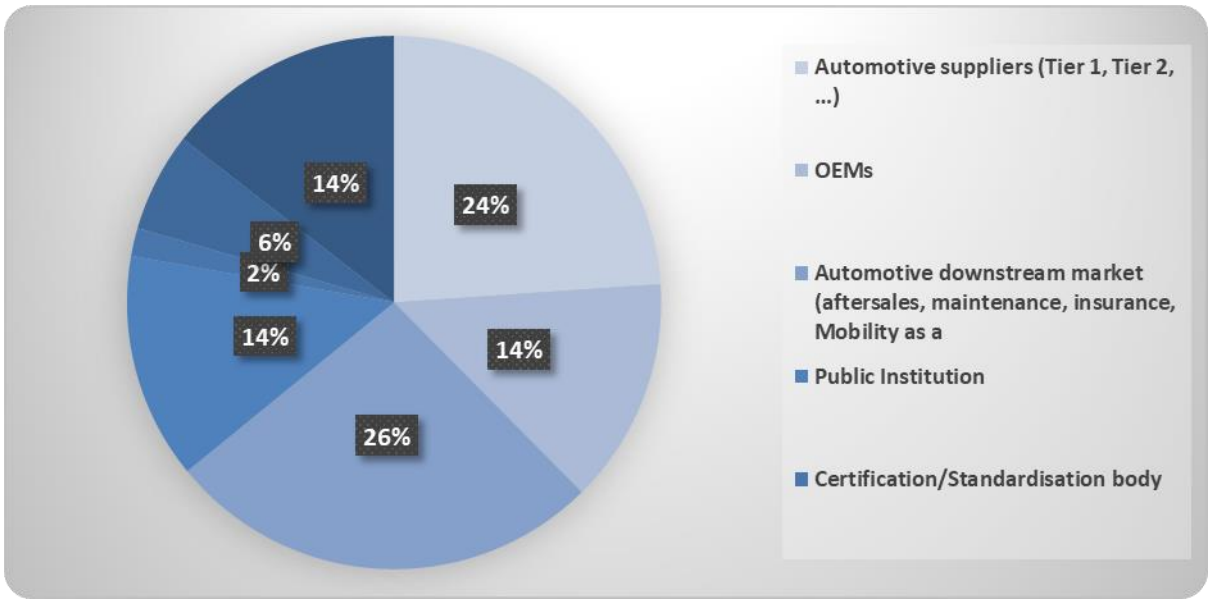
The survey was launched on 07/06/2018 and closet on 10/07/2018. The survey received 218 Individual responses from which 58 were complete answers (all the questions were answered). **Each single question, received at least 70 answers**.

Representatives of the survey sample

For the stakeholders' survey, the project team compiled a list of relevant stakeholders. After filtering of duplications and quality check of the responses, the final list contained 116 unique contacts, that have been used for the elaboration of the results.

The survey was promoted to the stakeholder database created for the project and promoted via the Commission Newsroom, as well as professional social media. to further increase response rate, stakeholders were asked to share the survey with their colleagues/members/partners with relevant knowledge for the study.

The survey shows a very good representation of respondents from the key stakeholder categories, featuring, among others, user representatives, aftermarket players OEMs and suppliers, as well as insurance and finance and telecoms representatives. **43% of the answers were provided by associations.**



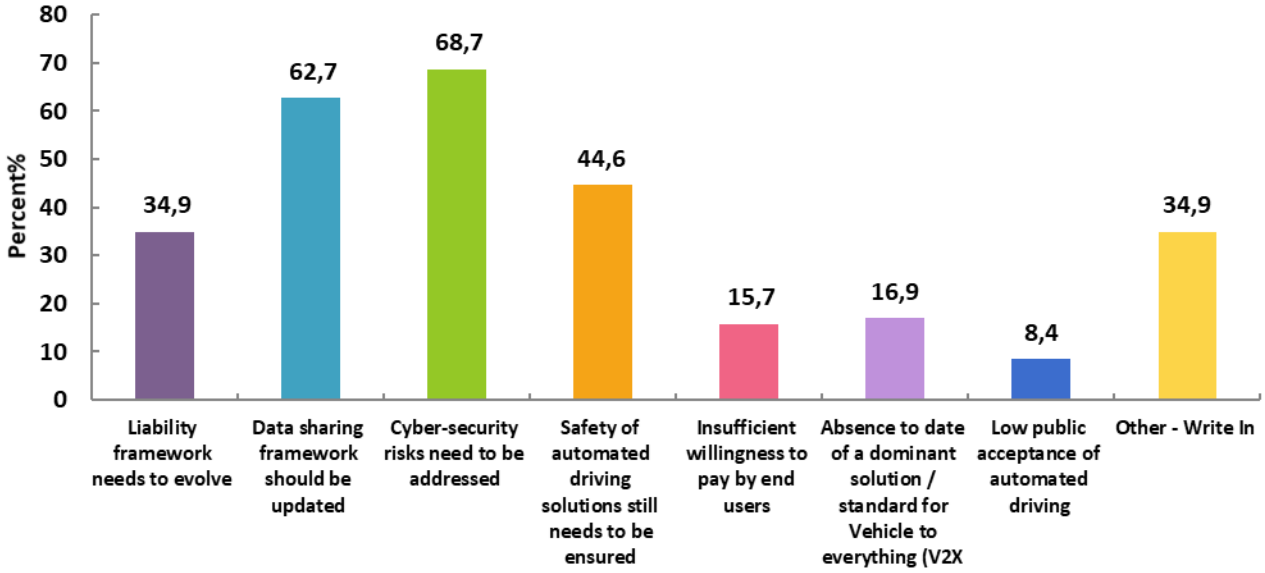
Most of survey respondents is composed by stakeholders from all over Europe, which makes a very good European coverage for the study analysis and shows that there is high interest in CCAM across Europe.

After the completion of the survey, some stakeholders offered to have a follow on to explain their answers and provide additional sources of information for the study. The inputs from these post-survey consultations are considered in the Annex D Mapping of stakeholders' positions.

The main outcomes of the survey are outlined in the sections below.

12.5.2 Overview of the most relevant issues for CCAM uptake

The survey first identified the most relevant bottlenecks related to Connected Cooperative and Automated Mobility. Respondents were asked to indicate the **three most relevant issues** affecting the uptake of CCAM.

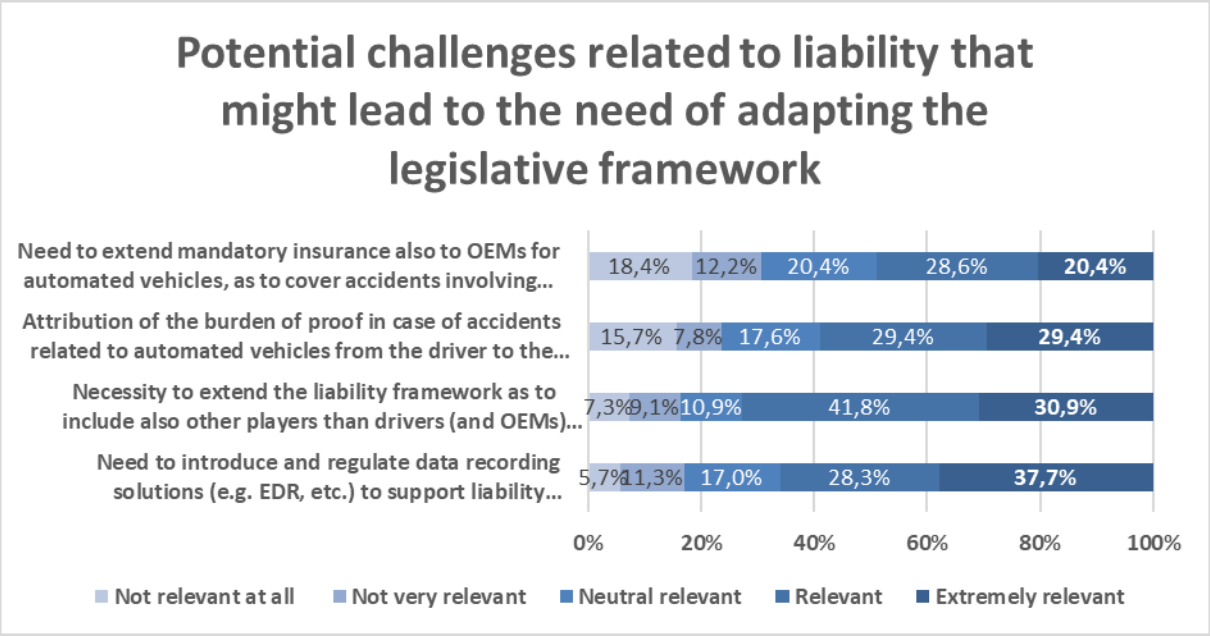


Respondents identified cyber-security as the most stringent challenge to be addressed, followed by the question of data access (data sharing) as well as safety-related aspects. Open responses often referred to the specific need for standardized communication solutions.

12.5.2.1 Liability

Challenges related to liability that might lead to the need of adapting the legislative framework

Below, we identified potential challenges related to liability that might lead to the need of adapting the legislative framework. Please, for each of them specify on a scale from 1 to 5 the relevance of the issue in terms of necessity to adapt the legislative framework, where 1 is not relevant at all and 5 is extremely relevant.

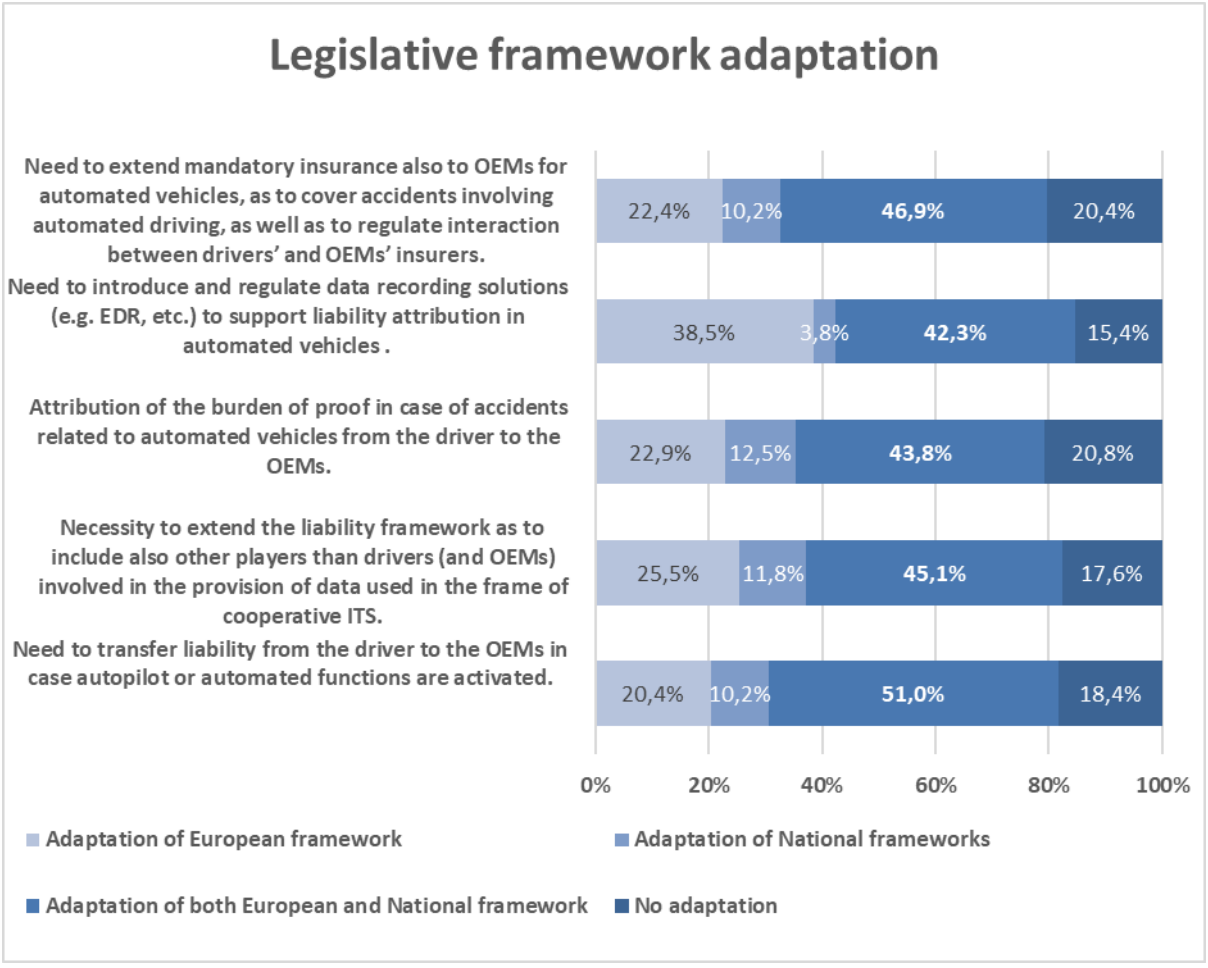


Respondents were asked to classify liability-related challenges in terms of the need for legislative framework adaptation. Data recording solutions as well as the necessity to extend the liability framework in such a way as to incorporate other actors were jointly identified to be of first order importance. In relation to this, stakeholders view the attribution of the burden of proof in case of accidents related to CAD as another important challenge to address.

Some of the stakeholders were concerned with the reliability and robustness of EDRs over the vehicle's life. According to them, event data recorders (EDR) and data storage systems for automated driving vehicles (DSSA) should be considered for automated vehicles from SAE level 3 onwards and standards should only be defined if they are fitted in vehicles. Any direct monitoring should be limited to automation mode and should not occur by means of camera. All data used in this context should be securely transferred and stored. Liability schemes in case of an accident or infringement to the highway code need to be carefully designed for each level of automation and clearly communicated to the users to ensure a smooth transition between full driver liability to full manufacturer and road operator liability.

Adaptation of national or European legislation

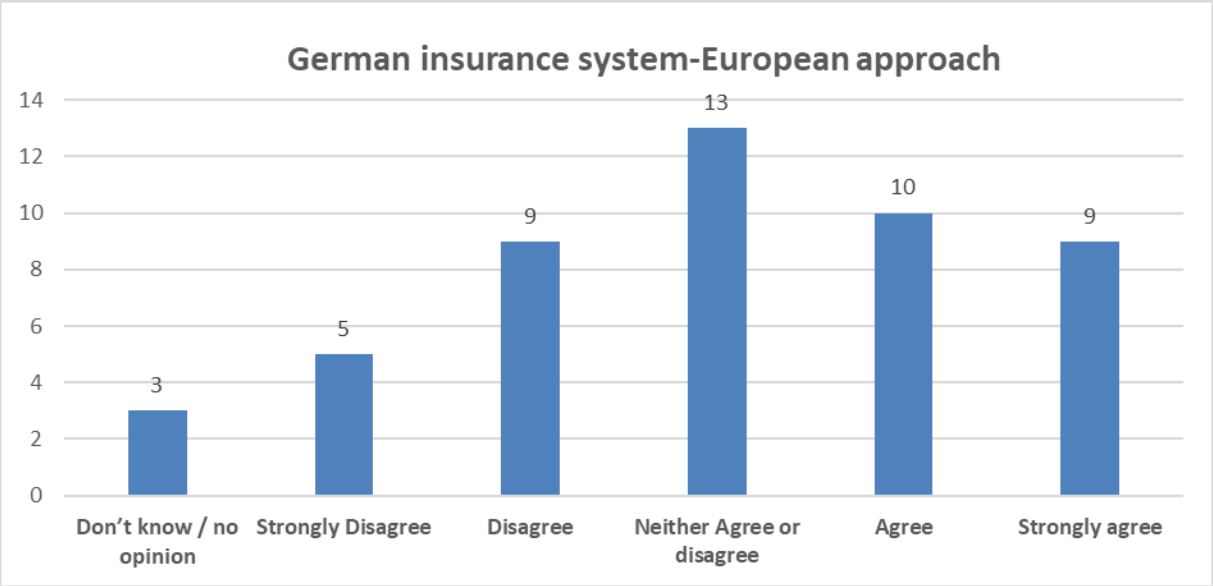
Can you please indicate, for the issues above, whether the legislative framework would need to be adapted at the European level (e.g. motor insurance Directive and Product Liability Directive), National level (e.g. civil liability, role and obligations of specific stakeholders, compensation mechanisms, etc.), both above, or none?



For all the potential challenges related to liability, the respondents consider adaptation of both European and National legislative framework. However, 38,5% suggest a National legislative framework for the regulation of data recording solutions. A bit more than 20% believe that no legislative adaptation is needed for the attribution of the burden of proof in case of accidents and the extension of mandatory insurance.

Insurance system

According to the German insurance system, the driver insurance will pay those who get injured by the accident. Then two insurances - one covering the car and the other one covering the driver - will establish who is liable, depending on black box information. The insurances of the OEMs and of the driver will be compulsory. Do you think that this approach could be considered a best practice to be encouraged and replicated in other Member States?

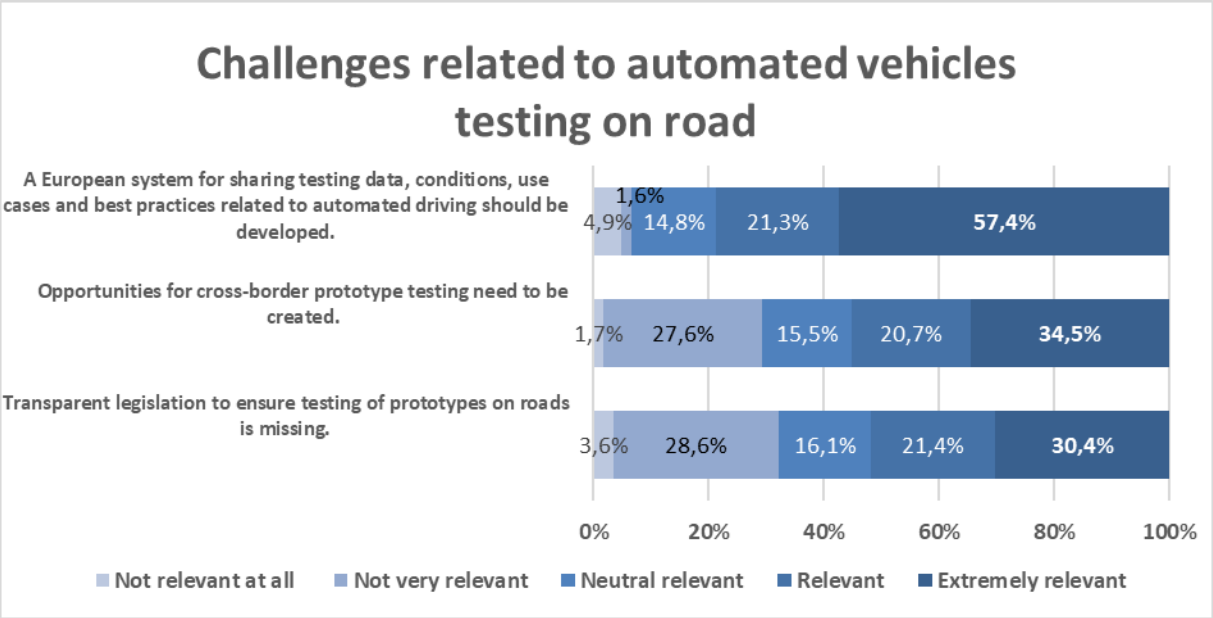


It appears from the answers that the uptake is at early stage and the definition of the best approach is not clear yet. The example of the German insurance systems was received as neutral, with possibly yes or possibly no to be the one Europe should adapt.

12.5.2.2 Testing and certification

Challenges related to testing on road

Below, we identified potential challenges related to automated vehicles testing on road (i.e. procedures that are necessary to allow the collection of real conditions data). Please, for each of them specify on a scale from 1 to 5 the relevance of the issue in terms of necessity to adapt the legislative framework, where 1 is not relevant at all and 5 is extremely relevant/important.



According to the survey, **57.4% of the participants consider as extremely relevant to have a European system for sharing testing data, conditions, use cases and best**

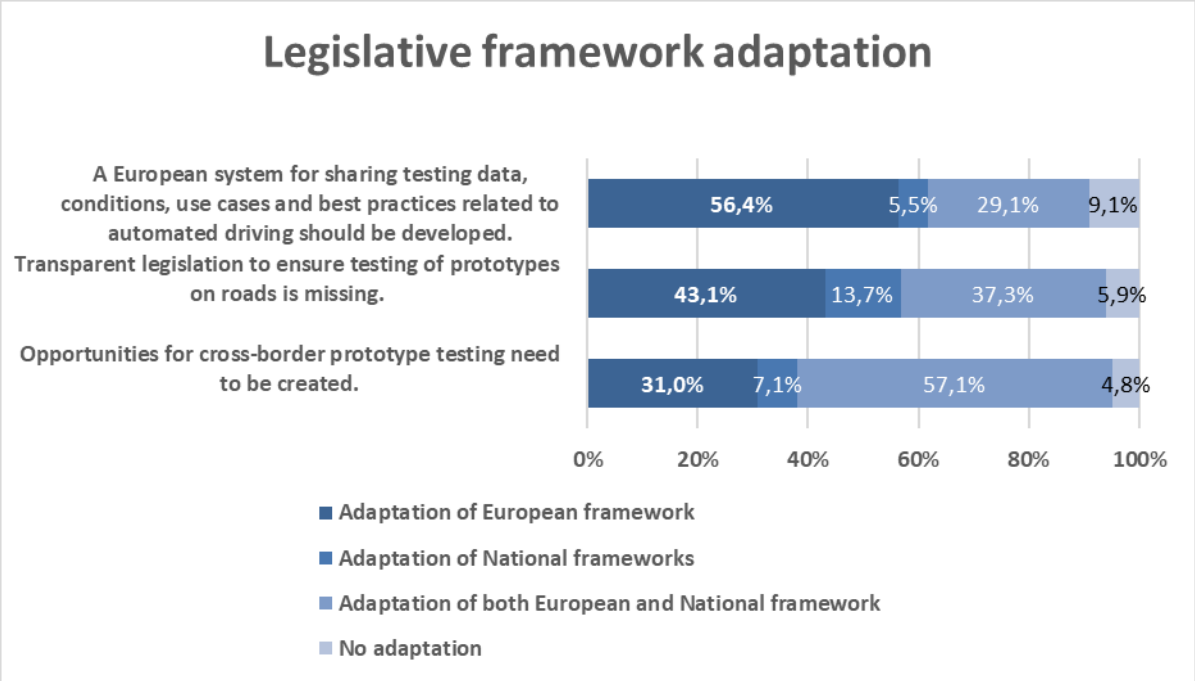
practices related to automated driving. 34,4% support the idea that cross-border prototype testing could be an extremely relevant opportunity for the Member States and finally only 30.4% is strongly pointing that transparent legislation to ensure testing and prototypes on roads is missing.

Additional comment was made, regarding the importance of mutual recognition between Members States of national testing authorizations.

Adaptation of national or European legislation

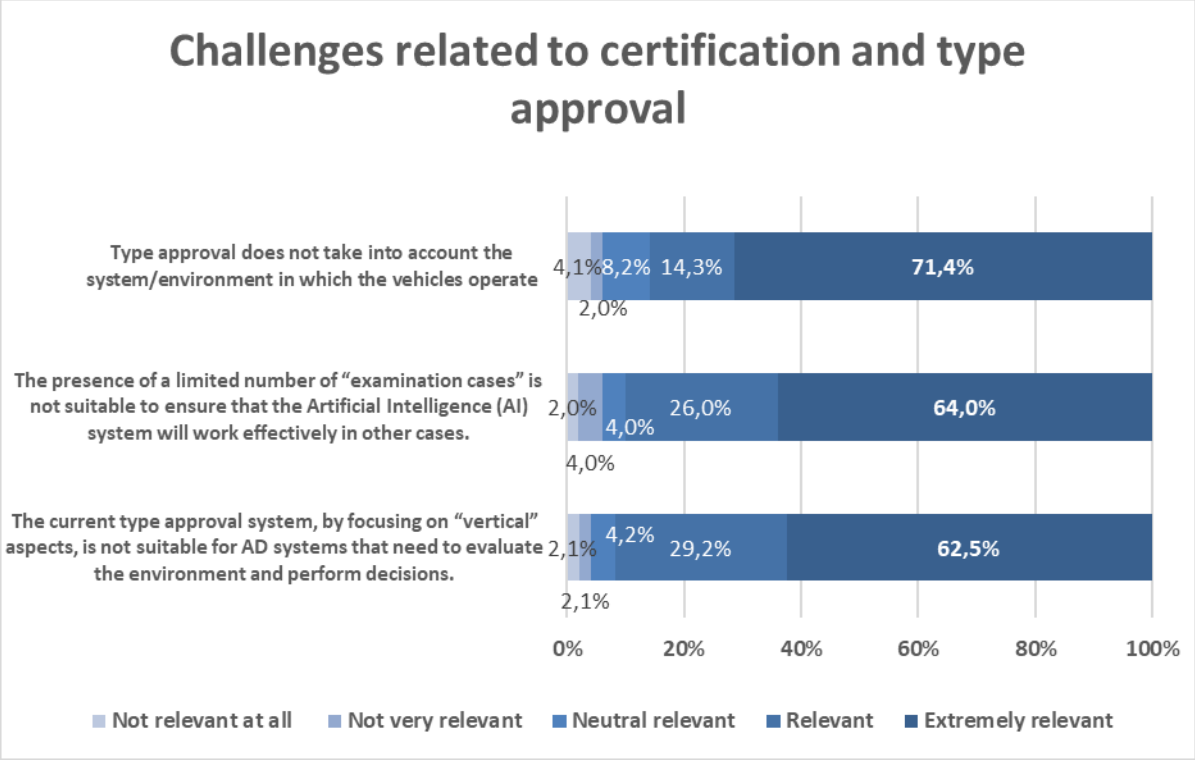
Can you please indicate, for the issues above, whether the legislative framework would need to be adapted at the European level, National level, both above or none?

A European system for sharing data, conditions, use cases and best practices related to automated driving should be developed at European level, according to 56.4% of the stakeholders. The issue of missing transparent legislation to ensure testing on prototypes on roads, interestingly, was suggested as relevant to be addressed at European level, according to the largest part of the sample. Cross-border testing legislation, as expected, was suggested as relevant to be addressed on both European and National level.



Challenges related to certification and type approval

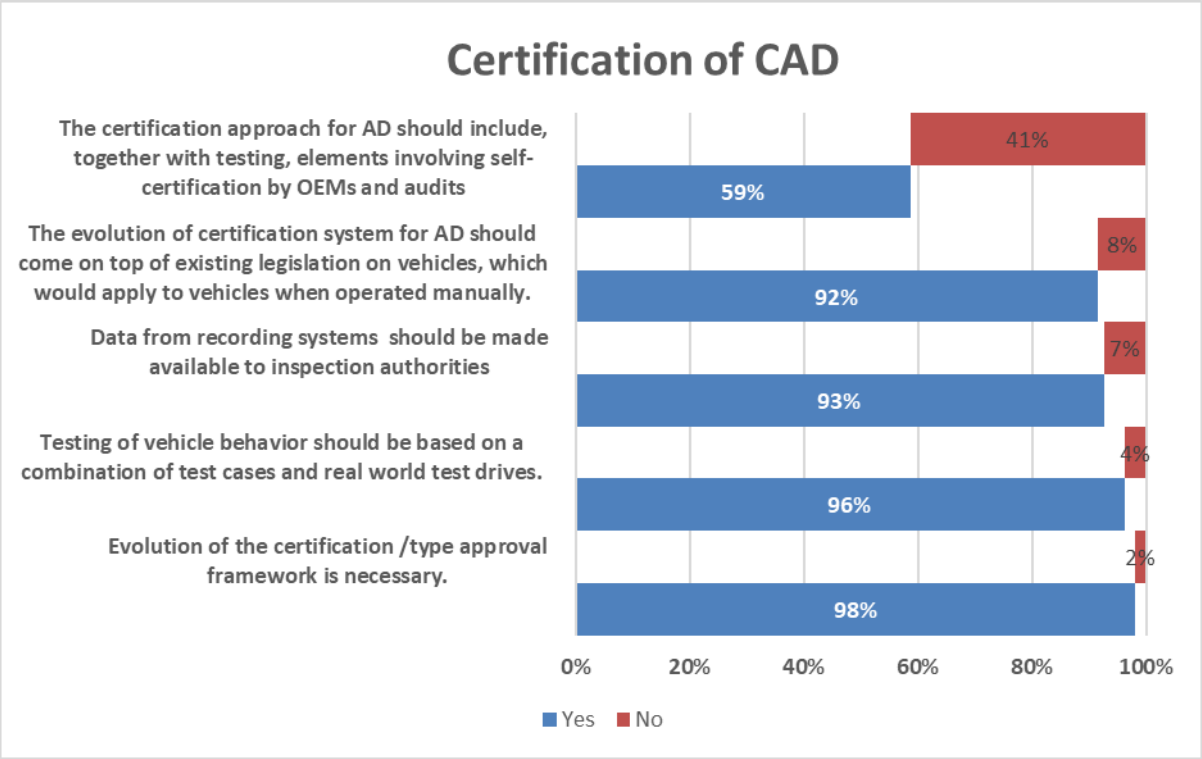
Below, we identified potential challenges related to certification and type approval in the frame of the uptake of automated vehicles (with a focus on levels 4 and 5). Please, for each of them specify on a scale from 1 to 5 the relevance of the issue, where 1 is not relevant at all and 5 is extremely important/relevant.



There are three main challenges related to certification and type approval and all were suggested to be extremely relevant and important bottlenecks. The most relevant one, according to our stakeholders (71,4%) is the fact that the type approval does not consider the system/environment in which the vehicles operate (presence of other vehicles, people, infrastructure). Around 64% of respondents believe that it is an extremely relevant issue the fact that there is limited number of "examination cases" and these cases are not enough to ensure efficiently working AI. Finally, 62.5% of respondents believe that the current type approval system is not suitable for AD systems because being "vertical", does not integrate the evaluation on the environment and decision, that an AD should take.

Certification for automated driving

Can you please indicate, considering the challenges above, whether you agree or not with the following statements on certification related to automated driving (AD)?



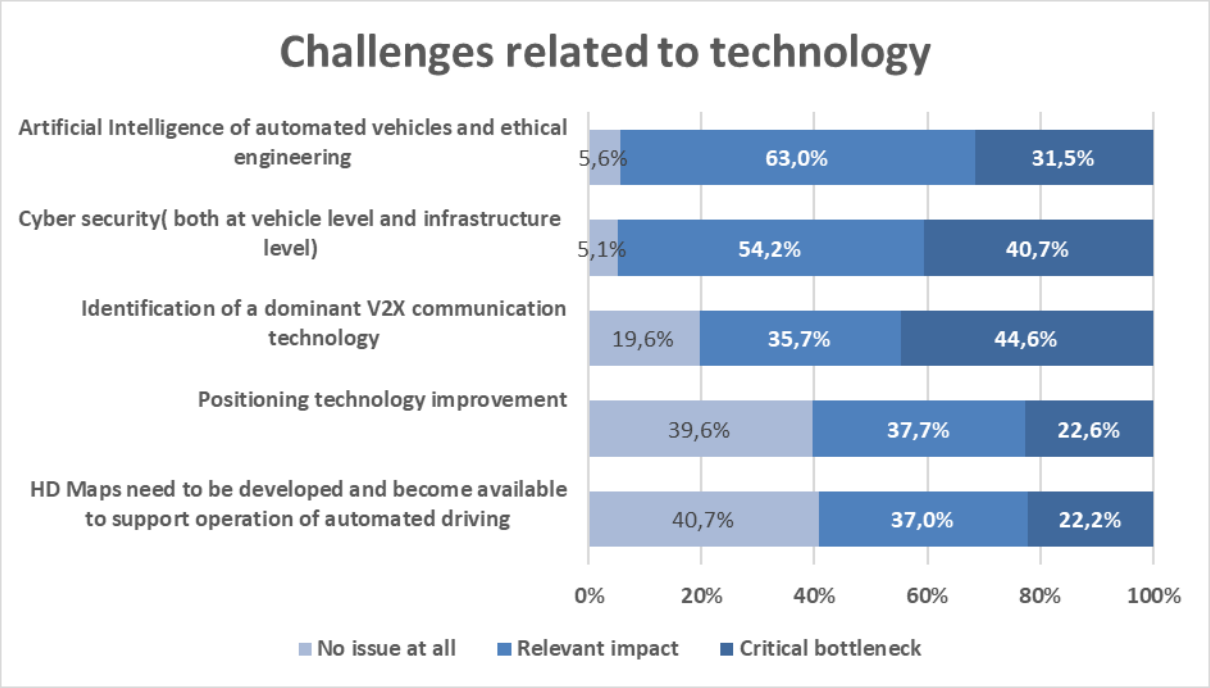
Almost all the proposed statements were welcomed by the stakeholders with great agreement. **Evolution of the certification/type approval framework is needed, according** to almost the total stakeholder population. The same trend goes with 96% for **testing which should be based on a combination of test cases and real-world test drives. 93% of the stakeholders think that data from recording systems** (e.g. Electronic Data Recorders, Data Storage System for Automated Driving) **should be made available to inspection authorities** to identify safety challenges during the lifetime of the vehicle. A very big part of the stakeholders 92% also consider that the evolution of certification system for AD should come on top of existing legislation on vehicles, which would still apply to vehicles when operated manually. The only statement where opinions are split almost by 50% is the proposition of certification approach which include together with testing, elements involving self-certification by OEMs and audits to provide a comprehensive assessment while containing costs.

12.5.2.3 Technology

Challenges related to technology that might slow down the uptake of CCAM

Below, we identified the challenges related to technology that might slow down the uptake of CCAM. Please, for each of them specify the importance of the issue on a scale from 1 to 3, where: 1 = No issue at all (challenge will soon be solved); 2 = this challenge has relevant impact on the time to market of automated vehicles; 3 = the issue could represent a critical bottleneck to the uptake of automated vehicles.

63% of the stakeholders consider the artificial intelligence of automated vehicles and the ethical engineering to be a relevant technical issue. Also, identification of a dominant V2X communication and cyber security are suggested to be of high relevance, with respectively 40.7% and 44.6% of stakeholders suggesting that the issues have critical relevance for the uptake of CCAM. 44.6% of the stakeholders consider cyber-security to be a critical bottleneck if CCAM is not protected from cyber-attacks both at vehicle and infrastructure level. It was specified that cybersecurity is a critical condition to the uptake of automated driving. By ensuring a strong security against cyberthreats, consumers would be more confident vis-à-vis automated vehicles and insurers would provide more affordable coverage.

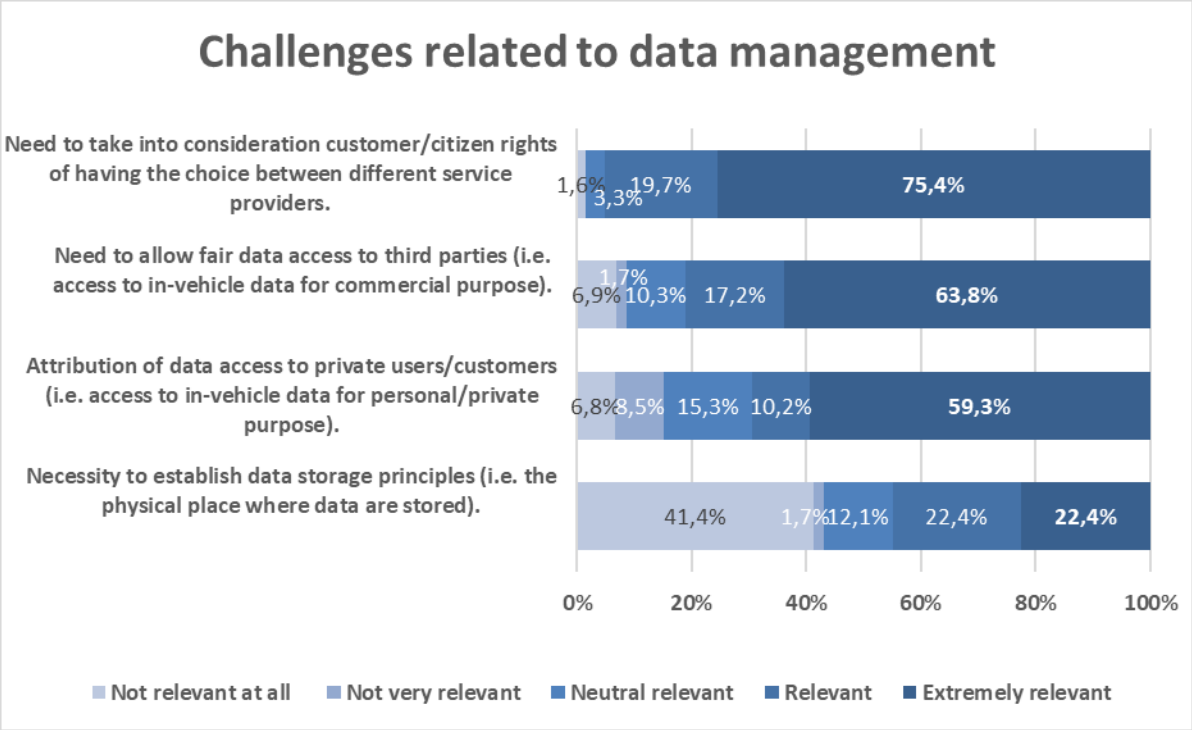


Additional comments were brought forward by respondents on the emergence of a dominant V2X communication technology being critical for the development of automated vehicles. When it concerns infrastructures, some of the stakeholders consider that upgrading them would lead to quicker and smoother cooperation between vehicles and would also facilitate car automation. It is possible that the performance will vary depending on the technology used and this will determine which technology is relevant for a given use case and, in the future, vehicles may be equipped with different technologies. Therefore, the focus should be on compatibility.

12.5.2.4 Data access

Challenges related to data management that might lead to the need of adapting the legislative framework

Below, we identified the challenges related to data management that might lead to the need of adapting the legislative framework. Please, for each of them specify on a scale from 1 to 5 the relevance of the issue in terms of necessity to adapt the legislative framework, where 1 is not relevant at all and 5 is extremely relevant.



75.4% of the stakeholders agreed that the customer choice is fundamental and 63.8% consider as extremely relevant the need of fair data access to third parties (i.e. access to in-vehicle data for commercial purpose). The attribution of data access to private users/ customers (i.e. access to in-vehicle data for personal/private purpose) was also flagged as extremely relevant. The necessity to establish data storage principles is consider relatively relevant, but not a priority challenge.

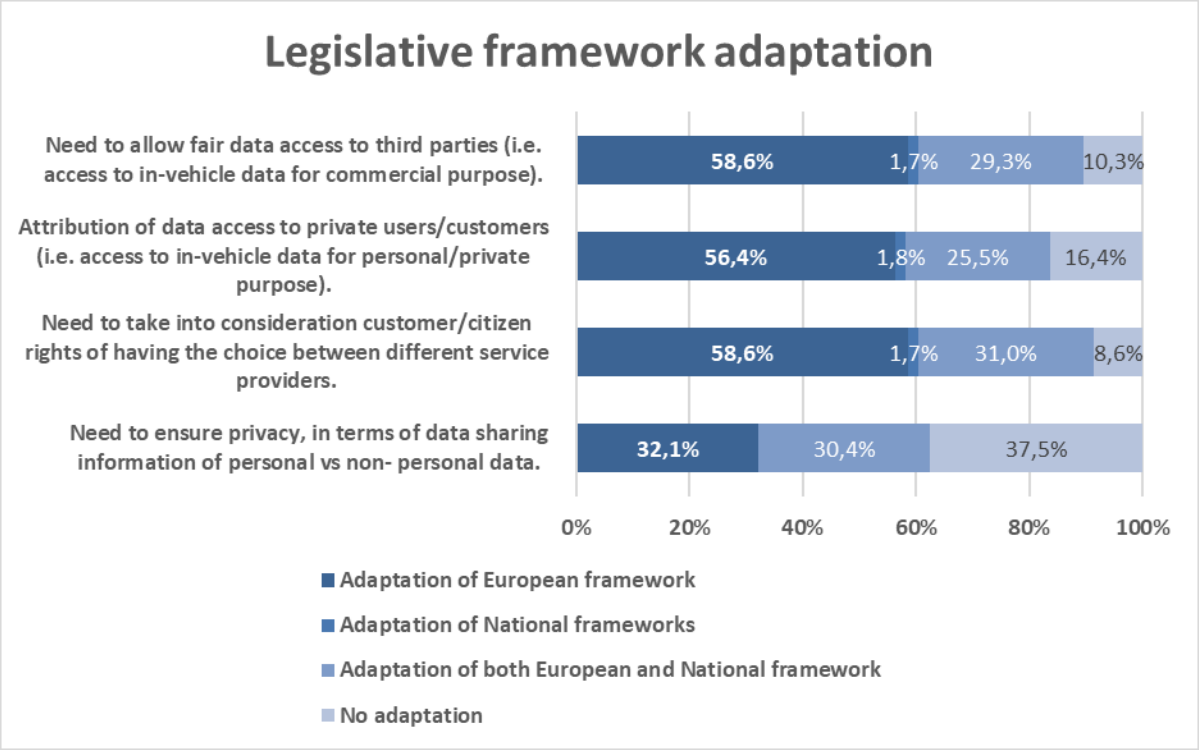
As additional remarks to this question, some respondents suggested that the current regulatory framework for data sharing in the current contract law and competition law is sufficient to deal with data sharing conflicts. However, if a new regulation was considered, it should prioritise safety and security. Stakeholders underlined that the access to data should be fair, but there is a disagreement if this data access should be given to all third parties or a selection of them.

Conversely, some respondents suggested that it is up to the car manufacturer to decide where to stare the data and how to share it with others, in condition to respect GDPR and ePrivacy regulation.

In conclusion, almost all respondents agree on the fact the European Commission should decide and communicate a recommendation or regulation proposal and the decision should ensure the protection of the principles of innovation, non-discrimination and technological neutrality.

Adaptation of national or European legislation

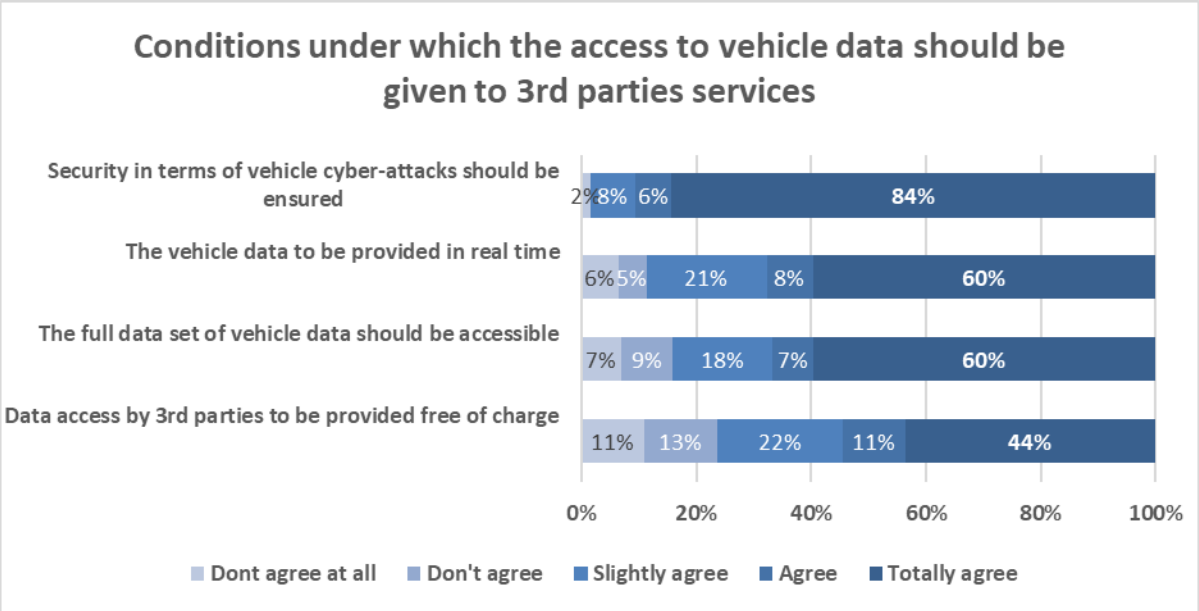
Can you please indicate, for the issues above, whether the legislative framework would need to be adapted at the European level, National level, both of the above or none?



For all the challenges related to data management, the respondents believe that there is a need to adopt European legislative framework, except for the privacy challenge where no legislative adaptation is needed, given the current GDPR. National frameworks are the least preferred solution.

Conditions for data access

Considering the conditions under which the access to vehicle data should be given to 3rd parties services, to what extent do you agree with the following statements?



The main condition under which data access should be ensured to third parties is security (90% of respondents agreed or totally agreed). Data to be provided in real time is equally important to the condition of data set to be complete. Only 44% of the stakeholders consider the free of charge data access to be a prerequisite condition.

Data access solutions

The following options were presented to the stakeholders, to choose the optimal solution for access of vehicle data.

Direct in-vehicle access *(in the on-board application platform and in-vehicle interface): This platform creates opportunity for all stakeholders to access data from the vehicle and to create a wide range of applications.*

In-vehicle interface*: This solution is the current OBD interface. This interface allows connection to devices outside the vehicle. The OBD interface allows access to a standardized set of data such as emissions, fault codes etc Independent and authorized repairers and workshops use the current interface using an OBD connector.*

Access to data through privately owned extended server: *The extended vehicle is a concept developed by OEMs where data generated by vehicle is sent over a secure and encrypted communication channel to a dedicated OEM server. Data made available at the OEM back-end server using a standardized interface will standardise sets of data that can be used by vehicle manufacturers or third-party participants for post processing and development of applications for vehicle users.*

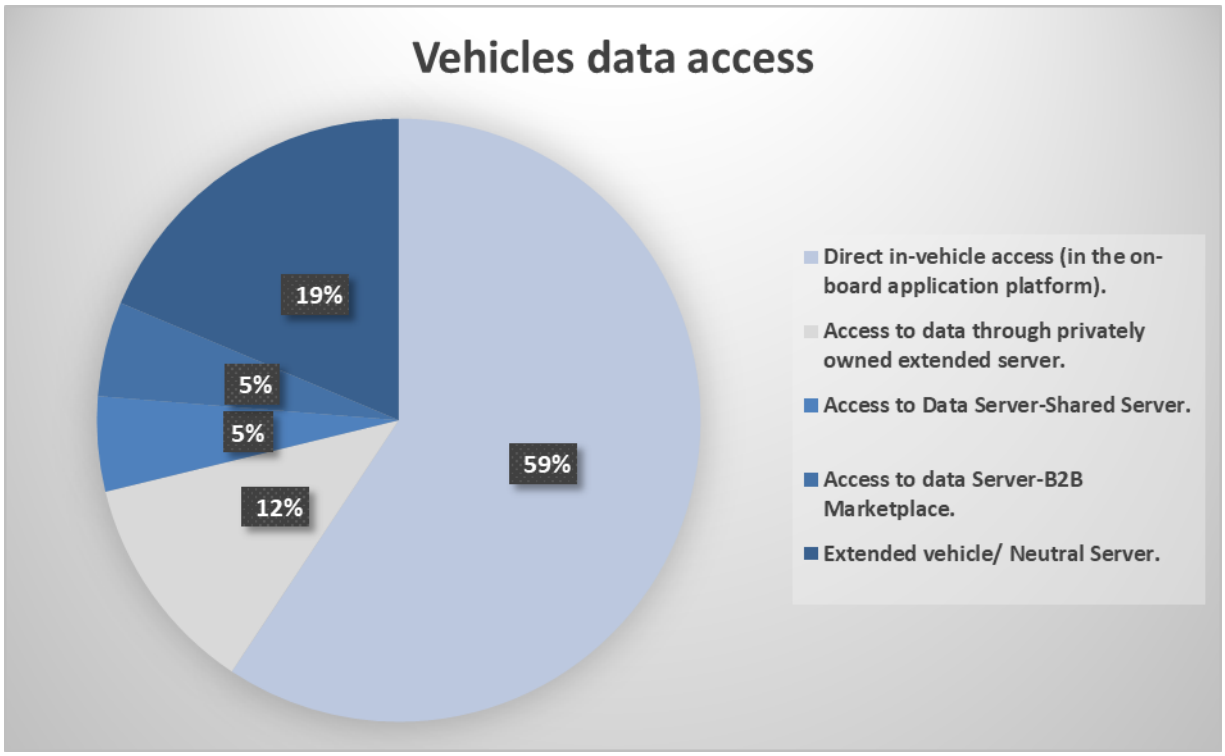
Access to Data Server-Shared Server: *The shared server is neither financed nor operated by an OEM. The OEM plays a role of a system administrator for the transfer of data between the vehicle and the shared server. Data available at the standardized interfaces should be of the same quality as the data of OEM back-end.*

Access to data Server-B2B Marketplace*: B2B marketplace technical solution is again like the other data server solutions but the 'marketplace' allows an independent third party to service and operate access to the vehicle manufacturer server.*

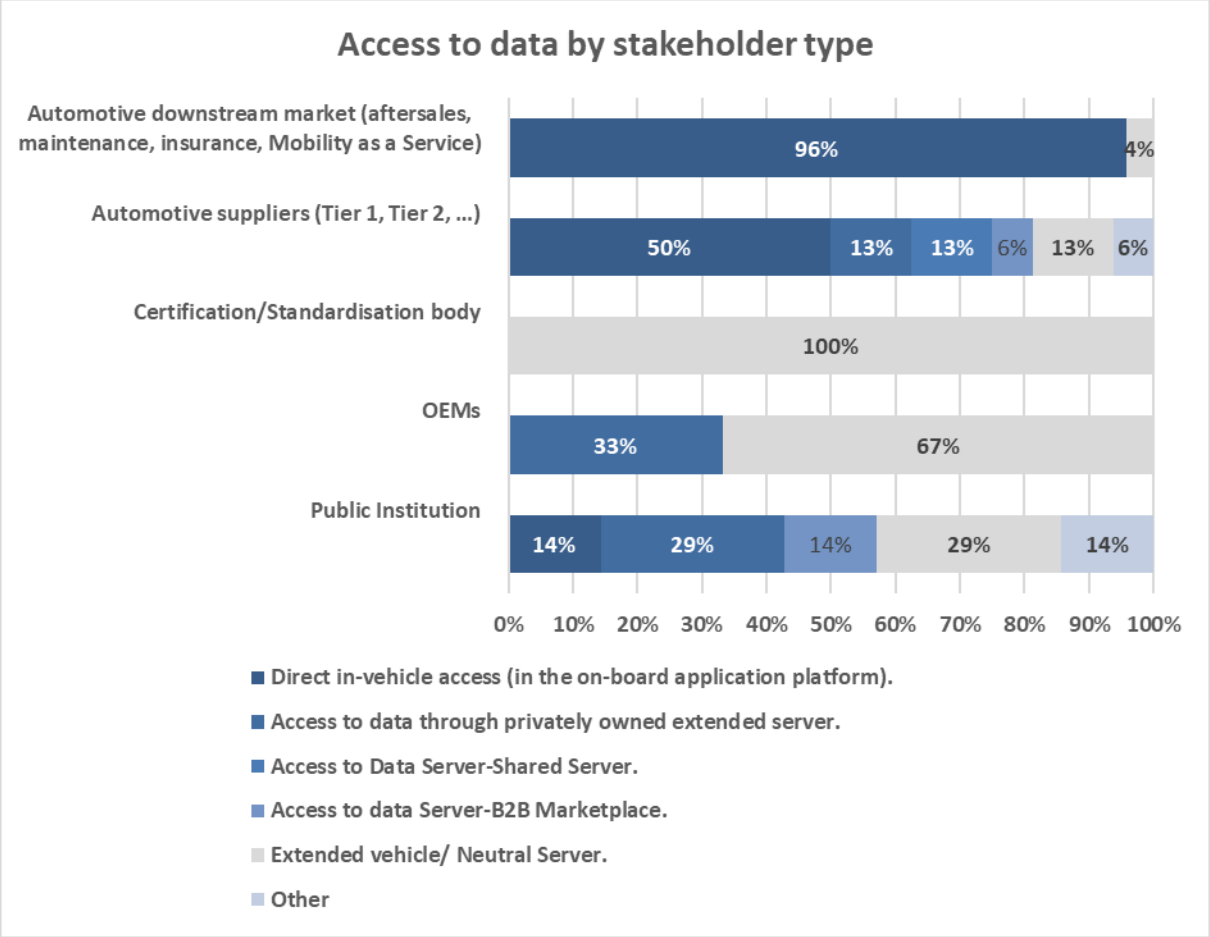
Extended vehicle/ Neutral Server: *Extended Vehicle solution with the addition of a 'neutral server'. The neutral server operator can negotiate with the vehicle manufacturers for additional data fields to be included on their servers without revealing by whom and how this data will be used.*

Which solution is the optimal one? Please explain why

Direct in-vehicle access in the on-board application platform is overall the preferred solution with 59.3% of the votes. The rest of the pie chard is split between the different options that exists for access to data through an extended server. This server could be neutral (18,6% consider this solution as the best one), it could be private (11,9% consider this solution as the optimal one), it could be shared or represent a B2B Market place (equally 5.1% each).



However, the answers received reflect a very strong polarisation according to the stakeholder categories, as evident from the in-depth assessment of answers below.

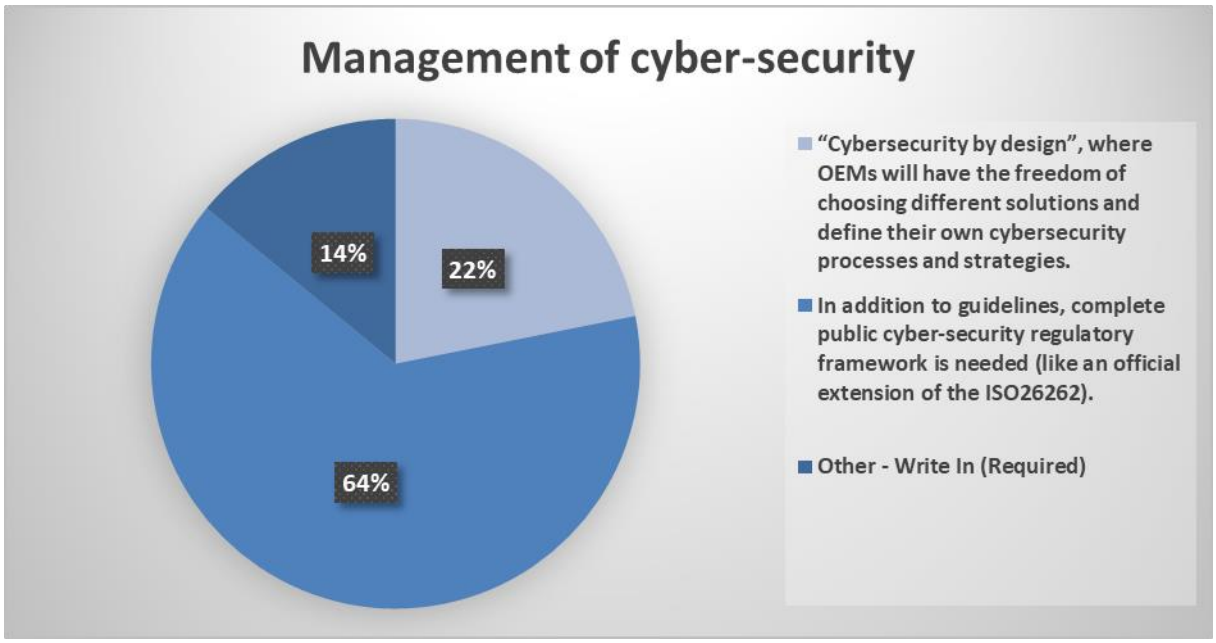


As expected, the survey shows the opposite positions taken by OEMs (extended server) and aftermarket (direct in-vehicle access). Public sector respondents have different positions, similarly to suppliers. Certification bodies support OEMs in the extended server solution.

12.5.2.5 Cyber-Security

Cyber-Security actions from governments

Part of ISO 26262" Road vehicles – Functional safety" is a guideline on cyber-security (SAE Cybersecurity Guidebook J3061). However, there are no regulations from European bodies or National road authorities that already take into full consideration cyber-security. What is your opinion on the way cyber-security should be managed?



64% of the stakeholders believe that complete public cyber-security regulatory framework is needed and 22% of them support the "cybersecurity" by design where OEMs will have the freedom of choosing different solutions and define their own cyber-security processes and strategies.

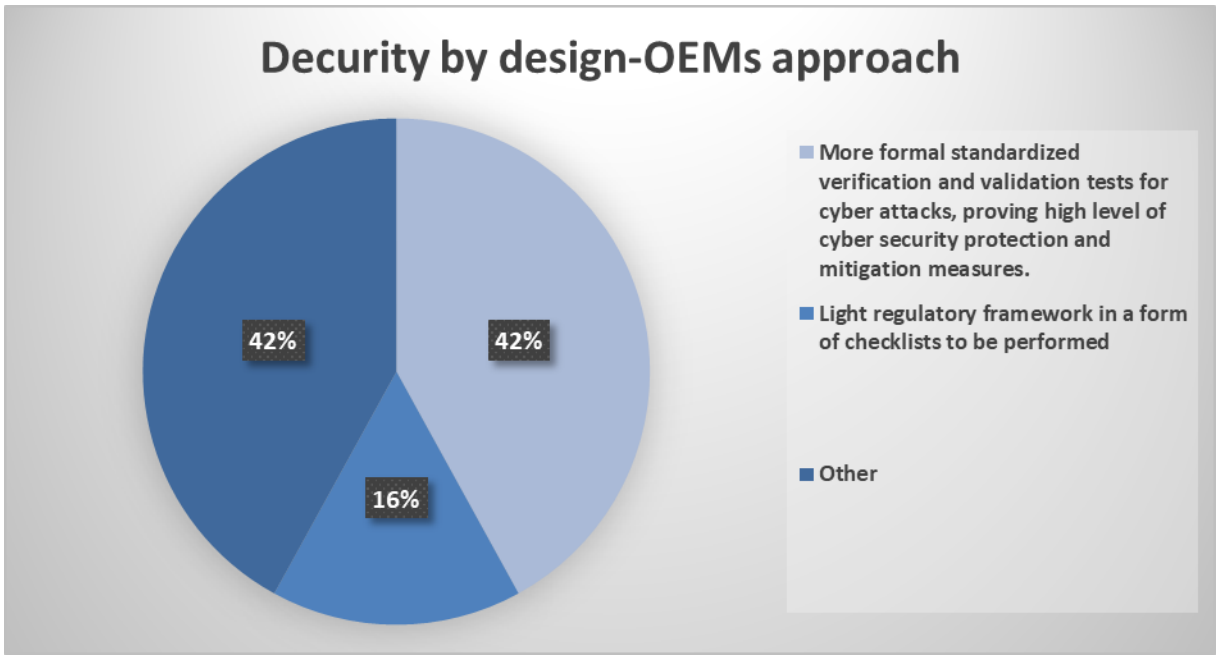
On the one hand, we identified a common opinion that OEMs should not be the only ones defining the security by design and this process should be shared across the value chain. On the other hand, we identified a common opinion that ISO 21434 will become the reference standard on which OEMS will base their security management.

Under "other" approaches to cyber-security management, a recommendation was shared that it is important to adopt cyber security legislation at UNECE level and develop an automotive annex within the general EU ENISA mandate for EU cyber security regulation.

One stakeholder suggested that there is a support for a certification approach that works in tandem with industry-led standardisation. Where safety-critical security features are concerned, mandating of such standards by legislation. Not in contradiction to a ´by design´ approach; it only decouples design intelligence from proprietary exclusivity. Such standards should be based on open specifications.

Cyber-security by design

If you think that the cyber-security should be managed by design, how the OEMs will prove that their cyber-security design is efficient and sufficient enough to allow/permit the automated and autonomous vehicles to driver on the public roads?



42% of the stakeholders also support the more formal standardised verification and validation tests of cyber-attacks, providing high level of cyber security protection and mitigation measures. Only 16% of the stakeholders are for light regulatory framework.

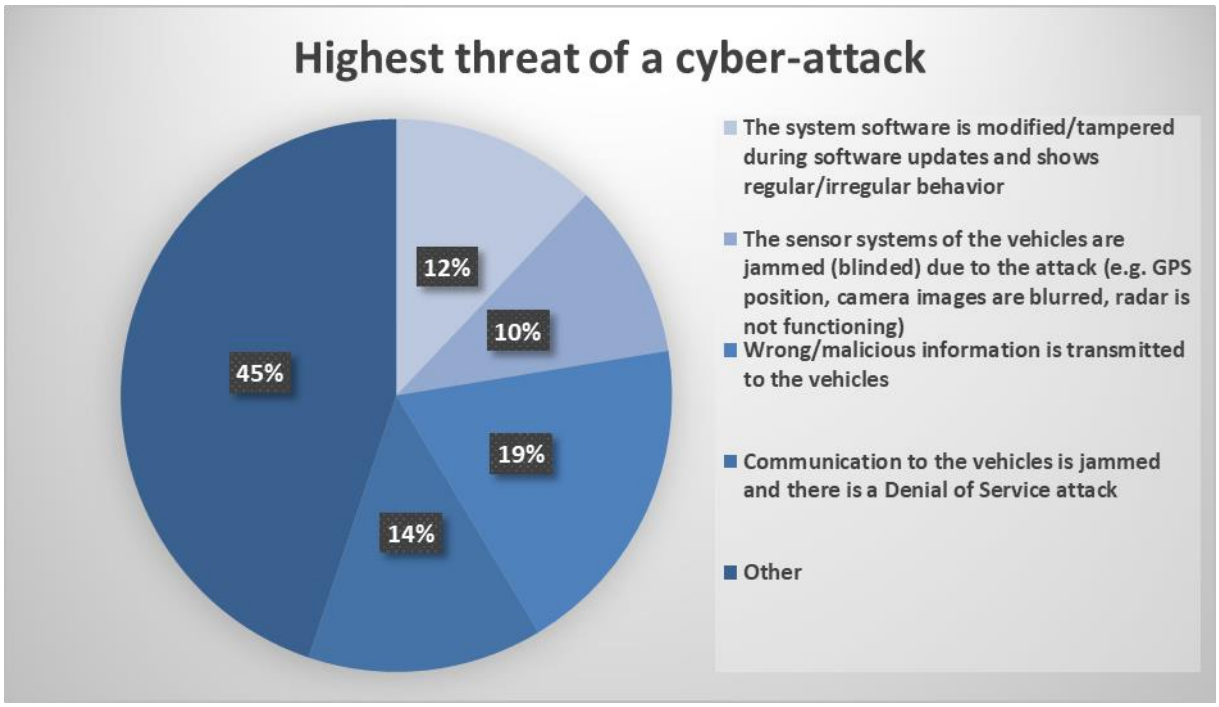
Under "other", which represent 42% of the stakeholder's responses, respondents expressed their view on the point that OEMs should not be fully responsible for cyber-security and public standards for cyber-security levels are needed. In addition, it was suggested that regulation should prohibit to concentrate all functions in one or few other back end servers. Regulation should impose to split the factors of risk and this should be aligned with UNECE activities.

Cyber-security threats

What is in your opinion the highest threat of a cyber-attack?

All the threats listed as potential options (see below) are equally high for most of the stakeholder. This statement was shared by several respondents under "others" since the survey does not provide a choice of "all of them". In addition, other treats are identified to be the combined SAE/ISO standardisation and Autoisac[209]. A reference was provided to the list of threads developed by UNECE cybersecurity Working Group.

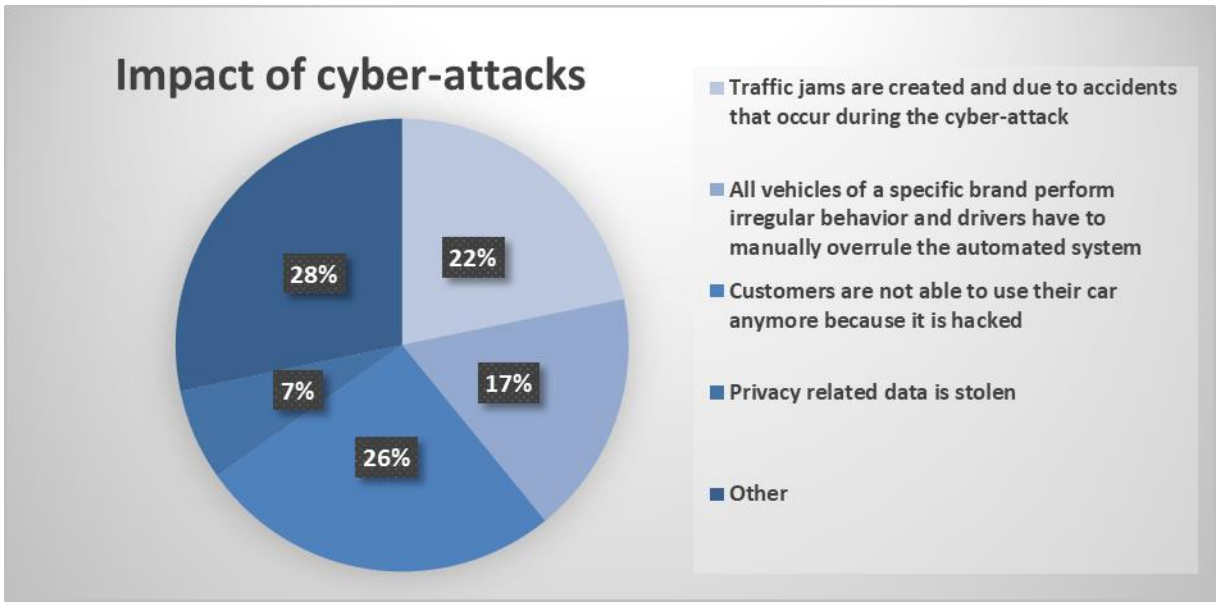
[209] (https://www.iso.org/standard/70918.html and https://www.automotiveisac.com/)



Cyber-security impact and knowledge

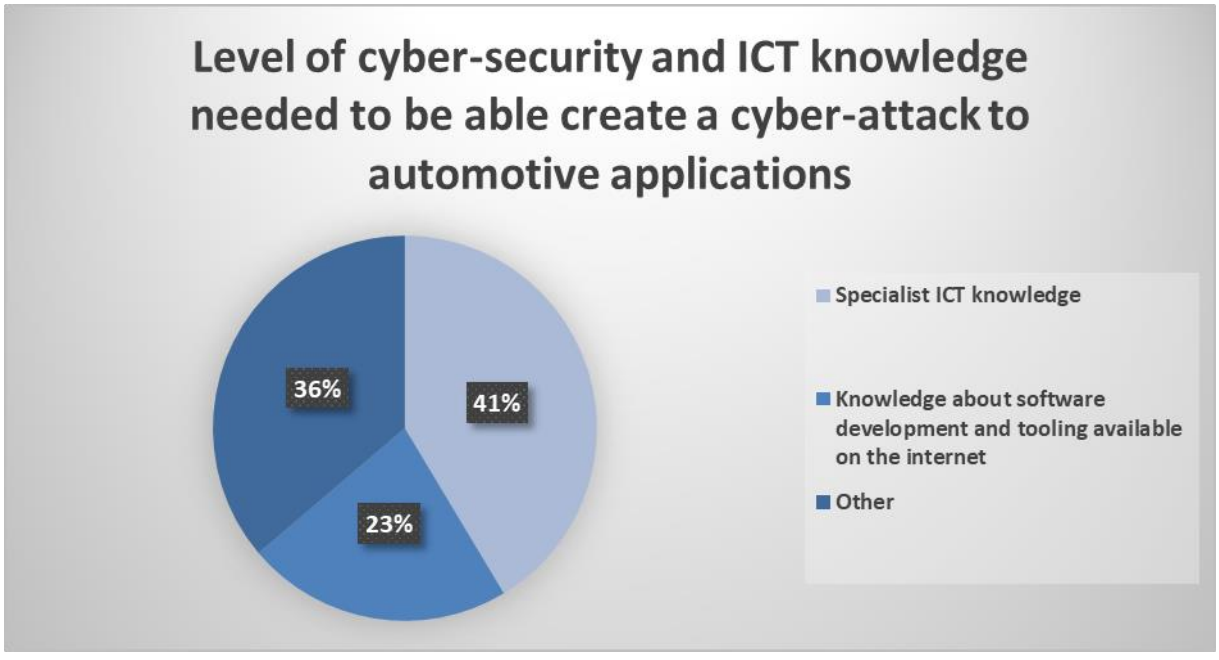
What is the highest impact a cyber-attack can have (even with cyber-security by design methodologies are incorporated)?

All of the impacts listed as potential options (see below) are considered equally of high importance, which is mentioned under "other", since an option "all of them" was not provided. Under other we also find impact on safety, mass manipulation of vehicles leading to traffic security and safety of passengers.26% of the stakeholders believe that the higher impact will be the fact that customers will not be able to use their cars because of the hacking. Another important impact could be the traffic jams created due to accidents that occur during cyber-attacks. 17% consider as the highest impact the irregular behaviour of different cars and the driver should take control of the vehicle. Privacy related stolen data is the least important impact (7%).



What is in your opinion the level of cyber-security and ICT knowledge needed to be able create a cyber-attack to automotive applications?

41% of the stakeholders believe it should be an ICT specialist. Then, stakeholders believe that the level of knowledge requirement is a combination of Specialist ICT knowledge; knowledge about software development of the car together with multiple knowledge on data communication security. It was also specified that it depends on the type of attack. 23% believe that it requires knowledge about the software development and tooling available on the internet.

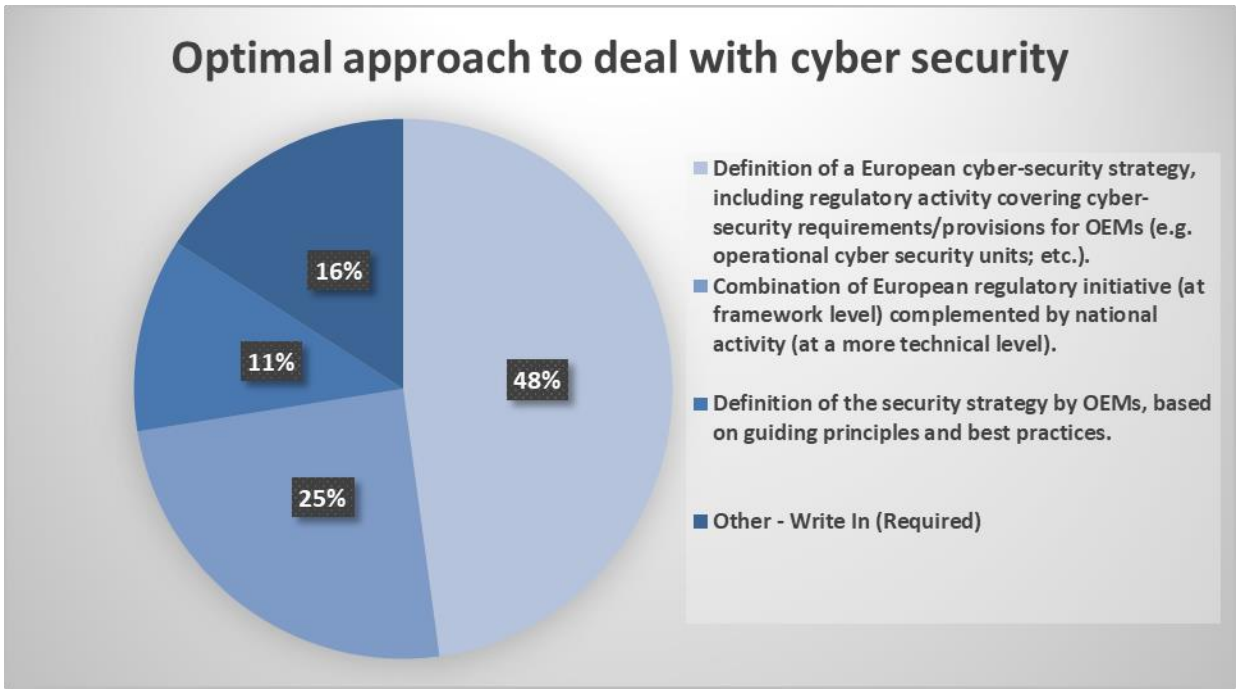


Cyber-security Solution

In relation to automated vehicles, which do you think is the optimal approach to deal with cyber security?

Almost 50% of the stakeholders welcome the definition of a European cyber-security strategy, including regulatory activity covering cyber-security requirements/provisions for OEMs (e.g. operational cyber security units; etc.). **25% support the combination of European regulatory initiative** (at framework level) **complemented by national activity** (at a more technical level) and only **11% are for a definition of the security strategy by OEMs**, based on guiding principles and best practices. Under "other", respondents shared that a minimum level of security should be ensured by legislation. However, the regulatory framework should not be an element of delay for the deployment of CCAM. Some stakeholders also believe that any effective approach to cybersecurity in CCAM should have (at least) a European dimension. The relation between EU and national domains is difficult to pre-specify but agreement and collaboration is necessary to avoid inconsistencies.

One respondent noted that Cyber-security is a subject that needs to be addressed at the global level (UNECE) and over the entire life (cradle to grave) of the vehicle. Another one suggested the setting up of a "European AUTO-ISAC: this body would provide cyber security analysis and share cybersecurity risks with the automotive sector in order to raise stakeholders awareness and exchange on ways to strengthens cars cybersecurity. This body should liaise with other AUTO-ISAC in the world to create synergies.

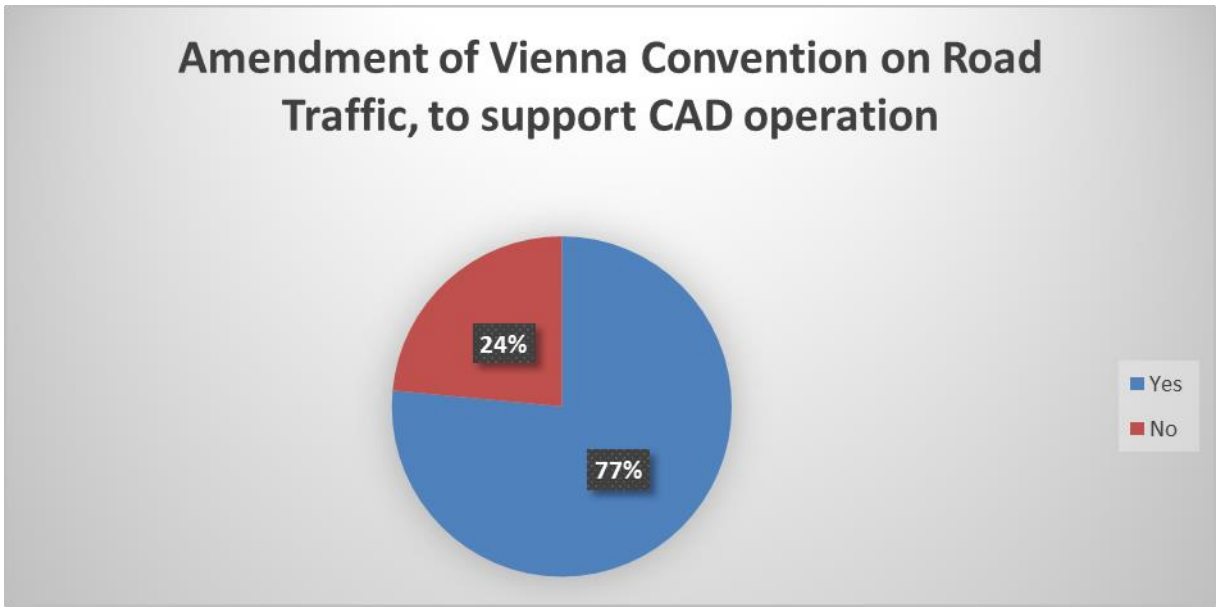


Road legislation

In relation to automated vehicles, do you consider necessary an action in the frame of the following road legislation (please specify only when relevant) a reform of the current road legislation? If yes, please summarize the action synthetically.

Regarding road legislation 77% of the stakeholders consider necessary further amendment of Vienna Convention. Actions in the frame of Mobility as a service regulatory reforms are

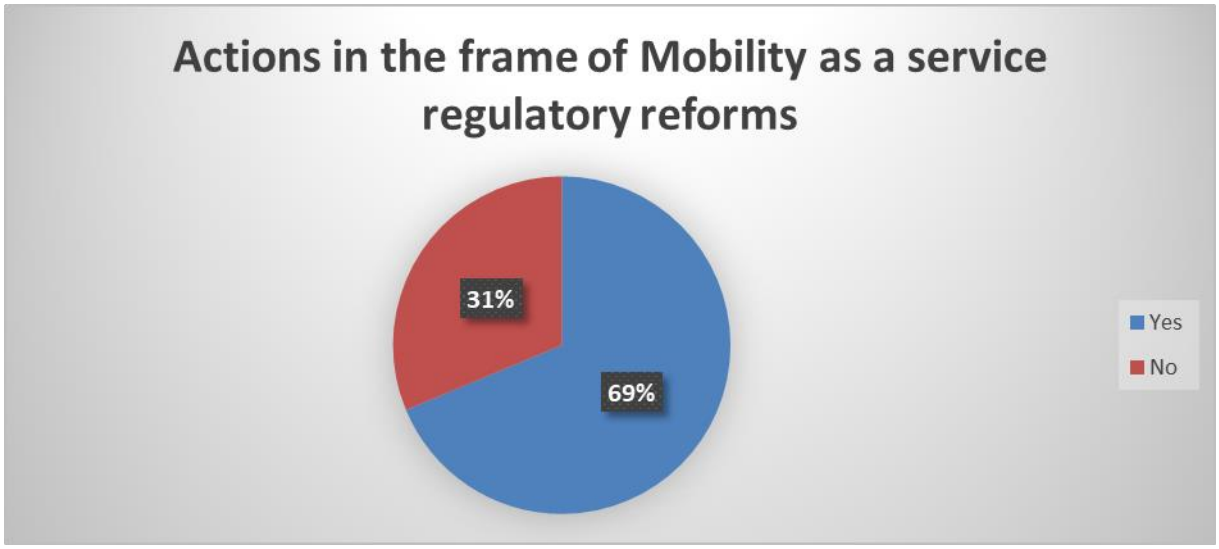
considered necessary by 69% of the stakeholders and only 36% believe that action in the frame of specific national road codes is required.



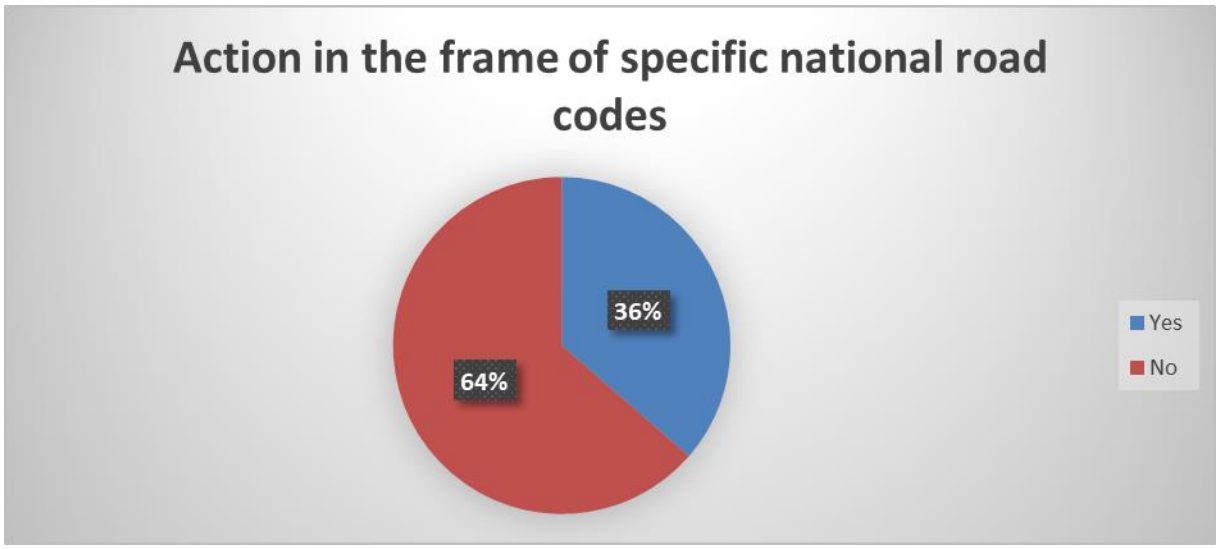
According to one stakeholder, the convention assumes that the driver is always fully in control and responsible for the behaviour of a vehicle in traffic, and this assumption no longer holds in a CCAM-enabled environment. Several respondents believe that further amendments are needed to allow the connected and automated vehicles to be on the market and the tests to be performed. Another one noted that it is necessary to amend the Vienna Convention, by suppressing any references to the driver.

It was also mentioned that it is important to specify under what conditions control needs to be taken back under level IV SAE, as well as anticipate required changes for Level V SAE.

Actions in the frame of Mobility as a service regulatory reforms



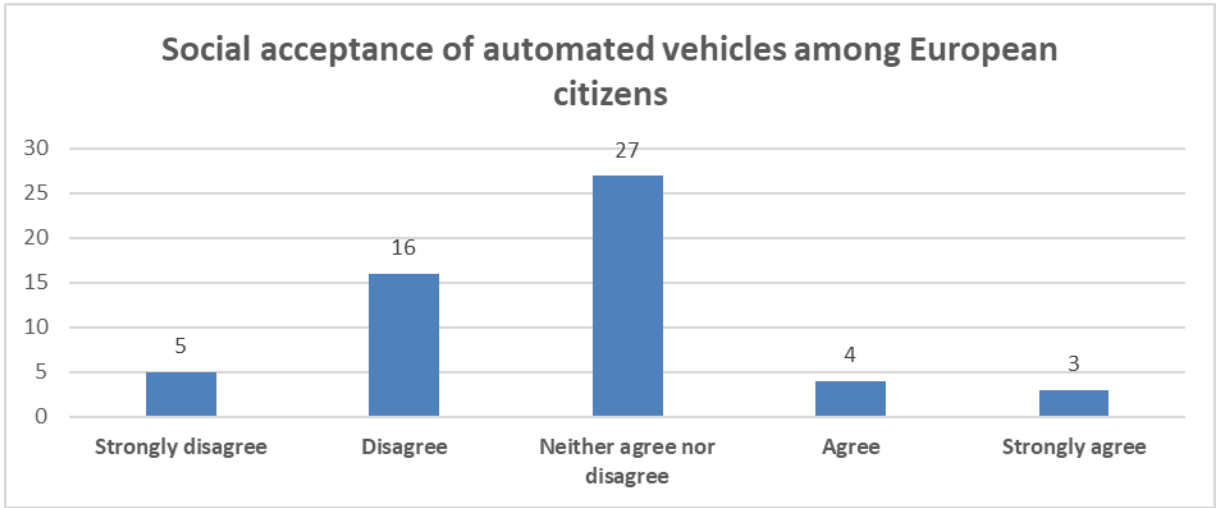
Action in the frame of specific national road codes



Enrich the driving license with a specific mention of Connected and Autonomous Vehicles leading to a driving authorization and ensure access to formation and develop drivers' skills was specified as recommendation from several respondents. It was also noted that curgently road traffic codes varies between countries and if not aligned it would increase complexity of the implementation and increase risk of errors. Additional comment was made on the short -term (prior to amendments to Vienna convention) that it might be needed to clarify at national level the role of the human driver performing "non-driving" activities while the system is in driving mode.

12.5.2.6 Social Acceptance

When considering social acceptance of automated vehicles among European citizens, do you consider the public opinion to be correctly informed about the risks linked to this new technology?



The stakeholder opinion is mitigated regarding their view on the social acceptance and more precisely the consideration of the public opinion and knowledge of risks linked to new technology.

12.6 Annex F: Appendix to the Assessment of the evolution of CCAM market

12.6.1 Announcements and roadmaps by major OEMs

Daimler gave birth to one of the most interesting collaborations in the sector when announcing in April 2017 a partnership with automotive supplier Robert Bosch Group, allowing the two companies to combine Daimler's auto manufacturing expertise with Bosch's systems and hardware skills to accelerate the development of self-driving taxis, the ultimate solution, in the opinion of the two companies, to reduce traffic congestion in cities while drastically improving road safety[210].

Fiat Chrysler Automobiles entered in August 2017 in a partnership with BMW Group – which already teamed up back in 2016 with chip manufacturers Intel – creating of the most interesting alliances in the Automated Driving cars market[211].

Ford, while having declared in April 2017 that it would have a car capable of driving itself in nearly all conditions by 2021, and that it would be available to customers between 5 and 10 years later, has lately announced a slow-down in its participation to the "race" of automated vehicles, opting for skipping semi-automated systems – level 2 and level 3 – to focus on full self-driving cars[212].

General Motors announced in November 2017 the interest to introduce an automated ride-sharing service to several big cities in 2019. Focus of the plan will be to ensure a higher degree of safety for passengers onboard automated vehicles compared with the ones conducted by humans. In addition to that, GM plans to integrate its automated vehicles with software that users can use to request rides on-demand. GM added self-driving expertise to its company know-how in the form of *Cruise*, a San Francisco-based start-up GM acquired in 2016, while fostering its automated vehicle division staff from 90 to 1200 employee[213].

Hyundai-Kia group plans to start mass production of Automated Driving system, able to drive on highways without human intervention, by 2022. The road map developed by the management board foresees to achieve this result based on two intermediate milestones, first to put Level 2 highway driving system into mass production by 2019, second to develop Level 3 Automated Driving by 2020, bringing it to mass manufacturing two years later[214].

Nissan Motor Co. and Renault joined their efforts in the development of an automated vehicle ecosystem in February 2017, focusing not only on the production of self-driving cars but also on the accessibility, easiness and safety of this technology. The partnership, which has also included Microsoft in September 2016, aimed to develop a single platform able to introduce next-generation services, like advanced navigation and remote monitoring, into cars with wireless Internet capability[215].

Independently, Nissan Co. declared in December 2017 that it aims to introduce fully automated cars to the market in 2022, making it one of the most advance car manufacturers in the driverless technologies. In a similar manner to other car manufacturers, the Japanese group plans to add Automated Driving functions step-by-step, moving from level 2 to level 3 by 2020[216].

---

[210] http://fortune.com/2017/04/04/daimler-bosch-self-driving-taxis/
[211] http://fortune.com/2017/08/16/fiat-chrysler-bmw-intel-mobileye-automated-car/
[212] http://fortune.com/2017/12/06/ford-automated-cars/
[213] http://fortune.com/2017/11/30/gm-automated-ride-share-2019/
[214] http://www.autonews.com/article/20170417/OEM10/304179938/hyundai-mobis:-level-3-self-driving-by-22
[215] http://fortune.com/2017/02/27/renault-nissan-driverless-vehicles/
[216] https://www.bloomberg.com/news/articles/2017-12-06/nissan-plans-to-introduce-fully-automated-driving-cars-in-2022

PSA Group released in June 2017 its Automated Driving strategy, "*Automated Vehicle for All*", delineating a plan that starting from current available Level 1 technology should see the first models equipped with Level 2 technology in 2018, Level 3 technology in 2020 to finally Level 4 and Level 5 Automated Driving after 2025[217].

Tesla, a smaller player on the market in terms of annual turnover but which has managed to almost monopolise the attention of both consumers and investors, which announced already in October 2016 that all new vehicles sold would have included the optional equipment capable of enabling the car to drive automatedly, without human intervention. Furthermore, the company has been the precursor of the implementation of many side technologies, as over-the-air software updates, that will be more and more fundamental in the development of Automated Driving vehicles.

Toyota, the biggest car manufacturer in terms of vehicles produced in 2016, has unveiled, at the end of September 2017, its next-generation self-driving test car, introducing for the first-time innovative technologies as a light detection and ranging radar (LiDAR) that measures distances using laser light to generate extremely accurate 3D map of the surrounding of the car[218]. Together with Suzuki Motor, Toyota has also created a new partnership aimed at developing Automated Driving systems, with the goal of sharing and building synergies upon the specific competences acquired in the past year on the Asian and Indian market[219].

Volkswagen group, the parent company of brands that include Volkswagen Passenger Cars, Audi, Bentley, Skoda, and Porsche, presented in March 2017 its fully automated concept called *Sedric*. The concept, that would apply under different forms to all the brands part of the VKG, foreseen a completely automated vehicle, which is not equipped neither with pedals nor with steering wheel, embracing therefore the idea of fully automated driving. Interestingly, Volkswagen brings the concept of Automated Driving beyond the concept of private ownership of the vehicle, foreseeing the opportunity to allow customers to switch between their own personal automated *Sedric*, under one of VW's brands, to a shared vehicle in another city. The group is known to be at the forefront of the implementation of new technologies, as detailed in the business plan "*2025 strategy*" adopted in June 2016. The goal is to push for a restructuring of the company's core automotive business to focus more on electric vehicles and Automated Driving technology, boosting profit margins, and possibly selling some assets. The company plans to introduce more than 30 all-electric vehicles over the next 10 years, with a goal of selling two to three million of these EVs in 2025[220].

Volvo, a company owned by China's Geely Automobile Holdings, is rapidly appearing as one of the most promising brands in terms of Automated Driving technology, with many models currently on the market already equipped with Level 2 technology. Interestingly, Volvo has been the car manufacturer chosen by the peer-to-peer transportation platform Uber to test and develop the driverless evolution of its car sharing service. In November 2017, Volvo stated that it will provide Uber with a model equipped with full automated technology between 2019 to 2021[221].

As it appears evident from the section above, all major OEMs are, with different degree of intensity, investing in Automated Driving technology.

---

[217] http://www.autonews.com/article/20170628/COPY01/306289965/psa-plans-hands-off-self-driving-cars-after-2020
[218] http://fortune.com/2017/09/27/toyota-self-driving-car-luminar/
[219] https://auto.ndtv.com/news/toyota-and-suzuki-officially-confirm-technology-partnership-agreement-1656899
[220] http://fortune.com/2017/03/07/volkswagen-self-driving-car-sedric/
[221] http://fortune.com/2017/11/20/uber-volvo-self-driving-cars/

European producers, notably Daimler, BMW group, Volkswagen group and Volvo are among the major players in the application of new technology to the automotive sector both in developing automated vehicles and services.

Compared to international competitors as Toyota and Hyundai, which are developing Automated Driving technology in their low-end / largely accessible vehicles, European car manufacturers seem to have targeted business and luxury consumers as their principal target, showing a clear differentiation in term of customers targeting strategy as well as a strong differentiation in the concept itself of CAD integration into vehicles. European strategy comes from a long-lasting tradition of offering ad-hoc premium configurations on selected models of its fleet, focusing on high-end business and luxury models.

Different viewers of the market foresee that in the future, a great part of connected car package will be sold as a part of smaller, less expensive cars, therefore moving down the price of this additional technologies proportionally. More importantly, European producers risk to lose their luxury differentiation element, and they would need therefore to act accordingly to maintain their leadership in the market. The shift may be positively influenced by support public sector could express in promoting the mobility as a service trough connected and automated public transport or open access to various private CAD services.

Finally, it is important to notice that impact on automation also impact the **commercial vehicles**. Aside cars, also the trucks' sector will represent an important area for OEMs in terms of testing of new technologies. One example of this is Uber, which is developing an automated truck. In the same way, Waymo also officially unveiled its own trucking pilot, using self-driving trucks to haul Google data centre freight in Atlanta, as well as Tesla. This trend is mostly seen in US, but it has a big potential in Europe.

European Commission

Title
Luxembourg, Publications Office of the European Union

2019– 165 pages

ISBN number: 978-92-79-99495-1
DOI number: 10.2759/448974

European Commission

Study on Safety of non-embedded Software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems

SMART 2016/0071

Annex 3

Task 3 & 4, A prospective foresight study on testing, certification, liability and insurance of advanced robots, autonomous and AI-based systems including connected and automated vehicles

TNO 2019 R10095

A study prepared for the European Commission
DG Communications Networks, Content & Technology
by:

TNO innovation for life
VVA CONSULTING
Sant'Anna Scuola Universitaria Superiore Pisa

Digital Single Market

This study was carried out for the European Commission by

Main Authors:

- Andrea Bertolini (SSSA) – task coordinator
- Erica Palmerini (SSSA)
- Francesca Episcopo (SSSA)
- Stefano Alberti (SSSA)

Authors contributing to §§2.5.2 – 2.5.5,2.6.2.5 – 2.6.3,3.2.3 – 3.2.5:

- Marc van Lieshout (TNO)
- Kristina Karanilokova (TNO)
- Tjerk Timan (TNO)
- Sven Janssen (TNO)

Interviews conducted by:

- Marco Bolchi (VVA)
- Maria Kirova (VVA)

Internal identification

Contract number: 30-CE-0887241/00-16

SMART number: 2016/0071

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN number 978-92-79-99495-1
DOI:number 10.2759/448974
Catalogue number: KK-04-19-076-EN-N

Executive Summary

This report addresses three aspects, namely (i) testing, (ii) certification, and issues regarding (iii) liability, insurance and risk management, concerning both industrial robots (IRs) and connected and automated driving devices (CADs).

Testing. Testing represents the procedures, evaluations and trials performed during the development of the product, to assess the performance and reliability of the device, against a series of benchmarks. The study identifies and assesses the legal framework applicable, and the techniques used, suggesting alternative approaches when needed.

Certification. Certification is the procedure each product has to undergo in order to be traded onto the EU market, assuring compliance with the minimum safety requirements put forth by applicable legislation and easing circulation of goods within the common market. Said requirements can be met through compliance with technical standards, especially if provided with reinforced legal value (such as harmonized ones). The analysis will determine whether IRs and CADs fall within existing safety regulations, whether the latter are adequate, and whether existing standards are sufficient and/or sufficiently narrow tailored for these novel applications.

Liability, insurance and risk management. Civil liability determines who bears the economic consequence of an accident, and – traditionally – provides *ex ante* incentives towards a high-level of product safety, while insurance allows such costs to be internalized and managed, and compensation to be secured.

The Risk Management Approach (RMA) decouples the traditional functions of liability, i.e. deterrence and compensation. It relies on *ex ante* regulations to obtain safety and security of products, and holds strictly liable the party that is best positioned to (i) minimize risks and (ii) acquire insurance, to grant prompt and adequate compensation *ex post*.

The study aims to determine applicable liability rules, identify criticalities and propose solutions to address them – pursuant to a RMA and other approaches when relevant –, while at the same time assessing the availability of technology-specific insurances and their impact on technological development.

INDUSTRIAL ROBOTS

Introduction. Absent any legal definition, and on the basis of international standards, an **industrial robot** can be defined as an «automatically controlled, reprogrammable, multipurpose manipulator, programmable in three or more axes, which can be either fixed in place or mobile for use in industrial automation applications» (ISO 10218-1:2011, ISO 8373:2012).

Given the breadth of the category, the study is performed on **three case studies**, which display different characterizing features of Industry 4.0 robotics, namely:

- **collaborative robots**: «robot[s] designed for direct interaction with a human» (ISO 8373:2012, ISO 10218-2:2011);
- **mobile robots**: «robot[s] able to travel under [their] own control» both «with or without manipulators» (ISO (8373:2012, ISO 19649:2017);
- **exoskeletons**: external structural mechanism with joints and links corresponding to those of the human body (see, for personal care robots, ISO 13482:2014).

As for the **subjects** involved in the testing, certification, liability and insurance of IRs, the study addresses:

- those who bear a direct **safety-related duty** (ISO 10218:1): **manufacturers**, **suppliers** of individual components, **integrators** and **business-users**;

- **other subjects**, who still play a fundamental role for depicting the general framework: potential victims – non-business-users and by-standers –, certification competent bodies – notified bodies, notifying authorities and notified authorities – and insurance companies.

Testing. Testing of IRs consists of the different procedures performed in the development and production of robotics, with the purpose of verifying goals and functionalities – so called «**performance** testing» –, and gathering knowledge about potential risks and failures connected to their use – so called «**reliability** testing». Despite a general duty to perform testing can be identified as underlying the overall framework on product safety, **there is no specific regulation** neither at the EU nor at the MSs level, establishing how testing should be performed for the purpose of obtaining functional and safe products, or setting procedures to be followed in order to carry out particular activities. However, the **general obligations related to the health and safety at work apply**, thus requiring testing to be performed in a way that does not put at risks operators and other subjects involved.

During the entire production cycle of the IRs, which comprises experiments and design, development, manufacturing and final validation, tests are performed through a series of techniques – such as mathematical modelling and simulation– which are used for each component and the assembled system, in combination with each other and according to a scrum methodology, starting from more computerized solutions and progressively inserting real-life trials.

In this process, **risk assessment and evaluation** take into account the extant **functional and safety requirements,** set in different EU legislative documents and international standards. The general duty to market safe products requires preventive measures against **unforeseen risks**. This is particularly important for Industry 4.0 robotics, as **machine learning solutions, cybersecurity risks and loosely structured work environments** bring about new scenarios which might make the human-robot interaction more dangerous, and that are, however, difficult to foresee and evaluate. Therefore, testing has to be adapted as to allow greater availability of data for software-training, and requires precautionary measures to avoid damages.

Against this picture, a lack of specific regulation seems to foster rather than hinder testing of IRs, since it allows businesses to develop the solutions which best fit their production without incurring in additional procedures and costs. Moreover, since testing, also when based on real-life scenarios, is performed in private locations, no regulation for ensuring safety, either than the one on working environments already in place, is required. Therefore, **no legislative intervention is needed**. However, the lack of shared benchmarks and experimental reproducibility, as well as the difficulties in accessing data and facilities for SMEs and researchers, and the uncertain realization of available standards, yields for the **creation of good practices** which could act as instruments of soft law, **and the establishment of Digital Innovation Hubs (DIHs)** across Europe, to create synergies and grant further resources.

Certification. Certification is the procedure each product has to undergo in order to be marketed within the EU, and assure compliance with minimum safety requirements.

Absent any rules specifically put into place for IRs, it is necessary to ascertain whether extant rules apply to IRs. On the basis of existing legislation:

- **all IRs** qualify as «machinery» or «partly completed machinery», hence **fall within the scope of the Machinery Directive;**
- **exoskeletons** may also be considered as «personal protective equipment», and, to a more theoretical extent, medical devices, and thus are subject to the **Personal Protective Equipment Directive** or **Medical Device Directive, and the Regulations repealing them**.

IRs may need **multiple certifications**, not only when they are marketed outside Europe, but also when falling within multiple classifications, when other rules – such as those related to certification of low voltage electrical equipment – apply, and even when further modification (e.g. by the business-user) are made to an already certified product.

Pursuant to the rules set out in the aforementioned legislation, harmonization is limited to the essential requirements, with technical specifications being set out in **harmonized standards** that, if applied, grant a **presumption of conformity** with the corresponding essential requirements, and, in some cases, a **simplified conformity assessment**.

As far as **cobots and mobile robots** are concerned, the study demonstrated that they are mostly qualified as machinery or partly completed machinery, and that – since manufacturers often rely on self-certification – the subject who faces the most relevant burden is the SI, who substantially modifies the original product also adding collaborative features, and will thus need to obtain certification again. Likewise, certification will be required also by business-users, should they decide to further adapt and modify the integrated machine.

Despite not specifically adopted for such kind of applications, both the **legal framework and the standards available appear sufficiently defined and enough in number.**

On the contrary, (i) the peculiar nature of industrial **exoskeletons**, (ii) the certification burden resting mainly upon the manufacturer alone, and (iii) the qualification pursuant to the applicable legal framework, are more ambiguous, leading to **uncertainties** and market-driven qualifications, which might create problems in the longer run. Additionally, only general standards apply to exoskeletons, since no specific ones could be found. Thus, framework amendment would be welcomed by stakeholders: **legal provisions concerning industrial exoskeletons would help clarifying duties that lie on manufacturers and the other involved subjects, issue of more standards would aid in pursuing the same goals**.

Despite mentioned by stakeholders operating primarily in the field of exoskeletons, the suggestion of **creating a public database and repository of already applied certification procedures that could ease the position of those seeking the certification of advanced devices** – which might not fall squarely under a specific regulation –, seems of greater value, and might be generalized to include other kinds of advanced industrial robotic applications. In such a perspective, intellectual property rights and relevant industrial secrets should always be protected and be left unaffected.

***Liability*.** Liability issues are tackled by a legislative and regulatory framework addressing both (i) **safety and health on the workplace** and (ii) **general private law liability burdening producers for defective products**.

Sub (i), a comprehensive set of European normative bodies – and national implementation acts – require business-users to ensure that workplace – to be intended as both working environment, equipment and working conditions – are not only safe, but globally healthy for employees.

Therefore, **in case of relevant accidents or illnesses, workers are entitled to obtain damage recovery**. In most Member States, liability regimes related to work accidents are coupled with **social insurance mechanisms**, so as to strengthen the employee's position and not to discourage entrepreneurship. Given certain conditions, social insurance bodies are then entitled to act in recourse against employers.

Sub (ii), both manufacturers, suppliers and integrators may qualify as producers, pursuant to the **Product Liability Directive** (PLD), which establishes a **semi-strict liability** regime burdening producers. PLD has been showed to offer **insufficient protection to the**

victims, providing sometimes difficult liability ascertainment and apportionment, and an uneasy burden of proof concerning defects and causal links.

Nonetheless, besides the general need of a PLD reform, under IRs' point of view **the current liability and insurance *status quo* is sufficient**, because the **victim may clearly identify the party *prima facie* responsible to provide compensation** – namely the business-user –, and **contractual agreements and business relations thoroughly bind relevant stakeholders**. Moreover, the absence of theoretical disproportion in negotiating power or access to technical evidence, and the likelihood that liability-related costs can be sensibly distributed along the value chain, sensibly reduce concerns that would otherwise be present due to some criticalities that emerge from the application of the PLD.

CONNECTED AND AUTOMATED DRIVING

Introduction. Automated driving has the **potential to bring many social benefits**, and most importantly to increase road safety by eliminating the major cause of accident, i.e. human error, and its introduction has been supported by the European Union through different policy initiatives.

CADs are vehicles which display two main features: (i) **they are connected with other vehicles, with the infrastructure, and/or with other devices; (ii) they have different degrees of automation**, which, for the purpose of this report, are indicated according to the SAE scale of automation.

At the EU and international level, both the definition of vehicle set out in the Framework Directive 2007/46/EC (FD), and in the Motor Insurance Directive (MID) do not include the human driver as a constitutive element. Likewise, many – but not all – MSs possess a definition of vehicle, that would accommodate CADs.

Testing. The amended **Vienna Convention on Road Traffic** allows automated driving, provided that the technologies used comply with the UN regulations, or can be overridden by the driver. Many MSs have regulated testing of CADs on public roads, according to different requirements and procedures. The majority only allow high automation, while others also accommodate trials of fully autonomous vehicles, or are taking actions in that direction.

Testing is performed both on whole vehicles, on components and on systems of components, usually according to a combination of different techniques. Physical testing can take place indoors, outdoors, in controlled environments and on public roads, while virtual testing involves computer modelling. During trials, it is fundamental to take into account CADs specific risks – related to machine learning, cyber-security, unpredictability of the driving environment (e.g. because of the behaviour of bystanders in real life testing), and the possible fall back of test-drivers –.

Fragmented regulation limits the possibility to test among MSs, creates additional burdens on companies, and hinders technological innovation. Only **EU level novel regulation** seems able to tackle the aforementioned issues, build a level playing field and enhance innovation, especially when higher degrees of automation are considered. This should be accompanied by **exploitation of virtual testing and common repositories of benchmarks and data sharing tools**. The creation of **Tokku zones and regulatory sandboxes**, derogating from regulation which is incompatible with testing of CADs, is suggested as a way of facilitating trials in real life condition.

Initiatives to foster research and development of technical solutions incrementing the accuracy, variety and complexity of the scenarios which CADs shall be tested against, especially through virtual testing, as well as tools for data-sharing and common benchmarks and practices, are needed.

Certification. For certificatory purposes CADs are compared to road vehicles, therefore, pursuant to the European applicable framework, the relevant conformity assessment procedure is the **type approval**, which in turn makes reference to **UNECE Regulations**, and is based on the principles of third-party assessment and mutual recognition.

UNECE Regulations, initially established in 1958, have **gradually and partially been amended in order to describe requirements for advanced devices involving automation.** Therefore, even if completely autonomous steering is still forbidden in any case, vehicles featuring steering aids can now be type-approved. As far as the braking function is concerned, as well, automated braking devices – able to prevent accidents and improve the vehicle's safety overall – are allowed and comprehensively regulated in UNECE Regulations. Concerning the lighting devices, on the other hand, UNECE Regulations now allow the automated switching on of emergency lights in case of danger, but still do not allow direction indicators to switch on independently.

Thus, **UNECE regulations appear capable of adapting** over time and encompassing major advancements. **Future reforms to accommodate emerging features could be awaited**, similarly to what already happened and was just described.

More globally, **the whole type approval procedure**, envisaged by the applicable European Framework, **does not seem perfectly consistent with CADs' peculiar features** and the advanced degree of technology shown.

First of all, type approval is focused on a static evaluation of a vehicle specimen at a given time. While this is consistent with the nature of traditional non-automated vehicles, which do not modify or update over time, it **fails to take into account the fact that AI applications – among which CADs – evolve their functioning, learning from previous experiences and receive constant and substantial updates**.

Components which are based on AI, moreover, do not interact among each other simply from a mechanical or electrical perspective, just like traditional road vehicles' parts, but they do so at a wholly different level, involving other CADs and infrastructures.

On side of that, a feature of CAD is not just the increasing degree of automation, but also the **novel connection that occurs both between different vehicles and between vehicle and road infrastructure**. A static evaluation method like traditional type-approval does not take this phenomenon into account.

Therefore, several stakeholders suggest that **the type-approval certification method should be amended, in order to adapt to new AI-based technologies, by introducing a more convenient and less burdensome approach, that may take advantage of virtual testing and modelling techniques, and that requires the monitoring of the performance of the vehicle over time**.

Liability. At a European Union level, relevant bodies of regulation concerning liability issues and CADs are **the Product Liability Directive (PLD) and the Motor Insurance Directive (MID)**, both of which have recently been subject to official evaluation, in order to assess whether technological developments suggest revisions or amendments. As far as the former is concerned, the conclusion was reached that the PLD is fit for purpose, while, as far as the latter, instead, a reform proposal has been developed but it does not address CADs.

More broadly, since almost the totality of CADs is to be legally considered as road vehicles, **regulatory framework concerning motor liability and insurance apply, also at MS level**. Research on different MSs' legal systems showed that the driver and owner are usually held liable, oftentimes in jointly and severally. Some MS chose fault-based rules for the driver's liability and semi-strict regime for the vehicle's owner, while others opt for no-fault systems and automatic compensation plans, in order to better protect road accident victims.

Some countries enacted **ad-hoc legislative provisions regulating CADs**. **Germany** enacted a system whereby **liability rests upon the driver in case he fails to supervise** the driving task and resume control in case of need. In the United Kingdom, instead, the Automated and Electric Vehicles Act 2018 extends to CADs the insurance duties that typically concern traditional, non-automated vehicles, while the vehicle owner is responsible to ensure that all safety-critical updates are installed in a timely fashion.

Until vehicles reach full automation (SAE level 5), the driving-task is handled both by the autonomous system and the human driver; thence, **both the PLD and traffic liability rules apply, and overlap in determining liability for any given accident**. This circumstance causes the **apportionment of liability** among potentially liable parties to become ever more **complex**. Moreover, some criticalities that are already today displayed by the PLD – namely the complex burden of proof the claimant needs to meet in order to establish defectiveness and the existence of a clear causal nexus between the event and the defect – are further exacerbated by similar scenarios, primarily to the **disadvantage of the victim and even more of the owner of the vehicle**. The latter, indeed, will most likely be sued and won't easily succeed in acting against the manufacturer in recourse.

With respect to the evidentiary burden, it shall be further stressed how the **limited access to the data recorded** by the vehicle, as well as its complex interpretation, requiring access to proprietary information possessed by the manufacturer, might substantially impair the possibility for the victim – or owner – to successfully bring a claim to court, giving rise to relevant problems of access to justice.

The simple provision of a duty to insure – despite useful – is incapable of successfully addressing the above described issues, for it should be clarified which party bears what risks.

It is argued that **the best solution**, in order to ease penetration of CADs into the market, while at the same time protecting other road users and enhancing innovation, **would come from ad-hoc legislation adopted at EU level**.

Indeed, absent EU initiatives, MSs would adopt different legislative and regulatory frameworks at national level, leading to regulatory and market fragmentation. A reform of the PLD, on the one side, would exceed the purpose, while, on the other side, requiring longer elaboration might induce MSs intending to act early to intervene, leading to a similar conclusion.

Ad-hoc EU legislation would be beneficial, with the aim of **creating a level playing field and to avoid fragmentation, both from a market and a technological point of view**: these two profiles are intertwined, since differing liability rules may yield different technological approaches, limiting cross-border market and operation of advanced AI-based vehicles.

It would be advisable to avoid focusing on the ascertainment of fault, while choosing a **Risk-Management Approach (RMA), therefore establishing *ex ante* to burden the party who is best positioned to minimize risks, to ensure compliance and to get insurance**.

RMA, in combination with **strict liability**, would identify a **clearly responsible party pursuant to a one-stop-shop approach**, easing distribution of costs along the value chain, primarily through contractual agreements, limiting litigation.

A viable example of a RMA, is that which burdens manufacturers and not users – unlike the UK law– with the duty to install safety-critical updates. While on the one hand, one could argue that the negligent user – who had been prompted to act and failed to do so – is to be reprimanded, the manufacturer is better positioned to ensure compliance, already in the way he designs and conceives the system and its updating functionalities.

Table of Contents

LIST OF TABLES

List of abbreviations

ABGB	Austrian Civil Code
ACSF	Automatically Commanded Steering Function
ADAS	Advanced Driver Assistance System
AGV	Autonomous Guided Vehicle
AI	Artificial Intelligence
AutoVeh	Automated Vehicle Testing
AV	Automated Vehicle
BEUC	European Consumer Organization
BMVIT	Austrian Ministry for Traffic, Innovation, and Technology
CAD	Connected and Automated Driving
CARTRE	Coordination of Automated Road Transport Deployment for Europe
CATI	Computer-Assisted Telephone Interview
CCAM	Connected Cooperative and Automated Mobility
CSF	Corrective Steering Function

DGEC	Director General of Energy and Climate
DGT	Dirección General de Tráfico
DIH	Digital Innovation Hub
DRW	Directive on Requirements for the Workplace
DSR	Road Safety Delegate
ECU	Electric Control Unit
EEA	European Economic Area
EESC	European Economic and Social Committee
EKHG	Austrian Railway and Motor Vehicle Third Party Liability Act
EN	European Standard
ESA	European Supervisory Authorities
EU	European Union
EU-OSHA	European Agency for Safety and Health at Work
EURON	European Robotics Research Network
FD	Framework Directive on type approval of vehicles
FESTA	Field Operational Test Support Action
FIA	Federation Internationale de l'Automobile
FII	French Insurance Code
FOT	Field Operational Test
GEM SIG	Good Experimental Methodology Special Interest Group
GPSD	General Product Safety Directive
hEN	Harmonized European Standard
HiL	Hardware in the Loop
I4MS	ICT Innovation for Manufacturing SMEs
IAD	Intelligent Active Device

IR	Industrial Robot
ISO	International Organization for Standardization
ITS/AD	Intelligent Transport System – Automated Driving
LVD	Low Voltage Directive
MD	Machinery Directive
MDD	Medical Device Directive
MDR	Medical Device Regulation
MID	Motor Insurance Directive
ML	Machine Learning
MS	Member State
NANDO	New Approach Notified and Delegated Organizations Information System
NCAP	New Car Assessment Programme
NDS	Naturalistic Driving Studies
NHTSA	National Highway Traffic Safety Administration
NoE	Network of Excellence
OEM	Original Equipment Manufacturer
OICA	Organisation Internationale des Constructeurs d'Automobile
PLD	Product Liability Directive
PPE	Personal Protective Equipment
PPED	Personal Protective Equipment Directive
PPER	Personal Protective Equipment Regulation
ProdHaftG	German Product Liability Act
RAM	Regulation on Assessment Methods
RAPEX	Rapid Alert System
RAS	Robotics and Automation Society

RIDC	Robotic Industry Development Council
RMA	Risk Management Approach
RV	Regulation on the approval of motor Vehicles
SAE	Society of Automotive Engineers
SCGD	Directive on Sales of Consumer Goods
SGGM	Subdirección General de Gestión de la Movilidad
SI	System Integrator
SME	Small and Medium sized Entreprise
SOTIF	Safety Of The Intended Function
TFEU	Treaty on the Functioning of the European Union
UNECE	United Nations Economic Commission for Europe
VCRT	Vienna Convention on Road Traffic
VDPTC	Vehicule à Délégation Partielle ou Totale de Conduite
WED	Directive for the use of Work Equipment
WFD	Work Framework Directive
WP.29	World Forum for Harmonization of Vehicle Regulation

1. INTRODUCTION AND BACKGROUND OF TASK 3 & 4

KEY FINDINGS

- This report addresses: (i) testing, (ii) certification, (iii) liability, insurance and risk management of industrial robots (IRs), and connected and automated driving (CAD).
- Testing consists in the trials performed during the products' development, to assess performance and reliability.
- For both IRs and CADs, the study identifies and assesses the applicable legal framework for testing and the techniques used in the different stages of product development, suggesting alternative approaches when needed.
- Certification is the procedure a product has to undergo in order to be traded onto the EU market, assuring compliance with the minimum safety requirements put forth by applicable legislation. Such requirements may be met by complying with technical standards, especially if provided with reinforced legal value.
- For both IRs and CADs, the report identifies and assesses the applicable legal framework and relevant standards, proposing reform where appropriate.
- Civil liability determines who bears the economic consequences of an accident, and – traditionally – it is used to provide *ex ante* incentives towards a high-level of product safety; *ex post*, it aims at providing adequate compensation to the victim.
- Insurance allows such costs to be internalized and managed, and compensation to be secured.
- The Risk Management Approach (RMA) decouples the traditional functions of liability, i.e. deterrence and compensation. It relies on *ex ante* regulations to obtain safety and security of products, and holds strictly liable the party that is best positioned to (i) minimize risks and (ii) acquire insurance, to grant prompt and adequate compensation *ex post*.
- For both IRs and CADs, the study aims to determine and evaluate the applicable legal framework, and, where needed, propose alternative solutions, pursuant to the RMA or other relevant approaches.

1.1. Purpose of the study

This third interim report, part A describes results of task 3 and 4 of the Study on Safety of non-embedded software (SafeNES)[1]:

- Task 3: Prospective foresight study on how advanced robots, autonomous and AI-based systems including connected and automated vehicles could be tested, certified and insured (including new risk management schemes)
- Task 4: Evidence gathering and analysis of Member States' legislation related to testing of advanced robots, autonomous and AI-based systems including connected and automated vehicles and prospective foresight study on how a European testing framework could look like

Tasks 3 and 4 of the report jointly constitute a prospective foresight study on testing (§1.2), certification (§1.3), liability and insurance (§1.4) of innovative robotic applications. They aim

[1] Part B of the third interim report describes the results of task 5 and is reported as a separate document.

to determine how high levels of product quality and safety can be ensured, and how liability rules can be shaped in order to provide desirable incentives to all players involved, also by determining a framework for robot testing in Europe, which could ease the assessment of risks and thence their management, as well as technological research.

Given the profoundly different technical characteristics robotic applications display[2], the analysis will address two specific domains, notably connected and automated driving solutions (henceforth, CADs) and industrial robots (henceforth, IRs).

With respect to the latter, in particular, three subcategories are taken into account as case studies[3], allowing us to point out the peculiarities that give rise to specific issues or concerns and which might require action or intervention.

As far as methodology is concerned, the study will feature an in-depth review of the existing legal and technical literature, case law, when existing and relevant, as well as international and European standards, and will analyze the results of stakeholders' interviews conducted to acquire information and validate findings and conclusions.

1.2. Testing

For the purpose of the current section, «testing» refers to the amount of procedures, evaluations and trials that characterize the design and development process: this entails both performance testing, aimed at verifying goals and determining the most appropriate robot for each use, and reliability testing, carried out to gather knowledge about potential risks, failures and the frequency of their occurrence[4]. Trials and assessments performed for the purpose of certification have a different structure and functions, and will be addressed separately in the dedicated section (§1.3).

1.2.1 Function

Definition and role. The function of testing is to assess the performance of devices, in order to define and refine design before putting them into production. To this end, products are contrasted with benchmarks, desirable references in a given business sector, which allow an objective performance evaluation[5].

Benchmarks. Differently from traditional and more established business areas – such as the automotive industry – where benchmarks – like vehicle's speed and torque – are clearly identified and universally recognized, advanced robotics doesn't benefit from as clear a framework. When assessing the performance of a robot companion[6], intended to be used

---

[2] Andrea Bertolini, "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules," *Law Innovation and Technology* 5, no. 2 (2013).

[3] Collaborative robots, mobile robots and wearable robots, see §2.3 below.

[4] B. S. Dhillon, "Robot Testing and Information Related to Robots," in *Robot Reliability and Safety* (New York: Springer, 1990).

[5] See Fabio Bonsignorio, Elena Messina, and Angel P. del Pobil, "Fostering Progress in Performance Evaluation and Benchmarking of Robotic and Automation Systems," *IEEE Robotics & Automation Magazine*, no. 3 (2014).

[6] The notion of robot companion is broad and encompasses a large set of applications that range from replicas of animals – real, such as Paro, made by Paro Robots and AIST, an advanced interactive robot disguised like a baby seal and intended to provide the same advantages that pet-therapy does, especially to patients in nursing homes or hospitals, see http://www.parorobots.com/index.asp, or fictional, such as Pleo, made by Innvo Labs, a pet dinosaur toy capable of interacting with children and the environment and of learning from its experiences, see http://www.pleoworld.com/pleo_rb/eng/index.php last accessed on July 17th 2018 – to android robots used for the care of the elderly or, more simply, pure domestic purposes. Agreement on one single definition wasn't reached, see Andrea Bertolini and Giuseppe Aiello, "Robot Companions: A Legal and Ethical Analysis," *The Information Society. An International Journal* 34, no. 3 (2018).. The example here provided depicts what may be defined as a domestic robot, namely an autonomous mobile robot, often provided with navigation and planning capabilities,

within the home environment to help with multiple and diversified every-day tasks, different aspects may be of relevance: the ability of the robot to learn, improving its performance and adapting to the environment, is closely related to that of reacting to unexpected external stimuli. The latter is known in the literature as antifragility and, despite developed as a notion outside the technical debate[7], it is today widely referred to in the engineering literature to define the capacity of the machine to benefit from hazards and unexpected occurrences to learn and further adapt. However, how such a characteristic ought to be defined in a technical perspective, what criteria ought to be observed and measured in order to describe it, is widely debated[8]. Absence of clarity in this respect causes the comparison among alternative applications, intended to perform a similar if not identical task, to be highly problematic.
Indeed, in particular with respect to more advanced applications, evaluation procedures are not always widely shared, and consensus upon which parameters are to be measured is often far from being achieved. In a similar setting the subjective judgement of experts on robot's performance often still prevails[9], and that causes greater uncertainty, and lack of scientific objectivity.

Risk-assessment. Testing is also necessary in order to identify potential risks, some of which might lead to malfunctioning, and eventually accidents, assess their likelihood and the possible legal consequences that might arise in case of their occurrence. Ultimately, information acquired through testing is also necessary in order to develop adequate insurance products (see §1.4 below), thence facilitating their distribution on the market.

Experiment reproducibility. Product testing is closely related to scientific experimenting. An experiment is a narrowly defined repeatable[10] set of reproducible behaviours in a well limited set of environments, and defines the scientific method itself. In the areas of robotics, automation, and AI, however, reproduction of the results that are published through papers is often difficult or even unattainable, thus hampering comparison and validation of the results, as well as delaying industrialization[11]. Indeed, data provided in academic publications is most often insufficient to fully describe all necessary parameters, given the remarkably large sets of robotic applications, the variety of the methodologies employed, the large number of hardware and software solutions adopted to perform one single function, as well as the different environments in which applications are intended to be used. Information incompleteness about all the relevant aspects of the experiments carried out, including the methodology and tools employed, radically hinders the possibility to reproduce the experiment and objectively assess results.

Indeed, even a factor that may seem irrelevant when considered in the global architecture of a scientific experiment, may have a bearing on its development and the results that can be found. At times, even minor differences in the equipment used could lead to different results, preventing the exact repeatability and replicability of the test, and, more broadly, its validation. Accurate reference to every hardware component employed minimizes such risk. In light of such considerations, in a paper concerning a simulated experiment of a wheelchair-mounted assistive manipulator – designed to help elderly people grasp objects – , scientists thoroughly explained the brand name and model of the simulated sensors and of

---

intended to perform domestic tasks, see David Fleer, "Human-Like Room Segmentation for Domestic Cleaning Robots," *Robotics* 6, no. 4 (2017).

[7] Nassim Nicholas Taleb, *Antifragile: Things That Gain from Disorder* (London: Penguin, 2012).

[8] Bonsignorio, Messina, and del Pobil.

[9] Ibid.

[10] See Francesco Amigoni, Monica Reggiani, and Viola Schiaffonati, "An Insightful Comparison between Experiments in Mobile Robotics and in Science," *Autonomous Robots* 27 (2009).

[11] See Fabio Bonsignorio and Angel P. del Pobil, "Toward Replicable and Measurable Robotics Research," *IEEE Robotics & Automation Magazine*, no. 9 (2015).

the monitor which displayed the simulation itself[12], as prescribed by the guidelines on experiment methodology (see *infra*). Similarly, when an experiment involves at the same time a robotic device and a human being – which may be the case for collaborative robots (see §2.3.1) – also instructions given to participants are of great relevance and should therefore be thoroughly stated and published, to enable reproducibility[13].

On this matter, «Good experimental methodology guidelines»[14] (henceforth GEM guidelines) with a strong focus on reproducibility and replicability of experimental results were developed by the «Good experimental methodology Special interest Group» (henceforth GEM SIG), within the European Robotics Research Network (henceforth, EURON)[15], both in general and for specific fields of robotics, such as grasping[16] and visual servoing[17]. Said guidelines aim at ensuring the repeatability and replicability of a given experiment, and thus require that scientific publications provide (i) a complete description of the experiment conducted, release (ii) data sets and (iii) complete code identifiers, and provide all (iv) hardware specifications[18].

1.2.2 Object of the study

The testing of advanced robotics and AI systems requires thence to address both technical and legal issues.

Testing procedures and techniques. On a pure technical basis, it is necessary to determine what testing techniques are today used to assess the performance of a specific device by the industry and research institutions alike, in particular as a response to the limitations above briefly sketched. How the specific applications here considered are tested, what techniques are used, whether experiments happen only within the restricted environments of the laboratory or require real-life settings, if software simulation is needed to overcome possible material or legal limitations, is discussed; best practices are described and assessed.

Regulatory solutions. On a legal basis, the testing of advanced robotic applications outside restricted facilities such as laboratories and factories might be problematic if not outright illicit. Most often, advanced applications conflict with extant bodies of regulation, whose revision might require time and political action. The absence of an adequate legal framework on such matter would therefore delay innovation.

In such a perspective, it shall however be noted that the radical reform of an entire body of regulation, for the mere purpose of allowing testing in real-life environments, might largely exceed the given purpose. Indeed, while the use of the device presupposes a comprehensive reform, testing might be temporarily allowed in order to (i) develop the technology, (ii) assess its feasibility, (iii) identify potential risks associated to its use, (iv) determine whether there might be an interest for the market in such a product, and ultimately also (v) define

---

[12] Martin F. Stoelen et al., "Distributed and Adaptive Shared Control Systems. Methodology for the Replication of Experiments," *IEEE Robotics & Automation Magazine*, no. 12 (2015).
[13] See ibid.
[14] Fabio Bonsignorio, John Hallam, and Angel P. Del Pobil, *Gem Guidelines* (EURON - GEM SIG, 2008). See http://www.heronrobots.com/EuronGEMSig/downloads/GemSigGuidelinesBeta.pdf, last access July 16th, 2018.
[15] EURON is a Network of Excellence (henceforth, NoE), a networking-oriented, European-funded project. EURON is now part of euRobotics AISBL, an international non-profit association for stakeholders in European robotics, now also the private part of the European Public-Private Partnership on Robotics. For further information, see https://www.eu-robotics.net/eurobotics/about/about-eurobotics/index.html, last access July 5th, 2018.
[16] Robot grasping is the ability to dexterously manipulate objects of varying geometric and physical properties. See Domenico Prattichizzo and Jeffrey C. Trinkle, "Grasping," in *Springer Handbook of Robotics*, ed. Bruno Siciliano and Oussama Khatib (Berlin: Springer, 2008).
[17] Visual servoing is a method of controlling a robot's motion via a vision sensor, such as a camera. See François Chaumette and Seth Hutchinson, "Visual Servoing and Visual Tracking," in *Springer Handbook of Robotics*, ed. Bruno Siciliano and Oussama Khatib (Berlin: Springer, 2008).
[18] Bonsignorio and del Pobil.

what regulatory action would be best suited in order to accommodate it within the legal system. So understood, extensive testing ought to precede ad-hoc legislative intervention. Delaying testing – under safety conditions – would also thence impair the very possibility of developing necessary policies.

To address such issues, Japan established «Tokku» Special Zones for Robotics Empirical Testing and Development (RT special zones)[19]. This practice was implemented because an effective testing procedure of advanced robotic devices, designed to perform their duties in an open environment, cannot simply take place in laboratories, but needs to be carried out in co-existence with humans. A «Tokku» zone is a legally approved conceptual[20] region, under the authority of a Robotic Industry Development Council (henceforth, RIDC), where practical testing may be authorized. In order to facilitate testing, both de-regulation and accessory measures are ensured. With respect to the former, a revision of traffic regulations and exemptions from certification-based restrictions clear and adapt the legal framework, enabling trials that would otherwise be illicit. With respect to the latter, support to government-industry cooperation is ensured and a system of incentives for start-ups undergoing robot testing is implemented.

A request to a RIDC for authorization for robot testing within a Tokku zone, needs to be accompanied by a risk assessment study – evaluating factors such as the accident's probability as well as the potential damage that may result in such cases, in particular once the weight and speed of machinery is taken into account –, adequate insurance coverage to account for said risks. At the same time, the request must state that robots are designed to abide – to the best of their capabilities – traffic regulations[21]. Once the testing is completed, if the locally adopted regulation proves efficient, its adoption might be extended at national level, thus allowing innovation of the overall legislative framework[22].

Within Europe (henceforth, EU), under the action of the ICT Innovation for Manufacturing SMEs (henceforth, I4MS) policy initiative, itself part of the Digital Single Market strategy[23], a number of digital innovation hubs (henceforth, DIHs) were organized within the facilities of university and research centers[24]. Through such action, SMEs are entitled to both financial and technological support offered by a single DIH. These, in fact, provide necessary testing facilities and expertise to conduct research and test prototypes, enabling access to knowledge, machinery, solutions and expertise that would otherwise fall beyond the financial and technological capabilities of small-to-medium enterprises[25]. Despite strategically important, such initiatives do however profoundly differ from Japanese Tokku zones, in as much as they do not allow the disapplication of existing laws and might not therefore authorize experiments that would conflict with extant regulation as described above.

In order to tackle this last concern, the European Commission in its Communication on Artificial Intelligence for Europe of April 25th 2018[26] (henceforth, Communication on AI) calls for the creation of «regulatory sandboxes», which are intended to be «testing grounds for

---

[19] Yueh-Hsuan Weng et al., "Intersection of "Tokku" Special Zone, Robots, and the Law: A Case Study on Legal Impacts to Humanoid Robots," *International Journal of Social Robotics*, no. 7 (2015).

[20] Tokku zones are defined as «conceptual» regions to avoid ambiguity with Japan's both traditional regions and prefectures.

[21] Weng et al.

[22] Ibid., p. 842.

[23] Digital Single Market is a DG CONNECT policy, launched in 2015, and focussed on three pillars, namely better access to digital goods, improving conditions in order to enhance digital networks and helping the growth of digital economy. For further information, see https://ec.europa.eu/digital-single-market/, last access July 14th, 2018.

[24] As of now, €144 million in EU funding have been employed for DIHs.

[25] For further information, see http://i4ms.eu/about, last access July 13th, 2018.

[26] *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Artificial Intelligence for Europe* (Brussels: European Commission, 2018). See https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe, last access July 16th, 2018.

new business models that are not (yet) regulated»[27]. The Communication does neither provide a definition, nor a detailed description of how such entities are intended to operate. This concept was however already advanced by other European documents, related to FinTech[28] and start-ups[29]. In accordance to those, sandboxes are set up by regulators, aimed at allowing innovative enterprises, such as start-ups, to conduct live experiments, involving real users. Said environments operate under the supervision of an administrative regulatory institution, thus allowing innovative businesses to address perceived regulatory barriers in conjunction with public authorities[30], while the latter are entitled to apply a margin of discretion, which is deemed useful to support technological innovation testing.[31] The European Commission, in cooperation with European Supervisory Authorities (henceforth, ESAs) shall define a set of best practices[32], dealing with issues such as sandbox organization, activities and supervision itself[33].

Structure and goals of this section. The study will therefore try to (i) identify and discuss the testing techniques employed to overcome the technical issues described, and (ii) determine in which cases and under which conditions it might be necessary to resort to legal solutions such as Tokku zones and regulatory sandboxes to ease the emergence, understanding and regulation of the applications considered.

1.3 Certification

Certification is the procedure each product that is intended to be traded onto the European market has to undergo, so as to assess whether it meets the minimum safety requirements put forth by applicable legislation, and receive the «certification mark» or «conformity mark», that entails compliance with regulation[34].

1.3.1 Function

Definition and role. The purpose of certification (notably, European Conformity, CE mark) is twofold, ensuring high levels of product quality and safety, thence strengthening users' confidence and protection, and easing free movement of goods across Member States (henceforth, MSs), facilitating the activities of manufacturers through uniform regulation.

The European approach to certification. To this end, the so called «New Approach»[35], adopted by the EU since 1985, on the one hand provides an exhaustive list of safety requirements that must be met, leaving the manufacturer free to decide how to satisfy said

---

[27] Ibid.

[28] *Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions. Fintech Action Plan: For a More Competitive and Innovative European Financial Sector* (Brussels: European Commission, 2018), https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf. See https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf, last access July 16th, 2018.

[29] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Europe's Next Leaders: The Start-up and Scale-up Initiative* (Strasbourg: European Commission, 2016). See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0733&from=EN, last access July 16th, 2018.

[30] Ibid. p. 9.

[31] *Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions. Fintech Action Plan: For a More Competitive and Innovative European Financial Sector*. See esp. p. 9.

[32] The first report on FinTech best practices for sandboxes is expected by Q1 2019.

[33] *Frequently Asked Questions: Financial Technology (Fintech) Action Plan* (Brussels: European Commission, 2018). See https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjKicWRjKTcAhVGz4UKHablBM4QFggpMAA&url=http%3A%2F%2Feuropa.eu%2Frapid%2Fpress-release_MEMO-18-1406_en.pdf&usg=AOvVaw1FJAJgo1r3UR_XEBuyvEiQ, last access July 16th, 2018.

[34] Elena Bellisario, "Il Danno Da Prodotto Conforme Tra Regole Preventive E Regole Risarcitorie," *Europa e diritto privato*, no. 3 (2016).

[35] *The "Blue Guide" on the Implementation of Eu Products Rules* (Brussels: European Commission, 2016). See http://ec.europa.eu/DocsRoom/documents/18027/, last access July 16th, 2018.

criteria; on the other hand, it establishes a legal presumption of conformity whenever a product meets a harmonized technical standard (henceforth, hEN)[36], while its use remains voluntary. The Machinery Directive[37] (henceforth, MD) applicable to most robotic devices is a fundamental case in point.

Therefore, producers intending to market their goods in the EU and the European Economic Area (henceforth, EEA) need to design their products in accordance with applicable safety regulation, primarily EU directives.

However, issues of certification and issues of liability are de-coupled, so that compliance with safety requirements does not *per se* exclude the possibility for the product to be found defective, whenever an accident results from its use, causing the producer to be held liable pursuant to – among other – the Directive on Liability for Defective Products [38] (henceforth, Product Liability Directive, or PLD). This issue will be addressed separately in the subsequent section (see §1.4 below).

European safety regulation is thus intended to operate *ex ante* defining a level of safety that is demanded of every specific product. To do so, a large number of directives was adopted, each encompassing a wide array of applications. To exemplify, it shall suffice to recall how the definition of «machinery» for the purposes of the MD, entails

> «an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application […]».

Most, if not all, robotic applications would fall under such a broad definition (§2.6).

Standards. The breadth of said rules is thence coupled with a much greater number of narrow-tailored standards, most of which are adopted by international (such as ISO) and European (CEN-CENELEC, ETSI) organizations, and in some cases even national authorities. Industry-led organizations such as IEEE also play a primary role in standard setting for robotics, fostering standardization-related research through the Robotics and Automation Society (henceforth, RAS). Within RAS, many technical committees exist, dealing with applications such as logistics, wearable robotics, collaborative and mobile robots, and digital manufacturing.

It shall be stressed that standards are not binding regulations, therefore compliance is required with directives and other legislation, not technical norms. However, they profoundly contribute to both identify what the best practice or state of the art in a given area or with respect to a given application is, and ease the position of manufacturers in identifying what specific criteria their devices need to meet in order to ensure to comply with the relevant legislative safety requirements. Nonetheless, manufacturers are still free to satisfy legislative prescriptions in alternative ways, radically disregarding eventually existing standards.

Despite the voluntary application, the James Elliott ruling has recently clarified that hENs do form part of EU law[39], and as such fall within the jurisdiction of the Court of Justice under

---

[36] A hEN differs from a non-harmonized one (EN) since the former develops from a mandate by the European Commission, and is aimed at bringing harmonised technical requirements throughout the European Union, while the latter must be transposed as a national standard and does not allow presumption of safety.
[37] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) (Text with EEA relevance) OJ L 157, 9.6.2006.
[38] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210, 7.8.1985, henceforth PLD.
[39] CJEU c-613/14, James Elliott, EU:C:2016:821, §40.

Article 267 of the Treaty on the Functioning of the European Union (henceforth, TFEU). It is still debated whether, besides interpretative issues, this judicial opening also embraces matters of validity of hENs, which would open to a review of their contents[40].

1.3.2 Object of the study

Structure and goals of this section. Within this framework, the analysis of the applications here considered will thus address three main issues: (i) whether such applications clearly fall within existing safety regulation; (ii) whether extant certification procedures are adequate with respect to said devices, allowing to take into account the technical peculiarities that characterize them; (iii) whether sufficient standards exist, providing guidance to manufacturers, or instead relevant gaps may be identified, leaving uncertainty with respect to how legal requirements may be satisfied.

Certification. In particular, *sub* (i) a given application, because of its novelty, might fall under more distinct regulations, each of which was not conceived to accommodate it. Indeed, no EU safety legislation was adopted so far with a specific focus on one or more classes of robotic applications. At the same time, its technical traits might allow it to be qualified in different ways, leading different bodies of law to overlap. Uncertainty about what safety requirement needs to be met, what legislation is applicable, and therefore how the product needs to be certified, delays if not prevents the emergence of innovation.

Standards. Further building on such considerations, the certification procedures provided for the specific applications here considered will be analyzed *sub* (ii), as well as existing applicable standards *sub* (iii), discussing the need for the development of ad-hoc, narrow tailored technical norms.

1.4 Liability, Insurance, Risk Management

Liability. Civil liability rules determine who is supposed to bear the negative economic consequences arising from an accident[41]. Typically, the party is held liable, and thence bound to compensate, that is deemed to have caused the accident, and therefore is responsible for it. The underlying idea is that of sanctioning a socially undesirable deviation from an intended and expected conduct.

Insurance. Insurance is the contract whereby one party – the insured –, exposed to a risk, pays to another party – the insurer – a fix sum of money – premium – in order to be relieved of the negative economic consequences that would arise, should the risk materialize.

1.4.1 Function

Civil liability. In so doing two distinct functions are pursued, namely *ex ante* deterrence – whereby agents will avoid the sanctioned behavior – and *ex post* compensation of the victim – theoretically forcing the internalization of the negative consequences arising from the illicit behavior.

---

[40] Pierluigi Cuccuru, "European Standards at the Bar: Routes Towards a Meaningful Involvement of the Court of Justice in Technical Standardisation," *European Law Journal* (2018 (forthcoming)). See also Mariolina Eliantonio and Carlo Colombo, "Harmonized Technical Standards as Part of Eu Law: Juridification with a Number of Unresolved Legitimacy Concerns?," *Maastricht Journal of European and Comparative Law* 24, no. 2 (2017).

[41] Similarly, liability means «the law determining when the victim of an accident is entitled to recover losses from the injurer». See Steven Shavell, "Liability for Accidents," in *Handbook of Law and Economics*, ed. A. Mitchell Polinsky and Steven Shavell (Amsterdam: Elsevier, 2007).

Product liability directive. Civil liability rules are primarily established at MSs level, and display some degree of variation[42]. However, since robotic applications are products[43], product liability rules also apply, namely the PLD [44]. Such body of law is largely uniformly enacted – despite not affecting additional remedies offered by single MS under tort or contract law (see art. 13 PLD) – and establishes the (semi)strict liability[45] of the manufacturer for all damages arising from the use of his products.

The PLD has been recently evaluated[46], also with the aim of assessing whether it is fit for regulating contemporary advanced technological products. Some critical elements have been identified, primarily uncertainty as per the qualification of software as product[47], the implications and effectiveness of the development risk defense (art. 7, let. E PLD), and the cost and difficulty of exactly ascertaining the existence of a defect – in particular in design –, as well as of a causal nexus between the fact and the damage. The latter, in particular, burden the claimant substantially, discouraging litigation. Indeed, of the over 798 cases considered by the evaluation study[48], in around 20% of the times the Courts ruled according to a legal basis different from the PLD. Among them, around two thirds of the cases were decided resorting to national contract law rules, and one fifth through the application of general tort law principles[49].

When advanced robotics is considered, tight human-machine interaction causes different bodies of law to overlap. Indeed, if a single task is handled together by the human agent and by a machine, when an accident occurs it might be due to the fault of the former or a defect (or malfunctioning) of the latter. Apportioning liability among the two – agent or manufacturer – might therefore require complex factual ascertainment and articulate legal analysis[50].

Insurance. Insurance contracts are typically used to shield potential tortfeasors – both human agents and enterprises – from liability, and rest on two fundamental conditions. On

---

[42] See art. 2043 of the Italian Codice civile, art. 1382 of the French Civil code and §823 of the German BGB. As far as the Principles of European Tort Law (henceforth, PETL) are concerned, see esp. art. 1:101, 2:101. PETL are a set of guidelines provided by the European Group on Tort Law (henceforth, EGTL) with the scope of harmonizing tort law. For further information, see http://www.egtl.org/, last access July 14th, 2018.

[43] Bertolini.

[44] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210, 7.8.1985, henceforth PLD.

[45] Liability can be considered as semi-strict because the plaintiff is not required to prove fault, but the defendant is entitled to seek exemption from liability by proving one of the defences allowed by PLD. Carlo Castronovo, *La Nuova Responsabilità Civile* (Milano: Giuffrè, 2006). See esp. pp. 700 ff.

[46] *Commission Staff Working Document. Evaluation of Council Directive 85/374/Eec of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products* (Brussels: European Commission, 2018). See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018SC0157, last access July 16th, 2018.

[47] *Commission Staff Working Document. Liability for Emerging Digital Technologies* (Brussels: European Commission, 2018). See https://ec.europa.eu/digital-single-market/en/news/european-commission-staff-working-document-liability-emerging-digital-technologies, last access July 16th, 2018, esp. p. 18. The issue is debated since long, see also the European Commission (Answer of the Commission to written question n° 706/88, O.J.E.C. 114/42, of May 8th, 1989), stated that software should be considered among products only when sold on a support, such as a CD, but more recently software is generally classified among products, regardless of the support. See Ulrich Forste and Friedrich Graf von Westphalen, *Produkthaftungshandbuch* (Munich: Beck, 2012).

[48] Ernst&Young, Technopolis, and VVA, *Evaluation of Council Directive 85/374/Eec on the Approximation of Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products* (Brussels: European Commission, 2018).See https://publications.europa.eu/en/publication-detail/-/publication/d4e3e1f5-526c-11e8-be1d-01aa75ed71a1/language-en, last access July 16th, 2018.

[49] Ibid. «it also appears that claimants sometimes invoked the national law implementing the Directive as main law, but the courts allowed for compensation on a different legal basis, either tort or contract law, in around 20% of the cases. In those cases, on average, the legislation allowing the injured persons to raise a claim was contract law in 68% of the cases, general tort law in 21% of the cases», seep. 22.

[50] Andrea Bertolini, "Insurance and Risk Management for Robotic Devices: Identifying the Problems," *Global Jurist*, no. 2 (2016).

the one hand, it is necessary to determine who is exposed to a risk or, in the cases here considered, whom would be held liable for a given accident. On the other hand, it is necessary to identify the risks that may materialize, and assess the likelihood of their occurrence. Indeed, the premium is calculated as a function of these.

While uncertainty with respect to which party might be held liable in case of an accident resulting from the use of an advanced robotic application – entailing tight human-machine cooperation – negatively affects the possibility of clearly identifying whom is to be insured – and against which risks –, unforeseeable occurrences emerging technologies inevitably bring about cause calculations to become less precise. Indeed, new technical solutions might give rise to novel risks – e.g.: cyber risks – that were until then unheard of, and in some cases that might be impossible to clearly identify *ex ante*. In such a perspective the issue of testing as previously defined (see §1.2 above) is of paramount importance and tightly connected with that here defined.

Risk Management Approach. The so called Risk Management Approach (henceforth RMA) is grounded on the idea that liability should not be attributed on the basis of considerations of fault – defined as the deviation from a desired conduct – typical of most tort law systems, rather on the party that is best positioned to (i) minimize risks and (ii) acquire insurance[51].

One fundamental consideration underpinning such alternative approach is that liability rules are not always efficient in ensuring adequate incentives towards a desirable *ex ante* conduct, be it a safety investment – such as in the case of producers' liability (as it will be further explained in §2.7.6 and §3.3.5) – or a diligent conduct – such as the driver's in the case of road circulation (§3.3.5) –. That end is best attained through the adoption of detailed *ex ante* applicable regulation, such as safety regulation, abundant at EU level and susceptible of further perfecting.

1.4.2 Object of the study

Structure and goals of this section. The study therefore (i) determines what bodies of national and EU liability rules are applicable to the robotic devices here considered, and (ii) what incentives said rules determine to the parties involved, based on theoretical considerations as well as case-law analysis, when relevant incidents are identified. The possibility to adopt alternative legislative solutions will be specifically considered, also pursuant to a RMA, whereby the liable party is the one who is best positioned to minimize and manage risks, and acquire insurance.

The study then further investigates (iii) the existence of ad-hoc insurance products and of an existing or potential market, as well as (iv) the sufficient availability of data on the risks to be insured, as well as the (v) existence of alternative techniques eventually employed in order to identify and assess novel risks beforehand.

---

[51] Ibid. The viability of such an approach was also considered in the *European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(Inl))* (European Parliament, 2017), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN., (paragraphs 53 and 55) that stated: «[the European Parliament] considers that the future legislative instrument should be based on an in-depth evaluation by the Commission determining whether the strict liability or the risk management approach should be applied [… Moreover, the European Parliament] notes that the risk management approach does not focus on the person who acted negligently as individually liable but on the person who is able, under certain circumstances, to minimise risks and deal with negative impacts».

2 INDUSTRIAL ROBOTS

KEY FINDINGS

- There is no legal definition of IR. International standards defined the latter as an «automatically controlled, reprogrammable, multipurpose manipulator, programmable in three or more axes, which can be either fixed in place or mobile for use in industrial automation applications».
- In smart factories, technologically advanced robotics are often used out of the cage, display high degrees of automation, interact among one another and with humans.
- The study considers three case studies, which are representative of the characterizing features of such Industry 4.0 robotics: (i) collaborative robots, i.e. robots designed for direct interaction with a human; (ii) mobile robots, i.e. robots able to travel under their own control, both with or without manipulators; (iii) exoskeletons, i.e. external structural mechanism with joints and links corresponding to those of the human body.
- As for the subject involved in testing, certification, liability and insurance of IRs, the study addresses: (i) those who bear a direct safety-related duty, namely manufacturers, suppliers of individual components, system integrators (SI) and business-users; and (ii) other subjects, who do not bear a direct safety-related duty, namely potential victims (non-business-users and by-standers), certification competent bodies, as well as insurance companies.

2.1 Introduction

Industry 4.0 and smart factories. Technological innovation is profoundly affecting production techniques[52], and the very conception of what a factory is, how it is structured, and how it functions. Such a phenomenon is referred to as the fourth industrial revolution, or Industry 4.0[53], and entails, among others, the evolution of traditional plants into smart factories[54].

A smart factory is a manufacturing environment where cyber-physical systems monitor processes, adapt themselves, learn, make decisions, and carry out manufacturing in autonomy[55], entailing the adoption of novel solutions that make production more flexible, allowing for relevant variations in size and timing, as well as reducing waste[56] and ensuring the possibility to rearrange and modify what is being produced, according to tailor-made and on-demand methodologies[57].

---

[52] Ron Davies, *Industry 4.0 Digitalisation for Productivity and Growth* (European Parliament, 2015), http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/EPRS_BRI(2015)568337_EN.pdf.
[53] Alexander Leopold Till, Saadia Zahidi, and Vesselina Ratcheva, *The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution* (World Economic Forum, 2016), http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf.
[54] *Communication Investing in a Smart, Innovative and Sustainable Industry. A Renewed Eu Industrial Policy Strategy* (European Commission, 2017).. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank, *Investing in a smart, innovative and sustainable Industry*. *A renewed EU Industrial Policy Strategy*, September 13th, 2017.
[55] Jan Smit et al., *Industry 4.0* (European Parliament, 2016), http://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf.
[56] D. Verzijl et al., *Smart Factories - Capacity Optimisation* (European Commission, 2014).
[57] Various, *Digitising European Industry - Digital Industrial Platforms* (European Union, 2017), https://ec.europa.eu/futurium/en/system/files/ged/dei_wg2_final_report.pdf.

Novel applications. Indeed, even if robots have been included in the factories since the 1950s[58], applications that qualify a smart factory differ profoundly, in particular in light of the close interaction with human beings they bring about. Previous machines were large, powerful, and kept within restricted environments, away from any meaningful human contact. Industry 4.0 solutions are cooperative, intended to function in direct contact with the user, and, in some cases, be worn, such as exoskeletons. Despite the great variety, they might thence be classified as either fixed, mobile, or wearable.

Before proceeding with the analysis, however, the very notion of «industrial robot» shall be provided.

2.2 Definitions of industrial robots

***Industrial Robots*.** As per the very term robot[59], «industrial robot» also represents a synthetic expression encompassing a wide range of solutions that profoundly differ from one another, both in a technical perspective and for the legal and social issues they give rise to. Thence, in order to undergo their assessment, it is necessary to identify specific applications to be singularly discussed.

In such a perspective, the concept of hybrid interaction between machines and human workers, which is foreseen as the most probable trend in manufacturing environments within the next ten years[60], is of particular importance.

This interaction between humans and robots can be simple coexistence, collaboration, when they perform tasks at the same time in the same place, or cooperation, if they work jointly on the same product[61]. Collaboration and cooperation are especially crucial in fixed collaborative robots, in many mobile robots, and in wearable robotics, all falling under the notion of «industrial robots», defined by official standards as:

- **ISO 8373:2012**[62], 2.9 an «automatically controlled, reprogrammable (2.4)[63], multipurpose (2.5)[64] manipulator (2.1)[65], programmable in three or more axes (4.3)[66], which can be either fixed in place or mobile for use in industrial automation applications. Note 1: The industrial robot includes: — the manipulator, including actuators (3.1)[67]; — the controller, including teach pendant (5.8)[68] and any communication interface (hardware and software). Note 2 to entry: This includes any integrated additional axes». The aforementioned standard quotes **ISO 10218-1:2011**[69], 3.10, which in turn features two more notes: «note 3 The following devices are considered industrial robots

---

[58] Martin Hagele, Klas Nilsson, and J. Norberto Pires, "Industrial Robotics," in *Springer Handbook of Robotics*, ed. B. Siciliano and O. Khatib (Berlin: Springer, 2008).
[59] Bertolini, "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules." See Erica Palmerini et al., *Guidelines on Regulating Robotics* (2014).
[60] S. L. Muller et al., "Subjective Stress in Hybrid Collaboration," in *Social Robotics*, ed. A. Kheddar (Cham: Springer, 2017).
[61] W. Bauer et al., *Leichtbauroboter in Der Manuellen Montage - Einfach Einfach Anfangen. Erste Erfahrungen Von Anwenderunternehmen* (2016), http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-4151100.pdf.
[62] https://www.iso.org/obp/ui/#iso:std:iso:8373:ed-2:v1:en, last access May 21st, 2018.
[63] «designed so that the programmed motions or auxiliary functions can be changed without physical alteration (2.3)».
[64] «capable of being adapted to a different application with physical alteration (2.3)».
[65] «machine in which the mechanism usually consists of a series of segments, jointed or sliding relative to one another, for the purpose of grasping and/or moving objects (pieces or tools) usually in several degrees of freedom (4.4). Note 1: A manipulator can be controlled by an operator (2.17), a programmable electronic controller, or any logic system (for example cam device, wired). Note 2: A manipulator does not include an end effector (3.11)».
[66] «direction used to specify the robot (2.6) motion in a linear or rotary mode. Note: "axis" is also used to mean "robot mechanical joint"».
[67] «power mechanism used to effect motion of the robot (2.6). Example: a motor which converts electrical, hydraulic or pneumatic energy to effect motion of the robot».
[68] «hand-held unit linked to the control system (2.7) with which a robot (2.6) can be programmed or moved».
[69] See https://www.iso.org/standard/51330.html, last access June 26th, 2018.

for the purpose of this part of ISO 10218: – hand-guided robots; – the manipulating portions of mobile robots; – collaborating robots. Note 4 Adapted from ISO 8373:1994, definition 2.6». The same definition is provided by **ANSI/RIA R15.06-2012**[70], 3.10;

- **ISO 10218-1:2011**, 3.11, «industrial robot system: system comprising: – industrial robot; – end-effector(s); – any machinery, equipment, devices, external auxiliary axes or sensors supporting the robot performing its task. Note 1: The robot system requirements, including those for controlling hazards, are contained in ISO 10218-2. Note 2: Adapted from ISO 8373:1994, definition 2.14». The same definition is provided by **ANSI/RIA R15.06-2012**, 3.11.

2.3 Case studies

In order for the subsequent analysis to be sufficiently narrow-tailored and concrete, three different case studies will be considered, namely collaborative industrial robots (§2.3.1), mobile robots (§2.3.2), and wearable robots (§2.3.3).

2.3.1 Collaborative industrial robot (also co-robot, cobot and intelligent active device)

Definition. The term «collaborative industrial robots» refers to robots designed to physically interact with humans in a shared workspace, thus encompassing everything that goes from a fixed industrial robot whose protective guards have been removed, to interactive robots capable of a higher degree of autonomy and interaction.

No European legal act provides a definition of collaborative robots, yet they are mentioned in an Opinion of the European Economic and Social Committee (henceforth, EESC)[71], stating that: «a new generation of so-called 'collaborative robots' can become physical partners for workers»[72].

A Commission Staff working document[73] mentions the necessity to develop harmonized standards[74], to better ensure safety and market access, for new technologies, including collaborative robots.

To the contrary, relevant and authoritative definitions of collaborative robots can be found in official standards at the international level, as indicated below, pursuant to which a collaborative robot is:

- **ISO 8373:2012**[75], 2.26 a «robot (2.6[76]) designed for direct interaction with a human»; within this line, the standard defines a collaborative operation as a «state in

---

[70] See https://webstore.ansi.org/RecordDetail.aspx?sku=ANSI%2FRIA+R15.06-2012, last access May 23rd, 2018.
[71] Opinion of the European Economic and Social Committee on the 'Provision and development of skills, including digital skills, in the context of new forms of work: new policies and changing roles and responsibilities' (exploratory opinion requested by the Estonian Presidency) (2017/C 434/06), O.J.E.U. C 434/36 of December 15th, 2017.
[72] See esp. §§1.5 and 3.5.
[73] Commission Staff Working Document on the implementation of the actions foreseen in the annual Union work programme for European standardisation for 2018. Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The annual Union work programme for European standardisation for 2018, see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0284&rid=3, last access June 6th, 2018.
[74] According to Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast).
[75] According to ISO 8373:2012, 2.26, see https://www.iso.org/obp/ui/#iso:std:iso:8373:ed-2:v1:en, last access June 5th, 2018.
[76] «Actuated mechanism programmable in two or more axes (4.3) with a degree of autonomy (2.2), moving within its environment, to perform intended tasks. Note 1 A robot includes the control system (2.7) and interface of the control system. Note 2 The classification of robot into industrial robot (2.9) or service robot (2.10) is done according to its intended application».

which purposely designed robots (2.6) work in direct cooperation with a human within a defined workspace[77]» (closely resembled by **ISO/TS 15066:2016**[78] 3.1, which refers to it as «state in which a purposely designed robot system and an operator work within a collaborative workspace», quoting ISO 10218-1:2011, 3.4);

- **ISO 10218-2:2011**[79], 3.2 a «robot designed for direct interaction with a human within a defined collaborative workspace (3.3) », meaning a «workspace within the safeguarded space where the robot and a human can perform tasks simultaneously during production operation». The same definition is provided by **ANSI/RIA R15.06-1999** and **RIA TR R15.206-2008**, where a cobot is described as a «robot designed for direct interaction with a human within a defined shared workspace»[80];

Three other definitions of collaborative robots, referred to as intelligent active devices (henceforth, IAD), are advanced in the draft 2002[81] ISO safety standard on «Workspace within the safeguarded space where the robot and a human can perform tasks simultaneously during production operation», which, however, were not adopted in the 2016 final updated version[82].

The mentioned draft advances three alternative definitions of IAD as:

- a single or multiple axis device that employs a hybrid programmable computer-human control system to provide human strength amplification and may include path limiters[83];
- a force based control device that ranges from single axis payload balancing to multiple degree of freedom articulated manipulators[84];
- a single or multiple axis device that employs a hybrid programmable computer-human control system to provide human strength amplification, guiding surfaces, or both. These multifunctional assist devices are designed for material handling, process and assembly tasks that in normal operation involve a human presence in its workspace[85].

In the standardization and engineering environment, collaborative robots are also defined as:

- multi-robot systems working together for the same industrial task such as robotic assembling […] collaborative robots are envisioned to work together as coworkers, operate safely with humans, and adapt to versatile tasks and dynamic environments[86];
- devices for human/robot interaction, in which axes of motion are coupled to one another by computer-controlled continuously variable transmissions rather than individually driven by servomotors[87].

---

[77] According to ISO 8373:2012, 2.25, see https://www.iso.org/obp/ui/#iso:std:iso:8373:ed-2:v1:en, last access June 5th, 2018.
[78] See https://www.iso.org/standard/62996.html, last access June 26th, 2018.
[79] See https://www.iso.org/standard/41571.html, last access June 26th, 2018
[80] According to ANSI/RIA R15.06-1999 *National Robot Safety Standard*, and RIA TR R15.206-2008, see https://www.robotics.org/product-catalog-detail.cfm?productid=2953, last access June 5th, 2018.
[81] RIA BSR/T15.1, *Draft standard for Intelligent Assist Devices – Personnel safety requirements*, see http://peshkin.mech.northwestern.edu/publications/2002_T15.1_DraftStandardForTrialUse_IntelligentAssistDevicesPersonnelSafetyRequirements.pdf, last access June 6th, 2018.
[82] https://www.iso.org/standard/62996.html, last access June 6th, 2018.
[83] P. v. of the Draft standard.
[84] P. 1. of the Draft standard.
[85] P. 3. of the Draft standard.
[86] L. Kong and al., "Adasharing: Adaptive Data Sharing in Collaborative Robots," *IEEE Transactions on Industrial Electronics* 64, no. 12 (2017).
[87] C. A. Moore, M. A. Peshkin, and J. E. Colgate, *Cobot Implementation of 3d Virtual Surfaces*, *Proceedings 2002 IEEE International Conference on Robotics and Automation (Cat. No.02CH37292)* (Washington, D.C.: 2002).

Pursuant to all definitions above recalled, collaborative robots may be indistinctively fixed or mobile. Indeed, no specific reference is made to immovable or movable nature of the machine. The latter, in particular, being by definition intended to roam around, outside any restricted environment, will require to have sufficient collaborative features, so as to ensure that they do not expose human beings, who happen to operate within their surroundings, to any danger[88].

However, §2.3.2 and the corresponding case study will be entirely devoted to such applications.

Therefore, the current section and the related case study will instead focus on fixed applications such as manufacturing robots designed for finishing.

Applications. A European Parliament Resolution[89] mentions the increasing use of smart collaborative robots, for example in industrial production, hospitals and retirement homes.

Among the most common industrial applications of cobots, the aforementioned French report[90] shows grinding[91], assembling[92], retreading, regrooving and repairing tires[93] while other sources show picking and placing, machine tending, packaging, gluing, welding and inspecting[94].

2.3.2 Mobile robot

Definition. No general definition of mobile robot is provided by any European legal act, but an Authorization for State Aid adopted in 1992 provides the following description:

> «Autonomous remote controlled vehicles capable of operating separately or together in situations where human intervention is impossible or too dangerous.» [95]

Other definitions may be found in international standards such as:

- **ISO 8373:2012**[96], 2.13 «A robot (2.6) able to travel under its own control. A mobile robot can be a mobile platform (3.18)[97] with or without manipulators (2.1)». The same definition is provided by **ISO 19649:2017**[98], 3.1.1;

In the standardization and engineering environment, a mobile robot is also defined as:

---

[88] Rasmus Eckholdt Andersen et al., "Integration of a Skill-Based Collaborative Mobile Robot in a Smart Cyber-Physical Environment," *Procedia Manufacturing*, no. 11 (2017).
[89] EU Strategic Framework on Health and Safety at Work 2014-2020 European Parliament resolution of 25 November 2015 on the EU Strategic Framework on Health and Safety at Work 2014-2020, of November 25th, 2015, in O.J.E.U. C 366/17 of October 27th, 2017.
[90] Jean-Jacques Atain Kouadio and Adel Sghaier, *Les Robots Et Dispositifs D'assistance Physique: Etat Des Lieux Et Enjeux Pour La Prévention* (Paris: Institut National de Recherche et de Securité, 2017), http://www.inrs.fr/dms/inrs/Publication/NOETUDE-P2017-120-01/ns354.pdf.
[91] P. 26. A small cobot, providing six levels of assistance, has been employed for deburring.
[92] P. 16. In this case, a worker is helped in the task of inserting pieces.
[93] P. 21. Physical stress has been highly reduced during the operations of removing faults from used tires.
[94] Carlos Gonzalez, "7 Common Applications for Cobots," accessed. http://www.machinedesign.com/motion-control/7-common-applications-cobots., last access June 6th, 2018.
[95] *Authorization for State aid* pursuant to Articles 92 and 93 of the EEC Treaty Cases where the Commission raises no objections (92/C 276/03), in O.J.C., 276 of October 24th, 1992, p. 5.
[96] https://www.iso.org/obp/ui/#iso:std:iso:8373:ed-2:v1:en, last access June 9th, 2018. For this very reason, a collaborative industrial robot of the kind described above, §2.3.1, might be installed onto the mobile robot itself.
[97] «assembly of all components of the mobile robot (2.13) which enables locomotion. Note 1 A mobile platform can include a chassis which can be used to support a load (6.2.1). Note 2 Because of possible confusion with the term "base" (3.8), it is advisable not to use the term "mobile base" to describe a mobile platform».
[98] See https://www.iso.org/standard/65658.html, last access June 26th, 2018.

- a machine mounted on a movable platform. Typically, mobile robots are designed to move to a certain area or environment following the controller instructions[99];
- A robot system that is capable of moving within an environment or terrain where it performs the tasks[100];
- A class of electromechanical system(s) capable of autonomous motion[101];
- A complex mechatronics system which synergistically blends multidisciplinary solutions and methods from mechanics and embedded control system[102];
- A device that can move autonomously from place to place to achieve a set of goals[103].

Mobile robots are generally kept separate from driverless vehicles and unmanned automated vehicles (henceforth, UAVs)[104], because robots belonging to the former category gained acceptance before and generally move in structured environments, while the tasks performed by the latter are more ambitious.

Automated Guided Vehicles. A sub-category of mobile robots is that of so called Automatic Guided Vehicles, Automated Guided Vehicles or Autonomous Guided Vehicles, or AGVs, which primarily differs in light of the kind of control mechanism tackling the driving task. Indeed, AGVs are described as:

- **ISO 8373:2012**, 3.20 «a mobile platform (3.18) following a predetermined path (4.5.4)[105] indicated by markers or external guidance commands, typically in the factory. Note: International standards on AGV are developed by Technical Committee ISO/TC 110, Industrial trucks»;
- A Computer-Controlled, Non-manned, Electric Powered Vehicle Capable of Handling Material[106];
- An automatic guided vehicle is a programmable mobile vehicle. The automatic guided vehicle (AGV) is a mobile robot used in industrial applications to move materials around a manufacturing facility or a warehouse[107];
- An automatic guided vehicle is a mobile robot that follows marks and wires in the floor or uses vision or lasers[108].

Applications. Industrial applications of mobile robots include painting, maintenance and repair of large, uneven or inconvenient surfaces[109]. Both mobile robots and AGVs (see

---

[99] Phey Sia Kwek et al., *Development of a Wireless Device Control Based Mobile Robot Navigation System*, *IEEE Global High Tech Congress on Electronics* (2012).
[100] G. N. Tripathi and V. Rihani, "Motion Planning of an Autonomous Mobile Robot Using Artificial Neural Network," *CS&IT-CSCP* (2012).
[101] Paola Andrea Niño-Suarez, Eduardo Aranda-Bricaire, and Martin Velasco-Villa, *Discrete-Time Sliding Mode Path-Tracking Control for a Wheeled Mobile Robot*, *45th IEEE Conference on Decision & Control* (San Diego: 2015).
[102] R. Oftadeh et al., *Mechatronic Design of a Four Wheel Steering Mobile Robot with Fault-Tolerant Odometry Feedback*, *l6th IFAC Symposium on Mechatronic Systems* (Hangzhou: 2013).
[103] M. Shneier and R. Bostelman, *Literature Review of Mobile Robots for Manufacturing* (National Institute for Standards and Technology, 2015), http://dx.doi.org/10.6028/NIST.IR.8022.
[104] B. Siciliano and O. Khatib, eds., *Springer Handbook of Robotics* (Berlin: Springer, 2008)., pp. 799 ff., 1009 ff., 1175 ff.
[105] «Ordered set of poses».
[106] N. D. Chinchkhede and A. T. Shende, "Automated Guided Vehicle as an Office Boy," *International Journal of Scientific Research in Science and Technology* 4, no. 3 (2018).
[107] K. Kishore Kumar et al., " Design of Automatic Guided Vehicles," *International Journal of Mechanical Engineering and Technology* 3, no. 1 (2012).
[108] M. Mohanty and A. Bhardwaj, *An Exploration of Robot Utilization for Vehicles in Tracking Shortest Route*, *International MultiConference of Engineers and Computer Scientists* (Hong Kong: 2014).
[109] https://aircobot.akka.eu/, last access June 6th, 2018.

below) are widely used for moving, conveying and stocking[110], but the technology of the latter is more widespread.

AGVs are generally used industrially for transporting goods and materials in manufacturing systems[111] at all stages, such as storage, retrieval, handling and delivery.

2.3.3 Wearable robot: industrial exoskeleton

Definition. There is no European legal act providing a definition of industrial exoskeleton.

Similarly, no established technical standard has been found, providing an official definition, at neither the international nor European level.

An indirect definition can be derived by international standard; indeed,

- **ISO 13482:2014**[112], 3.15.1, on personal care robots, mentions exoskeletons by defining a restraint type physical assistant robot as a «physical assistant robot (3.15)[113] that is fastened to a human during use. Example: This includes wearable suits or non-medical physical assistance exoskeletons».[114]

Other definitions may be found in some reports and statements, as indicated below, describing exoskeletons as:

- An external structural mechanism with joints and links corresponding to those of the human body. Worn by the human, the exoskeleton transmits torques from proximally located actuators through rigid exoskeletal links to the human joints[115];
- A mechanical or textile system[116], worn by a worker and aimed at bringing him physical assistance while performing tasks, by compensating his efforts or empowering his capabilities (strength boosting, movements assistance and so on)[117];
- Mechanical armatures enveloping all or part of the body to animate it[118];
- An articulated and motorized equipment fixed on the body at the level of legs and the pelvis, or even on the shoulders and the arms[119];
- A human-machine interface comprising robotics and computers, or more specifically, motors, sensors, software and novel algorithms that combine the former. Exoskeletons

---

[110] Kagan Pittman, "Automating Material Transportation with Mobile Industrial Robots," accessed. https://www.engineering.com/AdvancedManufacturing/ArticleID/14627/Automating-Material-Transportation-with-Mobile-Industrial-Robots.aspx., last access June 6th, 2018.

[111] S. Y. Lee and H. W. Yang, "Navigation of Automated Guided Vehicles Using Magnet Spot Guidance Method," *Robotics and Computer-integrated Manufacturing* 28 (2012).

[112] See https://www.iso.org/standard/53820.html, last access June 26th, 2018.

[113] «personal care robot (3.13) that physically assists a user (3.26) to perform required tasks by providing supplementation or augmentation of personal capabilities».

[114] It is worth noting that one of the interviewees, as producer of exoskeletons providing back support in the workplace, pointed out that the definition provided in this standard is not completely on the spot, because it does not include the correspondence to the human body as a technical requirement.

[115] J. C. Perry, J. Rosen, and S. Burns, "Upper-Limb Powered Exoskeleton Design," *IEEE/ASME Transactions on Mechatronics* 4 (2007).

[116] Jean Theurel et al., *10 Idées Reçues Sur Les Exosquelettes* (Institut National de Recherche et de Securité, 2018), http://www.inrs.fr/publications/essentiels/exosquelettes.html., p. 3.

[117] In French, Un exosquelette est un système mécanique ou textile revêtu par le salarié et visant à lui apporter une assistance physique dans l'exécution d'une tâche, par une compensation de ses efforts et/ou une augmentation de ses capacités motrices (augmentation de la force, assistance des mouvements, etc.).

[118] In French, *les exosquelettes sont des armatures mécaniques enveloppant tout ou une partie du corps pour l'animer*. See, more broadly, L. Bougrain and B. Le Golvan, "Les Neuroprothèses," *L'Évolution psychiatrique* 81, no. 2 (2016).

[119] In French, un équipement articulé et motorisé fixé sur le corps au niveau de jambes et du bassin, voire également sur les épaules et les bras, Various, *Utilisation Des Robots D'assistance Physique À L'horizon 2030 En France* (Institut National de Recherche et de Securité, 2015), www.inrs.fr/dms/inrs/PDF/rap-2030-version-2015/rap-2030-version-2015.pdf. P. 19. See on p. 82, robots are useful and worthy because they perform tasks that are too hard or dangerous for people.

also present a […] technology for able bodied workers in industries requiring stamina, repetitive motion and hard labor[120].

Applications. Apart from medical and military purposes[121], exoskeletons are employed to help hikers carry large loads[122], ascend stairs and slopes[123], squatting[124] and to provide general worker assistance[125]. In a factory environment, exoskeletons are used to perform tasks that cannot be completely automated and that would be extremely hard or fatiguing for workers alone[126].

Among the latter, six categories are generally recognized:

- tool holding exoskeletons, that consist in a spring-loaded arm supporting a heavy tool, while linked to a lower body exoskeleton and a counterweight;
- chairless chairs, that are worn on legs and lock, in order to help workers to stand in the same position or crouch for extended amounts of time;
- back support, that help maintaining a correct posture and mitigating loads on the spine and the back muscles while a worker is lifting objects;
- powered gloves, that enable workers to perform a stronger grasp on objects;
- full body powered suits, that enhance several movements performed by workers;
- additional or supernumerary robotics[127], that provide another pair of hands in order to help workers perform tasks that are normally unattainable by a single person.

Full body powered suits are being abandoned by developers and supernumerary robotics are still at an ambitious stage.

As far as the most widespread uses of exoskeletons are concerned, a French report[128] showcased heavy commodities storing[129], masonry[130], and plastering[131], while other research mentioned lifting, holding, carpentry, farming and construction work[132].

2.3.4 Use of case studies

Representative nature of the cases studies. The above-described applications have been selected as cases studies because they are representative of the most common applications of robotics in smart factories, so that can be deemed as sufficiently representative of the overall object of this study – i.e. industrial robots – in its most current uses (§2.2). At the same time, the taxonomy thus developed highlights how different types of IRs may display a variety of characterizing features that may occasionally require each class of applications to be treated autonomously.

---

[120] Dov Greenbaum, "Ethical, Legal and Social Concerns Relating to Exoskeletons," *SIGCAS Computers & Society* 45 (2015).
[121] See http://www.wearablerobotics.com/wearable-robots/, last access June 6th, 2018.
[122] http://bleex.me.berkeley.edu/research/exoskeleton/exohiker/, last access June 5th, 2018.
[123] http://bleex.me.berkeley.edu/research/exoskeleton/exoclimber/, last access June 5th, 2018.
[124] H. Kazerooni, "Exoskeletons for Human Performance Augmentation," in *Springer Handbook of Robotics*, ed. B. Siciliano and O. Khatib (Berlin: Springer, 2008).
[125] https://www.cyberdyne.jp/english/, last access 5th, 2018.
[126] J. Van der Vorma, R. Nugent, and L. O'Sullivan, *Safety and Risk Management in Designing for the Lifecycle of an Exoskeleton: A Novel Process Developed in the Robo-Mate Project*, *6th International Conference on Applied Human Factors and Ergonomics*.
[127] Bobby Marinov, "22 Exoskeletons for Work and Industry into 6 Categories," accessed. 22 Exoskeletons For Work and Industry Into 6 Categories.
[128] Institut National de Recherche et de Securité, *Les robots et dispositifs d'assistance physique: états des lieux et enjeux pour la prevention, 2017*, see http://www.inrs.fr/inrs/recherche/etudes-publications-communications/doc/publication.html?refINRS=NOETUDE/P2017-120/NS354, last access June 6th, 2018.
[129] P. 14. For this task, a full body exoskeleton with two powered arms has been employed.
[130] P. 28. Exoskeletons have been used for lifting heavy material, for holding and displacing it and for holding tools.
[131] P. 30. For example, to aid workers in sanding ceilings.
[132] Michiel P. De Looze et al., "Exoskeletons for Industrial Application and Their Potential Effects on Physical Work Load," *Ergonomics* (2015).

Common features. Indeed, it is commonly acknowledged in technical-engineering literature[133] that there is a common trend in technological development, which, at least in the industry-related field, is fostering:

- *sensor fusion*: the ability to combine sensory data from multiple sources in order to reduce the amount of uncertainty the robots may encounter in understanding the context of their surroundings, and allowing them to act independently and appropriately in complex situations;
- *human-robot interaction*: the ability to communicate and share goals and information with humans, making the robots part of the human environment;
- *cognitive and learning systems*: the ability to learn new tasks, operate and behave in adaptive ways, depending on the changing of the surroundings;
- *mobility and motion*: the ability to move or, for robot based on fixed platform, to make use of flexible and extensive arms or end-effectors;

Peculiarities. Although all Industry 4.0 robots share those features, despite to different degrees, it is nevertheless true that each class of application may give rise to specific concerns. For example, exoskeletons need to be biomimetic, thus displaying a significant level of anthropomorphism to support, protect or enhance the human body and its movements, whereas cobots and movable robots need sensors for orientation and navigation in the working environment, specifically for collision avoidance. The peculiarities of each case study reflect on their technical outtake and, consequently, on the legal framework regulating their development and use[134].

Use of case studies. Therefore, in order to address those peculiarities without incurring in needless repetition, the description and evaluation of the legal framework applicable to testing, certification, liability and insurance will not be performed for each class of application autonomously; on the contrary, the analysis will be referred to industrial robots as a general category, while the singularities of one or more classes of application will be considered only when their technical peculiarities may give rise to issues bearing specific concerns from a legal point of view.

2.4 Subjects involved

Many subjects are involved in the production, transfer, marketing and use of robotics in the industrial workspace.

From a technical point of view, it is important to consider the entities who are directly involved in the different stages of development and use of the robots; according to an economic perspective, it is necessary to pinpoint the subjects whose activities constitute the value-chain of industrial robots. Under a legal approach, the analysis shall identify those entities who bear legal duties pursuant to the development, marketing and use of such applications.

For the purpose of this report, a legal perspective will mostly be adopted, but a combination of the other two points of view will also be used whenever relevant.

2.4.1 Subjects bearing a direct safety-related duty

Safety-responsible subjects. Despite the complexity of the legal framework, the most fundamental principle underlying all rules and regulations is that the robots and the operations in which they are involved shall be as safe as possible.

---

[133] Simon Forge and Colin Blackman, *A Helping Hand for Europe. The Competitive Outlook for the Eu Robotics Industry* (European Commission, Joint Research Centre, Institute for Prospective Technological Studies, 2010).

[134] For a methodological account of the legal analysis of robotic applications based on selected case studies, and the general criteria for their selection (identification of the most novel, imminent, social pervasive and useful application), see Palmerini et al.See esp. pp. 26 ff.

Pursuant to **ISO 10218:1**,

> «[p]roviding for a safe robot system or cell depends on the cooperation of a variety of «stakeholders», sharing the responsibility for the ultimate purpose of providing a safe working environment. Stakeholders may be identified as *manufacturers, suppliers, integrators and users* (the entity responsible for using robots), but all share the common goal of a safe (robot) machine»[135].

Accordingly, the standard specifies that the requirement set by ISO 10218 may indeed apply to subjects to whom such duties are not specifically assigned to, in so far as they share the responsibility of assuring safety[136].

Nevertheless, despite this common ground, all stakeholders play a different role in the development and use of industrial robotics applications, leading their responsibilities and legal positions to be shaped correspondingly.

Moreover, the very apportionment of those responsibilities may vary, depending on the nature and number of the entities concretely involved.

Practical overlap of roles among different subjects. Theoretically, in very small enterprises, or in case of not-yet-developed markets, the same subject could work as a «one-man-band» performing multiple roles: e.g. the business-user of IRs who also produces them and/or integrates them in the production line of his own factory. On international and highly developed markets, on the contrary, all the aforementioned subjects are likely to play a specialized and narrow-tailored function: e.g. the business-user who only purchases the main industrial robots from a producer, and have them assembled/and or installed within the production line by an integrator, using auxiliary products purchased by suppliers[137].

Use of subjects-reference in the study. Despite sometimes more functions could be performed by the same subject, it is nevertheless important, from a methodological point of view, to distinguish such roles in each stage of the development and use of the industrial robots, since each function is burdened with specific technical and legal implications. Indeed, once the regulatory framework applicable to each phase and operation is identified, the degrees of specialization and distribution of tasks among the subjects involved may give rise to additional challenges or opportunities, therefore requiring a stand-alone analysis.

2.4.1.1. Manufacturers

General activities. As for the very notion of robots and industrial robots (§2.2), no unique and official definition of the «manufacturer of industrial robots» is available. In economic and engineering literature, the term usually designates the original designer and supplier of a branded product[138].

Desk research[139] and interviews showed that manufacturers commonly perform the following activities:

- in-process research and development;
- system design;
- software development and test (through bought-in software components);
- prototype integration and test (through bought-in software environments);
- assembly and test (through bought-in hardware components);
- marketing;

---

[135] Italics added.
[136] ISO 10218, Introduction, p. 13 (italics added).
[137] However, interviews showed that even big industrial players may perform multiple roles.
[138] Forge and Blackman. Main manufacturers of IRs are, for example: ABB, KUKA, COMAU, Aldebaran, Reis Robotics, British Aerospace, IGM, Stäubli.
[139] Ibid., 77.

- delivery and installations;
- after sales service.

Legal definition and safety obligations. Such picture – describing what a manufacturer is, and what tasks he generally performs – is not sufficient for the purpose of this report. In order to identify the rights and obligations that manufacturers bear in developing and marketing a product, we need to understand what it means to be a «manufacturer» according to the framework applicable for testing, certification, liability and insurance, as well as by the relevant standards thereof.

By comparing the general definition set above with the ones provided by specific regulations, we will be able to better understand whether the latter are more restrictive – thus not covering the entire class of original designer and suppliers of branded products – or broader – thus covering also entities which qualify differently (e.g. as supplier of auxiliary products, system integrators, etc.) – then the former.

Two sets of legal definitions allow us to more narrowly define this category for the purpose of this report.

In the legislative acts relevant for certification (§2.6.2), the manufacturer is generally defined as «any natural or legal person who is responsible for designing or manufacturing a product and places it on the market under his own name or trademark»[140]. Furthermore, although falling outside this definition, the responsibilities of the manufacturer apply also to any natural or legal person who assembles, packs, processes or labels ready-made products and places them on the market under his own name or trademark, as well as who changes the intended use of a product in such a way that different essential or other legal requirements will become applicable, or substantially modifies or re-builds a product (thus creating a new product), with a view to placing it on the market or for putting it into service[141]. Therefore, the economic operator who places the product on the market under his name or trademark, or substantially modifies a product which he intends to market, becomes automatically the manufacturer for the purposes of Union harmonized legislation, and he must ensure that the product complies with the applicable legislation and the appropriate conformity assessment procedure has been carried out[142].

Additionally, both the General Product Safety Directive[143] (henceforth GPSD) and the PLD, with a parallel terminology, define the «producer» as comprising both the actual manufacturer of the product, its legal representative in the European Union, or – absent the latter – the subject who imports the product in the EU, as well as any other person presenting himself as the manufacturer by affixing to it his name, trade mark or other distinctive mark, or the person who reconditions the product, and even other professionals in the supply chain, insofar as their activities may affect its safety properties[144].

2.4.1.2. Suppliers

General activities. Suppliers are economic operators who, on basis of a contractual agreement, provide bought-in products either directly to the manufacturer of the branded product or to the system integrator. Desk research[145] and interviews showed that, depending on the products and services concretely offered, they can be either:

---

[140] *The "Blue Guide" on the Implementation of Eu Products Rules*.
[141] Ibid.
[142] MD, art. 2; MDD, art. 2; MDR, art. 2; PPER art. 2. No explicit definition of manufacturer is provided for by the PPED.
[143] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 11, 15.1.2002, p. 4–17.
[144] GPSD, art. 2; PLD, art.3.
[145] Forge and Blackman., 37-38.

- *suppliers of special components*: engineers selling tools and subsystems to end-users, as well as to robot manufacturers or system integrators of value-added, such as sensors, actuators, end-effectors etc.;
- *value-added resellers*: intermediaries who buy a robot as part of a total system and resell it in an integrated package to end-users, thus also acting as reseller channel for robot suppliers;
- *supplier of standard components*: economic operators selling basic unbranded components such as sensors, motors, actuators, electronics etc. to robot builders[146];
- *independent software vendors*: suppliers who sell generic or robots-specific software packages, such as virtual simulation capabilities for robots in action.

Legal definition and safety obligations. Differently from the case of manufacturer, the relevant legal framework for testing, certification and liability does not provide any definition of «supplier». However, from the considerations developed above (§2.4.1.1) it is already possible to see that, from a legal perspective, suppliers might, for certain purposes, share the same responsibilities of the actual manufacturer and, therefore, be treated as such (e.g. for apportioning liability in case of a defective product, in case the producer cannot be found, pursuant to art. 3 PLD). Whenever relevant, an in-depth analysis of the functions and roles of suppliers for the purpose of this report will therefore be carried out, in order to understand: (i) whether suppliers may be assimilated to manufacturers under the applicable regulations, and (ii) how contractual agreements generally regulate the apportionment of the responsibilities for the performance of certain tasks (e.g. related to testing and certification), and as well as of the liability arisen by damages caused by the component or software supplied.

2.4.1.3. System integrators

General activities. Standard IRs are generally sold not in a complete form, but rather as flexible systems to be customized and programmed for a target task and work environment. System integrators (henceforth SI) are economic operators who offer planning and integration work to build robot systems that can complete the required tasks by incorporating in the customer production line all the mechanical systems, robotics hardware, software and special subsystems, e.g. for positioning, and then program robot for its task, often with simulation beforehand. For this purpose, they often act as major reseller channel for robot suppliers (e.g. M3, Geku).

Desk research[147] and interviews showed that SI generally offer the following services:

- consultancy and feasibility studies: identification of the correct robot, tooling, work cell for the application needs;
- target system design: preparation of the target environment, which may include many major activities (e.g. construction of a whole building an its interior for robots with strengthened floors and no stairs);
- integration of auxiliary systems: combination of the robots purchased with auxiliary tool systems, such as sensor systems, actuator systems, end effectors, safety systems interlocks, power and utility systems, control, communication and coordination systems etc.;
- robot systems and environment integration: installation of the robot or the system within the overall production line, with the required adjustments to the factory-specific needs and requirements;
- site test and commissioning; testing of the robot or the system integrated within the production line and eventual adjustment to meet the functional and qualitative criteria requested by the customer;
- training: training of the IRs operators

[146] E.g. Faulhaber; HarmonicDrive AG, Pilz GmbH, SSB Duradrive SEM, Parvex.
[147] Forge and Blackman.

- after sale services: help and supported offered after the integration has been completed as a form of post contractual obligations.

Legal definition and safety obligations. Once again, no legal document gives a definition of SI. However, a definition of both integrator and integration is provided by harmonized standards:

- **ISO 10218-2:2011** integrator: «entity that designs, provides, manufactures or assembles robot systems or integrated manufacturing systems and is in charge of the safety strategy, including the protective measures, control interfaces and interconnections of the control system»;
- **ISO 10218-2:2011** integration: «act of combining a robot with other equipment or another machine (including additional robots) to form a machine system capable of performing useful work such as production of parts»;

Apart from the one mentioned above, no other definition can be found in the relevant legal framework for testing, certification and liability. However, given the specific activity performed, the SI is responsible for assuring the safety of the IRs handled both on a ground of general liability and on the basis of contractual obligations with the customers; additionally, in so far as the SI radically modify or alters the robots or the system, he may share the legal obligations provided under, for example, the PLD and the GPSD. As for the supplier, whenever relevant, the study will offer an in-depth analysis of the functions and roles of SI, aiming to understand (i) whether SI can be assimilated to manufacturers under the applicable regulations, and (ii) how contractual agreements generally regulate the apportionment of the responsibilities for bringing about certain tasks (e.g. related to testing and certification), and as well as of the liability arisen by damages caused by the service offered, as well as the auxiliary devices, components and software used.

2.4.1.4. Business-users

General activities. Business-users are the commercial entities using IRs in their own factories, generally after having purchased them by the manufacturers and having had them integrated in the targeted working environment (see §2.4.1.4).

Legal definition and safety obligations. A very general definition of user is offered in harmonized standards:

- **ISO 10218-1:2011** 2.27, defines user as the «entity that uses robots and is responsible for the personnel associated with the robot operation»

In the harmonized legislation on the manufacturing and commercialization of products within the EU – differently from other economic operators such as manufacturers and their legal representatives, distributors and importers – end-users are not defined.

Provided that they use the product according to the intended use, and comply with the indication given by the manufacturer, they are not directly bearer of any specific legal requirement connected to the testing and certification of IR. However, duties might indeed arise when the nature of the product purchased and installed are modified as to basically make it a «new product», because this might lead the business-user to qualify as a «manufacturer», e.g. for the purpose of certification (§2.6).

In any case, business-users are subjects to specific obligations as regards the use of work equipment by workers at the workplace, and that also relates to the use of IR by the individual workers. According to the Directive 2009/104/EC concerning the minimum safety

and health requirements for the use of work equipment[148] (henceforth, WED), the employer must take all measures necessary to ensure that the work equipment is suitable for the work carried out, and may be used by workers without impairment to their safety or health, and complies with the provisions of the applicable legislation set at the time of its first use, or, if no other legislation is applicable or is only partially applicable, the minimum requirements laid down in Annex I of the Directive. Furthermore, the employer must also take the necessary measures to ensure that work equipment is maintained at that level of security, and that the workers are provided with the adequate information and training as regards the use of work equipment.

According to the Directive 89/656/EEC concerning the minimum health and safety requirements for the use of personal protective equipment by workers at the workplace, and the Regulation 2016/425/EU repealing it[149], such equipment must comply with the relevant Union provisions on design and manufacture with respect to safety. The equipment must be appropriate for the risk involved, correspond to existing conditions at the workplace, take into account ergonomic requirements and the worker's state of health, fit the wearer correctly, and be compatible where more than one piece of equipment must be used simultaneously. The employer is required, before choosing the personal protective equipment, to assess that it satisfies the requirements.

2.4.2. Other subjects involved

In addition to the ones already identified – i.e. the manufacturers, suppliers, integrators and business-users – three other subjects might come into play in the testing, certification, liability and insurance of IRs: non-business-users and by-standers, notified bodies and insurance companies.

2.4.2.1. Non-business-users and by-standers

General activities. Non-business-users are workers operating the IRs, or directly collaborating with them, whereas by-standers are either workers who, despite not making direct use of the robots, share their workspace with the latter, or individuals who are not co-workers but rather occasional invitees who happen to be in the working space. Both non-business-users and by-standers are relevant for the purpose of this analysis, at least as far as liability issues are concerned.

Legal definition and safety obligations. On the one hand, although the employer is the ultimate subject responsible for the safety and security of the working environment, workers might share a certain degree of responsibility in assuring the safety, if not of the robot itself, at least of the operation performed and of the working environment. Indeed, according to the Directive 89/391/EEC on the introduction of measures to encourage improvements in the safety and health of workers at work, workers have a general responsibility to take care, as far as possible, of their own safety and health and that of other persons affected by their acts at work[150]. For instance, they must make correct use of machinery, apparatus, and other means of production, and the personal protective equipment, accordance with the training and the instructions given by their employer.

---

[148] Directive 2009/104/EC of the European Parliament and of the Council of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work (second individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) (Text with EEA relevance) *OJ L 260, 3.10.2009, p. 5–19.*

[149] Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC, in OJ L 81, of March 31st, 2016. Council Directive 89/686/EEC of 21 December 1989 on the approximation of the laws of the Member States relating to personal protective equipment, OJ L 399, of December 30th, 1989.

[150] Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work, *OJ L 183, 29.6.1989.*

At the same time, should an accident occur, non-business-users and by-standers working in close contact with the robots (or being occasionally in contact with them), they are most likely to suffer damages and thus be entitled to compensation or to social security schemes.

2.4.2.2. Notified bodies, notifying authorities and notified authorities

Notifies bodies, Notified Authorities and Accreditation Bodies are subjects who, within different roles, perform a relevant function in the certification of products.

Notified Bodies. Notified Bodies are independent entities entitled to provide verification and certification services. They perform conformity assessment – which may include inspection of the working environment, examination of the products, their design and the processes associated with them – to assess whether the product, i.e. the industrial robots and/or a specific application, system or production line, meets the preordained requirement to be placed on the market, and label the product with the CE mark[151].

Notifying Authorities. Notifying Authorities are governmental or public bodies tasked with designating and notifying conformity assessment bodies under Union harmonization law. The Notifying Authority notifies the Commission and the other MSs when a body, which fulfils the relevant requirements, has been designated to carry out conformity assessment according to a directive, thus becoming a Notified Body; such notification is performed through the New Approach Notified and Designated Organizations Information System (henceforth, NANDO), which is the electronic notification tool developed and managed the Commission, which, among other functions, features a website, providing lists of notifying authorities, notified bodies and accreditation bodies, divided by country and product category.

Accreditation Bodies. The Accreditation Body, instead, is the only one body which each Member State may appoint according to Regulation 765/2008/EC[152] to perform third-party accreditation of conformity assessment bodies, that is the «attestation that a conformity assessment body meets the requirements set by harmonized standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity»[153].

The presence of an Accreditation Body, and of the accreditation certification, makes the procedure for obtaining notification significantly easier, as, when the body submitting an application does not provide an accreditation certificate, the notifying authority must provide the Commission and other Member States with the documentary evidence relevant to the assessment and its evaluation.[154]

2.4.2.3. Insurance companies

For the purpose of this report, insurance companies are companies offering insurance contracts to the subjects bearing a direct safety-related duty, through a combination of different policies, such as those related to commercial property loss or damage, employer's injury, equipment breakdown, mechanical malfunctioning etc., as well as to the law suit which could arise in connection with these events.

In particular, a distinction needs to be made between private insurance companies, and social security authorities, which specifically govern workers' compensation insurance program, determining the amount of benefits an injured employee is entitled to, what types

---

[151] *The "Blue Guide" on the Implementation of Eu Products Rules*. See esp. p. 75.
[152] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, *OJ L 218, 13.8.2008, p. 30–47*
[153] *The "Blue Guide" on the Implementation of Eu Products Rules*. See esp. p. 89
[154] Ibid. See esp. p. 89.

of injuries are covered, and how medical care will be delivered, income replacement and death benefits.

2.5. Testing

KEY FINDINGS

- Testing consists in the procedures performed to verify the robots' goals and functionalities (performance testing), and gather knowledge about their potential risks and failures (reliability testing).
- There is no EU or national legislation specifically regulating how testing of IRs should be performed. However, few legislative documents refer to testing as necessary to ensure product safety, and the general obligations related to the health and safety at work apply.
- During the entire production cycle, components, sub-systems and systems are tested, starting from more computerized solutions (mathematical modelling, simulation) and progressively inserting real-life trials (physical testing).
- Risk assessment is based on functional and safety requirements set by international standards. However, machine learning, cybersecurity, and loosely structured work environments may give rise to additional risks which are difficult to foresee and evaluate. The stronger the human-robot interaction, the more precaution should be adopted in order to prevent damages that might be caused by such unknown unknowns.
- There is no need to regulate testing of IRs, neither at MSs' nor at the EU level. Lack of specific regulation allow business to develop application-specific solutions without additional procedures and costs.
- Since testing is performed in private locations, no regulation for ensuring safety, other than that on working environments already in place, is required.
- Broadly accepted criteria to measure the performance of IRs – such as benchmarks, international standards, and good experimental practices – need to be promoted to facilitate testing and improve its reliance.
- Digital innovation hubs (DIHs) shall be promoted and established across Europe, to create synergies and grant further resources, especially for SMEs and universities.

2.5.1. Introduction

Definition. During the entire cycle of production, IRs are tested, to prove their inerrant safety and their functionality. Despite inherently intertwined, these two objectives require different form of testing, i.e. performance testing and reliance testing.

Performance testing. Performance testing takes place in the development and production of IRs, with the purpose of verifying the robots' goals and functionalities, and it is mostly market oriented[155]. Despite purchase of completed IRs, as originally designed by the developer, is not exceptional in the IRs market, more frequently companies produce partly-

[155] On the qualification of IRs as partly-completed machinery for the purpose of the Machinery Directive, see §2.6.2.1.

completed robots, which will be further developed (either by the manufacturers themselves or by SIs) and adjusted on the basis of the customers' desires and requests[156]. Therefore, the technical requirements of IRs will mirror those of the products, as expressed by the demand-side of the market.

Reliance testing. Reliance safety, instead, aims at gathering knowledge about potential risks and failures connected to their use, and it is mostly based on the requirements set in different EU legislative documents, on international standards published by organizations such as ISO/CEN/CENELEC, as well as on the specifications required by conformity assessment procedures established for the purpose of certification (see §2.6), which often make an explicit reference to the said standards.

These types of testing is part of the normal scientific methodology used by IRs developers and engineers, and offers a manner of gathering evidence about the correctness of the design – and its development – in specific components and subsystems, as well as of performing the related risk assessment and evaluation.

Trials and validations performed for the purposes of obtaining certification serve the different function of demonstrating conformity of the product with the relevant safety essential requirements necessary for marketing a product within the internal market, and are performed once the robot is finalized and ready to be commercialized. Given this substantial and functional difference, certification-oriented testing falls outside the scope of this section, and – whenever relevant – it will rather be considered in §2.6. However, it is important to highlight that manufacturers of components or full robotic systems rely on the standards to demonstrate safety of equipment in spatial environments in which the robotic systems need to function, both during the testing cycle of the products under development, and during the procedures to obtain certifications.

Structure and aim of the section. This section firstly investigates the legal framework on testing of IRs (§2.5.2). Secondly, it will describe how tests are performed (§2.5.3), and what risks are identified and evaluated, with particular focus on those novel risks that Industry 4.0 robotics bring about, because of their advanced and collaborative technology (§2.5.4). On the basis of such analysis, technical and legal bottlenecks, preventing adequate assessment of the performance and reliance of the IRs, will be identified (§2.5.5). Lastly, the overall state of art of testing is evaluated; where needed, possible policy strategies for reform are also formulated (§2.5.6).

According to the overall methodology described in §2.3, the three case studies will be addressed in an holistic manner, unless specific reference to the individual applications were required, due to their peculiarities.

2.5.2. Legal framework

***Lack of specific legislation*.** Desk research and interviews demonstrated that, differently from other technological applications – such as CADs (§3.2.2) – no legal framework has been adopted to specifically regulate testing of IRs, neither by the EU nor by MSs.

Such lack of regulation is due to the fact that IRs are intended to be used in factories, and hence testing is performed in private locations, such as laboratories and factories' premises (whether those of the manufacturer, of the SI, or of the business-user). Since no real-life testing in public spaces is required, there is generally no need to derogate specific legislation prohibiting the activities performed with testing, nor specific rules and standards to assure safety of the general public. When testing occurs in the confines of a private space, such as a factory or a laboratory, safety requirements for testers and by-standers need to be taken

[156] See §2.4.1.4.

into account. This requires fulfilment of specific safety procedures and obligations, which will be described in the upcoming sections.

However, while this is always the case for mobile robots and co-bots, interviews showed a partially different scenario as far as exoskeletons are concerned.

Indeed – and as it is further discussed in the section on certification (§2.6) – exoskeletons for industrial use might be developed by businesses that also produce exoskeletons intended primarily for medical purposes, such as those used in clinics to help patients during rehabilitations. Most likely, businesses will first develop and test exoskeletons as medical devices, since this allows them to reach a broader and more established market, and then also market them for industrial use, after having adjusted their design and development, whenever needed. Thus – at least during the product development and manufacturing stages – exoskeletons will be tested not just in private locations, but also in public spaces, e.g. hospitals and clinics; hence, specific authorization from the hospital and informed consent of patients is needed, and – at least in some country (e.g. Italy) – notification to the Ministry of Health is also required[157].

A part from this limited case, in which regulations meant for non-industrial technological devices also indirectly affect a peculiar class of wearable IRs, the present study found no other legislation setting standards and rules on how testing should be performed.

Testing is mostly based on commonly shared practices, as well as in-house schemes and procedures, which manufacturers – and the other subjects which are required to test IRs, their components, or the production line they are integrated in, like SIs – adopt on a discretional basis.

General safety-related duties. Once clearly stated that no legislation sets binding, comprehensive and narrow tailored rules on how testing of IRs shall be carried out, it is nevertheless important to take into account that through a systemic interpretation of the overall normative framework applicable to IRs, it is possible to identify widely recognized principles, which are relevant for testing.

Testing as a requirement for product safety. The first principle underlying all the legislative documents and practices, is that testing should indeed be performed in order to ensure safety of IRs, both during the development of the product, and after its release. In this sense, testing is relevant as a means for ensuring safety of the product tested.

Indeed, reference to the need for reliance testing can be found in different legislative documents. Art. 5(1) of the GPSD refers to sample-testing of marketed products as a measure which producers shall use in order to «(a) be informed of risks which these products might pose; (b) choose to take appropriate action including, if necessary to avoid these risks, withdrawal from the market, adequately and effectively warning consumers or recall from consumers». Art. 10 GPSD mentions establishing testing project as a means to enhance and enforce collaboration between surveillance authorities, while Recital 25 enumerates testing as a means for enhancing the exchange of information on potentially unsafe products.

Pursuant to art. 5 of Workplace Equipment Directive (WED)[158]

---

[157] In this case, testing is performed for developing, and further certifying, a medical device. However, since this will be the starting point for further elaborating similar types of exoskeletons, to be certified most likely as machinery or personal equipment, the first round of trials is also indirectly functional for the experiments of the non-medical version of the device.

[158] Directive 2009/104/EC of the European Parliament and of the Council of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work (second individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) OJ L 260, 3.10.2009.

> «In order to ensure that health and safety conditions are maintained and that deterioration liable to result in dangerous situations can be detected and remedied in good time, the employer shall ensure that work equipment exposed to conditions causing such deterioration is subject to: (a) periodic inspections and, where appropriate, testing by competent persons within the meaning of national laws and/or practices […]».

Safety of testing. The second principle is that testing shall be safe for both the operators of the product, as well as co-workers and by-standers. Here, the concern lies not on the safety of the product tested, but rather on the safety of testing as a procedure which is performed as within the working environment (regardless of whether it is performed within the premises of the employer, those of the business-user, or in public spaces). Safety procedures for preventing the exposure of employees (which can be scientific workers at universities or – for instance – at a digital innovation hub) to unacceptable risks will be part of normal operating procedures at any test facility.

On this matter, the obligations according to which the employer has to ensure safety within the workplace (which art. 5 WED also refers to), will be further addressed within the section on liability, when dealing with health and safety at the workplace (§2.7.2). In this section we will rather discuss whether the testing of robotics (cobots, mobile robots or wearable robots such as exoskeletons) is in need of additional legal safeguards because of new dangers or risks arising from these new technologies.

The most relevant regulations in respect are the Machinery Directive (MD), the Work Equipment Directive (WED), the General Product Safety Directive (GPSD), the Low Voltage Directive[159] (LVD) and for specific applications such as medical use of exoskeletons the Medical Devices Regulation[160] (MDR).

The MD refers to testing in two separate Annexes: in Annex 1 (Essential health and safety requirements relating to the design and construction of machinery), testing is mentioned in respect to «the conditions in which the machinery meets the requirements of stability during use, transportation, assembly, dismantling when out of service, *testing* or foreseeable breakdowns»[161] as part of an instruction manual that needs to be part of the machinery (art 1.7.4.2 (o) of Annex I). Two further references are made in reference to the full quality assurance (Annex X) of which the first (article 1) mentions testing as being a part of an approved quality system and the second (article 2.1) refers to the need to lodge an application for assessment of the quality system to a notified body of his (i.e. the manufacturer's) choice. Though not explicitly stated, testing in this article seems to refer to testing the full functionality of the entire system before putting it onto the market. This will be covered in the next section. Article 1.7.4.2 (o) of Annex I contains instructions that need to be met by a manual that is sufficiently detailed to enable non-trained experts to determine the conditions of stability of the machinery, among others during testing.

The WED refers to testing in article 5(2) sub a, where testing is related to the proper functioning of the equipment after a specific period of time. This may be needed in order to determine whether the functioning of the equipment has deteriorated in such a manner that it may cause safety issues for the workers. This directive does not directly relate to performance and reliance testing – which is the focus of this section – except when testing equipment is used during a longer period of time such as observational units (for instance a

---

[159] Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits Text with EEA relevance, in OJ L 96, 29.3.2014.

[160] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 117, 5.5.2017.

[161] Italics added.

potential deterioration of sensors that observe functioning of the robots during a test phase[162]).

The GPSD[163] mentions testing in Recital 25, where it is mentioned as one of the enforcement means to enhance the exchange of information on potentially unsafe products. Article 5 refers to sample testing of products in order to determine the overall safety of these products. Article 10 identifies testing project as a tool for enhancing and enforcing collaboration between surveillance authorities. Testing is used for determining the safety of products already on the market rather than testing functionalities of a product under development.

The LVD determines safety procedures for equipment to be used within specific voltage limitations. It does not contain a reference to testing procedures. The safety constraints as presented in Annex I refer to products put on the market (and that thus need to be accompanied by a CE mark accordingly). Components, subsystems or entire systems that are tested in a laboratory condition cannot be equated to products put at the market place.

The MDR poses several safety requirements to medical devices. The MDR shall apply in its entirety from 26 May 2020 onwards. Various parts of the regulation are already applicable, such as those related to the functioning of the Notified body (art 35 – 50), as well as article 101 (Competent authorities), article 102 (Cooperation) and art 103 (Medical Device Coordination Group). For the sake of convenience, we will follow the text of the MDR on testing, in which we consider testing to be aimed at component, subsystem or system validation and improvement, rather than for the sole purpose of conformity assessment. The MDR refers in several articles to legal obligations concerning testing of (components of) products. Art 1, sub 10 refers to Directive 2004/23/EC for devices which incorporate «as an integral part, non-viable tissues or cells of human origin or their derivatives that have an action ancillary to that of the device». This will only be applicable to industrial robots acting in a medical setting. In this situation, Directive 2004/23/EC obliges the manufacturer to meet specific safety requirements concerning dealing with human tissue.[164] Since we do not expect this to play a major role in the setting of industrial robots in scope for this report, we will not treat this subject in more detail. Article 2, item 39 refers to testing in case of reprocessing, meaning «a process carried out on a used device in order to allow its safe reuse including cleaning, disinfection, sterilization and related procedures, as well as testing and restoring the technical and functional safety of the used device». In this situation testing might refer to testing functional requirements in laboratory or other settings that mimic the functioning of the device. Again, the scope refers to using medical devices in specific medical settings. Our expectation is that industrial robots will generally not fall under this category. Similarly, art 61 and 62 refer to non-clinical testing (art 61) and «the use of testing results for the conformity procedure» (art 62), while art 71 takes a similar position as art 62 with respect to assessments done by Member States. Art 86 refers to the need to provide period safety update reports that should be based on actual information concerning incidents. Annex II (Technical documentation), art 3, sub a, mentions the need to provide «information to allow the design stages applied to the device to be understood». While sub b refers to information concerning the final testing, and sub c refers to the provision of information that enables the «identification of all sites, including suppliers and sub-contractors, where design and manufacturing activities are performed».
To conclude this section on applicable legal frameworks, except for the Medical Devices Regulation no specific legislation is in place to guide the testing phase of industrial robots,

---

[162] S. Arosh, Suryaprakash, S.K. Nayak. S.P. Duttagupta (2015). Fitness function based sensor degradation estimating using Hoo filter. Procedia Computer Science 58, 172-177 http://creativecommons.org/licenses/by-nc-nd/4.0/

[163] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 11, 15.1.2002, p. 4–17.

[164] See Directive 2004/23/EC on setting standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells.

considering testing is meant for validation and improvement of components, subsystems and full systems rather than for meeting the requirements of a conformity assessment.

2.5.3. Testing cycle and techniques

Industrial Robots are complex systems and as such different levels of testing might be needed, from testing the software, to the mechanical, mechatronic and electric parts. Each of the systems would usually undergo a cycle in which the system is designed, single components and the overall solution are tested, validated and prepared for market introduction. Indeed, testing occurs several times within the aforementioned cycle, with specific approaches that are catered to different business-users, taking into account market trends and needs, and in the view of highlighting the characteristics of the product.

The following stages have been identified through desk research and interviews[165]:

- *experimentation and design stage;*
- *product development stage;*
- *manufacturing stage;*
- *final validation stage*.

Experimentation and design stage. In the so-called «initialization phase», developers collect information regarding a potential project, and perform preliminary testing to assess its feasibility. The initial phase of a new project is usually an ideation phase, in which the concept of a new approach is developed and comparisons with already existing products are made to understand the space for improvement of existing products and the novelty of the new product[166]. According to the UX-website (User eXperience):

> «Ideation is the process where you generate ideas and solutions through sessions such as Sketching, Prototyping, Brainstorming, Brainwriting, Worst Possible Idea, and a wealth of other ideation techniques.»[167]

From the perspective of the structured Technical Readiness Levels (TRLs), ideation covers the very initial phase of arriving at technical readiness, usually restricted to TRL1 and 2.[168] The products of the ideation phase are «soft products», reports that present functional requirements for a concept to be developed. When using prototypes in this phase, these will be software produced prototypes, with no or very limited physical components.

In the actual «design phase», different concepts and scientific solutions are developed, and basic components are created, to be used together with the existing equipment. Here, tests aim to validate the functionality of the initial concepts, and to empirically assess whether the system meets the technical specifications elaborated in the original design. This implies that not only the test results should demonstrate a perfect alignment of the behaviour of the system with preset functional requirements, but also that the system will not go beyond what is needed for their accomplishment. As an example, developing a mobile robot that is able to move at a determined speed of 3 mph not only requires that the robot is able to do

---

[165] Forge, S. and C. Blackman (2010). A Helping Hand for Europe. The Competitive Outlook for the EU Robotics Industry. JRC Scientific and Technical Reports. M. Bogdanowicz and P. Desruelle, European Commission, Joint Research Centre, Institute for Prospective Technological Studies.

[166] J. Chan and al., "On the Benefits and Pitfalls of Analogies for Innovative Design: Ideation Performance Based on Analogical Distance, Commonness, and Modality of Examples," *Journal of Mechanical Design* 133, no. 8 (2011), http://dx.doi.org/doi:10.1115/1.4004396.

[167] See https://www.interaction-design.org/literature/article/what-is-ideation-and-how-to-prepare-for-ideation-sessions (last accessed 13 November 2018).

[168] TRL1: basic principles observed; TRL2: technology concept formulated; see https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf (last accessed 13 November 2018).

this, but one also needs to demonstrate that the robot is not able to move at a speed that, for instance, is higher than 4 mph.

Given that robots do not only capture a software architecture but will consist of a physical part as well, development methodologies are needed that are able to cover both the intricacies of software development processes and the constraints and limitations posed by physical systems[169].

As showed by interviews, at this stage tests are mostly performed in laboratories or within the premises of the producers and their contractual partners, and use models that mimic the behaviour of the robot[170]. These models need to reflect both the software architecture in place and the physical components (sensors and actuators, moving parts) guided by and influencing the instructions of the system. Furthermore, the models themselves must be fully compatible with the functioning of the cyber-physical system, which is a far from trivial challenge. Coping with this challenge has attracted the attention of a large group of scientists[171]. The interaction patterns between physical components – such as sensors and actuators – and the underlying software is complex, and may lead to instabilities and fragility in the solutions of specific movements[172].

Methods in use to test these functionalities range from simulation experiments in which typical behaviour is simulated through digitally equivalent systems (so-called digital twins[173]) to using benchmarks and modelling studies. Each of these methods has its benefits and pitfalls, having to deal with the peculiarities of testing the behaviour of software systems and the corresponding behaviour of the physical components that are providing input to the software systems (by sensors) and that are receiving output to perform a specific action (by the actuators). One method that has gained prominence in recent years is using a so-called digital twin. A digital twin is – as is indicated by the name – the digital variant of a cyber-physical system. The digital twin has the relevant features of the cyber-physical system that need to be tested. By using the digital twin, expensive remodeling of physical components can be prevented at a stage when design choices still have to be made. The digital twin however, faces the same problems, which are already known from simulation models: physical features are not always easy to model in a algorithmic process, given the existence of multiple equilibrium solutions and non-deterministic equations[174].

Mathematical modelling comes close to algorithmic simulations but restricts itself to describing the behaviour of the cyber-physical system as a set of mathematical (differential)

---

[169] See E.A. Lee, *Cyber Physical Systems: Design Challenges*, *IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)* (2008). See also T. Sanislav and L. Micla, "Cyber-Physical Systems – Concepts, Challenges and Research Areas," *Control Engineering and Applied Informatics* 14, no. 2 (2012).

[170] See S.K Khaitan and J.D. McCallen, "Design Techniques and Applications of Cyberphysical Systems: A Survey," *IEEE Systems Journal* 9, no. 2 (2015). They distinguish between various classes of models that have been developed in recent years. These models run from meta-models to formal semantic approaches such as denotational, axiomatic, operational, or a hybrid of these, multi-agent semantic models, event-based semantic models and actor-oriented design models, to computational models based upon continuous time, finite state machines, discrete events, and process networks. For each of these approaches Khaitan and McCalley present a number of examples and analyse the advantages and the disadvantages of the approach.

[171] The societal relevance of these activities has attracted the attention of the European Commission as well. In recent years, various networks of robotics researchers have been created and supported. See for instance the ECHORD/ECHORD++ network (https:// http://echord.eu/; last accessed October 24, 2018). This network brings together seven relevant European players in the robotics market It presents itself as the European Coordination Hub for Open Robotics Research.

[172] See the previously quoted work on antifragility by Taleb. See, for a presentation on ill-defined and undefined solutions for mobile robotics, Gregory Dudek and Michael Jenkin, *Computational Principles of Mobile Robotics'* (New York: Cambridge University Press, 2010).

[173] M. Schlusse and J. Rossmann, *From Simulation to Experimentable Digital Twins: Simulation-Based Development and Operation of Complex Technical Systems*, *IEEE International Symposium on Systems Engineering (ISSE)* (2016). See also E. Negri, L. Fumagalli, and Macchi. M., "A Review of the Roles of Digital Twins in Cps-Based Production Systems," *Procedia Manufacturing*, no. 11 (2017).

[174] See footnotes 172 and 173.

equations. Similar problems to solving stability issues and multiple equilibrium solutions as with digital twins are present in mathematical modelling. The advantage of using a mathematical model is that it enables the exploration of unstable behaviour or the presence of so-called anomalies (unforeseen or unpredictable situations)[175]. Benchmarks enable comparing specific features against a proven set of already acquired results. These results can be a set of functions that have proven to be correct or a specific dataset[176]. Benchmarks enable comparing the profiles of specific systems, for instance their profile against preventing unwanted data intrusions[177]. Constructing a trustworthy benchmark instrument is a costly undertaking which may take considerable time to realize. The very moment the benchmark is constructed it may be extended and improved with follow-up results of experiments and tests that are done using the benchmark. The benchmark may become more robust and valuable over the years, as long as the techniques that need to be tested fulfil requirements that meet the features of the benchmarking tool.

The reliance on mathematical modelling and simulation has been substantially increasing over the last twenty years. This is shown both by interviews and desk research[178], and can also be exemplified by the substantial shift in attention that such techniques have been receiving in engineering literature.

A brief exploration of one scientific journal that enables tracing articles on the basis of keywords per year yields the following results:

Table 15: Prevalence of articles on the basis of single keywords in selected periods.

Period/Keyword	Test	Simulation	Benchmark	Mathematical modelling
2000-2004	166	134	5	38
2005-2009	211	176	20	58
2010-2014	191	153	27	50
2015-2018	339	276	68	82

Source: Autonomous Robots (https://link.springer.com/journal/10514)

The table, although only meant for indicative purposes, highlights some interesting topics. The presence of articles that have at least one of the keywords increases over time. While the first – «testing» – may be considered to be a rather generic keyword, the other three– «simulation», «benchmark» and «mathematical modelling» – point at more specific methods of testing. Each method shows an increase in prominence. Simulation and mathematical modelling have more than doubled over the past fifteen years (even more so when realizing that the last period only covers slightly less than four years while the others cover five years; date of search being 24 October 2018; the last journals of 2018 are not included). The awareness for benchmarking as a tool has substantially increased, being close to absent in

[175] See https://www.quora.com/What-are-the-benefits-of-using-mathematical-models (last accessed 13 November 2018).
[176] M. Jamil and Yang X-S., "A Literature Survey for Benchmark Functions for Global Optimization Problems," *Int. Journal of Mathematical Modelling and Numerical Optimisation* 4, no. 2 (2013), http://dx.doi.org/DOI: 10.1504/IJMMNO.2013.055204. See also A. Shiravi et al., "Toward Developing a Systematic Approach to Generate Benchmark Datasets for Intrusion Detection," *Computers & Security* 31, no. 3 (2013), http://dx.doi.org/https://doi.org/10.1016/j.cose.2011.12.012.
[177] See Shiravi et al.
[178] Ibid.

the initial period (2000-2004) and increasing to the same level of presence as mathematical modelling [179].

This demonstrates the increased usefulness of these testing techniques. This usefulness can be attributed to two main features of these testing techniques: they are less costly than constructing a real prototype and they are easily adaptable to new features that need to be tested.

Product development stage. The second phase consists in the actual development of new or updated components which will be assembled to create the designed product.

At this stage, an encompassing system directed at testing the functionalities of these components/systems will be put in place. Each component needs to be subject to a «bench test», i.e. a test aiming to check that each individual element fulfils the functional and technical specifications formulated in the design phase.

Product development is related to achieving technical readiness levels from 3 till 5: experimental proof of design, technology validated in lab, and technology validated in real-life environment. The test protocols in use to test components and subsystems of the product to be developed are essentially similar to the ones used in the previous phase. While in the experimentation and design phase many development activities may be executed by using digital equivalents (digital twins and simulation models), in this stage components will be tested on their physical features. Physical behaviour of (components of) industrial robots will be tested against safety standards that emanate from ISO standards.

Interviews also showed that, in this phase, testing is driven by market trends – as long as they are relevant for the specific components or (sub-)systems under development –, by standards set for the reliance assessment (§2.5.4), as well as by in-house requirements, which businesses set to affirm their products' identity and quality.

Again, in this phase, testing is still performed in the manufacturer's premises, or – whenever needed – in laboratories.

Manufacturing stage. In the manufacturing stage, individual components are assembled to create the designed products.

In this phase further «quality testing» is required to ensure that the products conform to the required specifications, and meet the expectations of the customers. Here, all the individual functionalities are again tested, starting from assemblies, all the way to the finished product, and performance indicators are used as assessment benchmarks.

Testing of components of the robotic system is done by manufacturers. Testing of, for instance, data governance related to the robotic systems (communication with software that controls the robots, or communication with other robots using digital communication protocols such as Bluetooth, Wifi, Zigbee and – in the future – 5G) can be done in house as well, as long as no dependencies are built in from systems that may influence settings of parameters of the robots. Creating the product means gluing together the various components, and checking the mutual interaction of the components on each other. Quality assurance tests are performed in order to guarantee the proper function of the robotic system[180]. New features have to be involved in these testing procedures.

In case of passive exoskeletons for back support in the workplace, for example, this means involving users, possibly replicating real-life scenarios, in order to measure the outcome of

[179] A topical analysis might help understanding in depth the change over time in terms of tools and techniques used. This is however, out of scope for this study.

[180] J. Laval, L. Fabresse, and N. Bouraqadi, *A Methodology for Testing Mobile Autonomous Robots.*, *IEEE/RSJ International Conference on Intelligent Robots and Systems* (2013).

the models, torques, electromyography data about the pression of the back, etc., and thus evaluate the subjective experience of the test-users (e.g. through questionnaires).

At his stage, testing is usually performed within the premises of either the manufacturer, the SI, or the customer. As anticipated above (§2.5.2), exoskeletons might be tested in clinics and hospital, in light of their peculiar nature.

Final Stage. The stage before the robot will be put in the market will essentially bring together the various testing situations that have been used in the previous phases as well. Having thoroughly tested the various components of the industrial robots including the interdependencies of the components and the way they influence the functioning of each other (for instance by hand over of data arising from sensors, meant for actuating other components) in the product development stage and the manufacturing stage, the final testing will be dedicated to proving the system meets quality criteria as indicated in the functional requirements and as induced by international standards.

These quality criteria will most likely be the same that will be required for obtaining certification.

2.5.4. Identification of risks through testing and risk assessment

Assessment of acknowledged risks. The methods of testing described above refer to the ability to understand the behaviour of the machine produced and to determine whether it functions as prescribed by its functional requirements. Manufacturers use testing to determine the limits of the robotic machineries, to identify the potential hazards involved in their production and use, and to estimate the risks of the hazards thus identified. Through such analysis and evaluation, manufacturers can develop the necessary solutions to reduce such hazards and the likelihood of their occurrence, and further increase the robots' safety and security.

Standards. Specific requirements posed by (harmonized) standards not only serve the purpose of demonstrating compliance with applicable legislation – as it will be further analyzed in §2.6.2 – but they also offer guidance on how to design and implement functional specifications (e.g. the reach of a cobot arm manipulator), and constitute a benchmark against which performance and reliance testing shall be performed. Indeed, the number of relevant standards to incorporate in the design process of an industrial robot (be it a cobot, a mobile robot or an exoskeleton) is rather high. The official website of DG Growth mentions a large number of standards that a manufacturer might need to be aware of when intending to put a machinery on the market [181] The table below offers a brief overview, which is not intended to be exhaustive, of the main standards available for dealing with safety aspects of industrial robots.

[181] See http://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/machinery/ (last accessed 25 October 2018). Standards are differentiated in A-standards (only one, specifying basic concepts, terminology and design principles applying to all categories of machinery), B-standards (a quick scan counted 62 different standards that might need to be taken care of) and C-standards (a quick scan arrived at more than 500 different instantiations of standards that can help to demonstrate compliance – with many instantiations referring to the same standard – differentiating in part 1, part 2, etc.).

Table 16: Standards relevant for validation testing.

Standard	Description
ISO 8373:2012. Robots and robotic devices – Vocabulary	ISO 8373:2012 defines terms used in relation with robots and robotic devices operating in both industrial and non-industrial environments.
ISO/TR 13309:1995. Manipulating industrial robots -- Informative guide on test equipment and metrology methods of operation for robot performance evaluation in accordance with ISO 9283	ISO/TR 13309:1995 supplies information on the state-of-the-art of test equipment operating principles. Additional information is provided that describes the applications of current test equipment technology to ISO 9283.
ISO/TR 20218-1:2018. Robotics -- Safety design for industrial robot systems -- Part 1: End-effectors	This document provides guidance on safety measures for the design and integration of end-effectors used for robot systems. The integration includes the following: — the manufacturing, design and integration of end-effectors; — the necessary information for use. This document provides additional safety guidance on the integration of robot systems, as described in ISO 10218-2:2011.
ISO/TR 20218-2:2017. Robotics -- Safety design for industrial robot systems -- Part 2: Manual load/unload stations	ISO/TR 20218-2:2017 is applicable to robot systems for manual load/unload applications in which a hazard zone is safeguarded by preventing access to it. For this type of application, it is important to consider the need for both access restrictions to hazard zones and for ergonomically suitable work places. ISO/TR 20218-2:2017 supplements ISO 10218-2:2011 and provides additional information and guidance on reducing the risk of intrusion into the hazard zones in the design and safeguarding of manual load/unload installations.
ISO/TS 15066:2016. Robots and robotic devices -- Collaborative robots	ISO/TS 15066:2016 specifies safety requirements for collaborative industrial robot systems and the work environment, and supplements the requirements and guidance on collaborative industrial robot operation given in ISO 10218-1 and ISO 10218-2.

	ISO/TS 15066:2016 applies to industrial robot systems as described in ISO 10218-1 and ISO 10218-2. It does not apply to non-industrial robots, although the safety principles presented can be useful to other areas of robotics.
ISO 9409-1:2004. Manipulating industrial robots -- Mechanical interfaces -- Part 1: Plates	ISO 9409-1:2004 defines the main dimensions, designation and marking for a circular plate as mechanical interface. It is intended to ensure the exchangeability and to keep the orientation of hand-mounted end effectors. It does not define other requirements of the end effector coupling device. It does not contain any correlation of load-carrying ranges, as it is expected that the appropriate interface is selected depending on the application and the load-carrying capacity of the robot.
ISO 9409-2:2002. Manipulating industrial robots -- Mechanical interfaces -- Part 2: Shafts	ISO 9409-2:2002 defines the main dimensions, designation and marking for a shaft with cylindrical projection as mechanical interface. It is intended to ensure the exchangeability and to keep the orientation of hand-mounted end effectors. The mechanical interfaces specified in ISO 9409-2:2002 will also find application in simple handling systems which are not covered by the definition of manipulating industrial robots, such as pick-and-place or master-slave units.
ISO 9946:1999 Manipulating industrial robots -- Presentation of characteristics	No description is provided.
ISO 11593:1996. Manipulating industrial robots -- Automatic end effector exchange systems -- Vocabulary and presentation of characteristics	Defines terms relevant to automatic end effector exchange systems used for manipulating industrial robots. The terms are presented by their symbol, unit, definition and description. The definition includes references to existing standards.
ISO 14539:2000. Manipulating industrial robots -- Object handling with grasp-type grippers -- Vocabulary and presentation of characteristics	No description is provided.
ISO 18646-1:2016. Robotics -- Performance criteria and related test	ISO 18646-1:2016 describes methods for specifying and evaluating the locomotion

methods for service robots -- Part 1: Locomotion for wheeled robots	performance of wheeled robots in indoor environments.
ISO/AWI 18646-4. Robotics -- Performance criteria and related test methods for service robots -- Part 4: Wearable robots	No description is provided. Standard is under development.
ISO 19649:2017. Mobile robots -- Vocabulary	ISO 19649:2017 defines terms relating to mobile robots that travel on a solid surface and that operate in both industrial robot and service robot applications. It defines terms used for describing mobility, locomotion and other topics relating to the navigation of mobile robots.
IEC 61508:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems	IEC 61508 series features Part 1: General requirements, Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems, Part 3: Software requirements, Part 4: Definitions and abbreviations, Part 5: Examples of methods for the determination of safety integrity levels, Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3, Part 7: Overview of techniques and measures.
ISO 9787:2013. Robots and robotic devices -- Coordinate systems and motion nomenclatures	ISO 9787:2013 defines and specifies robot coordinate systems. It also provides nomenclature, including notations, for the basic robot motions. It is intended to aid in robot alignment, testing, and programming. ISO 9787:2013 applies to all robots and robotic devices as defined in ISO 8373.
IEC TR 60601-4-1:2017 Medical electrical equipment - Part 4-1: Guidance and interpretation - Medical electrical equipment and medical electrical systems employing a degree of autonomy	IEC TR 60601-4-1:2017(E) is intended to help a manufacturer through the key decisions and steps to be taken to perform a detailed risk management and usability engineering processes for medical electrical equipment or a medical electrical system, hereafter referred to as MEE or MES, employing a degree of autonomy (DOA). This document provides a definition of DOA of MEE or MES and a medical robot, and also provides guidance on: - methodologies to perform the risk management process and usability engineering for an MEE or MES with a DOA;

	- considerations of basic safety and essential performance for an MEE and MES with a DOA; and - identifying the use of DOA, and similar concepts in existing ISO/IEC standards dealing with MEE or MES with the goal to facilitate alignment of standards by consistent use of the concept of DOA; and - distinguishing between medical robots, and other MEE and MES. Unless specified otherwise, this document considers MEE and MES together. The manufacturer of an MEE or MES with a DOA is expected to design and manufacture an MEE or MES that fulfils its intended use and does not have unacceptable risk throughout its life-cycle. This document provides guidance to help the manufacturer in complying with the requirements of IEC 60601-1:2005 and IEC 60601-1:2005/AMD1:2012 for MEE and MES with DOA. The document is also intended as guidance for future standard writers.

Source: www.iso.org, www.iec.ch and the Standard Organizations' official websites

Further analysis of the said prescription on the relationships between the legislative framework and the (harmonized or not harmonized) standards will be made (§2.6). However, it is important to point out that such requirements do not comprehensively provide exact indications on how testing shall be performed; also, they tend to be very broad, and were adopted with less-advanced technological applications in mind. Hence, precautions against such risks might not be sufficient in the light of the duty to manufacture and market safe products.

Assessment of novel risks. Therefore, manufacturers (and subjects assimilated to them such as SIs) have a duty to identify risks that may be unknown at the time of defining the functional requirements but that may impact upon the functioning of the device. An example is the risk that a robot is hacked and that the software that steers the actuators of the robots is manipulated[182]. These risks are hard to define in extenso at the design stage (they may

[182] C. Cerrudo and L. Apa, *Hacking Robots before Skynet* (IOACTIVE, 2017), https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf (last access 25.10.2018). The authors identify potential security issues when robots will be hacked. Concerning IRs, they observe that hacking of industrial robots belong to «one of the most dangerous scenarios, as industrial robots are usually larger, more powerful, and programmed to make precise movements and actions. A hacked industrial robot could easily become a lethal weapon.» (page 13). Notwithstanding that the authors have a clear interest in matters related to securing robots (the paper produced has been published as a white paper of the organization of which they are CTO respectively Senior Security Consultant), their concern should be taken seriously.

partly belong to the so-called «unknown unknowns»[183]) but need to be taken into account in testing, since they may impact the proper functioning of the robotic system[184].

Thus, on the basis of the presented functionalities of any kind of machinery in the current standardization documents, additional risks need to be identified and subsequently integrated in these safety testing procedures. This is particularly relevant for Industry 4.0 robotics, as some of their peculiar features bring about new risks that are particularly difficult to evaluate. Although the specific configuration of the risks, as well as of the precautionary safety measures which should be adopted, will differ between depending on the type of robot and of the working environment, some fundamental and common risks may be identified.

Three major hypotheses, which are strictly intertwined with one another, and need to be taken into account are[185]:

- *Machine-learning risks*;
- *Cybersecurity risks*;
- *Working environment-related risks.*

Machine learning risks. Machine learning (henceforth, ML) is a field of artificial intelligence that studies and constructs algorithms allowing computer systems to «learn» (e.g., progressively improve performance on a specific task), by giving them the ability to acquire and make prediction from data, through instruments of (structured or unstructured) data mining[186], computational statistics[187] and mathematical modelling[188], without necessarily being explicitly programmed for executing the said task, but rather being able to develop itself over time[189]. This latter feature relates to whether the approach falls under supervised learning, unsupervised learning or semi-supervised learning[190]. Supervised learning means that an algorithm is trained on executing its task by using a training data set of which it is known what it consists of. An example is facial recognition. By feeding a machine learning algorithm a data set of many (thousands of) faces, the system will optimize its learning strategy in order to be able to recognize appropriate features of the faces it has been offered. In the end, the system may be able to differentiate a face from another object, and may also be able to recognize a typical face from a data set[191]. In an unsupervised learning situation, the algorithm creates its own set of decision rules by randomly checking for similarities in the data set it is offered. It creates an ontology and decision rules that help categorizing and identifying new objects offered[192]. Unsupervised learning enables clustering

---

[183] An unknown unknown is a circumstance that not only is obscure with respect to its nature, characteristics and potential consequences, but that is also not perceived or identified as a relevant issue overall, mostly because it relates to implications of advanced technologies which cannot be foreseen at the present stage.

[184] A. Sutcliffe and P. Sawyer, *Requirements Elicitation: Towards the Unknown Unknowns*, *21st IEEE International Requirements Engineering Conference* (2013).

[185] Anne Jansen et al., *Opkomende Risico's Voor Arbeidsveiligheid: Werken in Dezelfde Ruimte Als Een Cobot ('Emerging Risks for Safety at Work: Working in the Same Space as a Cobot').* (TNO, 2017).

[186] Tim Menzies, "Beyond Data Mining," *IEEE Software,* 30, no. 3 (2013).

[187] Austen C. Duffy, "Where Do Computational Mathematics and Computational Statistics Converge? ," *Wiley Interdisciplinary Reviews: Computational Statistics* 6, no. 5 (2014).

[188] Frank Hickman, "Application of A.I. Techniques to Formulation in Mathematical Modelling " *Mathematical Modelling* 8 (1987).

[189] See A. Samuel, "Some Studies in Machine Learning Using the Game of Checkers," *IBM Journal of Research and Development* 3, no. 3 (1959).

[190] https://www.techemergence.com/what-is-machine-learning/ (last accessed 13 November 2018).

[191] This recognition may produce results that are highly questionable from an ethical perspective. See for instance https://www.forbes.com/sites/mzhang/2015/07/01/google-photos-tags-two-african-americans-as-gorillas-through-facial-recognition-software/#b6dc939713d8. A facial recognition programme in use by Google mistakenly tagged two African-Americans as gorilla. The features of the two African-Americans apparently were quite similar to the features with which the algorithm was trained to recognize gorillas.

[192] https://towardsdatascience.com/unsupervised-learning-with-python-173c51dc7f03 (last accessed 13 November 2018).

of data and distilling patterns from these data. Semi-supervised learning is a hybrid form of both approaches.

Helping robots to predict what they should do given a specific input can be optimized by using either a supervised learning model or an unsupervised one. When a robot needs to recognize typical features and categorize objects, it can be done by unsupervised learning. Overall, for specific situations, training sets will be used that enable scoping the problem and making sure the robot performs as expected. Problems in the functioning of the robot may arise from flaws in any of the capacities that are embedded in the robotic system (perception, recognition, prediction, decision, interaction, and feedback).

Since a ML-based robot progressively improves its performance on a specific task by continuously optimizing the strategy it uses to execute its tasks, the risks of having unpredicted and unpredictable behaviour depends on a variety of issues, namely[193]:

- *Length and completeness of the trials*: ML software will perform differently at the design stage and at runtime. From a testing-related perspective, this means not only that long term trials are needed, but also that it might be difficult to establish the moment when the algorithms might be deemed sufficiently «experienced» to ensure safety. Also, software components can have bugs that only become active at runtime, and which reliance testing cannot account for;
- *Variability of scenarios in which the ML will be required to perform*: even after a long training period, a major shift in the data acquired once the product is released and fully functioning, may determine unexpected behaviors. Indeed, the algorithm may reach incomplete or inadequate solutions because the actual situation encountered differs from the one learned, or because a faster reaction is needed than the one taken into account by the software developers. This creates additional challenges when assessing the reliability of the machine in smart factories, where collaboration between IRs and humans – and even physical interaction between the two – is likely to happen in a loosely-structured working environment. In case of cobots, for example, manufacturers might need to adjust the overall functionalities as to ensure a wider safe zone (i.e. a distance which the cobot is not allowed to pass, in order to avoid collision or physical harm to the operator), and compared to the one identified during tests, or by the relevant standard (ISO 9946-1999), because the unpredictability of the robot's behaviour yields for a precautionary approach in setting safety-related specifications;
- *Quality of data*: if a learning strategy is based on flawed information, this can lead to mistaken behaviour. Training a robot on a data set that itself is not accurate or that contains unreliable, outdated and/or incomplete data, the learning strategy of the robot will be compromised from the beginning. One would expect errors to become visible by wrong decisions made by the robots during the test phase, but when flaws are subtle one can imagine that the resulting decision rules will also only marginally deviate from a desirable outcome. Only over time will this result in behaviour that is clearly outside set boundaries[194].

All these variables may affect the robots' perception and recognition of the environment, consequently affecting its prediction – its ability to assess the impact of its own actions and of actions of other objects (for example, it might be difficult to predict human behaviour). Thus, the safety and efficiency of the human-robot interaction may be put at stake. Indeed, the knowledge representation on which the machine relies may encompass mistakes, due to cybersecurity risks (further explained below); furthermore, the network of IRs and other technological application elements featuring IT, software, sensors, actuators and connectivity, allows such devices to connect and exchange data, creating opportunities for

---

[193] Jansen et al. See esp. p. 18.

[194] https://becominghuman.ai/bad-data-is-ruining-machine-learning-heres-how-to-fix-it-31ae9f4cef3f (last accessed 13 November 2018).

more direct integration between the physical world and computerized systems. Yet, the shared cloud may enable sharing learning strategies, so that when the information is copied into another robot, errors are passed from one application to the other through the cloud.

Furthermore, the effects of a faulty ML-based strategy could be long-lasting, as they also affect the robots' capacity to present a transparent and readable model of its own actions and decisions, which developers and operators normally use as feedback-inputs to correct and further improve the performance of the tasks[195].

If additional testing methods are necessary, they should incorporate the potential flaws, related to these robot capacities. In scientific literature, for example, the development of cyber-physical systems is studied from the perspective of their adaptively and flexibility in exception handling[196]. Being able to respond automatically to changing circumstances presupposes self-organizing and self-adaptive capacities of robotic systems. This should help coping with new and unforeseen situations as well.

Standards relating to machine learning risks. Given the crucial role that novel risks can cause to advanced robotic systems, and the importance of machine learning both as a desirable feature and as a delicate issue from the risk point of view, some authoritative international bodies are carrying out studies and other initiatives on this point. Namely, the ISO/IEC JTC 1/SC 42 group[197] is currently developing ISO/IEC WD 23053, in order to provide a Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML).

As of now, ISO/IEC WD 23053 is being elaborated by the Foundational standards working group (WG1) and is at its 20.20 stage, that is a preparatory stage when the Working draft (WD) study has already been initiated. This WG's broader aim is to build common framework and vocabulary, in order to ease communication among stakeholders coming from diverse backgrounds and foster the pursuit of further work[198]. This working group is developing AI concepts- and terminology-related standard ISO/IEC AWI 22989, as well, and within the same body, Study Group 3 will be in charge of describing applications and use cases using the terminology and concepts defined by these two forthcoming standards.

Cybersecurity risks. Cybersecurity is – in its most basic definition – the practice of defending networks, hardware and software from malicious attacks[199]. Given the breadth of this definition, many perspectives can be distinguished that cover various aspects of cybersecurity threats. Network security, application security and information security more or less relate to the distinction made above. Operational security, disaster recovery and business continuity and end-user education focus on other aspects of cybersecurity that are nonetheless just as relevant as the perspectives focusing on the technology.

The threat that cybersecurity vulnerabilities pose to robotics is mentioned by several authors[200]. Leenes et al. refer to the failing inclusion of cybersecurity threats in, among

---

[195] See footnote 191 and 194.

[196] Y. Zhang et al., "Agent and Cyber-Physical System Based Self-Organising and Self-Adaptive Intelligent Shopfloor," *IEEE Transactions on Industrial Informatics* 13, no. 2 (2017), http://dx.doi.org/DOI: 10.1109/TII.2016.2618892. See also H.-A. Kao et al., "A Cyber-Physical Interface for Automation Systems," *Machines* 3, no. 2 (2015), https://doi.org/10.3390/machines3020093 (last accessed 7 November 2018).

[197] The JTC 1 is a Joint Technical Committee of ISO (International Organization for Standardization) and (International Electrotechnical Commission) and Sub-Committee 42 is indeed focussing on Artificial Intelligence.

[198] For further information, see https://jtc1info.org/technology/artificial-intelligence/, last access November 11th, 2018.

[199] https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (last accessed 13 November 2018).

[200] See C. Cerrudo and L. Apa, *Hacking Robots before Skynet – Technical Appendix* (IOACTIVE, 2017), https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet-Technical-Appendix.pdf (accessed 7 November 2018).

others, the MDD, a failure that according to their analysis is only partially restored by the MDR.[201] Cerrudo and Apa present an analysis of the kind of cybersecurity threats that should be taken into account for robotics[202]. They refer to authentication/authorization issues, insecure transport control protocols, physical attacks, incongruent documentation, jamming or intervening on remote firmware updates and the like.

Cybersecurity risks may be of various kind. They may be caused by malware, hacking, technical and human errors[203].

Cybersecurity risks are associated with flaws in the communication (see item 2, 3, 4 and 5 in the table below), flaws in the software (see item 6 and 7 in the table below) and flaws in the sensors of the robotic system (see item 1). They can be directly experienced through direct contact of the robot with a human being or indirectly, through a robotic action causing an infringement. Testing of robots thus should include testing whether the robots are able to cope with information and network security vulnerabilities.

Table 17: Cybersecurity risks

Risk	Causes
Inaccurate sensor information	• Deliberate manipulation (malware, hackers) • Technical malfunctioning • Human error (configurational errors)
Disrupted communication between sensors and the robots	Various kinds of communication means can be used: Wifi, Zigbee, Bluetooth, LoRa
Blocking of communication channel	• Jamming of frequencies • Denial of service attacks • Overload of channel
Disrupted communication between the robot and the 'home base'	• Disruption of mobile communication • Disruption of fixed connections (e.g. when the robot is connected to a charge station)
Disrupted communication between robots	• Disruption of mobile communication • Compromised cloud services • Denial of service attacks
Manipulated software or instructions	• lack of software updates

See Ronald Leenes et al., "Regulatory Challenges of Robotics: Some Guidelines for Addressing Legal and Ethical Issues," *Law Innovation and Technology* 9 (2017). See also J. McClean et al., *A Preliminary Cyber-Physical Security Assessment of the Robot Operating System (Ros)*, *Proc. SPIE 8741. Unmanned Systems Technology XV* (2013). See also H. Alemzedah and al., *Targeted Attacks on Tele-Operated Surgical Robots: Dynamic Model-Based Detection and Mitigation*, *46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (2016).

[201] Leenes et al. See esp. pp. 38 ff.

[202] Cerruda and Apa.

[203] Wouter Steijn et al., *Opkomende Risico's Voor Arbeidsveiligheid Als Gevolg Van It-Koppelingen Van En Tussen Arbeidsmiddelen (Emerging Risks for Safety at Work Because of It-Coupling from and between Work Machinery)* (TNO, 2016).

	• intrusion in updating facility
Unreliable control center	• Malware, break-in, human error • Incorrect instructions (e.g. putting robot in night-shift mode during the day, or in 'normal' functioning during maintenance)

Standards relating to cybersecurity risks. A way to demonstrate that the robots are able to cope with these vulnerabilities is through compliance with the indicated ISO/IEC standards. Over the past years, ISO network security standards have been added to the already existing stack of security standards. These network security standards include the ISO 27033 package that run from guidelines for the design and implementation of network security (27033-2: 2012), reference network scenarios dealing with threats, design techniques and control scenarios (27023-3: 2010), using security gateways to secure communications between networks (27023-4: 2014), using VPNs to secure communication between networks (27023-5) to securing wireless IP-access (27023:6: 2016). Similarly, information security standards have been constructed. These standards are also a part of the 27000 series, having standards 27000-27011 and 27013-23019 consequentially covering separate sections of information security management (including risk management strategies, information security governance issues and some sector specific standards)[204]. Including these standards in the design process from an early stage onwards (see above) prevents that in the end it will show problematic to abide by the various requirements standards pose. Though requirements can be rather detailed, overall they reflect good engineering practices.

Working environment-related risks. Specific conditions of the IRs working environment may erode the stability of the robotic systems and cause unwanted inference with the IRs' functioning. Desk research showed the following potential impact:

- *Sensor degradation*.[205] Due to degradation of the resolution of a sensor, data acquired through the sensor may become less reliable. When these data are meant to guide an actuator, problems with the accuracy of the actuator may arise. Degradation of a sensor can be caused by unbeneficial environmental circumstances (high radiation, large temperature gradients, atmospheric disturbances)[206].
- *Impact of radiation*. IT components (sensors, chips) are vulnerable in environments with energy intensive radiation. It may lead to malfunctioning of the chips and the sensors.[207]
- *Unstructured or novel working environment*. When a robot is placed in a new environment, it might need to adapt itself to the new situation, depending on the degree of agility of its algorithms. What remains to be seen, is whether the new situation will pose conditions that are outside the parameters for which the robot has been tested. When this occurs, it needs to be signalled[208].

Such risks need to be taken into account during the testing procedures of the quality of subsystems in the robots and can be attributed to the quality assurance that needs to be

[204] See https://en.wikipedia.org/wiki/ISO/IEC_27000-series for an overview.
[205] S. Arosh et al., "Fitness Function Based Sensor Degradation Estimating Using Hoo Filter," *Procedia Computer Science* 58, (2015), http://creativecommons.org/licenses/by-nc-nd/4.0/.
[206] J.P. Oakley and B.L. Satherley, "Improving Image Quality in Poor Visibility Conditions Using a Physical Model for Contrast Degradation," *IEEE Transactions on Image Processing* 7, no. 2 (1998).
[207] F. Faccio and G. Cervelli, "Radiation-Induced Edge Effects in Deep Submicron Cmos Transistors," *IEEE Trans. Nucl. Sci.* 52 (2015), http://dx.doi.org/DOI: 10.1109/TNS.2005.860698.
[208] Jansen et al.

provided by the manufacturer of the sensors. As such, they do not pose new criteria. They may increase the complexity of the testing procedure but some of these risks may be ruled out at beforehand (for instance the impact of radiation).

2.5.5. Bottlenecks and industrial trends

Types of bottlenecks. In general terms, bottlenecks may be classified as either of a technical or regulatory nature. The former is determined by the limits of the technologies available, or by the methodology used in testing, in manufacturing, or in the broader research activities. The latter derive by the lack, or the inadequacy, of the regulatory framework, which creates negative incentives (e.g. prohibiting a testing technique which is fundamental for the process), or fail to give positive incentives to technological development (e.g. not fostering research and innovation).

In the following paragraphs, it will be examined whether technical (§2.5.5.1) and regulatory (§2.5.5.2) challenges hinder testing of IRs, and – if so – they will be briefly sketched, together with the solutions adopted by stakeholders in order to overcome them.

2.5.5.1. Technical challenges

Limited data available and difficult assessment of novel risks. Lengthy, costly and cumbersome testing models are required to gather a sufficient amount of data, which is in turn crucial for evaluating the performance and reliability of the device, and acknowledging novel risks. When ML technology is involved, lack of sufficiently broad, comprehensive, and high-quality data is particularly problematic, as it hinders the necessary trials and learning processes, which the machine needs to acquire before being able to perform its tasks.

Importance of simulation for collaborative robots. The more complex and collaborative IRs are, the more important it is to test them thoroughly before allowing any trial with human operators, as this allows safety from earlier on, and avoids problems connected to testing with humans, especially at initial stages.

Need for a precautionary approach. When dealing with testing of IRs, several new challenges need to be met, relating to the risks posed by Industry 4.0 IRs, and that are absent in less technological advanced devices. The test procedures of machinery are overall strongly focused on physical risks of the functioning of the device in a spatial environment, and are of relevance for ensuring both safety of the robots tested, and the testing procedure *per se*.

Indeed, bringing together tested and validated components into one working system and having this system tested in an unstructured environment outside the self-controlled constraints of a laboratory may bring new vulnerabilities or safety issues to the fore. One of the purposes of testing in a real-life situation is to confront the robot with potentially unforeseen situations in order to check whether the robot is able to cope with these situations. However, this impose further constrains to ensure safety of those performing the test. Also, due to the substantial relevance of unknown unknowns (§2.5.4), testing might not be able to assess and evaluate all risks connected to the use of a robot.

Therefore, it is necessary to adopt precautionary measures to prevent the emergence of the aforementioned risks, such as emergency stop procedures, prevention of reach and speed of a machine, use of materials that prevent physical injuries, and the use of additional

precautionary measures such as cages, curtains, camera's[209], as well as zoning[210] and power limitation[211].

Limited experimental reproducibility and lack of shared benchmarks. Reproducibility of experimental results is crucial for the reliability of the research and, as a consequence, for the credibility and trustworthiness of the product that is tested[212].

However, just as in other domains of science, it is less interesting to repeat an already performed experiment. The publish or perish mentality that determines much of scientific enterprises prevent attention to be paid to work that will not be rewarded just as high as performing original work. Also, and most importantly, repeating already done experiments encounters technical problems, since it will be hard to demonstrate that the evidence produced is decisive (either demonstrating the earlier acquired results are in line with the newly acquired results, or are deviating from the newly acquired results).

In order to stimulate research that is reproducible, researchers express the need for methodologies that enable such reproduction. This is enforced by «good experimental methodologies» that can be used in order to acquire specific quality standards[213]. A European expert group on Good Experimental Methodologies has produced an outline that indicates the conditions for performing an experiment that can be replicated[214]. The work of the expert group has led to a series of conferences that specifically aim at the issue of reproducibility of experimental results. In the past three years four of these workshops have been held, demonstrating the relevance of this approach for the robotics community[215].

2.5.5.2. Regulatory challenges

[209] See IEC 61496-2: 2013 «Safety of machinery - Electro-sensitive protective equipment - Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs)»; IEC6149-3: 2008 «Safety of machinery – Electro-sensitive protective equipment – Part 3: Particular requirements for Active Opto-electronic Protective Devices responsive to Diffuse Reflection (AOPDDR)»; IEC-6149-4-2: 2014: «Safety of machinery – Electro-sensitive protective equipment – Part 4-2: Particular requirements for equipment using vision based protective devices (VBPD) - Additional requirements when using reference pattern techniques (VBPDPP)»; IEC-6149-4-3: 2015: «Safety of machinery – Electro-sensitive protective equipment – Part 4-3: Particular requirements for equipment using vision based protective devices (VBPD) - Additional requirements when using stereo vision techniques (VBPDST)» for specifications of these precautionary measures.

[210] See ISO 13854: 2017: «Safety of machinery - Minimum gaps to avoid crushing of parts of the human body»; ISO 13855: 2010: «Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body»; ISO 13857: 2008 «Safety of machinery – Safety distances to prevent hazard zones being reached by upper and lower limbs».

[211] See ISO 10218-1 (5.10.5); ISO 12100:2010.

[212] See for instance Bram Vanderborght, "On Reproducible Research," *Robotics and Automation*, no. 4 (2018). In his editorial he refers to the so-called R-articles concept. This concept implies that researchers performing a test aimed at reproducing a previously performed experiment publish their findings in a journal paper text, following the guidelines of Good Experimental Methodology, as well as presenting the full data set used, the complete code identifiers and the hardware description of the simulation models. He also stipulates the problem of the publish or perish mentality and calls upon funding agencies to reward researchers willing to spend time to reproduce earlier research.

[213] See Lino Marques, "Good Experimental Methodologies for Mobile Robot Olfaction" (paper presented at the Workshop on Good Experimental Methodology in Robotics, part of the Robotics: Science and Systems Conference2009). See also F. Amigoni and V. Schiaffonati, "Good Experimental Methodologies and Simulation in Autonomous Mobile Robotics," in *Model-Based Reasoning in Science and Technology. Studies in Computational Intelligence*, ed. L. Magnani, W. Carnielli, and C. Pizzi (Berlin, Heidelberg: Springer, 2010).

[214] See http://www.heronrobots.com/EuronGEMSig/downloads/GemSigGuidelinesBeta.pdf. The guidelines consist of a set of eight questions addressing various aspects of a sound methodology: Is it an experimental paper? Are the system assumptions/hypotheses clear? Are the performance criteria spelled out explicitly? What is being measured and how? Do the methods and measurements match the criteria? Is there enough information to reproduce the work? Do the results obtained give a fair and realistic picture of the system being studied? Are the drawn conclusions precise and valid?

[215] Ljubljana, Slovenia, 23 March 2016: Workshop on Recent progress in Research Reproducibility in Robotics: A critical enabler of research exploitation at ERF2016; Singapore, 29 May 2017: Workshop on Reproducible Research in Robotics: Current Status and Road Ahead at ICRA 2017; Tampere, Finland, 13 March 2018: Workshop on Research Reproducibility and Benchmarking in Robotics at ERF 2018; Brisbane, Australia, 21 May 2018: Workshop on Reproducible Research in Robotics: the IEEE Robotics & Automation Magazine R-papers at ICRA 2018.

Lack of regulatory framework does not constitute a bottleneck. During the interviews, few critiques to the lack of regulatory framework were formulated, because it was said to force producers and SI to implement existing standards by developing testing procedures in-house, in uncertain scenarios and with no guarantees. However, the common view is that the present situation does not create any bottlenecks; on the contrary, regulation of testing is perceived as a negative intervention, hindering instead of fostering technological innovation.

The elaboration of more defined functional and safety standards is generally (yet not unanimously) affirmed. For example, interviewees claim that for exoskeletons, EMG data is hard to obtain and unreliable - e.g., it is difficult for example to measure users' fatigue in uncontrolled setting –, and the changing behaviour of the human in the loop further compromises the reliability of tests. In such situations, readily available and standardized benchmarks, requirements, and instruments (such as sensors) are seen as easing testing and making it less time consuming and more reliable.

Major support to SMEs. On the contrary, a series of problems related to the situation of researchers and SMEs has been identified by interviewees. In particular, need for solutions which facilitate sharing of data and benchmarks, offering testing tools and environments and different form of technical and other types of support, is perceived.

In this sense, DIHs are seen as a useful solution. DIHs are present in Europe that focus on testing robotics systems as well. One of these DIHs is specifically oriented at robotics. This ECHORD++ network (European Coordination Hub for Open Robotics Development) is the successor of the ECHORD network. Seven European parties form the key members of the consortium leading this hub. Three laboratory settings have been created that enable researchers to make use of a dedicated infrastructure for testing robotic systems. One of these Robotics Innovation Facilities is established at Bristol Robotics Laboratory, and focuses on Assisted Living and Medical Robotics. Another is situated at Paris-Saclay and focuses on exoskeletons. The third is situated in Pisa-Peccioli, is led by the Sant'Anna School of Advanced Studies and focuses on mobile robotics. Notwithstanding their application-specificity, all three innovation facilities offer a broad array of services to researchers, including legal advice.

2.5.6. Conclusions and recommendations

Definition. Testing consists in the procedures and trials performed during the entire cycle of the product design, development and manufacture, to prove their inherent functionality (performance testing) and safety (reliability testing), and to gather knowledge about their potential risks and failures

Legal framework. There is no EU or national legal framework specifically regulating how testing of IRs should be performed. Indeed, some directives refer to testing as necessary to ensure product safety, and the general obligations related to the health and safety at work apply (GPSD, MD, MDD, MDR, LVD, WED); but do not set a comprehensive framework prescribing when, how, and against which benchmarks experiments shall be performed.

Business-practice and testing techniques. During the entire production cycle, components, subsystems and systems are tested, starting from more computerized solutions (mathematical modelling, simulation) and progressively inserting real-life trials (physical testing).

Risk assessment is based on functional and safety requirements set by international standards. However, machine learning, cybersecurity, and loosely structured work environments may give rise to additional risks which are difficult to foresee and evaluate. The stronger the human-robot interaction, the more precaution should be adopted in order to prevent damages that might be caused by such unknown unknowns.

No need for regulation of testing. However, because testing occurs in controlled environments not accessible to the general public, reference to the employers' obligations to ensure health and safety of the working environment is sufficient for the purpose of making testing safe, while there is no real need to provide detailed regulation ensuring the safety of third parties, or derogating existing and otherwise applicable regulation (as opposed to CADs, see §3.2.6). Moreover, the absence of mandatory rules allows more flexible solutions, which are tailored-made to the peculiarities of different situations, and avoids additional costs.

Therefore, regulation would not improve the safety of current experimentation, but might instead limit more advanced and application-specific approaches, thus hindering, instead of fostering, technological innovation.

Identification of benchmark criteria. The need to identify broadly accepted criteria to measure the performance of IRs – as other robotics application more broadly – suggest the importance of promoting research and favors the adoption of international accepted standards and practices.

Further investment on research and development. DIHs would help facilitating testing for universities and SMEs, as such entities allow them to increase the number and variety of testing solutions, reduces the costs of trials, and also allows the creation of shared tools, techniques, practices and benchmarks, thus indirectly contributing to uniform and further validate testing procedures and techniques.

2.6. Certification

KEY FINDINGS

- According to European product safety legislation, IRs (especially mobile robots and cobots) can be considered machinery, or partly completed machinery, in most of the hypotheses.
- Industrial exoskeletons can be considered machinery, as well as medical devices, and personal protective equipment.
- The framework concerning personal protective equipment and medical devices is gradually shifting from being directive-centered to being regulation-centered, while machinery is still concerned by the Machinery Directive (MD).
- Harmonized standards (hEN) – that is technical norms fostered by the European Commission which yield conformity presumption – exist for both machinery, medical devices and personal protective equipment.
- Nonetheless, relevant hEN for robotic devices exist chiefly as far as machinery is concerned.
- Oftentimes, several subjects are required to undergo conformity assessment procedures for the same device – manufacturers, SI, and business-users –, and certainty could be further improved through ad-hoc interventions to simplify and rationalize such requirements.
- It is not always straightforward for stakeholders to identify the relevant product category for certification purposes when multiple categories are possible: that is the case of exoskeletons.
- More standards, and more narrow tailored ones, could help tackling this issue.
- Public repositories and database of procedures followed to certify IR would function as a valuable resource for subjects involved with advanced industrial robotics certification.

2.6.1. Introduction

***Lack of specifically designed certification procedure for IRs*.** The legal framework regulating IRs certification is complex. Indeed, no legal act has been set to regulate certification of IRs specifically; hence, reference shall be made to the general framework set at the European level. Given that such framework prescribes specific certification procedures for different products, to ascertain which set of rules is concretely applicable to IR, it is necessary to understand under which type of product a particular class of applications could be classified.

It is worth noting that the trend of shifting from directives to regulations for regulating product safety strengthens similarity and uniformity among different MS, thus helping the common market and, more in general, the building of a level playing field.

IRs as «machinery» or «partly completed machinery». Since IRs may be considered «machinery»[216] («an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application»), or «partly completed machinery»[217] («an assembly which is almost machinery but which cannot in itself perform a specific application»), both traditional stationary robots, as well as cobots, mobile robots and exoskeletons fall within the scope of the Machinery Directive (henceforth, MD)[218].

IRs as personal protective equipment. Additionally, industrial exoskeletons may also be considered as «personal protective equipment» (henceforth, PPE)[219] – i.e. «equipment designed and manufactured to be worn or held by a person for protection against one or more risks to that person's health or safety» –, leading them to be certified under the

---

[216] Machinery (proper) is further defined as « (i) an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application, (ii) an assembly referred to in the first indent, missing only the components to connect it on site or to sources of energy and motion, (iii) an assembly referred to in the first and second indents, ready to be installed and able to function as it stands only if mounted on a means of transport, or installed in a building or a structure, (iv) assemblies of machinery referred to in the first, second and third indents or partly completed machinery referred to in point (g) which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole, (v) an assembly of linked parts or components, at least one of which moves and which are joined together, intended for lifting loads and whose only power source is directly applied human effort».

[217] «assembly which is almost machinery but which cannot in itself perform a specific application. A drive system is partly completed machinery. Partly completed machinery is only intended to be incorporated into or assembled with other machinery or other partly completed machinery or equipment, thereby forming machinery».
In a general perspective, industrial robots can be considered as being «machinery» (proper) when thoroughly fitted, and «partly completed machinery» when no specific application can be determined, for instance because no end effector is installed.

[218] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC, in OJ L 157, of June 9th, 2006.

[219] Pursuant to PPED, Art. 1, PPE is any «device or appliance designed to be worn or held by an individual for protection against one or more health and safety hazards. PPE shall also cover : (a) a unit constituted by several devices or appliances which have been integrally combined by the manufacturer for the protection of an individual against one or more potentially simultaneous risks; (b) a protective device or appliance combined, separably or inseparably, with personal non-protective equipment worn or held by an individual for the execution of a specific activity; (c) interchangeable PPE components which are essential to its satisfactory functioning and used exclusively for such equipment».
Pursuant to PPER, Art. 3, PPE means: «(a) equipment designed and manufactured to be worn or held by a person for protection against one or more risks to that person's health or safety; (b) interchangeable components for equipment referred to in point (a) which are essential for its protective function; (c) connexion systems for equipment referred to in point (a) that are not held or worn by a person, that are designed to connect that equipment to an external device or to a reliable anchorage point, that are not designed to be permanently fixed and that do not require fastening works before use».

Personal Protective Equipment Directive, or the Regulation repealing it (henceforth, respectively, PPED and PPER).

IRs as medical devices. To a more theoretical extent, it is here suggested that industrial exoskeletons may also be classified as «medical devices»[220], i.e. as an

> «instrument, apparatus, appliance, material or other article […] intended by the manufacturer to be used for human beings for the purpose of: — diagnosis, prevention, monitoring, treatment or alleviation of disease, — diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap, — investigation, replacement or modification of the anatomy or of a physiological process […]»[221].

In particular, this may happen in two different scenarios: (i) when a worker with injuries or disabilities uses an exoskeleton specifically designed to be worn at the workplace, to facilitate him in performing his duties; (ii) when the exoskeletons is used not to enhance the worker's capabilities – e.g. allowing him to lift weight that he would not possibly lift otherwise – but to prevent an injury or an illness caused by the stress and fatigue connected to repetitive tasks[222]. In these cases, the exoskeleton may be considered as developed, respectively, for the «treatment, alleviation of or compensation for an injury or handicap», and the «prevention, … of disease», hence qualifying as a medical device.

It is worth stressing that such scenarios are currently very unlikely to happen, because referred to a relative small group of workers and to a type of exoskeletons that has not yet reached a significant level of development. However, we believe that the very theoretical possibility of interpreting the notion of medical device as encompassing industrial exoskeletons is worth being discussed, even if this may lead to excluding, at the current state of art, that certification shall be pursued according to the Medical Device Directive (henceforth MDD)[223], or the MDR. This not only allows a comprehensive and exhaustive analysis of the legal framework relevant for industrial robotic certification, but also represents a sign of possible confusion for manufacturers and other economic operators seeking to certify their devices, who might find it difficult to classify them (§2.6.4).

Against this background, in the following sections, we will analyze the conformity assessment procedures set out for all the products, i.e. «machinery», «medical device», and «PPE» (§2.6.2.2, §2.6.2.3). Given the fundamental role performed by the MD for the purpose of

---

[220] At a European level, regulatory framework for medical devices is, as of now, provided by both the aforementioned MDD and the Medical Device Regulation: the former is gradually being superseded by the latter.
Pursuant to Art. 1, MDD, «medical device» means any instrument, apparatus, appliance, material or other article, whether used alone or in combination, including the software necessary for its proper application intended by the manufacturer to be used for human beings for the purpose of: — diagnosis, prevention, monitoring, treatment or alleviation of disease, — diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap, — investigation, replacement or modification of the anatomy or of a physiological process, — control of. conception, and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means».
An almost identical definition is provided by Art. 2, MDR, according to which «medical device» means «any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes: — diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, — diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability, — investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, — providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means».
[221] Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC, in OJ L 81, of March 31st, 2016. Council Directive 89/686/EEC of 21 December 1989 on the approximation of the laws of the Member States relating to personal protective equipment, OJ L 399, of December 30th, 1989.
[222] SuitX, a California-based robot company that designs and manufactures both medical and industrial exoskeletons, recently announced the launch of a flexible and modular exoskeletons, that is indeed meant to reduce fatigue connected to specific operation (e.g. squats, for the LegX model).
[223] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, in OJ L 169, of July 12th, 1993.

certification of IRs in general, and in the light of its peculiar legal nature – i.e. being a directive, whereas rules for both medical device and PPE are now set by Regulations – special attention will be given to the tools and requirements set by the MD, as well as its national implementations.

Following such analysis, an overview of the safety requirements set both at the EU and MSs level will be performed, also highlighting what form of tests are required for the purpose of assuring safety and obtaining certification (§2.6.2).

Once that such overall framework will be sufficiently described, we will consider what challenges and bottleneck such rules create and how economic operators adapt to them (§2.6.4), critically considering whether such frameworks proves adequate for the development and marketing of industrial robots, and formulate recommendations for its improvement, when needed (§2.6.5).

***New Framework Approach*.** During the last years, regulation on product safety has been carried out according to the New Framework, which is based on the following principles:

> «(i) Legislative harmonization should be limited to the essential requirements (preferably performance or functional requirements) that products placed on the EU market must meet if they are to benefit from free movement within the EU, (ii) the technical specifications for products meeting the essential requirements set out in legislation should be laid down in harmonized standards which can be applied alongside the legislation, (iii) products manufactured in compliance with harmonized standards benefit from a presumption of conformity with the corresponding essential requirements of the applicable legislation, and, in some cases, the manufacturer may benefit from a simplified conformity assessment procedure (in many instances the manufacturer's declaration of conformity, made more easily acceptable to public authorities by the existence of the product liability legislation), (iv) the application of harmonized or other standards remains voluntary, and the manufacturer can always apply other technical specifications to meet the requirements (but will carry the burden of demonstrating that these technical specifications answer the needs of the essential requirements, more often than not, through a process involving a third party conformity assessment body)»[224].

In 2008, New Approach was further integrated by New Legislative Framework[225], with the aim of improving market surveillance rules, boosting confidence in product assessment and, among other aims, establishing a common legal framework for industrial products.

New Legislative Framework is made up chiefly of three bodies of law, namely a Regulation on accreditation and market surveillance[226], another Regulation on technical rules[227], and a Decision on marketing of products[228].

---

[224] *The "Blue Guide" on the Implementation of Eu Products Rules*. 1.1.3.
[225] https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en, last access August 6th, 2018.
[226] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, in OJ L 218, of August 13th, 2008.
[227] Regulation (EC) No 764/2008 of the European Parliament and of the Council of 9 July 2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision No 3052/95/EC, in OJ L 218, of August 13th, 2008.
[228] Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC, in OJ L 218, of August 13th, 2008.

2.6.2. Legal framework

2.6.2.1. The Machinery Directive framework

Classification and conformity assessment. The MD envisages different procedures, depending both on the type and function of the machinery involved, and on the device compliance with harmonized standards, which are European standards elaborated by a recognized organization, such as CEN, CENELEC or ETSI, after a request from the European Commission. Harmonized standards (henceforth, hEN) are then published on the Official Journal of the European Union.

It has been observed that an European model of standardization has been developed «featuring centralized private associations enjoying public recognition […], elaborating and promulgating standards according to a rather homogenous set of procedures built on the core principles of consensus, openness, and transparency»[229].

Machinery. Differently from medical devices and PPE, machinery is not divided into classes or categories for classification and assessment purposes, but, pursuant to art. 12, MD, procedures vary depending on whether but the machinery under examination falls within the scope of application of Annex IV, MD, which provides a list of 23 device categories to be deemed more dangerous than the others, thus needing to be certified in special ways.

Industrial robots, once fitted with an end effector, belong to the list mentioned in Annex IV if their features and functions are the ones generally mentioned in that list. For instance, pursuant to art. 9, Annex IV, a robotic «press for the cold working of metals, with manual loading and/or unloading, whose movable working parts may have a travel exceeding 6 mm and a speed exceeding 30 mm/s» would belong to that list, while a similar press, whose travel and speed did not exceed the limits set by MD, would fall out of its scope.

On the one hand, if the machinery involved is not mentioned in Annex IV, then manufacture is allowed to certify the machinery through the assessment of conformity with internal checks provided for in Annex VIII.

On the other hand, if the machinery is indeed mentioned in Annex IV, it is necessary to ascertain whether it complies with harmonized standards.

If it is manufactured complying with harmonized standards, and those standards cover all the relevant essential health and safety requirements, the manufacturer is allowed to choose among (a) the procedure for assessment of conformity with internal checks on the manufacture of machinery, provided for in Annex VIII; (b) the EC type-examination procedure provided for in Annex IX, plus the internal checks on the manufacture of machinery provided for in Annex VIII, point 3; (c) the full quality assurance procedure provided for in Annex X.

When the machinery belongs in the list provided at Annex IV, but the aforementioned criteria are not met, the manufacturer is allowed to choose among only two procedures: (b) the EC type-examination procedure provided for in Annex IX, in combination with the internal checks on the manufacture of machinery provided for in Annex VIII, point 3; (c) the full quality assurance procedure provided for in Annex X.

Partly completed machinery. Pursuant to Art. 13, MD, «partly completed machinery» do not need to be certified, but it is sufficient that «(a) the relevant technical documentation described in Annex VII, part B is prepared; (b) assembly instructions described in Annex VI

---

[229] Harm Schepel, *The Constitution of Private Governance. Product Standards in the Regulation of Integrating Markets* (Oxford: Hart, 2005). See esp. p. 101.

are prepared; (c) a declaration of incorporation described in Annex II, part 1, Section B has been drawn up».

Internal checks on the manufacture of machinery – Annex VIII. The procedure of «internal checks on the manufacture of machinery» is described as follows:

> «for each representative type of the series in question, the manufacturer or his authorized representative shall draw up the technical file referred to in Annex VII, part A. The manufacturer must take all measures necessary in order that the manufacturing process ensures compliance of the manufactured machinery with the technical file referred to in Annex VII, part A, and with the requirements of this Directive»[230].

More broadly, internal production control is to be deemed the simplest assessment method, it does not involve a notified body and, pursuant to it, «the manufacturer himself ensures the conformity of the products to the legislative requirements»[231], covering both design and production.

EC type-examination – Annex IX. Pursuant to Annex IX, EC type-examination is defined as

> «the procedure whereby a notified body ascertains and certifies that a representative model of machinery referred to in Annex IV (hereafter named the type) satisfies the provisions of this Directive […] For each type, the application for an EC type-examination shall be submitted by the manufacturer or his authorized representative to a notified body of his choice. The notified body, after having performed the exams and inspections detailed in Annex IX, «shall issue the applicant with an EC type examination certificate».

In a more general way, EC type-examination implies that «a notified body examines the technical design and or the specimen of a type and verifies and attests that it meets the requirements of the legislative instrument that apply to it by issuing an EU-type examination certificate»[232]. Since EC type-examination concerns only design, it needs to be coupled with production control, in order to assess production, too.

Full quality assurance – Annex X. In order to use «full quality assurance»[233], «the manufacturer must operate an approved quality system for design, manufacture, final inspection and testing […] and shall be subject to […] surveillance». The quality system, in particular,

> «must ensure conformity of the machinery with the provisions of this Directive. All the elements, requirements and provisions adopted by the manufacturer must be documented in a systematic and orderly manner, in the form of measures, procedures and written instructions. The documentation on the quality system must permit a uniform interpretation of the procedural and quality measures, such as quality programmes, plans, manuals and records».

Surveillance, indeed, is needed «to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system».

---

[230] Annex VIII, MD.
[231] *The "Blue Guide" on the Implementation of Eu Products Rules*. 5.1.7 A.
[232] Ibid. 5.1.7 B.
[233] Annex V, MD.

Full quality assurance, in a broader sense[234], assesses both design and production and asks the manufacturer to operate a full quality assurance system in order to ensure conformity to legislative requirements, while the notified body assesses the quality system.

The framework related to machinery is complemented by the Rapid Alert System (henceforth, RAPEX)[235], that is applicable to PPE, too, but not to medical devices. This tool «enables quick exchange of information between 31 European countries and the European Commission about dangerous non-food products posing a risk to health and safety of consumers»[236] and its website provides both a weekly report and a search engine that allows the public at large to be informed on dangerous products, belonging to more than thirty categories.

2.6.2.2. The Medical Devices Directive and Regulation

MDD – Classification. All medical devices are divided into four classes – namely Class I, IIa, IIb, and III, pursuant to Art. 9, MDD, in combination with Annex IX, MDD, which classifies medical devices according to several criteria, such as duration of treatment and invasiveness, pursuant to eighteen rules.

Should a MS consider that a decision is needed for classificatory purposes, or should it deem that a device ought to be classified differently from what stated in Annex IX, or that Art. 11 should be derogated, Art. 13, MDD, allows Member States to file a motivated request and the European Commission to take the necessary measures.

Pursuant to Rule 1, Annex IX, MDD, industrial exoskeletons would belong to Class I, since they are non-invasive (that is, they «do not penetrate inside the body, either through a body orifice or through the surface of the body», see definitions 1.2), especially if they are passive (non-powered). Otherwise, pursuant to Rule 9,

> «All active therapeutic devices intended to administer or exchange energy are in Class IIa unless their characteristics are such that they may administer or exchange energy to or from the human body in a potentially hazardous way, taking account of the nature, the density and site of application of the energy, in which case they are in Class IIb».

Therefore, powered industrial exoskeletons, when assessed through the MDD framework, would be considered as belonging to Class IIa or IIb, depending on the potential hazard.

It is noteworthy to point out the lack of literature and case law on the issue, and the fact that a different interpretation of the concept «energy administering» would determine to consider all industrial exoskeletons belonging to Class I.

MDD – Conformity assessment. According to the framework provided by Art. 11, MDD, certification procedures vary according to the class which the device under examination belongs to.

Class III. In the case of devices falling within Class III, other than devices which are custom-made or intended for clinical investigations, the manufacturer shall, in order to affix the CE marking, either: (a) follow the procedure relating to the EC declaration of conformity set out in Annex II (full quality assurance); or (b) follow the procedure relating to the EC type-examination set out in Annex III, coupled with: (i) the procedure relating to the EC

---

[234] *The "Blue Guide" on the Implementation of Eu Products Rules*. 5.1.7 H.
[235] https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/repository/content/pages/rapex/index_en.htm, last access August 7th, 2018.
[236] Ibidem.

verification set out in Annex IV; or (ii) the procedure relating to the EC declaration of conformity set out in Annex V (production quality assurance).

Class IIa. In the case of devices falling within Class IIa, other than devices which are custom-made or intended for clinical investigations, the manufacturer shall, in order to affix the CE marking, follow the procedure relating to the EC declaration of conformity set out in Annex VII, coupled with either: (a) the procedure relating to the EC verification set out in Annex IV; or (b) the procedure relating to the EC declaration of conformity set out in Annex V (production quality assurance); or (c) the procedure relating to the EC declaration of conformity set out in Annex VI (product quality assurance). Instead of applying these procedures, the manufacturer may also follow the procedure referred to in paragraph 3 (a), that is the first procedure mentioned in the following paragraph, sub Class IIb. As a general remark, sometimes New Framework directives and regulations allow to pursue conformity assessment to methods pertaining directly to more complex and/or dangerous device classes, owing to the principle of precaution.

Class IIb. In the case of devices falling within Class IIb, other than devices which are custom-made or intended for clinical investigations, the manufacturer shall, in order to affix the CE marking, either: (a) follow the procedure relating to the EC declaration of conformity set out in Annex II (full quality assurance); in this case, point 4 of Annex II (Examination of the design of the product) is not applicable (consistently with Class IIb being less complex and dangerous than Class III, which requires full quality assurance); or (b) follow the procedure relating to the EC type-examination set out in Annex III, coupled with: (i) the procedure relating to the EC verification set out in Annex IV; or (ii) the procedure relating to the EC declaration of conformity set out in Annex V (production quality assurance); or (iii) the procedure relating to the EC declaration of conformity set out in Annex VI (product quality assurance). […]

Class I. In the case of devices falling within Class I, other than devices which are custom-made or intended for clinical investigations, the manufacturer shall, in order to affix the CE marking, follow the procedure referred to in Annex VII and draw up the EC declaration of conformity required before placing the device on the market. In the case of custom-made devices, the manufacturer shall follow the procedure referred to in Annex VIII and draw up the statement set out in that Annex before placing each device on the market».

Conformity assessment procedures are different for systems and procedure packs, according to which, pursuant to art. 12, MDD, the manufacturer is required to state that «(a) he has verified the mutual compatibility of the devices in accordance with the manufacturers' instructions and has carried out his operations in accordance with these instructions; and (b) he has packaged the system or procedure pack and supplied relevant information to users incorporating relevant instructions from the manufacturers; and (c) the whole activity is subjected to appropriate methods of internal control and inspection».

***EC verification – Annex IV*.** Pursuant to Annex IV, MDD, EC verification involves a notified body and it is «the procedure whereby the manufacturer or his authorized representative established in the Community ensures and declares that the products which have been subject to the procedure set out in Section 4 conform to the type described in the EC type-examination certificate and meet the requirements of this Directive which apply to them».

Product quality assurance – Annex V. Pursuant to Annex V, MDD, in order to carry out EC declaration of conformity via product quality assurance, «the manufacturer must ensure application of the quality system approved for the manufacture of the products concerned and carry out the final inspection, as specified in Section 3, and is subject to the Community surveillance referred to in Section 4».

Production quality assurance – Annex VI. Pursuant to Annex VI, MDD, EC declaration of conformity via production quality assurance involves a notified body and is defined as

«the manufacturer must ensure application of the quality system approved for the final inspection and testing of the product, as specified in Section 3 and must be subject to the surveillance referred to in Section 4».

Declaration of conformity – Annex VII. Annex VII, MDD, describes the EC declaration of conformity as «the procedure whereby the manufacturer or his authorized representative established in the Community who fulfils the obligations imposed by Section 2 and, in the case of products placed on the market in a sterile condition and devices with a measuring function, the obligations imposed by Section 5 ensures and declares that the products concerned meet the provisions of this Directive which apply to them».

Custom-made devices – Annex VIII. Finally, Annex VIII, MDD, mentions that for custom-made devices the following information must be provided «(i) data allowing identification of the device in question, (ii) a statement that the device is intended for exclusive use by a particular patient, together with the name of the patient, (iii) the name of the medical practitioner or other authorized person who made out the prescription and, - where applicable, the name of the clinic concerned, (iv) the particular features of the device as specified in the relevant medical prescription, (v) a statement that the device in question conforms to the essential requirements set out in Annex I and, where applicable, indicating which essential requirements have not been fully met, together with the grounds. After the conformity assessment procedure has been carried out, the manufacturer is required to «inform the competent authorities of the Member State in which he has his registered place of business of the address of the registered place of business and the description of the devices concerned».

The MDD framework doesn't consist only in conformity assessment procedures, but it also states out that information on incidents involving medical devices is to be recorded, as well as inadequacy, malfunctioning, deterioration and recalls[237].

MDR – Classification. Four classes – again Class I, IIa, IIb, and III – are described at art. 51, MDR, in combination with Annex VIII, MDR, which provides twenty-two classifying rules.

Rule I, Annex VIII, MDR, states again that non-invasive devices belong to Class I, while Rule 9, Annex VIII, MDR, follows almost verbatim Rule 9, Annex IX, MDD. On this point, legal and regulatory framework has remained substantially unchanged after MDR entry into effect, and the same doubts on the classification of industrial exoskeletons remain.

MDR – Conformity assessment. Pursuant to the framework provided by MDR, conformity assessment of medical devices is to be carried out according to what follows.

Class III. Manufacturers of class III devices, other than custom-made or investigational devices, shall be subject to a conformity assessment as specified in Annex IX (conformity assessment based on a quality management system and on assessment of technical documentation). Alternatively, the manufacturer may choose to apply a conformity assessment as specified in Annex X (conformity assessment based on type-examination) coupled with a conformity assessment as specified in Annex XI (conformity assessment based on product conformity verification).

Class IIb. Manufacturers of class IIb devices, other than custom-made or investigational devices, shall be subject to a conformity assessment as specified in Chapters I and III of Annex IX, and including an assessment of the technical documentation as specified in Section 4 of that Annex of at least one representative device per generic device group. However, for class IIb implantable devices, except sutures, staples, dental fillings, dental braces, tooth crowns, screws, wedges, plates, wires, pins, clips and connectors, the assessment of the technical documentation as specified in Section 4 of Annex IX shall apply for every device.

---

[237] See art. 10, MD.

Alternatively, the manufacturer may choose to apply a conformity assessment based on type examination as specified in Annex X coupled with a conformity assessment based on product conformity verification as specified in Annex XI.

Where justified in view of well-established technologies, similar to those used in the exempted devices listed in the second subparagraph of paragraph 4 of this Article, being used in other class IIb implantable devices, or where justified in order to protect the health and safety of patients, users or other persons or other aspects of public health, the Commission is empowered to adopt delegated acts in accordance with Article 115 to amend that list by adding other types of class IIb implantable devices to that list or removing devices therefrom.

Class IIa. Manufacturers of class IIa devices, other than custom-made or investigational devices, shall be subject to a conformity assessment as specified in Chapters I and III of Annex IX, and including an assessment of the technical documentation as specified in Section 4 of that Annex of at least one representative device for each category of devices. Alternatively, the manufacturer may choose to draw up the technical documentation set out in Annexes II and III coupled with a conformity assessment as specified in Section 10 or Section 18 of Annex XI. The assessment of the technical documentation shall apply for at least one representative device for each category of devices.

Manufacturers of class I devices, other than custom-made or investigational devices, shall declare the conformity of their products by issuing the EU declaration of conformity referred to in Article 19 after drawing up the technical documentation set out in Annexes II and III. If those devices are placed on the market in sterile condition, have a measuring function or are reusable surgical instruments, the manufacturer shall apply the procedures set out in Chapters I and III of Annex IX, or in Part A of Annex XI.

Conformity assessment based on a quality management system and on assessment of technical documentation – Annex IX. Pursuant to Annex IX, MDR, conformity assessment based on a quality management system and on assessment of technical documentation involves a notified body, which shall audit the quality management system to determine whether it meets the requirements stated in MDR and then examine design, manufacture and performance of the device, as explained by the manufacturer, and carry out tests.

Type-examination – Annex X. Pursuant to Annex X, type-examination is described as a procedure where a notified body «ascertains and certifies that a device, including its technical documentation and relevant life cycle processes and a corresponding representative sample of the device production envisaged, fulfils the relevant provisions of this Regulation».

Conformity assessment based on product conformity – Annex XI. Finally, Annex XI, MDR, describes conformity assessment based on product conformity verification as a procedure divided into production quality assurance and product verification and consists briefly in «to ensure that devices conform to the type for which an EU type-examination certificate has been issued, and that they meet the provisions of this Regulation which apply to them».

Rules concerning assessment of systems and procedure packs are stated at art. 22, MDR, while derogation from conformity assessment procedures and incident reporting are disciplined at artt. 59 and 87, MDR, respectively, according to the same basis as for in MDD.

2.6.2.3. The Personal Protective Equipment Directive and Regulation

PPED – Classification and conformity assessment. In the PPED framework, PPE are to be divided into three categories, namely I, II and III[238], according to their complexity of design, I being the simplest.

Category I – «simple design». The PPE is defined by the exhaustive list at Article 8 (3). For this type of PPE, the manufacturer declares conformity by means of an EC declaration of conformity only.

Category II – neither «simple» nor «complex» design. The PPE is not defined by Article 8 (3) and (4) (a) are subject to an EC type-examination by a notified body and an EC declaration of conformity is then produced;

Category III – «complex design». The PPE defined by the exhaustive list at Article 8 (4) (a) are subjected to EC type-examination (see Article 8 (2)) and to one of the two quality assurance procedures as described at Article 11A and 11B (respectively 'EC' quality control system for the final product and System for ensuring EC quality of production by means of monitoring, both of which involve a notified body.) An EC declaration of conformity is then produced.

Pursuant to PPED framework, industrial exoskeletons would belong to Category II, because the functions they are designed for are neither mentioned under Art. 8 (3) nor under Art. 8 (4) (a).

***PPER – Classification and conformity assessment*.** PPER explicitly mentions the three risk categories at Annex I, according to a pattern similar to PPED.

Certification procedures are divided in accordance with risk category, as per Art. 19, PPER, pursuant to the following model.

Category I: internal production control (module A) set out in Annex IV;

Category II: EU type-examination (module B) set out in Annex V, followed by conformity to type based on internal production control (module C) set out in Annex VI;

Category III: EU type-examination (module B) set out in Annex V, and either of the following: (i) conformity to type based on internal production control plus supervised product checks at random intervals (module C2) set out in Annex VII; (ii) conformity to type based on quality assurance of the production process (module D) set out in Annex VIII.

As far as procedures that have been already mentioned, the definition is unchanged, while in the following section definition shall be provided for the remaining ones.

Module C «covers production and follows module B. Manufacturer must internally control its production in order to ensure product conformity against the EU-type approved under module B»[239].

Module C2 «covers production and follows module B. Manufacturer must internally control its production in order to ensure product conformity against the EU-type approved under

---

[238] *Ppe Guidelines Guide to Application of the Ppe Directive 89/686/Eec* (European Commission, 2017), http://ec.europa.eu/docsroom/documents/25121. 21 ff.
[239] *The "Blue Guide" on the Implementation of Eu Products Rules*. 73.

module B. C + product checks at random intervals tests on specific aspects of the product carried out by a notified body or in-house accredited body»[240].

Module D «covers production and follows module B. The manufacturer operates a production (manufacturing part and inspection of final product) quality assurance system in order to ensure conformity to EU- type. The notified body assesses the quality system»[241].

Pursuant to the PPER framework, industrial exoskeletons should be considered as Category II devices, too, since they fall out of risk category I and risk category III as stated in Annex I, PPER.

2.6.2.4. Other applicable legislative frameworks: The Low Voltage Directive

Transversal bodies of law relevant for the certification of IR. While the overall classification of IRs for the purpose of their certification has been extensively described above, it is however important to highlight that other legislative measures exist, requiring IRs to meet a series of additional and transversal safety and function requirements. Among the latter features the Low Voltage Directive (henceforth LVD)[242] applies.

Low Voltage Directive. The LVD complies with the New Legislative Framework, insofar as it entitles a presumption of conformity on the basis both of harmonized standards, and – even though to a different extent – of international and national standards, as well[243], while essential safety objectives are indeed clarified in Annex I, LVD. The said directive can be deemed relevant for at least some IR devices and systems, since it applies to equipment which functions with an operating voltage between 50 V and 1000 V (if they require alternating current) or between 75 and 1500 V (if they require direct current)[244]. Annex II, LVD, moreover, does not mention IR among equipment outside the scope of this directive.

Recital (9), LVD, endorses a law and economics rationale, according to which the manufacturer is the most suitable subject in charge of performing conformity assessment, because of his deep knowledge of the design and production of the device to be certified. Therefore, differently from the frameworks provided for machinery, medical devices and personal protective equipment, LVD provides only one conformity assessment procedure, namely the internal production control (module A)[245], and no intervention of notified bodies is ever required. The manufacturer is therefore required to prepare technical documentation, including reference to harmonized and non-harmonized standards, then to draw up an EU declaration of conformity and to affix the CE marking accordingly.

2.6.2.5. Contd: Some relevant national experiences

Uniformity of application among MSs. The MD has been transposed fully and consistently in all MSs. No additional, specific national legislation or regulations have been identified. This section provides an insight about a few relevant national experiences and data.

The Netherlands. Presently, the majority of accidents reported to the SZW Work Inspectorate in relation to IR occur because of insufficient guarding and protective measures and mainly during adjusting, correcting malfunctions, maintenance, cleaning and often as a result of lack of knowledge of safety measures and instructions.

---

[240] Ibidem.
[241] Ibidem.
[242] Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits Text with EEA relevance, in OJ L 96, 29.3.2014.
[243] Arts. 12, 13, and 14, LVD.
[244] Art. 1, LVD.
[245] Annex III, LVD.

The United Kingdom. To provide industry with guidance on the applicable safety standards for 'truly collaborative' applications, a «Cobot Working Group» published a 2017 overview with the responsibilities of the suppliers (manufacturer) and the users of collaborative applications, whose guidelines suggest principles (or steps) to be adopted as part of the risk assessment.

Furthermore, a report on «Collision and injury criteria when working with collaborative robots» concluded that «Although the force limits stated in the draft standard […] seem 'on the safe side', issues with conducting research on human tolerance to injury and pain, affect the validity of the available research for determining force tolerance limits». Additionally, the report has noted that organizational and psychological issues need to also be paid close attention, and that frequency of the injuries should also be included as criteria.

2.6.3. Technical requirements and standards

The ISO standards constitute a fondamental tool in the field of certification, as they constitute a way of demonstrating conformity with required assessment criteria to obtain certification. Indeed, tests performed to assess the product safety need to be assessed against such fundamental benchmarks.

A number of directives related to the development and use of IR explicitly refer to compliance to specific ISO standards. The following table presents the most relevant ones:

Table 18: Overview of European Directives and international standards related to industrial robots and safety requirements

EU Directives	Harmonised standards related to IR	Description
Machinery Directive	EN ISO 12100:2010. Safety of machinery – General principles for design – Risk assessment and risk reduction	ISO 12100:2010 specifies basic terminology, principles and a methodology for achieving safety in the design of machinery. It specifies principles of risk assessment and risk reduction to help designers in achieving this objective. These principles are based on knowledge and experience of the design, use, incidents, accidents and risks associated with machinery. Procedures are described for identifying hazards and estimating and evaluating risks during relevant phases of the machine life cycle, and for the elimination of hazards or sufficient risk reduction. Guidance is given on the documentation and verification of the risk

		assessment and risk reduction process.
	EN ISO 10218-1:2011. Robots and robotic devices - Safety requirements for industrial robots - Part 1: Robots (ISO 10218-1:2011)	ISO 10218-1:2011 specifies requirements and guidelines for the inherent safe design, protective measures and information for use of industrial robots. It describes basic hazards associated with robots and provides requirements to eliminate, or adequately reduce, the risks associated with these hazards. ISO 10218-1:2011 does not apply to non-industrial robots, although the safety principles established in ISO 10218 can be utilized for these other robots.
	EN ISO 10218-2:2011. Robots and robotic devices - Safety requirements for industrial robots - Part 2: Robot systems and integration (ISO 10218-2:2011)	ISO 10218-2:2011 specifies safety requirements for the integration of industrial robots and industrial robot systems as defined in ISO 10218-1, and industrial robot cell(s). The integration includes the following: the design, manufacturing, installation, operation, maintenance and decommissioning of the industrial robot system or cell; necessary information for the design, manufacturing, installation, operation, maintenance and decommissioning of the industrial robot system or cell;

		component devices of the industrial robot system or cell. ISO 10218-2:2011 describes the basic hazards and hazardous situations identified with these systems, and provides requirements to eliminate or adequately reduce the risks associated with these hazards. ISO 10218-2:2011 also specifies requirements for the industrial robot system as part of an integrated manufacturing system. ISO 10218-2:2011 does not deal specifically with hazards associated with processes (e.g. laser radiation, ejected chips, welding smoke). Other standards can be applicable to these process hazards.
	EN ISO 13482:2014. Robots and robotic devices - Safety requirements for personal care robots (ISO 13482:2014)	ISO 13482:2014 specifies requirements and guidelines for the inherently safe design, protective measures, and information for use of personal care robots, in particular the following three types of personal care robots: mobile servant robot; physical assistant robot; person carrier robot. These robots typically perform tasks to improve the quality of life of intended users, irrespective of age or capability. ISO 13482:2014 describes hazards associated with the use of these robots, and provides

		requirements to eliminate, or reduce, the risks associated with these hazards to an acceptable level. ISO 13482:2014 covers human-robot physical contact applications. ISO 13482:2014 presents significant hazards and describes how to deal with them for each personal care robot type. ISO 13482:2014 covers robotic devices used in personal care applications, which are treated as personal care robots. ISO 13482:2014 does not apply to: robots travelling faster than 20 km/h robot toys; water-borne robots and flying robots; industrial robots, which are covered in ISO 10218; robots as medical devices; military or public force application robots.
	ISO 11161:2007. Safety of machinery -- Integrated manufacturing systems -- Basic requirements	ISO 11161:2007 specifies the safety requirements for integrated manufacturing systems (IMS) that incorporate two or more interconnected machines for specific applications, such as component manufacturing or assembly. It gives requirements and recommendations for the

		safe design, safeguarding and information for the use of such IMSs.
	ISO 13849-1:2015. Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design	ISO 13849-1:2015 provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. For these parts of SRP/CS, it specifies characteristics that include the performance level required for carrying out safety functions. It applies to SRP/CS for high demand and continuous mode, regardless of the type of technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc.), for all kinds of machinery.
	ISO 13849-2:2012. Safety of machinery -- Safety-related parts of control systems -- Part 2: Validation	ISO 13849-2:2012 specifies the procedures and conditions to be followed for the validation by analysis and testing of the specified safety functions, the category achieved, and the performance level achieved by the safety-related parts of a control system (SRP/CS) designed in accordance with ISO 13849-1.
Medical device framework	IEC 60601-1-2:2014. Medical electrical equipment - Part 1-2: General requirements for basic safety and essential performance - Collateral Standard: Electromagnetic disturbances - Requirements and tests	IEC 60601-1-2:2014 applies to the basic safety and essential performance of Medical Equipment (ME) equipment and ME systems in the presence of electromagnetic disturbances and to electromagnetic disturbances emitted by me equipment and me systems. This collateral standard to IEC 60601-1 specifies general

		requirements and tests for basic safety and essential performance with regard to electromagnetic disturbances and for electromagnetic emissions of ME equipment and ME systems.
Personal Protective Equipment framework	None found	
Low voltage framework	None found	

Source: www.iso.org www.iec.ch, and the Standard Organizations' official websites.

2.6.4. Bottlenecks and industrial trends

No problems for cobots and mobile robots. Indeed, the consultation with producers of IRs confirmed that the majority of them do not find it difficult to qualify their robots for the purpose of certification, and that they usually certify them as machineries – in particular falling out of the scope of application of Annex IV – or partly completed machineries.

Qualification problems for exoskeletons. On the contrary, qualifying exoskeletons for the purpose of certification is unclear and generally more burdensome. Indeed, these devices may be considered both machinery, personal protective equipment and medical devices, and it is not clear how such complex nature shall be addressed. Should they be considered as medical devices, conformity assessment would necessarily be carried out by external bodies poses, thus, posing a series of difficulties, in particular for SMEs, as self-certification would be precluded. One interviewee in particular pointed out that in the progressive shift from the MDD to the MDR, the delay from MS in choosing notified bodies gives producers very limited time for applying to them. Indeed, notified authorities suffer a work-overload, and businesses (especially SMEs) find it is challenging to find a notified authority accepting new customers.

Certification burden on SI. Interviews also show that – whenever possible – stakeholders l rely on internal certification (a declaration of conformity for partly completed machinery, and a declaration of conformity for complete machinery), which is considered as neither difficult nor expensive.

On the contrary, the other procedures are seen as time-consuming, expensive and resource intensive, although generally appreciated as instruments for ensuring a high level of products' safety and quality. In general, this more complex forms of certifications are sought by SIs, which further modify the device provided by the manufacturer in order to meet the customers' needs and expectations. However, an interviewee pointed out that there is an increased tendency in reliance on external certificates, as the presence of such documents is often required by customers, and is thus need to accommodate the consumer-demand.

Practical realization of standards. Stakeholders rely heavily on standards. Some indeed believe that general standards are the ones allowing more flexibility and foster IRs development, others instead point out that when the practical realization of fundamental standards is unclear – as it was identified for ISO/TS 15066:2016 on specifies safety requirements for collaborative industrial robot systems and the work environment, and for ISO 13855, «Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body –», thus hindering the production. E.g. stakeholders mentioned the difficulties in understanding how big a safety zone should be in order to give

sufficient time for a robot to break to avoid collision with human, or what the maximum range of motion for exoskeletons would be in order to avoid any injury to the human operator wearing it.

However, it was highlighted that, although not preferred as an option, the procedure to obtain certification without reliance on hEN, and even the justification for not conformity with the essential safety requirements, are not excessively burdensome.

Multiple certification. Multiple certification is commonly needed for IRs, for a variety of reasons.

Firstly, in addition to the general certification (as a machinery, a PPE or a medical device), the robot will need to be certified under the specific legislation applicable because of a specific feature; active exoskeletons, for example, may to be certified pursuant to Directive 2014/35/EU related to low-voltage electrical equipment[246].

Secondly, multiple certification is generally sought by businesses working on the international market, in order to comply with the different rules applicable in the various jurisdictions. Indeed, not only business might lack universally applicable standards, but they also may need to adapt to radically different approaches to standard and certification: in Asia, for example, there is no such thing as harmonized standards, which make the compliance with standards only optional.

Lastly, business have to undergo multiple certification in cases of substantial modification to the original product. Most often, it is the very SI – or the machine dealer – that makes the IRs «collaborative», by including the sensors allowing the device to interact with the environment. However, sometimes it is the very business-user who modifies the products, and the latter might not be aware of the need to obtain further certification. Therefore, either because of misinformation, or sometimes because of the inherent costs, some subjects could fail to fulfil their certification duties, and stakeholders suggest simplified procedures.

Given that the certification procedure is costly and time consuming, some stakeholders suggested that certification should be simplified by allowing re-usability of previous certifications, instead of requiring a brand new procedure, or even having a broader approach to standardization, which would make it easier for business (like manufacturers of exoskeletons) to move their product from one application to another, and thus accessing different yet related markets.

Effects of difficult testing on certification. The need for prolonged testing activities, connected to the difficult safety evaluation and the lifetime testing, make time to market (TTM) longer. Moreover, sometimes prior certification is required even for performing the testing trials themselves.

2.6.5. Conclusions and recommendations

Definition. Certification is the procedure a product has to undergo in order to be traded onto the EU market, assuring compliance with the minimum safety requirements put forth by applicable legislation. Such requirements may be met by complying with technical standards, especially if provided with reinforced legal value.

---

[246] Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits, OJ L 96, 29.3.2014, p. 357–374.

Legal framework. According to EU product safety legislation, IR (especially mobile robots and cobots) can be considered machinery in most of the hypotheses, and thus are subject to the procedures and requirements set by the MD.

Industrial exoskeletons can be considered machinery, as well as medical devices (at least in theory, e.g. when used by a disabled worker), and personal protective equipment, and thus may fall within the scope of application of both the MD, the MDD and PPED (and the MDR and PPER repealing them).

The framework concerning personal protective equipment and medical devices is gradually shifting from being directive-centred to being regulation-centred, while machinery is still concerned by the Machinery Directive (MD). However, given the peculiar detailed nature of the MD, no fragmentation among the national implementations of the directive can be found.

Standards. Harmonized standards (hEN) – i.e. technical norms fostered by the European Commission which yield conformity presumption – exist for both machinery, medical devices and personal protective equipment. Nonetheless, relevant hEN for robotic devices exist chiefly as far as machinery is concerned.

No general legislative reform is needed. Despite not specifically adopted for such kind of applications, both desk research and interviews proved that, overall, the legal framework appears sufficiently defined, and thus – for the time being – does not require substantial and overarching modification.

Also, the gradual shift from directives to regulations is welcome, since it simplifies by reducing differences among MSs' variations, thus helping in creating a level playing field.

However, minor regulatory amendments, in combination with the development of standards concerning under-regulated product categories, and the development of tools like best practices and certifying models databases could help, at the same time, building a wider market and enhancing safety level and, therefore, general public confidence in such applications

Need for clarification. When assessing the applicable conformity assessment regulation concerning advanced IRs, one of the main issues is identifying how to evaluate a complex device which features elements belonging to more than one product category. This problem is even more apparent when smaller enterprises are involved: analysis and decision on the conformity assessment procedure would be too costly and burdensome. Indeed, and especially in case of exoskeletons, it is not always straightforward for stakeholders to identify the relevant product category for certification purposes when multiple classifications are possible.

Oftentimes, several subjects are required to undergo conformity assessment procedures for the same device – manufacturers, system integrators, and business users –, and certainty could be further improved through ad-hoc interventions to simplify and rationalize such requirements.

Certification levels. Another major issue is the duty, incumbent on both manufacturers, SI and business users, to pursue certification. Every further relevant adaptation or modification as of now entails another conformity assessment procedure, which is at the same time burdensome, costly and even difficult to ascertain. Therefore, this has a negative effect on compliance, especially as far as business users are concerned. A simplification of the regulatory framework on this specific matter would be, thence, advisable.

Public data bases and repositories. On this matter, the availability of public repositories and databases, featuring previous experiences and cases, would provide valuable help, so that anyone interested in pursuing certification for an advanced device could either find a

consolidated procedure, or, at least, a sound starting point over which elaborate in order to find a certificatory solution.

Cobots, mobile robots: sufficient standards. The study demonstrated that stakeholders heavily rely on the official EU legislative procedures in combination with standard setting as prescribed in standardization organizations such as ISO/CEN/CENELEC. Again, despite not specifically provided for Industry 4.0 robotics, both desk research and interviews showed that there is a high number of standards available, which sufficiently cover the various specifications that businesses need to develop in conformity with essential safety requirements in order to certify their IRs.

Exoskeletons: more standards needed. While this is true for cobots and mobile robots, it is not the case for exoskeletons, given that medical device standards are partly inadequate, and only limited – personal care – standards apply. Therefore, the elaboration of more narrow tailored regulation and standards for non-medical exoskeletons is required.

2.7. Liability

KEY FINDINGS

- IRs are produced and installed by manufacturers and system integrators, purchased by business-users, and operated by workers in factories.
- Thus, the relevant legal framework on liability and insurance of IRs comprises two different bodies of law, concerning, respectively: (i) health and safety of workers, and the relevant insurance schemes; (ii) compensation for damages caused by IRs, under general private law rules.
- The first body of legislation consists of the WFD, a series of further directives and regulations on safety at the workplace, and the national laws implementing them. Under MSs' social systems, workers benefit from compulsory insurance schemes or pensions covering job-related accidents.
- The second body of legislation consists of the PLD, and the national laws implementing it, which display substantial differences among one another. As for other technological devices, the PLD offers insufficient protection to the victim, due to the difficulties in ascertaining and apportioning liability, as well as in proving the defect of the product and the causal nexus between the defect and the damage.
- Interviews showed that manufacturers do not perceive liability as a risk, and believe that compliance with the safety regulation and standards will shield them from being held responsible for accidents involving their robots. This is incorrect.
- Despite the peculiar nature of advanced IRs is widely recognized, interviews pointed out that an insurance market specifically covering such technology has not developed yet.
- The study suggests that, as far as liability is concerned, the current *status quo* is sufficient, since (i) the framework on health and safety of workers, and the related national insurance system, ease the position of the victim, who may benefit from prompt and adequate compensation; (ii) business-users may sue the other subject of the value chain, directly or in recourse, on a contractual basis; (iii) the application of the PLD remains residual, and thus problems which it arises for other technologies have only little practical relevance.
- However, the limited application of the PLD confirms the broader and more general need for its reform.

2.7.1. Introduction

When considering IR, two are the perspectives that need be taken into account, namely (i) accident prevention on the workplace and (ii) liability *per se*.

The different level of analysis: the employers' liability and the manufactures' liability. Indeed, because of the peculiarities of these robotic applications, to be used within an environment which is not open to the general public (the smart factory) and in interaction with specific – and most commonly trained – subjects (the operators and final users), as well as in light of the peculiar legal relationship that bonds business-users and their employees (the employment relationship), a different set of concerns and issues arises, that needs to be dealt with separately (§2.7.2) from more traditional discussion on civil liability (§2.7.3).

Business-users are, in fact, at the same time the purchaser of the technology – entering into a sale and service contract with the other business players here considered, i.e. manufacturers and SIs respectively –, as well as the subjects responsible for the safety of workers on the workplace.

Such an interaction is therefore not only more structured from a technological point of view, but also from a legal one, and allows for a simpler identification of the subject to be held responsible in the first place, substantially easing the position of the claimant. Moreover, considered how the parties theoretically liable are professional agents, ideally provided with sufficient assets, comparable economic and negotiation power, access to information, what otherwise – primarily in other fields of application of the PLD – would raise relevant concerns with respect to the possibility of ensuring access to justice, is here, much more clearly laid out.

The two issues, liability towards employees and manufacturer's liability do therefore intertwine, but most likely to ensure greater protection to the final user – the operator – and not to his detriment. These need to be discussed in detail separately, but also allow to draw some more general conclusions (see §2.7.5).

2.7.2. The European Framework on Health and Safety of Workers at Work

The European framework concerning safety and health of workers is based on a Framework Directive[247] (WFD) and other bodies of law, which will be mentioned in the following sections.

These bodies of law are relevant for the implementation of IRs in manufacturing lines, in particular because they provide duties that rest upon employers, and, albeit to a lesser extent, on workers.

Employers' duties under the WFD. Art. 5, WFD, states that «The employer shall have a duty to ensure the safety and health of workers in every aspect related to the work […]. The workers' obligations in the field of safety and health at work shall not affect the principle of the responsibility of the employer».

More in detail, pursuant to Art. 6, WFD, «the employer shall take the measures necessary for the safety and health protection of workers, including prevention of occupational risks and provision of information and training, as well as provision of the necessary organization and means» and the employer is asked to carry out a risk-management measure, including

> «(a) avoiding risks; (b) evaluating the risks which cannot be avoided; (c) combating the risks at source; (d) adapting the work to the individual, especially as regards the

[247] Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work, in OJ L 183, of June 29th, 1989.

> design of work places, the choice of work equipment and the choice of working and production methods, with a view, in particular, to alleviating monotonous work and work at a predetermined work-rate and to reducing their effect on health; (e) adapting to technical progress; (f) replacing the dangerous by the non-dangerous or the less dangerous; (g) developing a coherent overall prevention policy which covers technology, organization of work, working conditions, social relationships and the influence of factors related to the working environment; (h) giving collective protective measures priority over individual protective measures; (i) giving appropriate instructions to the workers.»

Pursuant to Art. 6, WFD, moreover, «the employer shall […] ensure that the planning and introduction of new technologies are the subject of consultation with the workers and/ or their representatives, as regards the consequences of the choice of equipment, the working conditions and the working environment for the safety and health of workers».

In order to minimize the likelihood of injuries, Art. 12, WFD, focusses on training, imposing on the employer a duty to

> «ensure that each worker receives adequate safety and health training, in particular in the form of information and instructions specific to his workstation or job: (i) on recruitment, (ii) in the event of a transfer or a change of job, (iii) in the event of the introduction of new work equipment or a change in equipment, (iv) in the event of the introduction of any new technology».

Workers' duties under the WFD. On their side, workers, pursuant to Art. 13, WFD, are required to

> «(a) make correct use of machinery, apparatus, tools, dangerous substances, transport equipment and other means of production; (b) make correct use of the personal protective equipment supplied to them and, after use, return it to its proper place; (c) refrain from disconnecting, changing or removing arbitrarily safety devices fitted, e.g. to machinery, apparatus, tools, plant and buildings, and use such safety devices correctly; […]».

Further initiatives. Art. 16, WFD, obliges the Council to adopt further directives on special fields, such as PPE and work equipment, taking into account «(i) the adoption of Directives in the field of technical harmonization and standardization, and/or (ii) technical progress, changes in international regulations or specifications, and new findings», pursuant to Art. 17, WFD.

After WFD, in 1994 the European Agency for Safety and Health at Work (henceforth, EU-OSHA) was established[248], with the aim of awareness raising and prevention, providing risk-assessment tools, studying emerging risks, carrying out analysis and research in the topic of occupational safety and health.

European bodies adopted a wide number of directives – as well as regulations – on the most significant issues related to safety in the workplace.

Broadly speaking, they can be categorized according to the following criterion[249]: (i) Workplaces, equipment, signs, personal protective equipment; (ii) Exposure to chemical agents and chemical safety; (iii) Exposure to physical hazards; (iv); Exposure to biological

[248] https://osha.europa.eu/, last access August 8th, 2018.
[249] https://osha.europa.eu/en/safety-and-health-legislation/european-directives, last access August 8th, 2018.

agents; (v) Provisions on workload, ergonomical and psychosocial risks; (vi) Sector specific and worker related provisions.

When assessing the introduction of advanced IRs in manufacturing lines, bodies of law under (i) come into focus, especially the aforementioned MD[250], PPED, PPER, whose analysis has been carried out in §2.6.2, as well as, to a lesser extent, the work equipment directive[251] (WED), which imposes on employers duties of health protection, inspection and information, and which states minimum requirements – on control, start and stop devices, guards and protections – and the directive on requirements for the workplace[252] (henceforth, DRW), which determines minimum safety requirements, both for workplaces used for the first time[253] and for ones that are already in use[254].

2.7.2.1. Contd.: Some Member States experiences

As far as the sanctions are concerned, they are not regulated at a European level, but at Member State level, which is consistent with contemporary trends in EU law, which still leaves criminal matters to the autonomy of MSs.

Nonetheless, the same principles seem to be at the foundation of most European systems, namely the combination of civil, criminal and administrative liability and a focus shifting from pure repression to a more comprehensive preventive approach, that often involves the design and implementation of organizational models and procedures of risk assessment.

Italy. In Italy, the WFD was transposed by D. Lgs. 19 September 19th, 1994, n. 626, which, after thorough modifications, became the current main body of law related to safety and health of workers, embedded in D. Lgs. April 9th, 2008, n. 81[255], «*in materia di tutela della salute e della sicurezza nei luoghi di lavoro*» («pertaining to health and safety in workplaces») both civil, administrative, and criminal liability are foreseen for all subjects in charge of guaranteeing safety, that is, among others, manufacturers, suppliers, lessors, and employers[256].

More broadly, this body of law is applicable to almost every category of workers, whether in the private or in the public sector, and provides both general dispositions and detail regulations pertaining to workplaces which give rise to specific risks, like quarries, mines and building sites.

It has been questioned in Italian courts whether, in case of poor working condition, a worker is entitled only to pecuniary compensation, as argued by the majority of case law, or indeed to obtain a healthy and safe workplace, which seems more consistent with labor protection law; despite being the preferred solution, the latter is, however, more difficult to implement in practice[257].

---

[250] MD states the liability of the employer.
[251] Directive 2009/104/EC of the European Parliament and of the Council of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work (second individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC), in OJ L 260, of October 3rd, 2009.
[252] Council Directive 89/654/EEC of 30 November 1989 concerning the minimum safety and health requirements for the workplace (first individual directive within the meaning of Article 16 (1) of Directive 89/391/EEC), in OJ L 393, of December 30th, 1989.
[253] Annex I, DRW.
[254] Annex II, DRW.
[255] www.normattiva.it, last access October 6th, 2018.
[256] Irene Scordamaglia, "Malfunzionamento Delle Macchine E Delle Attrezzature Di Lavoro: Le Concorrenti Responsabilità Penali Del Datore Di Lavoro, Del Fabbricante E Del Fornitore," *Cassazione penale*, no. 4 (2014). See esp. pp. 1340 ff.
[257] For an overview, see Oronzo Mazzotta, *Diritto Del Lavoro* (Milan: Giuffrè, 2013). 573-574.

France. After a first phase of difficult adaptation of pre-existing national law[258], the French regulation of safety in workplaces is now provided by Code du travail («Labour code»), which has been extensively amended and modified accordingly[259].

Criminal and administrative liability for employers are now regulated at art. L4741 to L4754, while civil liability is automatic but the amount of the pecuniary compensation is fixed, except for the cases of gross negligence (art. 452-1 and 453-1 of the Social security code). Among the consequences entailed by making workers use dangerous and non-compliant machinery, besides compensation and fines, employers can be condemned to design and enforce a «*plan de securité*» (safety plan) in order to better protect working conditions and reduce the risk of further damages[260].

Moreover, criminal repression of such absence of safety is provided in the French Criminal code («code penal»), namely in the délits of «*atteinte involontaire à la vie et à l'integrité de la personne*» (Art. 221-6, 222-19, 222-20, R625-2 and R625-3), and «*risques causes à autrui*» (art. 223-1).

Spain. The WFD is transposed into Spanish law by means of the Real Decreto n° 396 of 1996, of March 1st, 1996, «por el que se aprueba el Reglamento sobre procedimiento para la imposición de sanciones por infracciones en el orden social»[261]. Among the most recent bodies of law related to this subject, there is the Ley 54 de 12/12/2003, de reforma del marco normativo de la prevención de riesgos laborales[262].

Germany. Germany transposed the WFD with the Gesetz zur Umsetzung der EG-Rahmenrichtlinie Arbeitsschutz und weiterer Arbeitsschutz-Richtlinien[263], adopted on the 7th of August 1996.

It has been noted that prior German regulation on health and safety at work was norm-oriented and technical, while the post-WFD one is organizational goal-oriented, thus impeding a seamless transition[264]. Nonetheless, implementation of the new framework is reportedly[265] strong, and both Land-based and city-based supervisory authorities and accident funds are in charge of surveillance.

It is reported that during the summer of 2015 a 22-year-old worker was trapped and then crashed onto a metal plate by a robotic arm, while operating near a robotic arm in a Volkswagen plant in Germany[266].

United Kingdom. Transposition of WFD in the UK was operated mainly via The Management of Health and Safety at Work Regulations 1992 S.I. n° 2051 of 1992[267], The Workplace

---

[258] Chantal Rivest, "France: From a Minimalist Transposition to a Full Scale Reform of the Ohs System," in *Regulating Health and Safety Management in the European Union*, ed. David Walters (Bruxelles: PIE, 2002). 81 ff.
[259] www.legifrance.gouv.fr, last access October 6th, 2018. Machines are chiefly regulated at art. R4311.
[260] Alain Coeuret, *Droit Pénal Du Travail* (Paris: LexisNexis, 2008). 207 ff.
[261] www.boe.es, last access October 6th, 2018.
[262] http://www.insht.es/InshtWeb/Contenidos/Normativa/TextosLegales/Leyes/2003/54_2003/PDFs/ley542003de12dediciembredereformadelmarconormativodel.pdf, last access October 6th, 2018.
[263] https://www.bgbl.de/xaver/bgbl/start.xav?start=//*%5B@attr_id=%27bgbl196s1246.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl196s1246.pdf%27%5D__1538842321740, last access October 6th, 2018.
[264] Marian Schaapman, "Germany: Occupational Health and Safety Discourse and the Implementation of the Framework Directive," in *Regulating Health and Safety Management in the European Union*, ed. David Walters (Brussels: PIE, 2002). 110 ff.
[265] Ibidem.
[266] https://www.telegraph.co.uk/news/worldnews/europe/germany/11712513/Robot-kills-man-at-Volkswagen-plant-in-Germany.html, last access October 7th, 2018.
[267] http://www.legislation.gov.uk/uksi/1992/2051/contents/made, last access October 6th, 2018.

(Health, Safety and Welfare) Regulations 1992 S.I. n° 3004 of 1992[268], and The Provision and Use of Work Equipment Regulations 1992 S.I. n° 2932 of 1992[269].

Transition from pre-WFD to WFD-transposing regulation is described as non-challenging because the British framework was already oriented towards prevention and process regulation[270].

Sweden. Transposition of the WFD in Sweden was operated through a series of amendment to the by the Swedish Work Environment Authority's regulations on systematic work environment management[271]. The employer's duty to provide a safe and healthy working environment is stated in the Work Environment Act, prescribing that «the employer must take all necessary measures to prevent the employee from being exposed to illness or accidents». The Act and the specifying regulations issued by the Work Environment Authority also emphasize that the employer should comply with their general preventive duties by organizing adequate «Systematic Work Environment Management», i.e. the Swedish implementation of EU's Framework Directive 89/391/EEC. These internal control provisions, as updated in 2001, are by far the most used and cited of all regulations, and safety representatives have a right and duty to monitor and participate in all aspects of the employer's Systematic Work Environment Management.

The Netherlands. In the Netherlands, the employer currently holds the responsibility to ensure that the health and safety of employees is protected with respect to «all employment-related aspects, and to this end shall conduct a policy aimed at achieving the best possible working conditions, taking account of the following factors in the light of the state of the art and professional provision of services».[272] This in essence means that the employer should make sure that all machinery used by employees is safe and complies with all safety regulations. The general civil liability provisions related to safety of the workplace are outlined in Article 7:658 of the Dutch Civil Law.[273] According to the Civil law provisions, the employer is responsible to give instructions and take safety measures to prevent damage (to a reasonable extent) of the employee. In case of a damage, the employer is liable to the employee for the damage suffered, unless the former can show that he has met his obligations or the damage is a result of the intent or deliberate recklessness of the employee[274].

---

[268] http://www.legislation.gov.uk/uksi/1992/3004/contents/made, last access October 6th, 2018.
[269] http://www.legislation.gov.uk/uksi/1992/2932/contents/made, last access October 6th, 2018.
[270] David Walters, "United Kingdom: From a Piecemeal Transposition to a Third Way," in *Regulating Health and Safety Management in the European Union*, ed. David Walters (Brussels: PIE, 2002). 235.
[271] Systematiskt arbetsmiljöarbete: Arbetsmiljöverkets föreskrifter om systematiskt arbetsmiljöarbete, 15/02/2001 AFS 2001:1 av 16/03/2001 (SG(2001)A/10150 du 17/09/2001).
[272] Article 3(1), Act of 18 March 1999, containing provisions to improve working conditions (Working Conditions Act), available at: https://www.arboineuropa.nl/en/legislation/wetgeving-in-het-engels
[273] For a translation as of 2012, see the ILO database here: http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=91671&p_country=NLD&p_classification=01.03
[274] Article 7:658 of the Dutch Civil Law states that (translation obtained from the ILO database) Article 7:658 Care duty of the employer: «- 1. The employer must arrange and maintain the spaces, rooms, machines and tools in which or with which work is performed under his responsibility and give instructions and take safety measures as is reasonably necessary to prevent that the employee suffers damage during the performance of his work.
- 2. The employer is towards the employee liable for damage which the employee has suffered from activities performed in the course of his work, unless he shows that he has complied with the obligations mentioned in paragraph 1 or that the damage to a substantial degree results from an intentional act or omission or from wilful recklessness on the part of the employee.
- 3. It is not possible to derogate to the disadvantage of the employee from paragraph 1 and 2 and from the statutory provisions of Title 6.3 of the Civil Code with regard to the liability of an employer.
- 4. A person who in the course of his professional practice or business enables other persons, with whom he has not concluded an employment agreement, to perform work, is liable towards these other persons in accordance with the previous paragraphs of the present Article for damage which these other persons have suffered from activities performed in the course of that work. The Subdistrict Court has jurisdiction to give a judgment on legal claims as referred to in the first sentence of this paragraph».

2.7.3. Manufacturers' liability: the European framework

IRs as products and subjective scope of application of the PLD. IRs certainly fall under the definition of product for the purposes of the PLD (art. 2, PLD), and therefore the directive applies.

Given the extremely broad definition of producer offered by art. 3, PLD, both the manufacturer, service providers, and the SIs could – under different conditions – fall under that notion, enlarging the number of potentially responsible parties, and consequently the assets that could be aggressed in order to ensure the victim receives compensation.

Indeed, all such parties could often be deemed co-responsible, thence be held jointly and severally liable, when they cooperated in the final design of the production line, through the use of IR.

The business-user, instead, would most commonly be the claimant, acting against any of the manufacturer, SIs or service providers. The loss could either be damages – both personal and economic – suffered directly as a consequence of the malfunctioning of a defective robot, or indirectly, was he acting in recourse after having been obliged to compensate the real victim, namely an operator, a co-worker not directly using the IR (see §2.4.2). The latter, in fact, when harmed by the functioning of the device could most clearly sue the employer – in light of his contractual relationship and further legal obligations to ensure the safety of the working environment, as further discussed above (see §2.7.2) – or, in case no such relationship was in place – as per the occasional non-worker by-stander –, through a wide set of civil law rules, specific to each legal order. Indeed, the factory owner could be held responsible towards any such subjects – often referred to as invitees, as they were allowed to enter the factory's premises – either on the grounds of tort law or contract law principles, such as the German notion of *Schutzpflichten*.

Most recurrent scenario: priority of application of the employer liability and subsequent litigation on product defectiveness. The detailed discussion of these scenarios falls beyond the scope and purpose of the current analysis, however, it can be most certainly concluded, that it would be possible to identify a subject primarily liable in case of an accidents towards such parties and that would not require the assessment of the defective nature of the product.

Instead, litigation under the PLD would most commonly occur among the identified business entities, the factory owner – or business-user – on the one hand, and the manufacturer, service provider, or system integrator on the other hand. Such parties would possess comparable negotiating power and access to information and technical expertise, relevant to demonstrate the existence of a defect – when that is the case – and of a causal nexus between that and the damage. Litigation would therefore not raise the same concerns that will instead be identified, defined and discussed in the corresponding section dedicated to CADs (see, section of CAD, §3.3).

Exception: exoskeletons acquired by the final user. The sole exception that on theoretical grounds could be identified, is potentially represented by exoskeletons. In such cases, should the final user – namely the operator – have purchased autonomously the device to use it on the workplace, easing his fatigue, was the device not provided to him as a personal protection of tool by his employer, in case the product caused some harm in its functioning, he would be required to sue the manufacturer on the same grounds of any other user of any other products. In such a limited hypothesis, most likely not a frequent one – for even exoskeletons used for industrial purposes will be either tools or personal protections provided directly by the employer within his contractual relationship with the operator –, the same concerns would raise, as discussed below (see, section of CAD, §3.3), primarily with respect to successfully demonstrate the existence of a defect and of a causal nexus by meeting the required evidentiary burden.

Most recurrent scenario: priority of contract-based litigation to PLD based litigation. In all other cases, PLD litigation would occur among the different businesses that, however, at the same time, would also be bound by a contractual agreement. This allows us to conclude that only seldom the parties will resort to the PLD, preferring contractual agreements and, eventually, (re)negotiation to distribute the economic consequences of the malfunctioning along the entire value chain. In so doing, they will most likely be more efficient than in court litigation, preserving ongoing relations.

To conclude, the specificity of the technology, its use, as well as the legal setting within which interactions occur, cause the application of product liability regulation to be less problematic, as well as less common, thence suggesting no specific action is, in such cases, required.

Manufacturers, and SI are liable under the PLD (SI, if operating as manufactures) and national tort law (e.g. for software). Users generally claim under the PLD, and are liable under general tort law for the wrong usage of the robots.

2.7.4. Insurance

2.7.4.1. Legislative framework

Lack of specific regulation on insurance of IR. Point 59 of the Recommendations to the Commission on Civil Law Rules adopted by the EU Parliament on the 16th of February 2017 on Robotics to the Commission, affirms that

> «when carrying out an impact assessment of its future legislative instrument, to explore, analyses and consider the implications of all possible legal solutions, such as: a) establishing a compulsory insurance scheme where relevant and necessary for specific categories of robots whereby, similarly to what already happens with cars, producers, or owners of robots would be required to take out insurance cover for the damage potentially caused by their robots».

At the present stage, both desk research and interviews with the stakeholders demonstrated that not only no legislation has been adopted at EU level to specifically regulate insurance products for IRs, but hardly any pre-existing measures on the topic apply.

Indeed, the legislative framework on insurance law in EU is quite scare, with few instruments actually harmonizing insurance products across MSs – the Motor Insurance Directive (extensively analyzed in the section on CADs, *infra*, §3.3.2.3), Regulation 2004/785 on insurance requirements for air carriers and air operators[275] –, and few other instruments ranging from the so called Solvency 2 Framework[276], and the Insurance Distribution Directive [277], which, however, fall outside the scope and object of this study.

Likewise, no legislation on insurance of IRs can be found at national level.

General insurance – insurance covering accident at the workplaces. However, as a consequence of the distinction between accident prevention on the workplace and (ii) liability *per se* set out in the introduction (§2.7.1), the analysis shall not be limited to insurance considered as an instrument to cover the risks associated with the use of a specific product, but also general forms of insurance related to a variety of accidents in the workplace, which

---

[275] Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on insurance requirements for air carriers and aircraft operators, OJ L 138, 30.4.2004.
[276] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (Text with EEA relevance) OJ L 335, 17.12.2009.
[277] Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast)Text with EEA relevance, OJ L 26, 2.2.2016.

could be relevant in case of accidents caused by the equipment and machinery used, no matter whether technologically advanced or not.

The current framework on health and safety of workers at the workplace – and most importantly the WFD and the WED – does not provide any form of compulsory insurance. On the contrary, MSs have systems providing insurance for work-related accidents. The following overview provides some relevant example.

Italy. In Italy, pursuant to the Decree No 1124 of 30 June 1965[278], all employer have an obligation to pay insurance contributions against accidents at work and occupational diseases to the Istituto nazionale per l'assicurazione contro gli infortuni sul lavoro – Inail. Such compulsory insurance covers every incident that occurred for «violent cause on the occasion of work» from which it derives death, permanent disability or absolute temporary disability for more than three days. It differs from the occupational disease because the triggering event is sudden and violent, while in the first case the causes are slow and diluted over time[279].

UK. The Employers' Liability (Compulsory Insurance) Act 1969 requires the employer to have at least a minimum level of insurance against any such claims. Employers' liability insurance will cover relevant work injuries or illness whether these are caused on or off site. However, any injuries or illness relating to motor accidents which occur while work may be covered separately by the employer's motor insurance[280].

Sweden. Social insurance is divided into a residence-based insurance, relating to guarantee benefit and allowances, and a work-based insurance, relating to benefits for loss of income. Both insurance categories apply equally to anyone living or working in Sweden. Swedish citizenship is not one of the insurance conditions. The Social Insurance Code covers most of the social security systems administered by the Swedish Social Insurance Agency and the Swedish Pensions Agency[281]. Those who are injured in the workplace or on the way to or from work can receive compensation from occupational injury insurance. Occupational injury insurance applies to an accident or an occupational illness; an injury that occurred at work in Sweden; expenses or lost income due to the occupational injury; or those who live in a country other than Sweden and need medical care due to the injury[282].

Austria[283], the Netherlands[284], Spain[285], and France[286] also have social compulsory insurance schemes for work related accidents.

---

[278] Decreto del presidente della repubblica 30 giugno 1965, n. 1124 ,Testo unico delle disposizioni per l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali, (GU n.257 del 13-10-1965 - Suppl. Ordinario), available at www.normattiva.it/urires/N2Ls?urn:nir:presidente.repubblica:decreto:1965;1124 (last accessed: 5th November 2018).

[279] https://www.inail.it/cs/internet/home.html (last accessed: 5th November 2018).

[280] Employers' Liability (Compulsory Insurance) Act 1969, available at https://www.legislation.gov.uk/ukpga/1969/57/section/6 (last accessed: 5th November 2018).

[281] Act (2010:111) on the introduction of the Social Insurance Code (2010:110). For further information, www.ilo.org/dyn/natlex/natlex4.detail?p_isn=88545.

[282] Information about the Sweden work insurance system can be found at the following link: https://www.government.se/495457/globalassets/government/dokument/socialdepartementet/socialinsuranceinsweden_august-2016.pdf.

[283] Bundesgesetz vom 9. September 1955 über die Allgemeine Sozialversicherung (Allgemeines Sozialversicherungsgesetz – ASVG.) StF: BGBl. Nr. 189/1955 idF BGBl. Nr. 18/1956 (DFB) (NR: GP VII RV 599 AB 613 S. 79. BR: S. 108.), available at the following link: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008147.

[284] There is no separate insurance scheme in the Netherlands for accidents at work and occupational diseases. Further information:

[285] Ley 42/2006 de 28 de diciembre - P.G.E. 2007, available at the fllowing link: http://www.seg-social.es/wps/portal/wss/internet/Trabajadores/CotizacionRecaudacionTrabajadores/10721/10957/583#582.

[286] Décret n°85-1354 du 17 décembre 1985 Relatif Au Code De La Securité Sociale.

2.7.4.2. Market for insurance products

Lack of IRs-specific insurance products. Interviews showed that insurers provide different insurance services connected to the production and use of IRs.

Indeed, some companies insure both manufacturers of cobots, mobile robots, and industrial exoskeletons, as well as system integrators (especially if they are substantially involved in the development of the robots), both against liability based on the PLD and on general tort law applicable in the national jurisdictions, for claims made by users of industrial robots (be they the business-users, or the actual worker or by-standers injured during an accident caused by the use of the robot.

Despite cobots, mobile robots and exoskeletons are all perceived as qualified by a higher degree of risks than the conventional (non-collaborative, in-cage) robots, comprising both damage to first-party and third-party property (e.g. in case of equipment or devices not owned by the business, but rather rented or leased by other parties), and physical damage, liability related to the use of such product is not insured differently than liability of traditional IRs. Thus, no insurance products aimed at covering specific risks arising from advanced Industry 4.0 robotics has yet been developed.

Three problems with PLD: risk evolves after time, reversal of burden of proof, cap is quite limited.

2.7.5. Bottlenecks and industrial trends

Distorted perception of risk. Interviews showed that stakeholders, and manufacturers in particular, do not perceive liability as an issue. Indeed, when asked about under which legal framework they may be held liable, many answered that the relevant rules on certification applied, thus confusing the obligation to comply with safety-regulation, and the duty to compensate for damages, should accidents arise, even in case of certification-compliant products.

This might imply that their perception of liability is distorted, because limited direct action on the basis of traditional tort law, or product liability claims, are brought about in order to seek compensation – since it will be most likely more efficient to base the claim on the contractual relationship between the business-user, the manufacturer, the service provider and the system integrator –, while comprehensive insurance

Interview showed that liability is not perceived as a problem by stakeholders, and especially by manufacturers, for a variety of reasons. Firstly, liability is seen as coupled, and dependent from, compliance with safety standards. Therefore, manufacturers believe that if they have certified the products, and complied with the relevant standards (especially hEN), they will not incur problems for damages caused by the IRs, and that – should an accident occur – the subject who will be held responsible will be the business-user, who has a specific duty to ensure safety and health of workers at the workplace, thus also for the IRs application and use.

However, it was also pointed out that safety rules specific for new technology – especially those with collaborative features – have not been written yet, and some confusion may arise on who exactly shall be responsible for which regulation.

Interviews also showed that an insurance market specific for IRs has not yet developed, and that manufactures generally rely on more traditional insurance products covering them from liability based on the PLD, on national tort law rules, as well as contractual liability, while business-user relay on public or private system of insurance to cover damages suffered by the employees, and private insurance for property damages which might occurred within their own premises.

2.7.6. Conclusions and recommendations

Definition. Civil liability determines who bears the economic consequences of an accident, and – traditionally – it is used to provide ex ante incentives towards a high-level of product safety; ex post it aims at providing adequate compensation to the victim. Insurance allows such costs to be internalized and managed, and compensation to be secured.

Double perspective. IRs are produced and installed by manufacturers and system integrators, purchased by business users, and operated by workers in factories. Liability for accidents caused by IRs occurs in a twofold perspective, as pertaining to (i) health and safety of workers, and the relevant insurance schemes; (ii) compensation for damages caused by IRs, under general private law rules.

Legal Framework. Thus, the relevant legal framework on liability and insurance of IRs comprises two different bodies of law, concerning, respectively: (i) health and safety of workers, and the relevant insurance schemes; (ii) compensation for damages caused by IRs, under general private law rules.

The first body of legislation consists of the Work Framework Directive (WFD), a series of further directives and regulations on safety at the workplace, and the national laws implementing them. Under MSs' social system, workers benefit from compulsory insurance schemes or pensions covering job-related accidents.

The second body of legislation consists of the Product Liability Directive (PLD), and the national laws implementing it, which display substantial differences among one another. As for other technological devices, the PLD offers insufficient protection to the victim, due to the difficulties in ascertaining and apportioning liability, as well as in proving the defect of the product and the causal nexus between the defect and the damage.

Assessment. Due to the peculiar relationship between the subjects involved, the victim – the operator of the IRs, or a coworker – will not face any difficulty connected to the identification of the subjects who is liable to compensate for the damages, i.e. the employer, and will benefit from the compulsory insurance for accidents occurred at the workplace, thus being overall better off as opposed to those injured by other types of technologically advanced devices (e.g. drones)[287].

Such mechanism is consistent with a RMA, as the subject who is held liable to pay for the damage is the one who is best positioned to (i) identify and manage the risk of its occurrence, thus adopting the most appropriate measure to prevent it, (ii) acquire insurance and thus manage the costs, once the damage has occurred, and finally (iii) redistribute such costs along the supply chain, when the damage is caused, for example, by a defect of the robots for which the manufacturer, or the SI, are responsible.

Indeed, it is likely that the business user, who has been called to compensate for the damaged suffered by one of his employee, decides to sue in recourse the aforementioned subjects, either to claim damages, or to re-negotiate the contractual agreement, as to make good for the expenses suffered.

The problems which typically arise because of the PLD (§2.7.3) do not arise in the case of IRs, at least not with the same degree of severity which comes about when other technologies are involved.

Liability not perceived as a risk. Interviews showed that manufacturers do not perceive liability as a risk, and believe that compliance with the safety regulation and standards will shield them from being held responsible for accidents involving their robots. This is incorrect.

---

[287] Bertolini, "Insurance and Risk Management for Robotic Devices: Identifying the Problems."

However, such a perception confirms the probable inefficiency of the PLD in ensuring the possibility to actually sue the manufacturer, either directly or in recourse.

Lack of specific insurance products. Despite the peculiar nature of advanced IRs is widely recognized, interviews pointed out that an insurance market specifically covering such technology has not developed yet.

No reform needed. The study suggests that, as far as liability is concerned, the current status quo is sufficient and does not require any intervention, since (i) the framework on health and safety of workers, and the related national insurance system, ease the position of the victim, who may benefit from prompt and adequate compensation; (ii) business-users may sue the other subject of the value chain, directly or in recourse, on a contractual basis; (iii) the application of the PLD remains residual, and thus problems which it arises for other technologies have only little practical relevance.

Need for broader reform of PLD is confirmed. However, the limited application of the PLD, as well as the problems that might be caused by as a consequence of its application, confirms the broader and more general need for its reform, as to facilitate apportionment and ascertainment of liability, proof of damage and casual nexus, and more appropriate liability exclusions and caps, allowing prompt and adequate compensation to the victim.

3. CONNECTED AND AUTOMATED DRIVING

KEY FINDINGS

- Automated driving has the potential to bring many social benefits, and most importantly to increase road safety by eliminating the major cause of accident, i.e. human error.
- The European Union supports the introduction of such technology through many policy initiatives, including the development of standards, co-funding of research projects, support actions and infrastructure pilots, also in areas – e.g. cybersecurity, 5G – which, despite having a broader scope, play a fundamental role in the roll out of automated driving.
- There is no unique definition of autonomous driving, and different nomenclatures are used often interchangeably.
- CADs – as will be referred to in this report – are vehicles which display two main features: (i) they are connected with other vehicles, with the infrastructure, and/or with other devices; (ii) they have different degrees of automation.
- For the purpose of this study, the SAE scale of automation will be used (levels 0 to 5).
- It is disputed to what extent CADs can be considered «vehicles» under current legislation. The issue is of twofold importance, as it affects the lawfulness of CADs on public roads, and the possibility to apply traditional traffic-liability rules, absent ad-hoc legislation.
- At the EU and international level, both the definition of vehicle set out in the Framework Directive 2007/46/EC (FD), and in the Motor Insurance Directive (MID) do not imply that a vehicle is such only if driven by a human driver.
- At national level, many MSs possess a broad definition of vehicle, that would accommodate CADs (e.g. Germany, Sweden, France), whereas others (e.g. Italy), expressly define vehicle as being man-driven, and thus require adaptation to include autonomous vehicles.
- The different subjects involved in the testing, certification, liability and insurance of CADs – whom the report will refer to, when needed – are: (i) the producer of the individual component; (ii) the service providers, (ii) the infrastructure providers, (iii) companies using CADs to provide a service; (iv) the human driver; (v) the owner of the vehicle, and (vi) insurance companies.

3.1. Introduction

Mobility is becoming even more automated, ranging from advanced driver assistance systems (ADAS)[288], to solutions where the device performs the majority or all of the dynamic tasks, being increasingly integrated and interdependent with large, complex operational design domains.

The benefits of automated driving. Such shift in the paradigm of mobility has the potential of bringing many social benefits. Given the vast majority of road accidents is due

[288] Examples include: night vision, lane departure warning, intelligent speed adaptation, hill descent control, GPS navigation, driver's drowsiness detection, collision prevention control, blind spot detection, automated braking, adaptive light control, adaptive cruise control.

to human errors, autonomous driving could substantially increase overall road safety, reducing the accident rates. Indeed, the vehicle would be able to monitor the environment continuously, thus outperforming the humans' driver natural lack of attention and promptness of reaction. Autonomous driving is expected to reduce traffic, by allowing better prediction of the most efficient route to follow, and speed to maintain, also considering the position of other vehicles on the road, also in connection with other vehicles, thus ultimately leading to reduced pollution, reduced travel-time-dependability, improved productivity – as users would be able to more efficiently employ their travel time.

Smart cities and new services. In general, autonomous driving is seen as a fundamental step in the development of smart cities, where the traditional networks and services are made more efficient with the use of digital and telecommunication technologies, for the benefit of its inhabitants and businesses. It means smarter and more inclusive urban transport networks, upgraded energy supply and waste disposal facilities, more interactive and responsive administration and safer public spaces[289].

European Union and national policy initiatives. The European Union has recognized that the development and large-scale deployment of Connected and Automated Mobility provides a unique opportunity to make our mobility system safer, cleaner, more efficient and more user-friendly, hence – within the Digital Single Market strategy – has taken the initiative to foster the development and diffusion of connected and automated mobility.

In this sense, the European Commission supports the introduction and deployment of autonomous vehicles through policy initiatives – such as the Communication from the Commission on the road to automated mobility, setting an EU strategy for mobility of the future –, development of standards, co-funding of research projects, support actions and infrastructure pilots, and, should it be needed, legislation.

In January 2016, it launched the High Level Group GEAR 2030[290], in an effort to ensure a coherent EU policy on vehicles. The group gathered several Commissioners, Member States and stakeholders representing the automotive, telecoms, IT and insurance industries. The group made recommendations to ensure that the relevant policy, legal and public support framework is in place for the roll-out of highly automated and connected vehicles by 2030.

In particular, and in relation to the inherent cross-border nature of road-mobility, MSs agreed to digital cross-border corridors[291], where vehicles can physically move across borders and where road safety, data access, data quality and liability, connectivity and digital technologies can be tested and demonstrated.

Furthermore, the European Commission is acting through a series of broad initiatives on cybersecurity[292], internet of things, 5G[293], privacy, data protection and free flow of data[294],

---

[289] For the EU initiatives on smart cities, please see https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en.

[290] For further information, see https://ec.europa.eu/growth/content/commission-launches-gear-2030-boost-competitiveness-and-growth-automotive-sector-0_en.

[291] For further information, see https://ec.europa.eu/digital-single-market/en/cross-border-corridors-connected-and-automated-mobility-cam.

[292] *Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building Strong Cybersecurity for the Eu* (Brussels: European Commission, 2017).

[293] GWS, Cair, and Ricardo, *Gear 2030 Strategy 2015-2017. Comparative Analysis of the Competitive Position of the Eu Automotive Industry and the Impact of the Introduction of Autonomous Vehicles: Final Report - Study* (European Commission, 2017).

[294] Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on

liability[295], and – more specifically on autonomous vehicles, through the so called Cooperative Intelligent Transport Systems (C-ITS)[296] – a system allowing the exchange of information between vehicles, and between vehicles and the road infrastructure –, and the C-ROADS Platform[297], which allows to harmonize the deployment of C-ITS activities across Europe.

3.1.1. Definition of CADs

Different nomenclatures and types of autonomous driving. As it most often happens in the field of robotics, there is no unique and specific definition for automated driving solutions. Indeed, different nomenclatures may be found: from adaptive driving advanced systems (henceforth ADASs), to automated vehicles (henceforth AVs), to connected and automated vehicles (henceforth CADs), to connected, cooperative and automated mobility (CCAMs). In some cases, the said terminology may be used indistinctively, either because these names are deemed synonyms, or because – although each one is meant to designate a unique combination of features the automated driving displays – an identical feature happens to be conveyed by many terms at the same time, thus leaving a margin of interchangeability.

Automation. All the types of innovative driving recalled above can be deemed autonomous, despite to a different degree and to a different level of characterization. Indeed, different levels of automations are commonly identified, according to a series of official classification systems, ranging from no-automation (traditional driving), to full automation (where the human is a mere passenger and does not perform any of the driving related tasks). The most famous classification is that set by SAE International (SAE J 3016); hence, – if not differently specified – reference to the different levels of automation made throughout this study will be based on the SAE nomenclature and standard. However, given that other classification are used within Europe – such as in the German law (§0) – the table below also offers a comprehensive and comparative overview of the said classification.

---

the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance);
Brussels, 13.9.2017 COM(2017) 495 final 2017/0228 (COD) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for the free flow of non-personal data in the European Union.

[295] European Commission Brussels, 25.4.2018 SWD(2018) 137 final COMMISSION STAFF WORKING DOCUMENT Liability for emerging digital technologies Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe COM(2018) 237 final. See also Tatjana Evas, *A Common Eu Approach to Liability Rules and Insurance for Connected and Autonomous Vehicles. European Added Value Assessment Accompanying the European Parliament's Legislative Own-Initiative Report (Rapporteur: Mady Delvaux)* (EPRS European Parliamentary Research Service, 2018).

[296] *Communication. A European Strategy on Cooperative Intelligent Transport Systems, a Milestone Towards Cooperative, Connected and Automated Mobility* (Brussels: European Commission, 2016)..

[297] https://www.c-roads.eu/platform/about/about.html.

Table 19: Levels of automation (main reference: SAE classification)

Summary of Levels of Driving Automation for On-Road Vehicles

This table summarizes SAE International's levels of *driving* automation for on-road vehicles. Information Report J3016 provides full definitions for these levels and for the italicized terms used therein. The levels are descriptive rather than normative and technical rather than legal. Elements indicate minimum rather than maximum capabilities for each level. "System" refers to the driver assistance system, combination of driver assistance systems, or *automated driving system*, as appropriate.

The table also shows how SAE's levels definitively correspond to those developed by the Germany Federal Highway Research Institute (BASt) and approximately correspond to those described by the US National Highway Traffic Safety Administration (NHTSA) in its "Preliminary Statement of Policy Concerning Automated Vehicles" of May 30, 2013.

Level	Name	Narrative definition	Execution of steering and acceleration/ deceleration	Monitoring of driving environment	Fallback performance of *dynamic driving task*	System capability (*driving modes*)	BASt level	NHTSA level
Human driver **monitors the driving environment**								
0	**No Automation**	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a	Driver only	0
1	**Driver Assistance**	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes	Assisted	1
2	**Partial Automation**	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes	Partially automated	2
Automated driving system **("system") monitors the driving environment**								
3	**Conditional Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task* with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes	Highly automated	3
4	**High Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes	Fully automated	3/4
5	**Full Automation**	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**	-	

Source: cyberlaw.stanford.edu/blog/2013/12/sae-levels-driving-automation

In this sense, the terms AVs, CADs and CCAMs cover a wider notion of vehicles, which mainly refer to the autonomous driving features, meaning that they have sensors and software capable of detecting in real time the environment and navigate it without or with limited guide by human intervention, thus being deemed autonomous; on the contrary, the term ADASs – which refer to a combination of hardware and software solutions which aim to facilitate or increase the safety of driving, without substituting the human in the main tasks (e.g. night vision, lane departure warning, intelligent speed adaptation, hill descent control, GPS navigation, driver's drowsiness detection, collision prevention control, blind spot detection, automated braking, adaptive light control, adaptive cruise control) –, can be seen not as a driving solution per se, but rather as a step in the progressive automation of driving.

Other features: connectivity and cooperation**.** While the term AVs simply displays the autonomous feature of driving, CADs and CCAMs also encompass other features, mostly based on the connected nature of the devices. Connected cars and trucks, for example, are provided with services, such as internet access and GNSS, by means of a wireless local area network, allowing the vehicle to share internet access with other vehicles (vehicle-to-vehicle, V2V), infrastructure (vehicle-to-infrastructure, V2I) and devices (vehicle-to-everything, V2X), both inside as well as outside the vehicle[298].

Furthermore, when talking about CCAMs, an additional element is taken into consideration, namely that of the cooperation. In this sense, special attention is given to the fact that

[298] Evas. See esp. p. 50.

vehicles enabled by digital connectivity interact directly with each other, with other road users, and with the road and transport infrastructure, through the Cooperative Intelligent Transport Systems (C-ITS), which will allow road users and traffic managers to share information and thus coordinate their actions. This cooperative element is expected to significantly improve road safety, traffic efficiency and comfort of driving, by helping the driver take the right decisions and adapt to the traffic situation, thus achieving a full integration in the overall transport system.

Chosen Terminology. Indeed, AVs, CADs and CCAMs may be used interchangeably or with slight different meaning, depending on the element – automation, connectivity or cooperation – which is mostly directly taken into consideration. However, since the aforementioned features are mostly complementary, and are expected to further build onto each other in the future, we believe that, for the purpose of this report, a general reference to CADs is most appropriate, as it covers the basic structure of all innovative mobility, which are of fundamental and pre-emptive importance for any assessment and recommendation on the issues of testing, certification and liability of the said technologies. On the contrary, explicit inclusion of the cooperative element does not seem to require additional change in the method and findings of the report. Thus, the study will mostly refer to CADs, and special reference to more simplified or complex form of mobility will be made whenever relevant and needed.

3.1.1.1. CADs as «vehicles» under current legislation

Despite referred to as autonomous and connected vehicles, it is indeed disputed to what extent CADs can be considered «vehicles» under current legislation. The issue is of twofold importance. Firstly, it directly affects the lawfulness of CADs on public roads (despite it does not exhaust the matter, as – given a broad definition of vehicle – other requirements may be set, as to impede the roll out of autonomous driving). Secondly, it determines the possibility to apply general liability of traffic rules for motor vehicles to CADs, absent specific legislation.

The European framework. At the European level, a harmonized definition of «vehicle» can be derived from Directive 2007/46/EC (also referred to as Framework Directive, henceforth FD, see §0 below), establishing a framework for the approval of motor vehicles[299] – which defines a vehicle as «any power-driven vehicle which is moved by its own means, having at least four wheels, being complete, completed or incomplete, whit a maximum design speed exceeding 25km/h»[300] –, and from Directive 2009/103/EC on the insurance against civil liability in respect of the use of motor vehicles[301] (henceforth MID), which states that «"vehicle" means any motor vehicle intended for travel on land and propelled by mechanical power, but not running on rails, and any trailer, whether or not coupled»[302].

The international framework. At the international level, the definition of vehicle – together with other fundamental rules on traffic – is set by the Vienna Convention on Road Traffic (henceforth VCRT)[303], which is an international treaty concluded in 1968 with 74 current State Parties, among which do not appear two of the major world powers – namely the United States and China –. According to the Preamble, the Convention «desires to

---

[299] Directive 2007/45 of the European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (OJ L 263, 9 September 2007, p. 1).
[300] Art. 3, n. 9.
[301] Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance of civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability (OJ L 263, 7 October 2009, p. 11-31).
[302] Art. 1, n. 1.
[303] Vienna Convention on Road Traffic, 8th November 1986; Legal Instruments in the Field of Transport, Convention on Road Traffic, Vienna (Nov. 8, 1968), United Nations Economic Commission for Europe (UNECE) website (last visited Dec. 14, 2016).

facilitate international road traffic and to increase road safety through the adoption of uniform traffic rules».

The VCRT defines a motor vehicle as a power-driven vehicle (i.e. self-propelled road vehicle other than mopeds and rail-borne vehicles) which is normally used for carrying persons or goods by road or for drawing, on the road, vehicles used for the carriage of persons or goods[304]. Therefore, the very definition of vehicle does not include the presence of a driver, and thus seemed to be able to accommodate CADs; however, this was indeed obstructed by other provisions.

Notably, **both the definitions of vehicles provided by the European directives and by the Vienna Convention do not imply that the vehicle shall be driven by a human driver.**[305]

However, also for a correct understanding of future references to the VCRT, it is important to point out that only 21 out of 28 EU MSs signed the Convention, and that different interpretations as of how its provision shall be interpreted can be found among different MSs. For example, Spain – one the MSs analyzed in this study – has not signed the Convention[306].

MSs framework accommodating CADs. At the national level, some MSs possess a sufficiently broad definition within their traffic code, that requires no adaptation. Under the German Road Traffic Act §1(2), motor vehicles are defined as land vehicles which are moved by machine power without being bound to railroad tracks[307], whereas the UK Road Traffic Act 1988 section 185 defines a motor vehicle as a mechanically propelled vehicle intended or adapted for use on roads[308]. Likewise, the French Code de la route defines a motor vehicle as «any land vehicle equipped with a propulsion engine ... and traveling on the road by its own means»[309], while the Spanish Traffic Law refers to motor vehicles as «vehicle equipped with engine for its propulsion»[310]. Similarly, Swedish law states that a vehicle is «a device on wheels, belts, joints or the like, which is arranged mainly for travel on the ground and does not run on rails»[311], and Austrian law defines it as «a means of transport intended for use on roads or used on roads or a mobile work machine, except wheelchairs, baby carriages, wheelbarrows and similar vehicles intended for off-road use and vehicle-like toys […] and winter sports equipment»[312]. Under Dutch law, motor vehicles are defined as «vehicles,

---

[304] Art. 8 VCRT.

[305] Indeed, this is also confirmed by the extant rule on type approval, especially on steering devices (§3.2.8.1).

[306] As it will be further discussed in §3.2.2.2, this has allowed Spain to be the first country in Europe to allow testing of CADs on public roads.

[307] «Als Kraftfahrzeuge im Sinne dieses Gesetzes gelten Landfahrzeuge, die durch Maschinenkraft bewegt werden, ohne an Bahngleise gebunden zu sein» (Art. 1 StVG), available at www.gesetze-im-internet.de/stvg/__1.html (last accessed 1 October 2018).

[308] « "motor vehicle" means … a mechanically propelled vehicle intended or adapted for use on roads»; available at https://www.legislation.gov.uk/ukpga/1988/52/section/185 (last accesses 1 October 2018).

[309] «Pour l'application du présent code, les termes, ci-après ont le sens qui leur est donné dans le présent article : 1. Le terme « véhicule à moteur » désigne tout véhicule terrestre pourvu d'un moteur de propulsion, y compris les trolleybus, et circulant sur route par ses moyens propres, à l'exception des véhicules qui se déplacent sur rails […]»; Article L110-1, available at https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006840863&cidTexte=LEGITEXT000006074228 (last accessed, 1 October 2018).

[310] «Vehículo provisto de motor para su propulsión. Se excluyen de esta definición los ciclomotores, los tranvías y los vehículos para personas de movilidad reducida»: Anexo I, Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial (BOE núm. 261, de 31 de octubre de 2015).

[311] «En anordning på hjul, band, medar eller liknande som är inrättad huvudsakligen för färd på marken och inte löper på skenor. Fordon delas in i motordrivna fordon, släpfordon, efterfordon, sidvagnar, cyklar, hästfordon och övriga fordon» Lag (2001:559) om vägtrafikdefinitioner, 2§ Beteckning Betydelse, available at https://lagen.nu/2001:559.

[312] «Fahrzeug: ein zur Verwendung auf Straßen bestimmtes oder auf Straßen verwendetes Beförderungsmittel oder eine fahrbare Arbeitsmaschine, ausgenommen Rollstühle, Kinderwagen, Schubkarren und ähnliche, vorwiegend zur Verwendung außerhalb der Fahrbahn bestimmte Kleinfahrzeuge sowie fahrzeugähnliches Kinderspielzeug (etwa

intended to be propelled other than along rails, exclusively or partly by a mechanical force, on or on the vehicle itself or by electric traction with power supply from elsewhere, with the exception of bicycles with pedal assistance»[313].

Thus, German, French, UK, Spanish, Swedish legislation do not require an amendment of the definition of vehicles to accommodate the introduction of CADs (while, obviously, other elements, such as type approval requirements, might still constitute an obstacle; see §0). The legislations which were introduced (Germany and UK) for regulating CADs are indeed focused on issues different from the definition of a motor vehicle[314], like the need for apportioning liability in case of accidents, as well as the choice to limit CADs circulation until a certain level of automation (Germany, whose amendment of the road traffic act excludes SAE level 5 of automation and provides for specific driving technical features necessary for human active driving), or the extension of compulsory insurance mechanism necessary to allow driving (UK) (see §0).

MSs framework non-accommodating CADs. On the contrary, other national definitions should be modified, in order to accommodate the introduction of CADs. The Italian Codice della Strada, for example, defines motor vehicles as all those man driven-machines which circulate on roads, therefore explicitly requiring the presence of a human driver.[315] Therefore, while a Google car would be considered a vehicle in France or in the UK, it would fall outside of this category in Italy, thus being denied circulation. However, it is worth noting that a system of recognition of homologations set out in other MS may allow the recognition of such vehicles on public roads, even in Italy[316]. Indeed, were the vehicles certified under the type approval framework – which will be discussed in §0 below –, its circulation shall not be impeded, leading to a complex legislative *impasse* and potential conflicts among MSs' jurisdictions.

3.1.2. Subjects involved

Even if the development of CADs concerns only the manufacturer and the manufacturer of the individual components (differently from the case of Industrial Robots, where the activity performed by the integrators is indeed fundamental for the actual configuration of the final product within business-users' production lines), the specific features of the product (§3.1.1) are such that, for the purpose of this report, other subjects involved in the testing, certification, liability and insurance need to be taken into consideration.

3.1.2.1. Producers.

The producer of the CADs is the manufacturer of vehicle as final, complete product. However, for liability purposes, such category also comprises the manufacturer of individual components – whose relationship with the former are regulated on a contractual basis –, who may be held responsible for the «manufacturing defect» of the component provided, and thus be condemned either to pay compensation to the victim, or to reimburse the

---

Kinderfahrräder mit einem äußeren Felgendurchmesser von höchstens 300 mm und einer erreichbaren Fahrgeschwindigkeit von höchstens 5 km/h) und Wintersportgeräte.»: StVO – Straßenverkehrsordnung – 1960 §2 Begriffsbestimmungen.

[313] WET van 21 april 1994, houdende vervanging van de Wegenverkeerswet, art. 1.

[314] Indeed, §1a of the German law amending the Road Traffic Act – «Motor vehicles with highly or fully automated driving function» – does set a specific definition of highly or fully automated driving function, but it is mostly aimed at selecting which kind of automated vehicles (e.g. a Tesla type car, where a steering wheel is essential) are allowed.

[315] Art. 46, Codice della strada, Decreto Legislativo N. 285 del 30/04/1992, G.U. n. 114 del 18/05/1992, available at: http://www.mit.gov.it/mit/site.php?p=normativa&o=vd&id=1&id_cat=&id_dett=0.

[316] Art. 75 C.d.S. cc. 1-3 / 5 «Mopeds, motor vehicles, motor vehicles, trailers and trailers, to be admitted to traffic, are subject to the verification ... of their correspondence to the technical prescriptions and to the constructive and functional characteristics required by the provisions of this code. The assessment referred to in paragraph 1 takes place by means of a visit and proof by the competent offices of the territorial directorates of the Department for land transport. The vehicles indicated in paragraph 1 ... produced in series, are subject to type approval. The approval, total or partial, issued by a foreign State, can be recognized in Italy on condition of reciprocity».

manufacturer of the final product, acting in redress after having compensated the injured party.

Despite not technically qualifying as «producers», other subjects are explicitly associated to the latter by art. 3 of the PLD: the entity who first imports a foreign product within the EU (e.g. an Italian company buying CADs produced in the US in order to sell them in the internal marker), and the dealer who re-sold the product, if the actual manufacturer cannot be identified. At least for liability purposes, such subjects share the same responsibility of the actual producer.

3.1.2.2. Service providers.

Together with the producer of CADs and of their individual components, other subjects who play a fundamental role in the value chain and could be subject to liability claim are those who provide services either necessary or accessory for the functioning of the automated vehicles. The actual identification of this category varies depending on how broad or narrow the very concept of producer is defined, as well as on the basis of the contractual agreement with the automotive manufacturer, and between the latter and end-users. Most relevantly, software producers and app-developers may be seen both as producers and as providers of additional services, depending on whether software is considered as falling within the scope of the PLD and thus constituting a product on its own, and whether the latter has been purchased directly by the end users or rather it was sold as part of the entire package[317].

3.1.2.3. Infrastructure providers.

The same consideration goes for a peculiar type of service – i.e. access to a telecommunications network or to the internet – which is considered as one of the elements of a broader «infrastructure», upon which the readiness of a state or jurisdiction for the roll out of autonomous and connected driving is tested against[318].

For the same purpose, alongside with the network providers, this report will also consider public authorities (State, local communities, independent authorities, private companies granted with a government concession) who own public ways, and are thus responsible for the maintenance and custody of such roads for the public to use. In some circumstances, even the owner of a private road could be considered for the purpose of the ascertainment and apportionment of liability.

3.1.2.4. Companies using CADs as an element of the service.

In the light of the business models that most likely will benefit from the introduction of CADs, special attention shall be brought to companies offering specific services to consumers, where the use of the vehicle constitutes a fundamental element of the contract.

This category comprises both rental companies, leasing companies, mobility-as-a-service sharing companies, who would put autonomous vehicles up to use to either consumers or professionals, according to a series of different contractual schemes.

3.1.2.5. Human Driver.

The last subject involved for the purpose of this report is the human «driver», i.e. the end-user of the vehicles. Depending on the level of automation, he will be responsible for a different series of driving-related tasks, ranging from the actual driving (when automation only offers forms of assisted driving – lane keeping and brake assistance, cruise speed etc. etc. – or when autonomous driving is possible but represents an option, which the human

---

[317] For this purpose, see 3.3.2.

[318] On this purpose, see KPMG, *Autonomous Vehicles Readiness Index. Assessing Countries' Openness and Preparedness for Autonomous Vehicles* (2017).

can switch off depending on his own desires or on the contingent circumstances), to supervision and control resumption in case the autonomous driving mode is on, to mere selection on driving modes and destinations, in a SAE level 5 (no-steering-wheel-needed) scenario (see §3.1.1).

3.1.2.6. Owner of the vehicle.

The owner of the vehicle shall be considered as an autonomous subject from the driver, since the two have different legal positions. As it will further be shown, the owner will most likely be responsible for specific activities, such as software updates and – possibly – the purchase of insurance product related to the use of the CADs. In some jurisdictions owners are held liable on strict or semi-strict grounds, typically jointly and severally with the driver himself. Such a distinction might be of particular relevance in shared-mobility scenarios.

3.1.2.7. Insurance companies.

Insurance companies already play a relevant role in the management of liability-related issues for traditional driving. Typically, MSs' as well as EU legislation in the field of motor vehicles establishes duty for owners and users – namely drivers – to insure for damages against third parties. First party insurance schemes are also provided for in some jurisdictions. The market for insurance products related to the motor vehicle industry is therefore mature and developed, yet might require adaptation, to address both new forms of mobility – shared mobility and mobility-as-a-service – and new technologies that cause the application of liability rules to become more complex (see §3.3.2).

3.2. Testing

KEY FINDINGS

- The amended Vienna Convention on Road Traffic allows automated driving, provided that the technologies used comply with the UN regulations, or can be overridden by the driver. Hence, MSs may permit testing of CADs on public roads.
- Indeed, many MSs – even before such amendment – have regulated testing of CADs on public roads, according to different requirements and procedures. The majority only allow high automation, while others also accommodate trials of fully autonomous vehicles (e.g. Sweden), or plan to do so.
- Testing of CADs is performed on components, sub-systems and systems, and relies on different techniques, ranging from virtual and combined, to physical testing. Trials take place in controlled environments, indoor, outdoor, and in public roads, with different degrees of involvement of the human driver and bystanders.
- Trails shall take into account CADs specific risks, in particular those related to machine learning, cyber-security, as well as those connected to the unpredictability of the driving environment – e.g. on public roads –, which raises safety concerns and exacerbates issues of experimental reproducibility, and on the possible fall back of test-drivers.
- Fragmentation of testing regulation limits the possibility to test among MSs, creates additional burdens on companies, ultimately hindering technological innovation. Collaborations among MSs to allow cross-border testing is to be welcomed, but is not sufficient to solve the issue.
- Regulation shall be adopted at the EU level, to create a legal common-playing-field and facilitate testing, expressly allowing higher degrees of automation.

- The creation of Tokku zones and regulatory sandboxes, derogating from regulation which is incompatible with testing of CADs, is suggested as a way of facilitating trials in real life condition.
- Initiatives to foster research and development of technical solutions incrementing the accuracy, variety and complexity of the scenarios which CADs shall be tested against, especially through virtual testing, as well as tools for data-sharing and common benchmarks and practices, are needed.

3.2.1. Introduction

Definition. During the entire cycle of production, CADs are subject to tests, to prove their inherent safety and their functionality (§1.2). Despite inherently intertwined, these two objectives require different form of testing, i.e. performance testing – where test is performed in the development and production of CADs, with the purpose of verifying goals and functionalities –, and reliance testing – which aims at gathering knowledge about potential risks and failures connected to their use –. These type of testing is part of the normal scientific methodology used by system developers and engineers, and offers a manner to gather evidence for the correctness and the development of the design in specific components and subsystems, and performing the related risk assessment and evaluation.

Trials and validations performed for the purposes of obtaining certification serve the different function of demonstrating conformity with requirements necessary for marketing a product within the internal market. Given this substantial and functional difference, certification-oriented testing falls outside the scope of this section, and – whenever relevant – will rather be considered in §0. However, it is important to highlight that manufacturers of CADs rely on the standards and requirements set in the type-approval to demonstrate safety of the vehicle, both during the testing cycle of the products under development, and during the procedures to obtain certifications.

Over the last decades an extensive set of requirements has been defined for vehicles with a human driver, which have to be met in order to be allowed to drive on the public road. This contains requirements on the vehicle to be initially allowed on the road (type approval), but also periodic evaluation for each vehicle. For example, specific tests can be performed to check if the vehicle brakes up to full avoidance for a crossing pedestrian: this is an objective test, with clear set-up and output criteria. However, it is particularly challenging to define the appropriate requirements for CADs, as this needs to combine both the hardware components of the vehicle, as well as those software components that make the vehicle «autonomous», thus substituting the instructions and decision taken by the driver.

Structure and aim of the section. This section will firstly investigate the legal framework on testing of CADs (§3.2.2). Secondly, it will describe how tests are performed (§3.2.2), and what risks are identified and evaluated, with particular focus on those novel risks that CADs bring about, because of their autonomous and connected technology (§3.2.4). On the basis of such analysis, technical and legal bottlenecks, preventing adequate assessment of the performance and reliance of the IRs, will be identified (§3.2.5). Lastly, the overall state of art of testing will be evaluated; where needed, possible policy strategies for reform will also be formulated (§3.2.6).

3.2.2. Legal framework

As it will be further discussed below (§3.2.2.2), the applicable legislative framework is mostly set at the national level, and consists of the national traffic rules and, in some cases, of the derogation provided for through amendment to the latter, or by specific legislation, in order to allow the use of automated vehicles on public roads. However, in the light of coordinating

and harmonizing the roll out of CADs, relevant international and European initiatives have also been adopted.

3.2.2.1. International and European framework.

International law. Despite the **VCRT** does not refer to vehicles as vehicles driven by a human driver – as the Italian traffic code does, for example –, still autonomous driving was originally not allowed, as article 8 of the Convention **required that «every moving vehicle or combination of vehicles shall have a driver», and that « [e]very driver shall at all times be able to control his vehicle [...]»**[319]. The signatory States were thus not supposed to allow autonomous vehicles on public roads, not even for testing purposes, and States like Spain – not having signed the Treaty – had a strong regulatory advantage compared to the others (§3.2.2.2). Also for circumventing this problem, some MSs – such as Sweden and the Netherlands (§3.2.2.2)– adopted a broad interpretation of the human-control requirement set by the VCRT, and, contrary to the main reading of art. 8, allowed CADs testing on public roads.

In 2014, the Governments of Belgium, France, Germany, and Italy proposed amending article 8 of the Convention to allow automated driving technologies[320], arguing that, since traffic accidents are predominantly caused by human error and that automated driving systems enhance road safety, the Convention needed to be revised as to give way to the roll out of CADs. The **amendment to the Convention entered into force on 23 March 2016**,[321] introducing **art. 8, 5bis**, which states:

> «Vehicle systems which influence the way vehicles are driven shall be deemed to be in conformity with paragraph 5 of this Article and with paragraph 1 of Article 13, when they are in conformity with the conditions of construction, fitting and utilization according to international legal instruments concerning wheeled vehicles, equipment and parts which can be fitted and/or be used on wheeled vehicles. Vehicle systems which influence the way vehicles are driven and are not in conformity with the aforementioned conditions of construction, fitting and utilization, shall be deemed to be in conformity with paragraph 5 of this Article and with paragraph 1 of Article 13, when such systems can be overridden or switched off by the driver»

Therefore, under the revised VCRT framework, it is possible the transfer of the driving tasks to the vehicle itself, **provided that the technologies used to are in conformity with the United Nations vehicle regulations, or can be overridden or switched off by the driver**. All the signatory MSs are thus now allowed to change their legislation accordingly and, indeed, many have already introduced specific regulations or are working in that direction.

European law. No legislation at European level regulating validation testing has been adopted. However, a vast number of policy initiatives support large scale and cross-border testing, through research funding programs and deployment projects. As summarized in the 3rd Mobility Package, «For the period 2014-2020, a total budget of around EUR 300 million from the EU's framework program for research and innovation «Horizon 2020» has been

---

[319] Convention on Road Traffic, Nov. 8, 1968, 1042 U.N.T.S. 15705, UNECE website. www.unece.org/fileadmin/DAM/trans/conventn/crt1968e.pdf.
[320] UNECE, Inland Transport Committee, Working Party on Road Traffic Safety, Report of the Sixty-Eighth Session of the Working Party on Road Traffic Safety (Apr. 17, 2014), UNECE website.
[321] Press Release, UNECE Paves the Way for Automated Driving by Updating UN International Convention, UNECE website (Mar. 23, 2016).

allocated to support research and innovation on automated vehicles»[322]. Concretely, the Commission undertook the initiatives to[323]:

- Create a priority list of transport use cases for testing with the support of MS;
- Identify possible synergies between connectivity and automation use cases;
- Establish one single EU wide platform grouping all relevant stakeholders to coordinate open road testing.

3.2.2.2. National frameworks

As far as the national legal frameworks on CADs testing is concerned, the major issue which needs to be addressed is whether or not MSs have regulated testing on public roads, and how. An overview of the MSs falling within the scope of this comparative study is provided below.

France. Since in-house testing of CADs – both in laboratories and in dedicated tracks – was not reputed sufficient to provide consistent and reliable outcomes, the French legislation was recently amended, in order to allow safety engineers and automotive entrepreneurs to conduct examination on some public roads.

The French system allows the circulation of vehicles featuring various degrees of autonomy («vehicules à délégation partielle ou totale de conduite», henceforth VDPTC), to be authorized, pursuant to three main bodies of law, namely (i) Ordinance No. 2016-1057 of 3 August 2016, relative à l'expérimentation de véhicules à délégation de conduite sur les voies publiques, (ii) Decree No. 2018-211 of 28 March 2018, relatif à l'expérimentation de véhicules à délégation de conduite sur les voies publiques, and (iii) Order of 17 April 2018, relatif à l'expérimentation de véhicules à délégation de conduite sur les voies publiques.

The authorization is especially aimed at ensuring high standards of safety, while experimentation of VDTPC is carried out for technical reasons or fine tuning, performance evaluation related to real-life situation and show to the general public[324].

A formal[325] request of such authorization needs to be addressed to Director General of Energy and Climate (DGEC) and to the Road Safety Delegate (DSR), either by the owner of the vehicle, or by a subject who can prove a link with him. Whoever asks for such an authorisation is required to provide both i) the questionnaire contained in Annex 1 of the aforementioned decree of 17 April 2018, ii) the official request letter, signed by a person with the capacity to represent his company in this process, iii) a technical file on the vehicle, and iv) a presentation of the test under examination. The Minister responsible for transportation is allowed to ask for further clarifications in order to better assess the experimentation and its dangers, and, after an audit provided by the Minister of the Interior, is in charge of giving his consent to authorization. Nonetheless, he remains entitled to further modify, suspend or even withdraw the authorization.

After that, the Minister of the Interior (in accordance with the presentation of the decision of the Minister of Transport) issues the WW DPTC certificate, which is required in order for the test to be carried out[326]. As of now, even though some roads still cannot be exploited by VDPTC, no request for authorization to perform testing has been wholly refused, but

---

[322]Available at: https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf , page 6.
[323]Available at: https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf , page 8.
[324] Art. 1, Decree 211.
[325] The form to bid for such an authorization is online, for further information see www.demarches-simplifiees.fr/commencer/autorisation-experimentation-vdptc, last access November 19th, 2018.
[326] Art. 9, Decree 211.

cooperation between the Ministries and the parties has helped in finding out viable solutions. Some more rules are provided with reference to how tests must be carried out.

Pursuant to art. 11, Decree 211, all VDPTC are required to feature a recording instrument, capable of recording relevant information concerning the degree of automation. Normally that information is to be deleted regularly, but in case of accidents it is to be saved for one year, in order to ease proof and evaluation.

Also, the subject who obtained authorization is required to provide with feedback and the results that came out from the testing.

Since a driver is always required to be ready to resume control of the VDPTC, it is likely that tests of CADs on public roads are allowed up to level 4 SAE of automation. However, France announced its intention to expand testing, allowing experimentation on public roads with no human operator behind the wheel by 2019.[327]

UK. The UK has worked in parallel with Germany to establish a national regulation for CADs, and has recently adopted its first binding legislation on this matter. At present, the law specifies that the driver has responsibility for the car and must remain in control, but a broad system allowing testing of driverless vehicles is in force.

In 2015 the Department of Transport released its paper The Pathway to Driverless Cars[328], stating that existing regulation does not constitute a barrier to testing autonomous vehicles on public roads, as long as a human sits in the driver's seat and remains prompt to resume control if needed.

In the same year the Department of Transport released a Code of practice for testing[329]. The document states that i) responsibility for testing rests with the testing organization; (ii) vehicles under testing must comply with all relevant road traffic law; (iii) test drivers or test operator shall have a suitable license – even if testing a vehicle's ability to operate entirely in an automated mode –, shall be reliable, skilled and specifically authorized and trained to perform this role by the organization responsible for conducting the testing; (iv) test drivers and test operators shall supervise the vehicle at all times and be ready and able to over-ride automated operation if necessary, and the test driver or test operator will be responsible for ensuring the safe operation of the vehicle at all times whether it is in a manual or automated mode, and shall always observe road traffic laws (v) testing organizations should conduct risk analyses of any proposed tests and have appropriate risk management strategies; and (vi) the statutory requirements on the holding of insurance apply.

The Vehicle Technology and Aviation Bill, presented in February 2017, was drafted as to introduce policies for automated vehicles and road vehicle testing, extending compulsory motor insurance requirement to include automated vehicle owners. The initiative came to a halt when the Parliament was dissolved in July 2017, and has now been translated in the Automated and Electric Vehicle Bill[330], which will be further discussed in §0 below.

---

[327] https://www.autovistagroup.com/news-and-insights/france-amend-legislation-autonomous-vehicle-trials

[328] Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401562/pathway-driverless-cars-summary.pdf, last accessed on the 23rd of January 2018.

[329] *A Pathway to Driverless Cars: A Code of Practice for Testing* (London: Department for Transport, 2015). Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/446316/pathway-driverless-cars.pdf.

[330] Available at https://services.parliament.uk/bills/2017-19/automatedandelectricvehicles.html, last accessed on the 22nd of January 2017.

Italy. In Italy, testing of connected and autonomous vehicles, as well as of Smart Road features, is allowed on public roads by art. 1, paragraph 72, of the L. 205/2017[331]. This body of law requires the Minister for Infrastructures and Transportation to issue a detailed decree, and allows an investment of € 1 million, for 2018 and for 2019 each.

The Decree[332] – which was issued on 28 February 2018 – states that authorization for testing of CADs is provided by the Ministry of Infrastructures and Transportation, Department for transportation, navigation, general issues and personnel, General Direction for motorization.

Authorization can be demanded by car manufacturers or by Universities and public or private research bodies which are pursuing testing; said subjects must provide, among other requirements, proof of ownership of the autonomous vehicle and of their entitlement to make use of the stretches of road and infrastructure involved. Applications for authorization imply a statement, by the requiring subject, of having already completed experimentation at least in laboratory, in separate tracks or on public roads for at least 6.000 kilometres, and that the vehicle is roadworthy and fit for the envisaged infrastructure, traffic and weather conditions. Further requirements rest upon automated driving systems themselves: for instance, vehicles must register constantly and frequently all data relevant to the operation, which may thereafter be provided to the authorising authority. The subject in charge of providing authorisation is allowed to require any document that may deemed necessary or useful in order to acquire further information and is entitled to suspend or cancel the authorization at any time, provided a violation of said authorisation is verified or unforeseen danger rises.

Authorization can be issued only with effect on vehicles which, deprived of CADs technology, are already approved, and is issued with regard to one or more vehicles; in the latter case, vehicles' automation features must be similar. Insurance for autonomous vehicles is compulsory, and the minimum coverage is four times the coverage for the non-autonomous specification of the vehicle under testing.

Once authorized, vehicles are noted in a special registry and must feature a special plate. The testing must be overlooked by a supervisor with relevant experience: pursuant to Art. 10, Decree, he or she must be a holder of a driving licence for the involved vehicle category for at least five years, and must have proof of education and experience, involving, at least, 1.000 km of autonomous driving experience. The supervisor must be able to switch from manual operation to automated one, and the other way, at any moment: vehicles, therefore, that do not feature at least a steering wheel, throttle and braking commands cannot be tested on Italian roads.

Furthermore, Art. 20, Decree, provides for the establishment of an Osservatorio per le Smart Road ed i veicoli connessi e a guida automatica, with extensive research, consultation and examining powers related to the introduction of advanced devices, features and infrastructures relevant for road transportation.

The Netherlands. Testing self-driving vehicles on Dutch roads has been possible since July 2015, when the Government adopted a Decision,[333] allowing tests to be carried out through a specific exemption from the Road Transport Agency, provided that driver was inside the vehicle, ready to take over control if necessary. The new technology needed to be tested on

---

[331] Legge 27 dicembre 2017, n. 205, Bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020. (17G00222) (GU Serie Generale n.302 del 29-12-2017 - Suppl. Ordinario n. 62), available at the following link: http://www.gazzettaufficiale.it/eli/id/2017/12/29/17G00222/sg.

[332] Decreto 28 febbraio 2018, Modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni di Smart Road e di guida connessa e automatica (18A02619) (GU Serie Generale n.90 del 18-04-2018), available at the following link: http://www.gazzettaufficiale.it/eli/id/2018/04/18/18A02619/sg.

[333] 248 Besluit van 15 juni 2015 tot wijziging van het Besluit ontheffingverlening exceptionele transporten (ontwikkeling zelfrijdende auto) Available at the following link https://zoek.officielebekendmakingen.nl/stb-2015-248.html

a closed area, and the Road Transport Agency was responsible for making sure that testing was not against the public safety through a risk assessment, also by determining which was the most suitable test site and whether additional requirements are necessary.

On 24 February 2017, the Dutch Government enacted The Autonomous Vehicles (Trials) Bill,[334] which further removes legal barriers to testing, allowing trials with autonomous cars without a driver on board, and enabling autonomous transport to be tested on a wider scale. Under the said bill, manufacturers are able to apply for permits to test vehicles that are controlled remotely by a human operator on public roads

The bill amends the Road Traffic Act by adding two new subsections to article 149a of the Act that expands a series of exemptions «to the extent necessary to conduct experiments with automated systems in vehicles», while the provisions on supervision, enforcement, and criminal responsibility remain unaffected. Under amended the Road Traffic, the Road Transport Agency, working in collaboration with the Institute for Road Safety Research, the road authority and the police, decides in advance where, and under what conditions, self-driving vehicles can be tested. Permits may, for example, stipulate that the manufacturer must take measures to warn other road users that the vehicle is remotely controlled. In the interests of road safety, motorists could be informed of the times and locations at which they might encounter a driverless vehicle on the road. The road tests will help the infrastructure minister decide whether regulations need further amendment to cater for new developments. This approach ties in with the government's wish to futureproof regulations by removing obstacles to innovation.[335]

Spain. Testing of CADs in Spain has been allowed since 2015, when the Subdirección General de Gestión de Movilidad (SGGM), belonging to the Dirección General de Tráfico (DGT) issued the Instruction 15/V-113 on the authorization of tests or research tests carried out with automated driving vehicles on open roads to general[336] (henceforth, Instrucción)

The aforementioned Instrucción clarifies three classes of requisite that must be complied with i) by the subject who aims to achieve the authorization, ii) by the vehicle which is to be certified, and iii) by the conductor who is going to drive the automated vehicle.

Only a limited number of subjects is entitled to obtain authorization, namely autonomous vehicles manufacturers, official laboratories, autonomous systems manufacturers, universities and research consortia.

As far as the requirements burdening vehicles themselves are concerned, a compulsory insurance coverage is required, as well as positive result after a detailed check performed either by Spanish or by EU accredited bodies, according to the Annex II, Instrucción, protocol.

This detailed check is divided into three parts: the first stage involves examination of papers provided by the subject who seeks authorisation – among which a detailed risk analysis –, the second implies an inspection of the vehicle, while the last one is based on dynamic assessment.

---

[334] Public Road Self-Driving Vehicles by Virtue of Experimental Testing Law, Binnenlands Bestuur (Feb. 27, 2017), information available at the following link: https://www.internetconsultatie.nl/experimenteerwet_zelfrijdendeauto/details.

[335] https://www.government.nl/latest/news/2017/02/24/driverless-cars-on-the-roads-. For further information, also see: www.loc.gov/law/foreign-news/article/netherlands-legislation-to-allow-more-testing-of-driverless-vehicles/.

[336] Instrucción 15/V-113, Asunto: Autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada en vías abiertas al tráfico en general, available at the following link: www.dgt.es/Galerias/seguridad-vial/normativa-legislacion/otras-normas/modificaciones/15.V-113-Vehiculos-Conduccion-automatizada.pdf.

Moreover, drivers must be aware of the tested vehicle's performance and technology, fit for driving. The driver is considered responsible for the vehicle's circulation at any time, and he must be able to be in full control of the vehicle at any time.

This latter issue, as well as the dynamic assessment characteristics, make it impossible to test vehicles which do not feature the implements necessary for the driver to get back to non-automated operation. Indeed, activation of the override mode must be possible at all times, through both the steering wheel, the throttle and the braking pedal: these three features are compulsory on every vehicle.

In order to obtain authorization, it is necessary to file an application to the SGGM, and provide a dossier featuring at least a short description of the technology upon which the vehicle is based, its safety systems and autonomy level, as well as the relevant education of drivers, exact identification of the area in which the testing procedure is envisaged, and testing protocols, and finally a certificate showing the aforementioned positive check result.

The SGGM remains entitled to amend or cancel authorisations, whether this might be advisable, pursuant to Art. 6, Instrucción.

When testing CAD, any issue or incident must be immediately communicated to the SGGM.

Austria. In Austria, tests of automated vehicles are regulated by the Ministry's Automated Driving Regulation (AutomatFahrV1)[337] which states that manufacturers, system developers and research institutes can submit an application in order to obtain a testing-permit for i) autonomous minibus, ii) motorway pilot scheme with lane-change, and iii) self-driving military vehicles.

The Regulation permits autonomous vehicles on public roads for the purposes of testing, provided that they have been sufficiently tested in advance, and that following documents are transmitted to the Federal Minister of Transport, Innovation and Technology (Bundesministerium für Verkehr, Innovation und Technologie, henceforth, BMVIT): i) details of the planned application; ii) name of the testing organization, iii) contact person and contact details; iv) details of the driver of the vehicle to be used for test drives; v) identification of the vehicle to be used for test drives; vi) written confirmation of insurance coverage of the activities performed during the test, according to the provisions of the motor vehicle liability insurance law 1994 (KHVG 1994, BGBl. Nr. 651/1994); vii) sum of the total number of real, virtual and experimental kilometres tested by the system; viii) beginning and end of the planned trial period; ix) planned test track; x) Demand for infrastructural requirements.

Under Austrian law, interested parties can submit a standardized test application to the contact point for automated driving (AustriaTech), which will make an initial assessment of permissibility according to the Regulation, or any necessary amendment to the Regulation, respectively. An independent Council of Experts, with extensive interdisciplinary expertise, also provides advice. The evaluation by the Council of Experts takes place on a quarterly basis. If the test case mentioned is not covered by the existing Regulation, it is possible to incorporate the case by amending the Regulation. The BMVIT will issue a temporary permit (generally for 3 month) on the basis of the test application and offer advisory expertise. After the permit period is expired, a report shall be issued to BMVIT, presenting, in particular, the critical situations or accidents, which might have occurred during the test drives particular. If the application refers to testing possibilities for vehicles or functions which are not currently regulated in accordance with AutomatFahrV, then the BMVIT may decide to

[337] 402. Verordnung des Bundesministers für Verkehr, Innovation und Technologie über Rahmenbedingungen für automatisiertes Fahren (Automatisiertes Fahren Verordnung –AutomatFahrV), Ausgegeben am 19. Dezember 2016, available at the following link:
https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2016_II_402/BGBLA_2016_II_402.pdfsig.

start the procedure to amend the regulation in order to accommodate the case within the said framework[338].

A non-binding code of conduct for testing was published by the BMVIT,[339] to promote responsible testing and provide supplementary guidance for organizations in addition to all appropriate statutory provisions, official procedures and other requirements.

Germany. As it will be further discussed in §0, Germany has adopted a law specifically authorizing driving CADs up to level 4 SAE. However, before that, special permissions for testing purposes could be obtained for certain automated driving functions of vehicles which were not permitted by extant legislation. According to the new law[340], a driver must be sitting behind the wheel at all times, and shall be ready to take back control if prompted to do so by the autonomous vehicle. The driver bears the responsibility for accidents that take place under his or her watch, unless the damage was caused by a defect while the self-driving system was in charge, as the manufacturer will be responsible instead. Additionally, the legislation requires the that black box is installed in the car, recording whether the human or the system is in charge of the driving.

In order to perform trials, a special permission shall be granted, subject to a detailed case-by-case analysis by the competent authorities. For this purpose, Germany set a specifically designate location, the A9 motorway in Bavaria, equipped with the digital A 9 motorway test bed, enable the testing of car-to-car and car-to-infrastructure communication through sophisticated sensor technology, high-precision digital maps and real-time communications, to reflect, analyse and support the increasing automation and connectivity of modern vehicles, thus allowing an appropriate infrastructure for industry and researchers to conduct trials. Due to the success of this experience, Germany intends to develop other test beds in cities – such as Ingolstadt – highways, and well as a combination of the two, as in Baden-Wuerttemberg.

Germany Federal Ministry of Transport and Digital Infrastructure advocates for the need to close gaps in the field of testing to be potentially concluded by mid-2019[341].

***Sweden*.** The Swedish Road Traffic Ordinance[342] is worded generally and provides room for exceptions to general provisions – such as the rule according to which the driver has to maintain control over the vehicle –, and therefore does not represent an obstacle for testing vehicles with a high degree of automation on public roads; furthermore, if the vehicles fail to meet the technical requirements set for its roadworthiness, the Vehicle Act and Vehicle Ordinance allow the Swedish Transport Agency to grant exceptions on the vehicles' equipment for the trials. In May 2017 The Swedish Government has adopted an ordinance setting the requirement that companies have to meet in order to obtain the relevant permit from the Swedish Transport[343]. The ordinance requires the presence of a physical driver in or outside the vehicle and provides for fines for those who conduct trials without a permit. Indeed, documents obtained by Swedish website DI Digital reveal that autonomous cars will be allowed for testing purposes on motorways and streets in the Gothenburg area under certain conditions. The presence of a trained driver that constantly keeps at least one hand

---

[338] Further information can be found at the following link:
https://www.bmvit.gv.at/en/verkehr/automated/framework/publicroads.html
[339] Code of Practice, Automated – Connected – Mobile Ministry for Transport, Innovation and Technology, available at the following link
https://www.bmvit.gv.at/en/verkehr/automated/framework/codeofpractice.pdf
[340] Gesetz vom 16. Juni 2017 (BGBl. I S. 1648).
[341] German Federal Ministry of Transport and Digital Infrastructure «Action plan automated and connected driving», available at the following link
[342] Trafikförordning (1998:1276), available at the following link:
http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/trafikforordning-19981276_sfs-1998-1276.
[343] See https://www.government.se/articles/2017/05/government-paves-the-way-for-self-driving-vehicles/.

on the wheel is officially required by Swedish Transport Agency. Furthermore, cars are not allowed to exceed 60 kilometres per hour when the self-driving features are activated.

Other MSs. In addition to the MSs which falling within the premise of the comparative study of this report, others have also regulated testing of CADs. In Finland, for example, an enterprise, agency or other organization engaged in research and development of automated vehicles may apply to Trafi for a test plate certificate, which entitles the bearer to test automated vehicles, up to level 5 SAE, to a limited extent and on a temporary (1 year, renewed automatically) basis, both in road traffic and off-road, without being liable for car and vehicle tax on that vehicle. During the tests, there has to be driver either inside or outside the vehicle, who is responsible for the correct performance of the trial and might be held liable in case an accident occurs. When applying for a test plate certificate, the applicant must also enclose a trial plan that includes i) a general description of the trials, ii) technical specifications of the test vehicles, iii) information on the road area where the trials are intended to be conducted, iv) proof of insurance cover for third party liability, v) description of how road safety will be ensured.

The test plate certificate holder must submit a report to Trafi on the trial results, describing, for example, how the trial plan was implemented and what kind of deviations from the plan were encountered. [344]

3.2.3. Testing cycle and techniques

Fractioned testing. Differently from verification testing – which, in principle, looks at the complete system and action of the CADs – performance and reliance tests assess and evaluate all, some or even single steps of the sense-plan-act robot control[345]. This is fundamental in order to ensure its full functionality and safety, since the overall driving act depends on a series of variables that, although related to one singular component or feature, might alter the system as a whole. Isolating a step during the testing procedure can help evaluate the different parts of the system and track down potential issues or causation, which is very relevant during the product development. For example, dedicated tests are commonly performed to check if the performance of the camera sensor varies depending on the different light conditions, such as bright sunlight, darkness or artificial light. Similarly, communication between vehicles should be tested on its own, as it represents a way in which CADs sense their environment and thus elaborate their driving system.

For this purpose, testing is performed for (and can thus be classified according to) the level of specificity of the element or step under control: component, sub-component and system.

- *Component testing*: a single component is isolated to be tested without interaction or disturbance of other components. For example, a camera sensor is tested in order to evaluate how it detects and classifies other road users, like pedestrians and cyclists.
- *Sub-system testing*: several components are tested together to evaluate the combined performance and interaction. For example, the complete set of detection sensor, including cameras, radars and LIDARs are evaluated together to see how it represents the overall environment.

---

[344] Further information on the procedures for obtaining a testing plate in Finland can be found at the following link https://www.trafi.fi/en/road/automated_vehicle_trials.

[345] The sense-plan-act (SPA) paradigm constitutes the basic structure of the robot programming and behaviour, being the predominant robot control methodology through 1985. «Sense» refers to the robot's ability to gather important information about its environment, like the presence of obstacles or navigation aids; «plan» represents its ability to take the sensed data and figure out how to respond appropriately to it, based on a pre-existing strategy; while «act» consist of the capacity to actually act to carry out the actions that the plan calls for. For further information, see David Kortenkamp and Reid Simmons, "Robotic Systemic Architectures and Programming," in *Springer Handbook of Robotics*, ed. Bruno Siciliano and Oussama Khatib (Wien: Springer, 2008).

- *System testing*: the total system is tested to verify that it behaves according to the designed functionalities. For example, the final CAD is tested to assess how it performs its driving function, handles obstacles and contingencies arisen in complex real-life scenarios, and avoids accidents with pedestrians and cyclists.

Techniques. Different testing tools are used to evaluate the performance of CADs:

- *Virtual testing*. CADs' components and complete systems are modelled and evaluated in a virtual environment, where their performance is simulated through several tools – such as simulation software or platforms, which display model creation, problem set-up, and performance analysis features –. Virtual testing has the advantage of being safe (as no human is physically involved in the trials), non-destructive and allowing a large amount and variety of tests to be performed. Furthermore, it also allows to test components and systems through small and/or isolated variations, where the other parameters are kept the same.
- *Combination of virtual and physical testing*. Several gradations of combined virtual and physical testing are available, ranging from situation where only limited physical testing is conducted, while mostly relying on virtual testing, to the opposite situation, where only few tests are virtual. This is often referred to as Hardware in the Loop (henceforth HiL) testing, where an actual piece of product hardware is being tested, while other components are modelled and executed in a virtual environment. HiL tests comprises a large variety of tests for different components/parts of the system. An example is the use of electric control unit (ECU) in a virtual environment, where test is performed by providing virtual signals to the ECU and evaluating the outputs, in order to see how the system handles certain situations. Likewise, in the case of driving simulators, the driver drives in a virtual world to evaluate the interaction of ADAS and CADs with human drivers.
- *Physical testing*. Physical testing consists in trials conducted on the component, *subsystem* or system, in real-life scenarios. Typically, professional test drivers or automated test systems execute defined scenarios either on a dedicated testing ground or on public roads. Faults occurring during these tests are then recorded in order to understand and repair the defect.

***Testing Environments*.** While virtual testing is mostly performed in-house, or other laboratories (such as those offered by a DIH), physical testing (or its combination with virtual testing) is performed in different environments.

- *Controlled environment*. The most controlled way to perform a trial – hence the first type of physical test generally undergone – is to develop in a controlled environment, where the external disturbances are limited, and where specific situations can be (re)built to evaluate the system against peculiar conditions.
- *Indoor*. Likewise, tests may be performed indoor as to reduce outdoor-specific interferences, such as climate and weather conditions, on the trial. However, due to the spatial domain required by CADs, from low speed to high speed, it is often only possible to execute a limited set of tests indoors.
- *Outdoor*. On the contrary, a large variety of CADs tests take place outdoor. This is often done on a test track with well described parameters, like road conditions, road markings and predefined behaviour of road participants. To be able to perform the test with high accuracy, thus allowing experimental reproducibility, external robots can be used to control the CADs, but also the other road users, including steering, throttle-brake robot to control a vehicle, or platforms to move impactable dummies representing cars, pedestrians and cyclists. Both legal and consumer test organizations (for example, in Europe, the Euro NCAP and, in the USA, the NHTSA

– US NCAP) have published well defined tests, that are used to evaluate the safety of vehicles[346].

- *Public road.* As the CADs need to be able to cover a large set of scenario with a vast array of variables and variations, tests on the public road are fundamental to assess performance and reliance of the vehicle at an advanced stage of development and testing, as it is the only real occasion in which CADs can be confronted with the different, non-pre-determined situation which autonomous vehicles are meant to encounter in real-life, as it will difficult/close to impossible to control all variables on the public road, such as the behaviour of other road users. However, this creates specific concerns for safety and security of the latter, and creates technical problems as far as the possibility of tracking, analyzing and reproducing the trials is involved. For this reason, public road tests may be supported by additional logging of the so called «ground truth» - information collected on location – of the other road users, in order to be able to reconstruct the exact situation afterwards[347].

  Different types of tests on the public road can be performed:

  - *Real world driving*. The most basic public road test would be to evaluate a vehicle by driving on the public road and gathering information of the sensor/system performance.
  - *Field Operational Test* (FOT). A Field Operational Test is defined as «a study undertaken to evaluate one or more functions under normal operating conditions, in environments typically encountered by the host vehicles, using quasi-experimental methods»[348], aiming at allowing comparative-assessment of the effect that the function or functions have on traffic, whit a baseline condition during which the function is not operating. Official European Commission documents define FOT as large-scale testing programs aiming at a comprehensive assessment of the efficiency, quality, robustness and acceptance of ICT solutions used for smarter, safer and cleaner and more comfortable transport solutions, such as navigation and traffic information, advanced driver assistance and cooperative systems[349].
  - *Naturalistic Driving Study* (NDS). Naturalistic Driving observation refers to studies undertaken using unobtrusive observation when driving in a natural setting. Both, Naturalistic Driving Studies and Naturalistic FOTs use this type of observation. Naturalistic Driving observation is a new approach among already applied traffic research methods. In NDS, the driver becomes unaware of the observation as the data collection is organized as discreet as possible and preferably drivers use their own vehicles. The data is used to study the relationship between driver-, vehicle-, and/or environment factors with crash risk[350].

Despite their own peculiarities, the tools above described are operational phases, where vehicles are driven on public roads in real traffic conditions, and hence share the same methodology. In Europe the FESTA methodology has been developed. To improve significance, comparability and transferability of available FOT results at the national and

---

[346] For further information, see https://www.euroncap.com/en/press-media/press-releases/testingautomation/, and https://one.nhtsa.gov/Vehicle-Safety/Test-Procedures.

[347] Ground truth allows image data to be related to real features and materials on the ground. The collection of ground-truth data enables calibration of remote-sensing data, and aids in the interpretation and analysis of what is being sensed. In machine learning and statistics ground truth is used for checking the results against the real world.

[348] FESTA Project: 'FESTA Handbook Version 2. Deliverable D6.4 of Field operational teSt supporT Action', 2008. Available at http://www.its.leeds.ac.uk/festa/

[349] http://fot-net.eu/context/, last access 27.11.2018.

[350] Y. Barnard, F. Fischer, and M. Flament, "Field Operational Tests and Deployment Plans," in *Vehicular Ad Hoc Networks*, ed. C. Campolo, A. Molinaro, and R. Scopigno (Cham: Springer, 2015).

European level, a common European FOT methodology has been developed. The European Commission funded project FESTA developed a handbook on FOT methodology which gives general guidance on organizational issues, methodology and procedures, data acquisition and storage, and evaluation.[351] Design, execution, analysis and assessment of public road testing through FOTs, NDS, and other projects throughout Europe mainly rely on the said methodology.

Human driver. Except for SAE level 5 (§3.1.1), the human driver plays a fundamental role in the driving system and thus needs to be taken into account when testing CADs. This can be done in at different level and with different tools as described above. For example:

- *Dedicated driver simulators* allow the human to drive in a virtual world, where his interaction with CADs is evaluated. For example, how is the transition of control handled when a SAE level 4 vehicle changes from autonomous driving to manual driving.

- *Naturalistic Driving Studies* (NDS), already mentioned above, provide insight into driver behaviour during every day trips by recording details of the driver, the vehicle and the surroundings through unobtrusive data gathering equipment and without experimental control. The EU FP7 project UDRIVE is an example of an NDS[352].

3.2.4. Identification of risks through testing and risk assessment

Risk assessment and evaluation. When testing the performance and reliance of CADs, manufacturers have to identify the potential hazards involved in their use, and the probability of their realization, as doing so enables them to prevent and limit such risks.

Indeed, the major argument for the introduction of CADs is that they have the potential of increasing road safety, since the majority of accidents are caused by human errors (§3.1). However, this does not mean that CADs will be intrinsically risk-free. In particular, two types of risks shall be taken into account, namely; (i) risks that traditional vehicles already pose, which CADs cannot radically eliminate, but that, due to the autonomous nature of the device, might materialize differently, and in a more articulated way; and (ii) risks which were not brought about by traditional vehicles, and are entirely due to the autonomous and connected nature of the devices. Some of those risks can be identified the design stage, despite difficult to assess – for example, due to a lack of statistically relevant data –, while others might may be unknown at the time of defining the functional requirements, and rather manifest themselves during the life-time of the device.

Since the aim of this section if to give an account of the risks specifically brought about by the autonomous nature of CADs, the following taxonomy will merely refer to the type of risks involved, without specifically distinguishing between traditional risks and brand-new risks; reference to their nature, and the consequences it creates for testing purposes, will be developed when needed.

Against this background, three major hypotheses, which are strictly intertwined with one another, and need to be taken into account are:[353]

---

[351] As part of the FOT-Net project, the FESTA Methodology has been revised. For further information, please see fot-net.eu/; and 2doubmisw11am9rk1h2g49gq.wpengine.netdna-cdn.com/wp-content/uploads/sites/7/2017/04/FOT-Net-D5.4-Updated-Version-of-the-FESTA-Handbook-v1-1.pdf.

[352] UDRIVE is the first large-scale European Naturalistic Driving Study on cars, trucks and powered-two wheelers. It aims to collect naturalistic data - - including video data showing the forward view of the vehicle and a view of the driver, as well as geographic information system (GIS) data - on passenger cars, trucks, and powered two-wheelers, as to bring knowledge in the various research areas well beyond the current state-of-the-art. For further information, see http://www.udrive.eu/.

[353] Jansen et al.

- *Machine-learning risks*;
- *Cybersecurity risks*;
- *Driving environment-related risks*;
- *Driver-related risks*.

Machine learning risks, cybersecurity risks have been extensively described in §2.5.4, and the basic description of how they arise still holds true in the case of CADs, and will not be repeated, unless necessary for the purpose of explaining how they shall be taken into account for testing.

Machine learning risks. ML consist in the construction of algorithms that allow computer systems to «learn», by giving them the ability to acquire and make prediction from data, being able to develop itself over time. In CADs, a series of different ML algorithms (decision matrix algorithms, cluster algorithms, pattern recognition algorithms and regression algorithms), allow the car to drive autonomously through a four-step-approach: (i) detection of surrounding objects; (ii) identification and recognition; (iii) localization and movement prediction; (iv) decision-making and action.

Whether a car needs to brake or take a left turn is based on the level of confidence these algorithms have on recognition, classification and prediction of the next movement of objects.

However, problems may arise: the images acquired by the system may not be clear due to a hardware problem (e.g. faulty camera), which makes it difficult for the CAD to locate and detect objects. Other times, the algorithms might fail to categorize and report it to the system, because of discontinuous data, lack of data or low-resolution images.

These problems may be limited or overcome by improving the algorithm systems and the connected hardware features, as well as by reinforcing security of the system against any form of cyber failure or attack which might affect its functioning. In particular, clustering algorithm and regression algorithms helps categorizing data and creating statistical models for efficient detection and learning.

As far as testing is concerned, ML features require trials to be set and performed as to allow maximum collection of data and driving scenarios. In order to ensure safety of testing itself, especially when performed in public places, such long trials must have already been done and information achieved through simulation processes.

Cybersecurity risks. Cybersecurity is the practice of defending networks, hardware and software from malicious attacks. Cybersecurity risks may be of various kinds. They may be caused by malware, hacking, technical and human errors; they can be associated with flaws in communication, flaws in software, and flaws in the sensors of the robotic system. Testing of robots thus should include testing whether the robots are able to cope with information and network security vulnerabilities.

Driving environment-related risks. A series of risks, which go beyond, the mere unpredictability of scenarios which we referred to while addressing ML risks. Indeed, unfit conditions of the lane, unclear marking sings, connectivity problems, and the overall networks and physical infrastructure may at times prove inadequate to accommodate the correct performance of CADs, as such conditions may erode the vehicles' stability and cause malfunctioning. This has a twofold effect on testing: in order to ensure safe testing conditions, testing ground should be built or selected as to ensure that the conditions are adequate for the vehicles functioning.

For this purpose, it should be ensured that the CADs performance is not affected by disturbances from external sources, or the system should detect this and react on it appropriately, for example stop if safe driving is compromised.

Driver-related risks. The major risk associated with driving is that of a collision of the vehicle with other road users or infrastructure.

This is what we can consider as a traditional risk, which has been addressed by (i) setting specific traffic rules which aim at coordinating driving and imposing precautionary measures, hence, addressing the behaviour of road users themselves; and (ii) by setting specific technical requirements posed by international standards, which not only serve the purpose of demonstrating compliance with applicable legislation – as it will be further analyzed in §3.2.8 – but also offer guidance on how to design and implement functional specifications (e.g. the steering, braking, sensors etc.), and constitute a benchmark against which validation testing shall be performed.

Especially in the near future, CADs will most likely display degrees of automation ranging from SAE level 2 to 4, thus requiring the vehicles to drive in two different modes, one in which the driving function is performed primarily or entirely by the human driver, and the other where the system instead is in charge. This gradual transfer of responsibility from the driver to the car is complex, as additional undesired risks may arise despite a fully-fledge functional and reliable device, precisely because of the residual driver's error, and the way automation affects its driving skills. Indeed, as it already occurred in different jurisdictions (see §3.2.2), the driver might misjudge the different mode of operation of the vehicle, thus adopting outright dangerous behaviours. This could be mitigated by ensuring clear and thoughtful information to the user, so that he or she are aware of the limits and features of the autonomous functions, and of the necessity for them to ready to take back control of the car when necessary.

Nevertheless, even if this might not be sufficient, as the very time required even for an alert driver to take back control might still exceed that necessary for avoiding collision. This can be tested and mitigated both by developing clear and effective human-vehicle interfaces, and by adopting degradation-strategies which might compensate for the lack of prompt human intervention. Ultimately, this might even lead towards opting for more automated versions of CADs.

3.2.5. Bottlenecks and industrial trends

Types of bottlenecks. As already indicated in the chapter on IR, bottlenecks may be classified according to their nature, as technical bottlenecks – caused by the limits of the technologies available, or by the methodology used in testing in manufacturing –, or regulatory bottlenecks – caused by the negative incentives brought about regulatory framework.

In the following paragraphs, both technical (§3.2.5.1) and regulatory (§3.2.5.2) challenges of CADs testing, will be examined together with the solutions adopted by stakeholders and policymakers to overcome them.

3.2.5.1. Regulatory challenges

Even if Europe is quite advanced in the implementation of testing for CADs, the study identified a series of relevant regulatory bottlenecks, hindering testing – and thus future development and marketing – of CADs.

Limits to testing of fully automated vehicles. Firstly, in many MSs, as well as under the VCRT – as interpreted by the majority of the contracting parties – it is not allowed to testing

vehicles on public roads without a driver in control – corresponding to level 5 SAE –, thus substantially limiting technological development and slowing the roll out of CADs.

Regulatory fragmentation. Different testing procedures among MSs make the overall implementation of testing on roads difficult for stakeholders, as it creates a fragmentation of the legal framework, under which some companies may not be able to test their vehicles in the MSs of establishment, or might have comparatively disadvantaged conditions for obtaining the authorization and performing the trials, thus impeding them to test CADs, or forcing them to resort to another country for that purpose.

Obstacles to cross-border testing. Different rules substantially impede or limit the availability of cross-border testing, which is particularly problematic since road mobility is itself cross border, and thus its performance and reliance needs to be assessed against cross-border conditions.

In order to overcome such problem, several on-going cross-border testing projects are being initiated in the Scandinavian Member States (e.g. Aurora and NordicWay in Finland and Sweden) and the French-German digital testbed between Metz and Merzig respectively[354]. However, interviews showed that more initiatives in that sense are needed, and that communication between projects should be encouraged.

At international level, the UNECE continues to address the topic trough the Global Forum for Road Traffic Safety (WP.1) group, that is the only permanent body in the United Nations system that focuses on improving road safety. The UNECE's World Forum for the Harmonization of Vehicle Regulations also continues its ongoing work on the development of technical provisions for automated vehicles, and at the first meeting of its newly established Working Party on Automated/Autonomous and Connected Vehicles (GRVA - 25-28 September 2018), addressed, inter alia, technical requirements, cybersecurity and software updates, and innovative testing methods, in particular the use of simulations[355].

In addition, there is an ongoing draft resolution on the deployment of highly and fully automated vehicles in road traffic[356].

3.2.5.2. Technical challenges

Despite the large variety of techniques used to assess the performance and reliance of CADs still tests still face several technical challenges.

Indeed, various projects around the world are looking into the challenges related to CADs testing, trying to allow more efficient and reliable techniques and tools. Within the European project CARTRE[357] – a Coordination and Support Action aiming to accelerate development and deployment of automated road transport by increasing market and policy certainties – two position papers have been created to discuss different topics related on, respectively,

[354] Available at: https://ec.europa.eu/digital-single-market/en/cross-border-corridors-cooperative-connected-and-automated-mobility-ccam.
[355] Further information. https://www.unece.org/info/media/presscurrent-press-h/transport/2018/unece-adopts-resolution-on-the-deployment-of-highly-and-fully-automated-vehicles-in-road-traffic/doc.html
[356] Available at: http://www.unece.org/trans/themes/transtheme-its/selfdriving/next-steps.html
[357] See https://connectedautomateddriving.eu/about-us/cartre/

«Safety validation and roadworthiness testing», and «Policy and regulatory needs, European harmonization»[358].

Technical challenges can affect both the function of testing – i.e. its ability to allow risk assessment and evaluation –, as well as the safety of testing itself, especially when performed on public roads.

Availability of data and Predictiveness of simulation tools. It has been stated that it would require unrealistically long time to physically test-drive CADs, to take into account every combination of sensor input and driving scenarios[359]. Indeed, the amount and variability of scenarios that a CAD should be tested against in order to ensure safety and – before that – to train its ML features, is so high that it is fundamental to elaborate alternative ways as to achieve adequate results in that respect.

However, in order to use virtual testing, it is essential to know to what extent the simulation is representative of the physical vehicle and how well the model can predict behaviour. Creation of accurate models that cover all phenomenon of the system is still very challenging, and one of the major difficulty is to identify what CADs should be tested against, taking into account representativeness and completeness of possible scenarios.

Indeed, different projects – PEGASUS, L3Pilot, ENABLE-S3 and ISO/TC 22/SC 33/WG 9 Test scenario of autonomous driving vehicle – are addressing this issue, in particular focusing on elaborating tools which could help in this regard. One solution which has been put forward is the development of databases, collecting information that can be used to select the scenarios which CADs need to be tested against. This information comprises data which is generally structured, processed, classified into a uniform description, but also virtual data (traffic and driving simulation data), accident data and even expert knowledge, in order to ensure representativeness and completeness of the database

The creation of such database thus needs to deal with:

- the amount of data which needs to be structured, processed, classified as well as stored, to ensure representativeness and completeness;
- the selection of a number of representative scenarios, which could help companies to determine which tests need to be performed virtually/physically;

Despite of great theoretical and practical utility, the creation of databases collecting and offering such information is still ongoing and has not reached a sufficient degree of availability and of quality of the information provided. Hence, further research and investment in this field is needed.

***Human fall-back*.** Failure of ADAS or CADs during testing could result in severe damage to people and properties and therefore should be done only with caution, and with fall-back systems into force. However, test with a 'safety driver' – where a human driver can resume control in case the system fails – do not necessarily offer the adequate level of safety, because the humans' ability to monitor the system is limited. Especially when the system

---

[358] *Position Paper on Safety Validation and Roadworthiness Testing* (Munich: CARTRE - Connected and Automated Road and Transportation Deployment for Europe, 2018).; *Position Paper on Policy and Regulatory Needs, European Harmonisation* (Munich: CARTRE - Coordination of Automated Road Transport Deployment for Europe, 2018).

[359] See Nidhi Kalra and Susan M Paddock, *Driving to Safety. How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?* (Rand, 2016). See esp. p. 1, «Autonomous vehicles would have to be driven hundreds of millions of miles and sometimes hundreds of billions of miles to demonstrate their reliability in terms of fatalities and injuries».

improves, and failure is rare, a human driver's attention might drop and hence the driver might not be able to correct the failure.

Robustness to disturbances. It should be ensured that CADs' performance is not affected by disturbances from external sources, alternatively, the system should detect this and react on it appropriately, for example stop by coming to a halt, if safe driving is compromised.

The stakeholder consultation performed within Task 2[360] – which strongly complements and feeds the present research on CADs – showed that 79% of respondents believe that a European system for sharing testing data, conditions, use cases and best practices should be developed, while 55.2% of the respondents support the idea of cross-border prototype testing, to ensure interoperability and connectivity between MSs, also considering the nature of mobility – which is intrinsically cross-boarded – as well as its role for the purpose of achieving a single market in EU.

Moreover, 51.8% of the respondents believe that transparent legislation to ensure testing of prototypes on road is missing. This outcome relates to the fact that in some countries it is challenging for stakeholders interested in testing on roads, to understand the conditions and rules to receive testing authorisation.

3.2.6. Conclusions and recommendations

Legal framework. The amended Vienna Convention on Road Traffic allows automated driving, provided that the technologies used comply with the UN regulations, or can be overridden by the driver.

Many MSs – even before such amendment – have regulated testing of CADs on public roads, according to different requirements and procedures. The majority only allow high automation, while others also accommodate trials of fully autonomous vehicles (e.g. Sweden), or plan to do so.

Business practice and testing techniques. As for IRs, there is no legislation at EU or MSs' level, prescribing how testing shall be performed. Manufacturers test both the subcomponents and the final products, relying on different techniques, with both virtual and physical testing. Trials take place in controlled environments, indoor, outdoor, and in public roads, with different degrees of involvement of the human driver and bystanders.

Trails shall take into account CADs-specific risks, in particular those related to machine learning, cyber-security, as well as those connected to the unpredictability of the driving environment (as real life trials on public roads) – which raises safety concerns and exacerbates issues of experimental reproducibility. Measures against a possible fall back of test-drivers should also be adopted.

Bottlenecks. Given that the current legal framework is highly fragmented, allowing diverging levels and types of testing, and that different procedures and requirements are set across MSs – especially for trials on public roads –, the current regulatory state of art could benefit from intervention.

Indeed, multiple, unclear or non-transparent requirements could discourage manufacturers and other relevant players to perform trials in a given country. Strong fragmentation of the market uptake and lack of cross-border testing could affect the optimal usage of CADs across borders, thus hindering the future roll out of CADs.

---

[360] See VVA, SSSA, and TNO, *Scenarios and Conditions for the Implementation of Cad and Proactive Mapping of Policy Measures. Interim Report 2* (European Commission, 2018).

Adoption of uniform EU rules on testing. In order to address these issues, uniform and clear requirements and procedures for testing shall be adopted at the EU level, expressly allowing higher degrees of automation.

Despite soft-law instruments – such as recommendations, monitoring and analysing the different interpretations of testing requirements, cross-fertilisation actions etc. – shall be welcomed, this study suggests that hard-law alternatives should be preferred, provided that the principles of proportionality and subsidiarity are respected, as this would better achieve a legal common-playing-field, ultimately facilitating testing, both within and across MSs' borders.

Regulatory ad-hoc derogation from current legislations. In order to facilitate testing on public roads, the creation of Tokku zones and regulatory sandboxes, derogating from regulation which impedes and hinders testing of CADs, would facilitate trials in real life condition, without excessive and disproportionate intervention on extant rules.

Research investment and cross-fertilization. the EU should establish stronger cooperation on testing across Europe, in order to further incentivize research and development of technological solutions – especially those related to simulation testing and elaboration of trial-scenarios –, and allow cross-fertilization among different activities.

In particular, the EU should foster the implementation of a European system for sharing testing data, conditions, use cases and best practices related to automated driving. As a complementary action, the EU could provide to SMEs with the possibility to perform consortium testing and participate in cross-border testing initiatives.
Certification

KEY FINDINGS

- CADs fall under the notions of road vehicles and thence need to be certified according to the type approval.
- Road vehicles (and advanced autonomous vehicles, as well) certification framework is based on conformity with UNECE Regulations and type approval, which always involves a notified body.
- UNECE Regulations have been adopted in order to accommodate the features of novel devices that have an impact on driving functions.
- As far as steering is concerned, UNECE Regulations allow and establish parameters for steering aids, while still forbidding totally autonomous steering.
- Automated braking functions, that prevent accidents and improve overall vehicle safety, are allowed by UNECE Regulations.
- UNECE Regulations concerning the lighting features, while allowing emergency lights to switch on automatically in case of danger, still do not allow automated operation of direction indicators.
- Overall, the type approval procedure does not seem perfectly fit for highly automated vehicles, because it is focused on a static evaluation, while AI applications evolve overtime and through their very functioning, benefitting from constant regular updates.
- Moreover, CADs' components interact with one another in more complex ways than what happens to regular components in traditional vehicles, and the most advanced technologies imply CADs interacting with one another and with the infrastructure.

- According to several stakeholders, therefore, type approval should be partially amended in order to foster a more streamlined and convenient approach, and many international bodies are pursuing studies in this way.

3.2.7. Introduction

Lack of CADs specific legislation. As far as conformity assessment and certification are concerned, autonomous vehicles and CADs are not provided with an *ad-hoc* legislative framework[361].

Certification of traditional cars. Indeed, road vehicles in general do not fall under the «New legislative framework» (§1.3), but their conformity assessment and certification are regulated according to a different model, that involves the incorporation of international law into EU law, itself an uncommon feature for European product safety regulation.

Absent specific regulation, the Framework Directive (FD, §3.1.1.1), conceived for traditional – non-autonomous – road vehicles applies to CADs, their components and systems.

The aim of the FD is on the one hand to replace MSs' legislation with a totally-harmonized Community approval system «for the purposes of the establishment and operation of the internal market»[362], on the other «to ensure that new vehicles, components and separate technical units put on the market provide a high level of safety and environmental protection»[363].

The FD is superseded by a Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (henceforth, RV)[364], entering into force on September the 1st, 2020.

The numerous relevant considerations[365] that led to the adoption of the RV, as phrased by its recitals[366], do not however openly include the need to address emerging technologies, such as CADs, that are not even directly mentioned in the text. Indeed, the rationales for the adoption of the regulation substantially equal those underpinning the directive[367].

The following analysis is primarily grounded on the FD, since that is the legislation manufacturers of CADs are currently required to apply and comply with. All observations in that respect would otherwise be prospective, and not supported by records derived from real-life application.

The FD makes reference to several bodies of EU law as well as to UN Regulations[368], provided by the World Forum for Harmonization of Vehicle Regulation[369] (henceforth, WP.29) of the

---

[361] https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en, last access October 1st, 2018.
[362] Whereas (2), FD.
[363] Whereas (14), FD.
[364] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (Text with EEA relevance.) PE/73/2017/REV/1, in OJ L 151, June 14th, 2018.
[365] Such as better market surveillance, clarification, stronger enforcement, neater delimitation of roles and responsibilities of operators in the supply chain, guaranteeing independence of authorities and third parties, preventing conflicts and improving alternative approval methods for niche markets, such as national small-series and individual vehicle approval.
[366] Whereas (4), RV.
[367] Whereas (1) states that «Internal market rules should be transparent, simple, consistent and effective, thereby providing legal certainty and clarity for the benefit of businesses and consumers"[367], therefore pursuing, according to Whereas (5), a «high level of safety and of health and environmental protection»[367].
[368] Annexes IV, «List of requirements for the purpose of EC type-approval of vehicles", and XI «Nature and provisions for special purpose vehicles», FD.
[369] WP.29 is an UNECE (see *infra*) working party in charge of creating and amending a uniform system of regulations for the design of vehicles, therefore enhancing international trade. For further information and resources, see

Sustainable Transport division of the United Nations Economic Commission for Europe (henceforth, UNECE)[370].

3.2.8. European legal framework: The Type approval

The type approval as unique conformity assessment procedure. Differently than many regulations belonging to the New Legislative Approach, the FD only provides one conformity assessment procedure for all kinds of products falling under its application, irrespective of any further characterization of the devices.

Vehicles are indeed classified according to different categories[371], yet, regardless of their features, only one system of conformity assessment is identified – namely the type approval model – that is to be applied to both whole vehicles, and vehicles at any stage of the building process, regardless of their size and nature[372].

The mutual recognition principle. The type-approval model is based on the mutual recognition principle, pursuant to which i) a manufacturer may apply for approval in any European Union country[373], and ii) once a vehicle, a component or a system is duly approved in a MS, all vehicles belonging to the same type can be registered – provided that they feature a certificate of conformity (see *infra*) – in any MS[374].

Third party assessment. At the same time, unlike other assessment procedures provided at European level[375], the type cannot be self- or in-house approved, but evaluation is always carried out by a national testing center.

The procedures. Pursuant to art. 3, n° 3 of the FD, the type approval is defined as:

> «the procedure whereby a Member State certifies that a type of vehicle, system, component or separate technical unit satisfies the relevant administrative provisions and technical requirements».

The same article, however, identifies three variations to the type approval, that differ according to both the number of certificates released along the procedure, the timing, as well as the content of application to be submitted. In such a perspective, a step-by-step type approval[376], a single-step type approval[377], and a mixed type-approval[378] are identified, among which manufacturers may freely choose (see art. 6, FD). Moreover, when incomplete

---

http://www.unece.org/trans/welcome.html, last access October 3rd, 2018. The 1958 Agreement constitutes the legal framework for the contracting parties, which agree on protocols and prescriptions for vehicles and their parts: as of now, there are more than 130 UN Regulations annexed to the Agreement. It is not necessary anymore to be a member of UNECE to be part of the Agreement, so that, as of now, besides the European Union and its Member states, also the whole of Russia, South Korea, Japan, as well as Australia, New Zealand and South Africa, among other countries, are part of the harmonised system, while United States and Canada are not, and in those countries a system based on self-declarations (and not on the evaluation by third parties) is employed.

[370] UNECE, established in 1947, is one among the five regional commissions directed by the United Nations, aimed at encouraging economic cooperation. As of now, it comprises 56 states, namely the vast majority of the European continent, the whole of Russia, some countries in the Middle East and central Asia. UNECE promotes policy dialogues, technical cooperation, negotiations of international legal instruments, developments of norms and regulations, exchange of technical expertise and best practices. For further information, see https://www.unece.org/info/ece-homepage.html, last access October 3rd, 2018.

[371] For instance, M and N that correspond to vehicles «designed and constructed for the carriage of passengers» and «for the carriage of goods» respectively (see art. A, Annex II).

[372] FD applies, e.g., to cars, vans, trucks, buses and coaches.

[373] Art. 6.6, FD.

[374] Art. 4.3, FD.

[375] For example, as far as machinery is concerned.

[376] Defined as «a vehicle approval procedure consisting in the step-by-step collection of the whole set of EC type-approval certificates for the systems, components and separate technical units relating to the vehicle, and which leads, at the final stage, to the approval of the whole vehicle» (art. 3.8, FD).

[377] Defined as which consists in «the approval of a vehicle as a whole by means of a single operation» (art. 3.9, FD)

[378] which is «a step-by-step type-approval procedure for which one or more system approvals are achieved during the final stage of the approval of the whole vehicle, without it being necessary to issue the EC type-approval certificates for those systems» (art. 3.10, FD).

vehicles are to be completed, a multi-stage type approval[379] applies, requiring the cooperation of the manufacturers of the different components[380] in the subsequent phases.

After the application, the technical services in charge – a body designated by the approval authority (see *infra*) to carry out tests and assessments[381] – are required to perform testing in order to assess the compliance of the given type with both EU and UNECE regulations. Virtual testing is also allowed, pursuant to Art. 11, FD, so long as the mathematical model reflects the complexity of the vehicle in combination with the requirements provided by the FD and applicable regulations, and the model is validated after a thorough comparison with actual test conditions, thus ensuring consistency. Moreover, «comparability of the results of the model with results of conventional test procedures must be proven»[382].

Approval is then granted by an authority, each Member State has to identify, that is competent for all certification procedures for vehicles, systems, and components or separate technical units (art. 3.29, FD).

In order to guarantee that every vehicle and/or component is made in accordance to the approved type, Art. 12, FD, requires Member States to take the necessary measures, such as an initial assessment, including control procedure evaluation, product conformity assessments, and continued verification arrangements[383].

Manufacturers issue a certificate of conformity to accompany every vehicle that is distributed on the market, and that allows the aforementioned principle of the mutual intra-European recognition.

3.2.8.1. Cont.: Type approval and CADs

The vast majority of the current road vehicle certification framework, which is applicable to all vehicles, regardless of their degree of autonomy, antedates the development of CADs.

It is therefore necessary **to analyze whether these advanced technologies may encounter possible bottlenecks in the FD-based system and in the formerly UNECE – now UN – Regulations, to whom reference is made**.

This task requires at first to analyze whether some specific regulations allow advanced automated driving technologies and, in cases where they were recently modified, whether the adopted amendments enable the introduction of CADs. Then it is advisable to assess, at a broader level, whether the type-approval based architecture, provided by the current legal framework, is still adequate.

***CADs feature challenging traditional rules*.** As far as the former issue is concerned, it is necessary to ascertain which are the features of a vehicle where introduction of automation may more directly challenge traditional regulation.

---

[379] Defined as «the procedure whereby one or more Member States certify that, depending on the state of completion, an incomplete or completed type of vehicle satisfies the relevant administrative provisions and technical requirements» (art. 3.7, FD).

[380] In such cases the application procedure is split. At first, the manufacturer is required to provide information and certificates in accordance with the state of completion of the vehicle, then, the manufacturer has to provide the previously issued type-approval certificate, as well as the information and certificates relevant to the current stage of completion (see art. 6.5, FD).

[381] See Art. 3.31, FD. Approval authorities are allowed to carry out themselves those tasks.

[382] See Appendix I, Annex XVI. Appendix I is wholly dedicated to «General Conditions Required from Virtual Testing Methods».

[383] See Annex X, FD.

Among these, steering and braking are functions that, together with the management of the lighting equipment[384], when automated raise relevant issues about the complex interaction with the surrounding environment.

Indeed, while the former essentially encompass and define all the aspects of the movement of the vehicle, the latter addresses the signalling and therefore the primary form of communication with other road users, in particular if not otherwise connected.

The automation of other components, such as the gearbox/clutch operation or the fuel management system, is, in this perspective, less problematic. On the one hand, it is less novel a development, on the other hand, they exert most of their influence within how the vehicle components interact with one another, with more limited consequences on the impact on the external environment.

For instance, both an autonomous steering device and an automated gearbox gather information from the environment, process it, and act upon it. Yet, while the latter would mainly determine the rotation speed of the engine and fuel consumption, the former would determine the vehicle's speed and direction within existing traffic, with radically different consequences.

Steering devices – the UNECE WP.29 UN-R79. Regulations on steering come from UN-R79[385], which was amended in March 2017 by UNECE WP.29, in order i) to provide a definition of Automatically commanded steering function[386] (henceforth, ACSF) and Corrective steering function[387] (henceforth, CSF), ii) to issue all data required for the type-approval of the less advanced among these aiding devices, while requirements needed to approve the remaining categories are scheduled for an undisclosed date.

More in detail, the latest amendments to UN-R79 classifies six categories of ACSF, namely A)[388], B1)[389], B2)[390], C)[391], D)[392], and E)[393], in increasing order of technical complexity and advancement.

---

[384] Adaptive, *Legal Aspects on Automated Driving* (2017). http://www.adaptive-ip.eu/index.php/deliverables_papers.html, last access October 6th, 2018, p. 64 ff.

[385] http://www.unece.org//fileadmin/DAM/trans/main/wp29/wp29regs/2017/R079r3e.pdf, last access October 4th, 2018.

[386] UN-R79, Art. 2.3.4.1, defines this feature as: «a function within an electronic control system where actuation of the steering system can result from automatic evaluation of signals initiated on-board the vehicle, possibly in conjunction with passive infrastructure features, to generate control action in order to assist the driver».

[387] UN-R79, Art. 2.3.4.2, defines this feature as «a control function within an electronic control system whereby, for a limited duration, changes to the steering angle of one or more wheels may result from the automatic evaluation of signals initiated on-board the vehicle, in order: (a) To compensate a sudden, unexpected change in the side force of the vehicle, or; (b) To improve the vehicle stability (e.g. side wind, differing adhesion road conditions «μ-split"), or; (c) To correct lane departure. (e.g. to avoid crossing lane markings, leaving the road)».

[388] 2.3.4.1.1. «"ACSF of Category A" means a function that operates at a speed no greater than 10 km/h to assist the driver, on demand, in low speed or parking manoeuvring».

[389] 2.3.4.1.2. «"ACSF of Category B1" means a function which assists the driver in keeping the vehicle within the chosen lane, by influencing the lateral movement of the vehicle».

[390] 2.3.4.1.3. «"ACSF of Category B2" means a function which is initiated/activated by the driver and which keeps the vehicle within its lane by influencing the lateral movement of the vehicle for extended periods without further driver command/confirmation».

[391] 2.3.4.1.4. «"ACSF of Category C" means, a function which is initiated/activated by the driver and which can perform a single lateral manoeuvre (e.g. lane change) when commanded by the driver».

[392] 2.3.4.1.5. «"ACSF of Category D" means a function which is initiated/activated by the driver and which can indicate the possibility of a single lateral manoeuvre (e.g. lane change) but performs that function only following a confirmation by the driver».

[393] 2.3.4.1.6. «"ACSF of Category E" means a function which is initiated/activated by the driver and which can continuously determine the possibility of a manoeuvre (e.g. lane change) and complete these manoeuvres for extended periods without further driver command/confirmation».

Indeed, **UN-R79 still prohibits fully autonomous steering**[394], therefore preventing European certification – and marketing – for CADs that could reach the highest level of automation (SAE level 5)[395]. Moreover, there are still some open issues related to the introduction of ACSF devices, namely how to effectively and accurately monitor the driver's state of alertness, while considering real-life reaction timing[396].

Braking devices – UN-R13-H. In the European framework on vehicle approval, regulations on the braking features for passenger cars (M1 category vehicles) are provided for by UN-R13-H[397].

This body of law defines two advanced devices, namely «automatically commanded braking»[398] and «selective braking[399] that differ among one another because the former is designed to decelerate the vehicle, while the latter is employed to improve stability. Both, however, allow high levels of automation and independent control over this essential task directly by the vehicle itself.

Thence, **extant regulation does not appear to be creating a bottleneck to the development of more advanced AI-solutions, such as those that CADs might adopt, even at the highest levels of automation** (SAE level 4 and above)[400].

Lighting – UN-R48. On the one hand, UN-R48[401], allows many hypotheses of automated activation of lights, which is a function – or set of functions – ever more widespread even among low-range vehicles.

Moreover, after a 2018 amendment, UN-R48, art. 6.6.7.2 expressly allows automation in hazard warning, by permitting the activation of the amber lights to signal the risk of imminent danger, as defined by applicable traffic regulation, to other road-users.[402]

---

[394] UN-R79, Introduction, points out that: «the Regulation does not permit the general approval of systems that incorporate functions by which the steering can be controlled by external signals, for example, transmitted from roadside beacons or active features embedded into the road surface. Such systems, which do not require the presence of a driver, have been defined as "Autonomous Steering Systems"». Moreover, UN-R79, Art. 2.3.3, describes the prohibited device as «a system that incorporates a function within a complex electronic control system that causes the vehicle to follow a defined path or to alter its path in response to signals initiated and transmitted from off-board the vehicle. The driver will not necessarily be in primary control of the vehicle». Furthermore, Arts. 1.2 and 1.2.2 state that: «This Regulation does not apply to […] Autonomous Steering Systems as defined in paragraph 2.3.3».

[395] Adaptive. See esp. pp. 66 ff.

[396] European Commission, Study on the assessment and certification of automated vehicles, Final report, TRL, December 2016, https://ec.europa.eu/growth/content/final-report-study-assessment-and-certification-automated-vehicles_en, last access October 6th, 2018, pp. 40 ff., 57 ff.

[397] http://www.unece.org/trans/areas-of-work/vehicle-regulations/agreements-and-regulations/un-regulations-1958-agreement/un-regulations-addenda-to-the-1958-agreement/old-version-of-regulations-pages/regs-1-20.html, last access October 3rd, 2018.

[398] «a function within a complex electronic control system where actuation of the braking system(s) or brakes of certain axles is made for the purpose of generating vehicle retardation with or without a direct action of the driver, resulting from the automatic evaluation of on-board initiated information», according to Art. 2.20, UN-R13-H.

[399] «a function within a complex electronic control system where actuation of individual brakes is made by automatic means in which vehicle retardation is secondary to vehicle behaviour modification», according to Art. 2.21, UN-R13-H.

[400] Adaptive. See esp. pp. 71 ff.

[401] http://www.unece.org/trans/areas-of-work/vehicle-regulations/agreements-and-regulations/un-regulations-1958-agreement/un-regulations-addenda-to-the-1958-agreement/old-version-of-regulations-pages/regs-41-60.html, last access October 3rd, 2018.

[402] According to a previous version of UN R-79, automation of the hazard-warning signal was limited to the hypotheses of emergency braking manoeuvres and collisions, while it was observed a high degree of automation would require this device to be automatically switched on in a larger number of situations Norms on this device are provided in section 6.6, UN-R48. The definition is provided at Art. 2.7.18, «the simultaneous operation of all of a

On the other hand, however, UN-R48 still notably avoids any specific reference to the automatic initiation of direction-indicator lamps[403]. Therefore, considering how such regulations detail what device might be present on a vehicle that is undergoing safety certification, the current formulation of the norm might result into preventing the adoption of solutions that entail the autonomous activation of direction-indicator lamps, for instance, when maneuvering to change lane.

3.2.9. Bottlenecks and industrial trends

Partial inadequacy of current UNECE norms to accommodate CADs. The current framework of UNECE norms that regulate road vehicle approval, despite addressing different autonomous systems that CADs feature, still, in the cases briefly sketched above, pose some limitations towards the adoption of more advanced solutions that higher levels of automation might presuppose. Yet, those very aspects could probably be easily dealt with through subsequent adaptations of the same regulations, similar to those already occurred, while technology itself advances[404].

Broader assessment of the Type-approval procedure. Beyond the analysis of specific regulations, related to single automotive features or equipment, it is necessary to assess whether, more broadly, the type-approval method is still adequate when CADs are considered.

Problems related to higher-levels of automation. Major concerns arise[405] when higher-levels of automation – pursuant to the SAE scale – are considered, primarily with respect to the (i) close interaction of components among themselves as well as with the external environment CADs presuppose, (ii) – systems' – security vis-à-vis external attacks, (iii) the need for constant updates.

Internal and external interaction. Sub (i), the close interactions of different components in CADs within themselves and with the surrounding environment profoundly determines the very functioning of the vehicle overall. Therefore, a certification approach that is grounded on the separate testing of the different components might prove inadequate. Similarly, the connected element of such applications – that defines and differentiates them from traditional vehicles – also challenges the assumption of environment neutrality. Indeed, the performance of the same system under different conditions and – potentially – with different infrastructures, as well as a diverse population of vehicles – with a higher or lower percentage of CADs over non-autonomous systems – on the road, is most likely going to vary sensibly.

Security from external attacks. Sub (ii), system's security in a connected vehicle is of the same importance as its technical safety. Indeed, issues of tampering and hijacking emerge, which require totally different testing, benchmarking and certificatory techniques.

Need for constant updates. Sub (iii), heavily resting on software and AI solutions that require constant update in order to address emerging concerns and unexpected occurrences, further perfecting the functioning of the system overall, a static assessment – occurring once for each new type – might be incapable of actually ensuring the desired standards of safety are met over time.

---

vehicle's direction-indicator lamps to show that the vehicle temporarily constitutes a special danger to other road-users». Adaptive. p. 77.

[403] Norms on these are provided at section 6.5, UN-R48. The definition is provided at Art. 2.7.11, as «the lamp used to indicate to other road-users that the driver intends to change direction to the right or to the left».

[404] Adaptive. See esp. pp. 72 ff.

[405] VVA/SSSA/TNO Scenarios and conditions for the implementation of CAD and proactive mapping of policy measures, DG CNECT Study, 2018, pp. 36 and 40.

Stakeholders' view: insufficiency of the vertical approach and lack of environment-related assessment. The survey conducted[406] has highlighted how a vertical approach to certification – such as that referred to *sub* (i) above – appears insufficient[407], in particular if the different environments of operation are not taken into account[408], preventing the exact prediction of the functioning of CADs.

To address such issues, the importance of simulation techniques[409], next to real-world testing[410], is emphasized, as well as the need to acquire and store data with respect to the system's performance, to be made available to public authorities[411].

Stakeholders' view: need for self-certification. According to about half of the interviewees, the approval methods should not impose third-party testing, but ought to allow self-certification and audits[412].

However, despite certainly more expensive and cumbersome, third party assessment is thought to guarantee higher standards of safety and reliability; to the contrary, simplified certification procedures would ease manufacturers' position.

EU current initiatives on assessment methods. The European Commission already took care of some among these issues with a 2015 Regulation on assessment methods[413] (henceforth RAM) which introduces self-testing (art. 5) and permits virtual testing (art. 6), thus allowing devices that fall outside EU or UNECE framework to be nationally approved.

The European Commission, more recently, stated its interest in a new and harmonized approach for automated vehicles certification, and in cooperating with Member States in order to pursue such a result[414].

The preparation of a regulatory testing protocol. In order to amend testing rules, within WP.29, under Intelligent Transport Systems – Automated Driving (henceforth, ITS/AD), an Informal Group Task Force on Automated Vehicle Testing (henceforth, AutoVeh) was established, that is expected to issue a regulatory test protocol by 2022. This initiative further pursues the one originally taken by the *Organisation Internationale des Constructeurs d'Automobile* (henceforth OICA)[415].

This new protocol, which is intended to supplement – not replace – the current one, shifting the focus from components to software, includes – in accordance with the initial OICA[416]

---

[406] Ibidem.
[407] More than 90% of the respondents showed concern about the type-approval system focussing on «vertical elements».
[408] 85% of respondents stressed the fact that environment isn't taken into account in the traditional type-approval procedure.
[409] Almost all respondents stated that the certification framework should evolve (98%), while both real-world and case testing should be employed (96%).
[410] 90% thought that testing, as described in FD, is not sufficient to guarantee that AI-based devices work predictably in different situations.
[411] Data from recording should be made available to authorities (93%).
[412] According to the other half (41%), the current methodology, based wholly on the involvement of third parties, remains reliable.
[413] Commission Regulation (EU) 2015/166 of 3 February 2015 supplementing and amending Regulation (EC) No 661/2009 of the European Parliament and of the Council as regards the inclusion of specific procedures, assessment methods and technical requirements, and amending Directive 2007/46/EC of the European Parliament and of the Council, and Commission Regulations (EU) No 1003/2010, (EU) No 109/2011 and (EU) No 458/2011 (Text with EEA relevance). C/2015/0439, in OJ L 28, 4.2.2015.
[414] 3rd Mobility Package, Brussels, May 17th, 2018, COM (2018) 283., p. 8.
[415] OICA is made up of 39 national trade associations around the world, and it maintains permanent committees dedicated to technical affairs, communications, statistics, and exhibitions. Its aim is to represent the interests of the automobile industry to governments, international organisations, other bodies, and the public at large. For further information, see www.oica.net/, last access October 3rd, 2018.
[416] For further information, see https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjF8qmkourdAhVno4sKHcxUAqoQFjAAegQIBxAC&url=https%3A%2F%2Fwiki.unece.org%2Fdownload%2Fattachments%2F50856157%2F%2528ITS_AD-12-11%2529%2520Certification%2520of%2520AVs%2520-

proposal – physical tests (in a traditional sense), tests to be carried out in the real environment, and other practices. The latter might span to include audits about compliance with industry standards or best practices based on self-declarations that would, themselves, be supported by internal testing, simulations and virtual testing alternatively.

ISO initiatives. Among the other current activities aimed at creating a CAD-ready certificatory framework, a key role is being played by the International Standardization Organization (henceforth, ISO).

On the one hand, ISO is conducting a revision of ISO 26262-series and SOTIF standards, developing also ISO/PAS 21448 in order to define a set of requirements for the software involved in the operations of autonomous vehicles.

On the other hand, ISO, in cooperation with SAE, is developing ISO/SAE 21434, in order to address cybersecurity issues in CAD vehicles, and the final version is due for early 2020[417].

Other organizations, such as the *Federation Internationale de l'Automobile*[418] (henceforth, FIA), have expressed concerns about CADs' security and reliability, stating that only tamper-proof systems should benefit of type approval[419]. The European Consumer Organization[420] (henceforth, BEUC) stressed the fact that software needs to be secure and up-to-date both at the moment of the first run and at during all stages of the lifecycle of the vehicle[421].

3.2.10. Conclusions and recommendations

Applicable legislation. There is no ad-hoc legislation on the certification of autonomous vehicles. Thence, since they fall under the notions of road vehicles, CADs need to be certified according to the type-approval set out in the FD (and the RV superseding it), which requires the vehicle to be compliant with UNECE regulations, and is based on the principles of third-party assessment and mutual recognition among MSs.

Type approval and CADs. UNECE Regulations have been adopted in order to accommodate the features of novel devices that have an impact on driving functions. In particular – despite totally autonomous steering is still forbidden – the said regulations now allow and establish parameters for steering aids, for automated braking functions, and for automatic operation of emergency lights in case of danger, whereas automated direction indicators are still not permitted.

Inadequacy of the current legal framework. Overall, the type approval procedure is not adequate for highly automated vehicles, because it is focused on a static evaluation, while AI applications evolve overtime and through their very functioning, benefitting from constant and regular updates. According to several stakeholders, therefore, type approval

---

%2520OICA%2520final.pdf%3Fapi%3Dv2&usg=AOvVaw1h93ZihEDB-cZHVqq4aT8X, last access October 3rd, 2018.

[417] https://www.iso.org/standard/70918.html, last access October 3rd, 2018.

[418] FIA is a global organisation focussed on promoting motor sport safety and, more broadly, safe, clean, sustainable and accessible mobility, through three areas of activity: Sport, Campaigns and Mobility. It is jointly administered by the Secretary General for Automobile Mobility and Tourism, the Secretary General for Motor Sport and the Chief Administrative Officer. For more information, see https://www.fia.com/, last access October 3rd, 2018..

[419] FIA-Region 1 (Europe, Middle East, Africa) Policy Position on Vehicle Type Approval Position Paper, Brussels, 2016, https://www.fiaregion1.com/wp-content/uploads/2017/05/20160603_policy_position_on_type_approval_fin.pdf, last access October 3rd, 2018.

[420] BEUC is a Brussels-based consumer organization, including 43 independent consumer organizations from 32 European countries, focussing on lobbying, defending consumers' interests and investigating EU decisions and policies. BEUC's special focus is now set on Financial Services, Food, Digital Rights, Consumer Rights, Enforcement and Sustainability. For more information, see https://www.beuc.eu/, last access October 3rd, 2018.

[421] *Cybersecurity for Connected Products. Position Paper* (Brussels: ANEC-BEUC, 2018). https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf, last access October 3rd, 2018.

should be partially amended in order to foster a more streamlined and convenient approach, and many international bodies are pursuing studies in this way.

Need for a dynamic assessment. Differently from traditional non-autonomous vehicles, for which a static evaluation system such as the type approval is suitable, CADs, being based on AI-solutions that are intended to adapt over time, require a novel and dynamic approach to certification. The certification procedure should thence require constant monitoring and assessment of the device, also after its distribution onto the market, in light of the changes that occur to its driving system, modifying its performance.

Safety and security issues. While traditional road vehicles are assessed mostly from the point of view of safety, CADs pose relevant security threats, being vulnerable to external – primarily cyber – attacks, posing novel risks that are today hard to precisely define and describe, in particular due to their connected nature. Thus, both safety and security issues need to be thoroughly assessed, either by substantial amendments to the relevant type-approval framework, or by the introduction of novel conformity assessment procedures.

New set of interactions. Moreover, CADs' components interact with one another in more complex ways than what happens to regular components in traditional vehicles, and the most advanced technologies imply CADs interacting with one another and with the infrastructure. The interaction among components in AI-based systems, which are also intended to be connected with other vehicles and infrastructures, poses unprecedented issues in the automotive field, ultimately challenging the adequacy of extant certification procedures. Indeed, the overall vehicle's performance is determined by the interaction of CADs' components among themselves as well as with external elements – other vehicles and the road itself – that are currently not considered in the certification procedure. A revision of the type approval should thence address this concern by requiring the testing of the vehicle framed within such a complex system of interactions.

New testing and certificatory approaches. Despite some stakeholders suggesting the type approval procedure is cumbersome and costly, and thence ought to be replaced by – a gradual and limited introduction of – self-certification tools, the dangers of reduced impartiality such an approach could bring about need to be taken into account.

Testing and certification. CADs' certification, instead, could benefit from a less traditional and more mixed approach to testing, that could imply both confined trials, real-life trials, and simulations.

3.3. Liability and insurance

KEY FINDINGS

- CADs are regulated at EU level by the PLD and MID.
- Both the PLD and the MID were subject to official evaluation to consider possible revision, also in light of technological development. As of now, the Commission decided not to modify the PLD, while a proposal of reform for the MID was developed, which, however, does not address CADs.
- Since CADs could fall – in most cases (§3.1.1) – under the definition of vehicle, MSs' legislation on traffic accidents and corresponding insurance requirements apply.
- MSs' legislation typically holds the driver and/or owner liable, often joint and severally.
- Some MSs resort to fault-based rules for the liability of the driver, and – semi – strict liability of the owner. Others enact no-fault schemes and automatic compensation solutions.
- Germany adopted ad-hoc legislation holding the driver of a highly automated vehicle liable for failing to supervise the driving task, and resume control when needed.
- The UK enacted a regulation that primarily extends insurance duties already in force for traditional vehicles. UK legislation burdens the owner of the vehicle with a duty to install safety-critical updates.
- Increasing automation in the driving task causes different bodies of legislation to overlap. The PLD and traffic liability rules will theoretically simultaneously apply to the same accident, so long as the vehicle is not fully autonomous and the driving task is shared between the human driver and the autonomous system.
- Apportioning liability in such cases becomes problematic, and exacerbates the major criticalities that current EU legislation (namely the PLD) displays. In particular, the burden of proof, and the limited access to data recorded by the vehicle, as well as the complexity of its interpretation might profoundly discourage litigation towards manufacturers, to the disadvantage of the human user or owner.
- Imposing duties to insure is per se insufficient, so long as it is not clarified which party bears what risk, and thence who is to be held liable for each kind of accident.
- Different alternative approaches are possible to handle this matter: (i) no action; (ii) reform of the PLD; (iii) adopting ad-hoc legislation;
- (i) no action will lead to MSs adopting legislation at national level, causing the fragmentation of the EU legal system and market.
- (ii) reform of the PLD might require more complex ascertainments due to its broad field of application – theoretically any product –, and might exceed the purpose.
- (iii) ad-hoc legislation could ease the penetration of CADs in the market with relevant economic and social benefits
- Ad-hoc legislation should favor a Risk Management Approach (RMA) and burden the party that is best positioned to insure and minimize risks (or ensure compliance).
- Strict liability rules identifying one clearly responsible party towards the victim (one-stop-shop approach) should be favored.

- The duty to update software should be rested on the manufacturer, to increase the probability of correct compliance.
- Legislation should be enacted at EU level, rather than at MSs' level, not only to create a level playing field, in a legal perspective, but also to avoid market and technological fragmentation.
- Liability rules influence which kind of technological solution will prevail. Thence, differing rules may favor diverging approaches to automation, limiting the possibility of a vehicle conceived to operate under a given legal framework to function and/or be used in a different one.

3.3.1. Introduction

Importance of liability and insurance for CADs' development and regulation. How liability is attributed and apportioned among the different players involved, and how such subjects are able to insure for such costs, is a matter of seminal importance. Not only does it determine the incentives to the very development and diffusion of CADs, but it also influences the adoption of specific technological solutions[422]. Liability rules, together with insurance regulation and market, hence, impact the development and diffusion of new technologies, by favoring some over others. Therefore, non-uniform approaches at MSs' level would lead to the emergence of different technological solutions, fragmenting the EU market, and not solely its legal system.

The further analysis will describe the legislative framework applicable to CADs, both at the European and Member States' level (§3.3.2) and the accidents reported so far (§3.3.3). Afterwards, the report will assess the legal framework, explaining how extant liability rules, conceived for traditional vehicles, might delay the diffusion of CADs, and how the choice among possible alternative approaches contributes to selecting the kind of innovation that will emerge and prevail (§3.3.5).

3.3.2. The legal framework

The legal framework applicable to CADs is constituted by the harmonized European legislation on product liability (§3.3.2.1), as well its national implementation (§3.3.2.2), the motor insurance directive (§ 3.3.2.3) and the national rules for traffic liability and the related insurance (§3.3.2.4).

3.3.2.1. European legal framework: the product liability directive

The Product Liability Directive. The Product Liability Directive[423] establishes the conditions under which the producer is liable for damages caused by defects in his products, which shall be understood as «all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable»[424].

Semi-strict liability of the producer. Despite sometimes defined as a hypothesis of strict-liability, the PLD actually sets a system of semi-strict-liability. Indeed, the producer – «the manufacturer of a finished product, the producer of any raw material or the manufacturer of

---

[422] See Andrea Bertolini and Massimo Riccaboni, *The Regulation of Connected and Automated Driving. A Law and Economics Analysis of Liability Rules* (2018).
[423] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products
[424] PLD, art. 3.

a component part and any person who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer» – or any subject identified by art. 3 (the importer of a product within the European Union, and the seller of the product – in case the producer cannot be identified), is responsible for the damages derived from the use of the product, so long as the product is defective, and a causal nexus between the defect and the damage can be established.

Defectiveness of the product. A product is defective when it «does not offer the safety that a person is entitled to expect, considering all circumstances»[425], such as the presentation of the product, its reasonably expected use, and the time in which it was put into circulation. A product might be deemed defective in three different sets of occasions: a single specimen might deviate from the intended design and thus from the other specimens of the mass-production, thus constituting a «manufacturing defect»; warnings about the potential dangers arising from the use of the device might not adequately communicated or signaled, thus determining an «information defect»; lastly, the very design of the product might be deemed defective, for it does not provide necessary level of safety, or is unreasonably dangerous, thus representing a «design defect». It is worth noting that while the manufacturer might be held liable for all the type of defects here described, other subjects involved in the value chain – most notably, the producer of individual components of the final product – could only be sued in case of a mere manufacturing defect.

Burden of proof. Despite the claimant is not required to identify the specific cause of the defect, showing that the product is indeed defective might still prove cumbersome, as they require technical skills and access to data which will most likely be lacked by the victim. Such burden would be particularly difficult in the case of design, as it will entail acquiring the expert opinion of a technician whom, once he has accessed data regarding the functioning of the device[426], is capable of analyzing it and demonstrating the existence of a defect in the way the product was conceived. The more technologically complex the product, the harder satisfying such a requirement is going to be.

Exceptions to liability. Moreover, manufacturers – pursuant to art. 7, PLD – might escape liability by advancing the following defenses:

a. that he did not put the product into circulation;
b. that, … it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that the product came into being afterward;
c. that the product was neither manufactured by him for sale or any form of distribution for economic purpose not manufactured or distributed by him in the course of his business;
d. that the defect is due to compliance of the product with mandatory regulations issued by the public authorities;
e. that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered;
f. in case of a manufacturer of a component, that the defect is attributable to the design of the product in which the component has been fitted or to the instruction given by the manufacturer of the products;

[425] Art 6 PDL.
[426] This in particular might be problematic, for the data generated by the sensors and eventually recorded by an event data recorder (EDR) could be claimed as proprietor information by the manufacturer, who opposes its disclosure for the purpose of protecting its industrial secrets.

However, the liability of the producer can also be reduced if he proves that the contributory negligence of the victim.

Level of harmonization. Since the PLD rests on a regime of maximum harmonization for claims based on product liability, art 13 PLD allows MSs to create or keep different liability rules, which the victim of an accident caused by a defective product may rely on, to the extent that such rules belong to a different system of contractual or non-contractual liability, such as fault or warranty in respect of latent defects[427] (see §3.3.2.2)

3.3.2.2. National framework: product liability rules

A detailed account of different implementations of the PLD at the MSs' level falls beyond the purpose of the current study. Relevant degrees of variations can be observed across MSs, both with respect to the scope of application of the directive, and to the choice among the options granted by the directive itself (see, for example, art. 9 PLD). On these matter, a brief comparison between Germany and France may be deemed exemplary, as it clearly shows the divergence among the national legal frameworks, despite harmonized[428].

Scope of application. As for the former, MSs have adopted a different approach as to the regulation of liability caused by defective products. Germany, for example, has enacted both the Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz, henceforth ProdHaftG)[429], which represents the general legislative framework on the matter, and other special liability statues for specific technologies, such as the Gesetz zur Regelung der Gentechnik, or the Atomgesetz[430]. On the contrary, France only has one single legislation, covering all the technology falling within the notion of product, as defined by the directive[431].

Discretionality: liability caps. With respect to the latter issue – the discretionality left to MSs in the implementation of the directive, for example, on the recoverability of non-pecuniary damages (art. 9, PLD) – the ProdHaftG provides for certain monetary limits on compensation. For cases such of death and bodily injury, a maximum amount of € 85million is recoverable, irrespective of whether the award is set to compensate several damages caused by a single defective product, or whether it the damages are caused by a series of products of identical terms.[432] On the contrary, French law – mirroring the choice adopted at the general level by the *code civil* – compensates any kind of damages, excluded those explicitly excluded by the directive, and no maximum limit on the award is set.

3.3.2.3. European legal framework: the Motor Insurance Directive

The Motor Insurance Directive. The European legislative framework for the insurance of autonomous vehicles consists of the Motor Insurance Directive (2009/103/EC, henceforth MID)[433], which sets a compulsory third party liability insurance for motor vehicles.

Pursuant to art. 3 of the MID, each MS has the duty to take appropriate measures to ensure that civil liability for damages deriving from the circulation of vehicles based in its territory

---

[427] CJEU, 25 April 2002, *María Victoria González Sánchez v Medicina Asturiana SA*, Case C-183/00, 2002 I-03901, ECLI:EU:C:2002:255, para. 23-34.
[428] Jean-Sébastien Borghetti, "Product Liability in France," in *European Product Liability. An Analysis of the State of the Art in the Era of New Technologies*, ed. Piotr Machnikowski (Cambridge: Intersentia, 2016); Ulrich Magnus, "Product Liability in Germany," in *European Product Liability. An Analysis of the State of the Art in the Era of New Technologies*, ed. Piotr Machnikowski (Cambridge: Intersentia, 2016).
[429] Gesetz über die Haftung für fehlerhafte Produkte vom 15. Dezember 1989 BGBl. I S. 2198.
[430] Gesetz über die friedliche Verwendung der Kernenergie vom 23. Dezember 1959 BGBl. I S. 814.
[431] Loi n. 98-389 of May 19 1998, modifying the French civil code.
[432] §10 ProdHaftG.
[433] Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability (OJ L 263, 7.10.2009, p. 11–31).

is covered by third-party insurance. This can lead to the adoption of different solutions, ultimately determining the breadth of the coverage provided. Each MSs shall ensure that the insurance also covers any loss or injury which is caused in the territory of other MSs, according to the law in force, as well as those suffered by national insurers' bureau responsible for the crossed territory, according to the national laws of the MS where the vehicle is normally based. However, insurance shall always cover damages to property, loss and personal injury inflicted on another party because of the actions of the policyholder[434]. Most importantly, the victim of an accident caused by a vehicle covered by insurance as referred to in Article 3 shall enjoy a direct right of action against the insurance undertaking the covering against civil liability of the person responsible[435].

Each MS shall ensure that the contract of insurance also covers any loss or injury which is caused in the territory of other MS, according to the law in force, and as well as those suffered by nationals of MS during a direct journey between two MS if there is no national insurers' bureau responsible for the crossed territory, according to the national laws of the MS where the vehicle is normally based.

Pursuant to art. 9, without prejudice to any higher guarantees prescribed at national level, each MS shall require compulsory insurance under art. 3 to cover a minimum amount of (i) 1 000 000 € per victim or 5 000 000 € per claim, whatever the number of victims, in case of personal injury; (ii) 1 000 000 € per claim, whatever the number of victims, in case of damage to property; (iii) every five years, such amounts shall be reviewed in line with the European Index of Consumer Prices pursuant to Regulation (EC) No 2494/95, and shall be thus adjusted automatically[436].

Issues of civil liability including compensation awards, as well as comprehensive cover for physical injury of the driver or damage to vehicles, on the contrary, fall outside the scope of the directive.

Pursuant to art. 12, the compulsory third party motor liability insurance shall cover liability for personal injuries to all passengers, other than the driver, arising from the use of a vehicle; members of the family of the policyholder, driver or any other person who is liable under civil law in the event of an accident, and whose liability is covered by the insurance referred to in art. 3, shall not be excluded from insurance in respect of their personal injuries by virtue of that relationship. Likewise, the compulsory insurance set shall cover personal injuries and damage to property suffered by pedestrians, cyclists and other non-motorized users of the roads who, as a consequence of an accident in which a motor vehicle is involved, are entitled to compensation in accordance with national civil law.

In addition to those specification, the MID obliges MS to institute specific guarantee funds for accidents caused by unidentified vehicles or vehicles not insured according to art. 3 MID[437], as well as for accident caused by a third-country vehicle[438]. It abolishes border checks on insurance[439], specifies the authorities responsible for compensation and some

---

[434] Art. 3 MID. However, according to art. 5 MID, MSs may derogate from Article 3 in respect of certain natural or legal persons, public or private, as well as of certain types of vehicle or certain vehicles having a special plate; a list of such persons and vehicles shall be drawn up by the State concerned and communicated to the other MS and to the Commission, and appropriate measures shall be taken up as to ensure that compensation is paid in respect of any loss or injury caused in its territory and in the territory of other Member States in such cases. In particular, MS shall designate an authority or body in the country where the loss or injury occurs responsible for compensating injured parties in accordance with the laws of that State in cases where Article 2(a) is not applicable, while the guarantee fund of the Member State in which the accident has taken place shall then have a claim against the guarantee fund in the Member State where the vehicle is normally based.

[435] Art. 18 MID

[436] Art. 9 MID.

[437] Art. 10, 11 MID.

[438] Art. 7, 8 MID.

[439] Art. 4 MID.

fundamental features of the compensatory procedures[440], and introduces a mechanism to compensate local victims of accidents caused by vehicles from another EU country[441]. The directive also requires the quick settlement of claims arising from accidents occurring outside the victim's EU country of residence[442], and entitles policyholders to request a statement concerning the claims (or absence of claims) involving their vehicle during the 5 years preceding the contract[443].

REFIT and proposed amendment to the MID. Together with the evaluation of the PLD[444], the European Commission has recently undergone the REFIT of the MID[445]: a public consultation was held between July and October 2017[446], ultimately leading to the adoption in May 2018 of a proposal to amend the motor insurance directive[447]. Following a detailed analysis of the current framework and it overall evaluation, three different issues were identified as problematic, namely: the protection of victims of accidents in case of insolvency of an insurer, minimum amounts of cover among different MSs, the portability of history claims for active cross-boarded subjects for the purpose of calculating no claims-discounts, and checks on insurance vehicles.

The proposed amendment provides that full compensation should be granted to the victims of motor vehicle accidents even when the insurer is insolvent makes it easier for authorities to combat uninsured driving, aligns the minimum levels of cover by motor insurance across the EU, and incorporates case law of the EU Court of Justice on the scope of the directive.

Most notably, **no amendments are suggested regarding insurance of CADs**. Indeed, both the public consultation and the feedbacks provided by relevant stakeholders suggested that, although technological development might indeed require future adjustments to insurance models, no such modification are yet needed, as CADs and other forms of automated mobility fall within the scope of the MID and are adequately regulated by the rules set out therein. In particular, it has been pointed out that it does not matter for the purpose of the directive whether the policyholder is also the driver of the vehicle, as the victim will be able to claim compensation under the MID. **The owner who has registered the vehicle is required to obtain third party motor insurance which will compensate the victim**; in a second step, which falls outside the scope of the directive, the insurer might indeed seek recourse against the manufacturer[448].

3.3.2.4. National frameworks: liability and insurance for accidents

Traffic liability rules are not set at European, but rather at the MSs' level, and are complemented by the national implementation of the MID which, being a minimum-harmonization directive, states that MS may maintain or adopt provision which are more favorable to the injured parties[449].

---

[440] Art. 19, 22, 24 MID.
[441] Art. 20 MID.
[442] Art. 11 MID.
[443] Art. 26 MID.
[444] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29–33).
[445] Information about the REFIT of the MID can be found at the following link https://ec.europa.eu/info/consultations/finance-2017-motor-insurance_en (last accessed 1st August 2018).
[446] Information about the REFIT of the MID can be found at the following link https://ec.europa.eu/info/consultations/finance-2017-motor-insurance_en (last accessed 1st August 2018).
[447] European Commission, Proposal for a Directive of the European Parliament and of the Council amending Directive 2009/103/EC, Brussels, 24.5.2018 COM(2018) 336 final 2018/0168 (COD); and Commission Staff Working Document – Impact Assessment Accompanying the document.
[448] Impact Assessment, p. 138.
[449] Art. 28 MID.

The analysis of a selected number of national frameworks applicable to CADs is provided below, showing a significantly varied scenario: (i) in some MSs, a specific legislation has been adopted for CADs (UK and Germany), while in other no such initiatives have been undertaken yet; hence, should an accident involving CAD occur, traditional traffic liability rules would apply (Italy, France, Spain, Sweden, the Netherlands, Austria); (ii) across MSs, different forms of liability apply, ranging from fault-based liability, to strict and objective liability, to a combination of the two[450].

Italy. Traffic liability in Italy is governed by art. 2054 of the Italian Civil Code[451], where it is stated that the driver of a vehicle without rails must compensate the damage caused to people or things from the circulation of the vehicle, if he does not prove that he has done everything possible to avoid the damage. Together with the actual driver, Italian law holds jointly liable the owner of the vehicle, who can avoid liability only if he succeeds in demonstrating that the vehicle was circulating against his will. According to established case law, the liability framework set up by art. 2054 c.c. covers all type of damages caused by the vehicles while driving, to third parties (pedestrians, cyclists, other drivers), as well as the passengers of the vehicle itself.

In order to ensure victim's compensation, a compulsory liability scheme is put forth by l. n. 990 of 1969 and subsequent amendments, now governed by Articles. 122 of Legislative Decree no. 209 of 2005, Code of private insurance. The injured person possesses a direct action towards the insurer of the responsible party, and, under certain conditions, against its own insurer, that will then act in recourse against the insurer of the responsible. Finally, the standard of care that applies to drivers is particularly high: in addition to behaving in a manner that respects the rules of the road, it must also provide for the possible imprudence of others (in particular children, the elderly, etc.).

France. In France, traffic liability is regulated by the Loi Badinter, which sets a system of almost absolute liability for the owner or keeper of the vehicle[452]. Indeed, the latter is liable *vis-à-vis* all traffic members, with the exception of the driver of his motor vehicle. If the victim was the driver of another motor vehicle, the keeper is automatically liable, but he may avoid liability by proving absence of fault by him or by the driver. If the victim is another subject – such as a pedestrian, a cyclist, a passenger, they must only claim they suffered damage from a traffic accident, the motor vehicle was directly involved, without being required to prove causality. The keeper has very limited defenses and can only escape liability if the victim was non-motorised or a passenger who intentionally got hurt or committed an inexcusable fault which was the exclusive cause of the accident, provided that the latter is not younger than 16, older than 70 or disabled over 80 percent. In case of property damages, however, traditional contributory negligence applies.

The aforementioned Loi Badinter, concerning motor liability in France, amended some parts of the French Insurance Code[453] (FII) as well, thus enhancing the effectiveness of the global motor liability and insurance framework.

Article L211-1 of the FII establishes compulsory insurance for everybody, both individual persons and legal entities, whose liability may arise because of accidents involving motorized road vehicles. Indeed, anyone who is in custody of a vehicle or drives it, even if unauthorized by the owner, is covered by insurance.

---

[450] For an in-depth comparative analyses, see Evas.
[451] Decreto Legislativo 30 aprile 1992, n. 285, Nuovo codice della strada. (GU n.114 del 18-5-1992 - Suppl. Ordinario n. 74), available at the following link http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:1992-04-30;285.
[452] Loi n° 85-677 du 5 juillet 1985 tendant à l'amélioration de la situation des victimes d'accidents de la circulation et à l'accélération, available at the following link: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068902&dateTexte=20100114.
[453] Décret no 76-667 du 16 juillet 1976.

Moreover, rules concerning a compensation fund are provided by Articles L420-1 and ff. Such fund is aimed at compensating victims when the insurance company is insolvent, or the damaging party is unknown or uninsured, primarily when damage concerns persons. Such compensation fund is a legal entity, endowed with legal personhood, and all companies authorized to sell motor insurance products contribute to it, as well as individual insured motorists and uninsured ones.

After having compensated the victims, such fund can act in recourse against the responsible parties.

Spain. Pursuant to the Law on Civil liability and insurance in the movement of motor vehicles (Ley sobre Responsabilidad Civil y Seguro en la Circulación de Vehículos a Motor)[454], the driver of the vehicle is responsible for the damages that may cause to the persons or in the goods other than by reason of the movement. Therefore, Spanish law establishes a presumption of responsibility on the driver for the damage and injuries that may arise from a traffic accident. The driver can demonstrate that he was not responsible. However, in case of personal injuries, he will need to prove that the damage was due to the exclusive fault of the injured party, or to force majeure foreign to the driving or operation of the vehicle. When the victim only contributes to the production of the damage, all compensations will be reduced correspondingly to the concurrent fault up to a maximum of 75%. The non-driver owner is vicariously liable for damages to persons and property caused by the driver when he is linked to him by any of the relationships that regulate articles 1.903 of the Civil Code and 120.5 of the Penal Code. Yet, he can escape this responsibility proving that he used all the diligence of a good parent to prevent the damage. The non-driver owner of a vehicle without the mandatory subscription insurance will be liable with the driver for the damage to the persons and the goods caused by it, unless it proves that the vehicle had been stolen. Compulsory insurance is required for every owner of motor vehicle, covering civil liability.

Austria. Civil law consequences of a traffic accident are asserted on the basis of the Civil Code (ABGB) and the EKHG (Railway and Motor Vehicle Third Party Liability Act). The owner of the vehicle is liable for damages caused by the circulation of the vehicles, unless the latter was used against his will, as in this case the driver will be held responsible instead. Exemptions are set in case of unavoidable events, and liability caps are set for both death and bodily injury and property damages. Third-party insurance coverage is mandatory.

The Netherlands. According to Article 185 of the Dutch Road Traffic Act[455], the owner and the keeper of a motor vehicle are liable for damage caused to non-motorised persons and objects – different from motor vehicle –, irrespective of the cause of the accident. For other victims, regardless of the type of damage (personal injury or death, damage to property) the liability of the owner or the keeper is fault-based and is regulated mostly by case law: absent gross negligence or intent of the non-motorised victim, they are always liable for at least 50 percent of the damage, unless they prove that an «unforeseeable and unavoidable» factor caused the accident (provided the victim was over fourteen years old).

Sweden. In Sweden, traffic liability provides fault-based rules, but rests on a regime of non-fault insurance for pecuniary and non-pecuniary damages related to personal injury or death of both motorized and not motorized vehicles, which is justified on grounds of social solidarity. All the victims of a traffic accident, be they motorized or not motorized, have a right to claim compensation from the insurer of the owner, possessor or driver of the vehicle, and such right is affected only in case of contributory negligence. The insurance company has a right to reimbursement against the insurer of the party who was at fault or, if absent the latter, against the Guarantee Fund. Drivers are even entitled to compensation in case of single-vehicle accidents.

---

[454] Available at the following link: https://www.boe.es/boe/dias/2004/11/05/pdfs/A36662-36695.pdf.
[455] Wegenverkeerswet 1994, available at the following link: https://wetten.overheid.nl/BWBR0006622/2018-07-28.

Victims injured by the operation of a motor vehicle can seek recovery from the liability of the motor insurance of the keeper, which covers all victims, including the driver himself in single-car-accidents- for all types of personal injuries and death, on a principle of social solidarity.

3.3.2.5. Contd.: MSs' ad-hoc legislation for CADs

Germany. Germany has started to regulate automated driving at the national level, adopting, on the 11th of June 2017, **Law amending the Straßenverkehrsgesetz**[456], which allows automated driving on German roads and regulates the behaviour of the driver of a high or fully automated vehicle. Despite the somehow misleading nomenclature[457], under this law the operator of the vehicle may not be completely disengaged from driving (§1a.1), and no-passenger driving systems are not allowed[458]. Indeed, such vehicles must possess the technical equipment necessary to: (i) steer upon activation and handle the task of driving, including longitudinal and lateral control; (ii) abide by the traffic regulations directed towards drivers, when the control system is active; (iii) manually be overridden or deactivated by the operator of the vehicle at any time; (iv) recognize when it is necessary for the driver to personally control the vehicle, and (v) indicate visually, acoustically, tactilely, or otherwise perceptibly to the vehicle operator, with sufficient time before the control of the vehicle is handled over to the driver, the necessity to personally control the vehicle, which on one of the system descriptions indicate contrary use.

The *Fahrzeugführer* is allowed[459], while performing medium-high or fully-automated functions, to avert his eyes from the road and defer control, but only as long as he remains vigilant and ready to resume it, (i) when the highly or fully automated system prompts him to do so, or (ii) if he recognize or, due to obvious circumstances, must recognize that the prerequisites for the intended use of the highly or fully automated driving functions no longer exist (§1b).

Therefore, ordinary fault-based liability rules apply for automated driving, although with specific caps – 10 million euro in case of personal damages, and to 2 million euro for property damages – (§12). The driver holds a duty to remain vigilant and resume control of the vehicle when needed or required to do so; if he breaches his duties and accident occurs, he will be held liable for the damages caused. If he is not at fault, the owner of the vehicle will be held accountable for the damages caused by the vehicle (§7 and §18 StVG). According to the general liability rules, the owner may sue the manufacturer of the vehicle, in case a liability claim can made.

Black boxes will constitute the major form of proof for understanding whether the driver involved in an accident while operating on the automatic mode was on fault or not[460]. Automated motor vehicles shall, indeed, (§63a) be designed as to allow storage of the

---

[456] BGBI. I pg. 1607, also available at https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl216s1306.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl216s1306.pdf%27%5D__1516706616435, last access on the 23rd of January 2018.

[457] The nomenclature adopted («Kraftfahrzeuge mit hoch – oder vollautomatisierter Fahrtfunktion») responds to the BASt (German Federal Highway Research Institute) level of automations, and should not be confused with the standards used by SAE (Society of Automotive Engineers) and later adopted by the NHTSA (National Highway Traffic Safety Administration). The German regulation allows up to only SAE-levels 3 and 4 driving systems («conditional automation and high automation»), while it excludes SAE-level 5 («full automation»).

[458] With the only exception of low-speed driverless parking systems on separated private grounds outside the public roadways (§6, 1, 14a). The law does not introduce standards for the approval of vehicles with automated driving systems, which remain governed by EU and international law. According to §1a.3, the vehicle must comply with the new international technical rules for automated systems that apply in Germany, e.g. international rules from the United Nation Economic Commission for Europe.

[459] Before this law was enacted, adaptive cruise control was allowed only under constant supervision.

[460] Major problems still persist: what if the system does not require the driver to take back control? How could the driver prove that he was properly relying on the system to tell him when to resume control? The only reasonable solution is to reverse the burden of proof: if the system does not alert when necessary the manufacturer should be held liable for the system malfunctioning unless he proves that the driver has violated his duty of vigilance.

position and time when the driver leaves the system in charge, as well as when he is requested to take over control, or a technical disturbance of the system occurs. Such data may be transmitted to the authorities responsible for the enforcement of traffic violations pursuant to the law of the country where the accident occurred, which may store and use them in order to perform their functions. Data transmission shall be limited to the extent necessary for enforcing traffic violations in connection with the procedures of the control carried out by those authorities. The owner of the vehicle shall have the data stored communicated to third parties, if it is required for the enforcement, fulfilment or defense of legal claims in connection with an incident where the vehicle was involved in this event. It could also be transmitted in an anonymous form to third parties for the purpose of accident research. The data stored by the vehicle shall be deleted after six months, if the vehicle is not involved in an accident.

The law does not set who is responsible for recording and deleting the data, neither the details on the technical design and the location of the data storage device, nor the methods of recording, nor the measures required to protect the data against unauthorized access in the event the vehicle is sold. These issues shall be implemented by legal decrees adopted by The Federal Ministry for Transport and Digital Infrastructure, in consultation with the Data Protection and Information Protection Officer (§63b).

In addition to the aforementioned law, in June 2017, specific **Ethics Commission Guidelines**[461] focusing on level 4 and 5 VDA (corresponding to level 4 and 5 SAE) were released. According the Guidelines, in the case of CADs, the accountability shifts from the motorist to the manufacturers and operators of the technological systems and to the bodies responsible for taking infrastructure, policy and legal decisions, and such transition shall be reflected by statutory liability regimes. Liability for damages caused by activated automated driving systems shall be governed by the same principles as in other product liability and manufacturers or operators are obliged to continuously optimize their systems where possible and reasonable[462]. If not fully autonomous, the system interface must be designed such that at any time it is clear and apparent whether the system or the driver is in charge, and the relevant information – especially handover procedures – shall be documented and stored. The systems must adapt more to human communicative behaviour rather than requiring humans to enhance their adaptive capabilities, and in emergency situations, the vehicle must be able enter autonomously, i.e. without human assistance, into a safe condition.

On the 6th of September 2017 the Federal Government adopted the **Federal Government Action Plan on the Report by the Ethical Commission on Automated and connected driving**[463], declaring that it will progress the technological evolution creating clear ethical rules.

United Kingdom. The UK has worked in parallel with Germany to establish a national regulation for CADs, and has recently adopted its first binding regulation on this matter.

After a series of initiatives[464], in September 2016 the Department of Transport released a consultation The Pathway to driverless cars: Proposals to support advanced driver assistance

---

[461] Available at https://www.bmvi.de/SharedDocs/EN/Documents/G/ethic-commission-report.pdf?__blob=publicationFile, last accessed on the 23rd of January 2018.

[462] The installation of automated systems is thus permissible and does not result in special liability risks if the manufacturers do everything that might be reasonably expected to make their systems as safe as possible and, in particular, minimize the risk of personal injury.

[463] Available at https://www.bmvi.de/SharedDocs/EN/publications/action-plan-on-the-report-ethics-commission-acd.pdf?__blob=publicationFile, last accessed on the 23rd of January 2018.

[464] The Pathway to Driverless Cars Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401562/pathway-driverless-cars-

systems and automated vehicle technologies, leading to Government to respond proposing: (i) a step by step pragmatic approach to legislative innovation, starting with a revision of the Highway Code to enable remote control parking, motorway piloting and HGV platooning, and (ii) an extension of compulsory motor insurance to cover both the drivers' traditional use of the vehicle and the CAD's technology[465].

The Vehicle Technology and Aviation Bill, presented in February 2017, was drafted as to introduce policies for automated vehicles and road vehicle testing, extending compulsory motor insurance requirement to include automated vehicle owners. The initiative came to a halt when the Parliament was dissolved in July 2017, and has now been translated in the **Automated and Electric Vehicle Bill**[466], presented in October 2017 at the House of Commons and adopted on the 19th of July 2018.

The Bill amends and supplements the provisions in the Road Traffic Act, making it compulsory for users of automated vehicles to have insurance that covers the technical failures of the CAD technology. It therefore places a first insurance liability on users (or the crown and public sector if self –insuring), **including damages caused to the driver in AVs who are legitimately disengaged from the driving tasks**. Differently from current law applicable to traditional vehicles, CAV may not benefit from the depositing of a bond for £500,000 with the Accountant General, as an alternative to the standard third-party insurance requirements.

The bill requires the Secretary of State to maintain a list of relevant automated vehicles to which the legislation would apply, including vehicles that: (a) are or might be used on roads or in other public places in Great Britain, and (b) are in the Secretary of State's opinion designed or adapted to be capable, in at least some circumstances or situations, of safely driving themselves without having to be monitored by an individual. Such vehicles should be identified either by their type, by their registration document, or otherwise (clause 1).

Clause 2 provides that, when (a) an accident is caused by an automated vehicle when driving itself, (b) the vehicle is insured at the time of the accident, and (c) an insured person or any other person suffers damage as a result of the accident (personal injury or death or third party property damage), the insurer would be held liable. If the vehicle is not insured at the time of the accident, and section 143 of the Road Traffic Act 1988 (exemptions to compulsory insurance), the owner of the vehicle will be held accountable instead. In both cases, liability would be limited according to section 145 of the Road Traffic Act 1988 section 145(4)(b) (limit on compulsory insurance for property damage, amounting to £1,000,000), which already applies to damages caused by traditional driving. With the only exclusion of the aforementioned cap, liability may not be limited or excluded by a term of an insurance policy or in any other way.
However, according to clause 3, when the injured party contributed in causing the accident, provisions under the Law Reform (Contributory Negligence) Act 1945 (Section 1 in particular) apply. Also, the insurer or owner of an automated vehicle is not liable under section 2 to the person in charge of the vehicle where the accident that it caused was wholly due to the person's negligence in allowing the vehicle to begin driving itself when it was not appropriate to do so. Under clause 4(1), insurers would be able to limit their liability if the damage suffered by the insured person are a direct result of software alterations made by the insured person himself, or with his knowledge, that are prohibited under the policy, or of a failure to install safety-critical software updates. If damage to a third party occurred

summary.pdf, last accessed on the 23rd of January 2018; **The Pathway to driverless cars: Proposals to support advanced driver assistance systems and automated vehicle technologies,** available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/536365/driverless-cars-proposals-for-adas-and_avts.pdf, last accessed on the 23rd of January 2018

[465] Government's response available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/581577/pathway-to-driverless-cars-consultation-response.pdf, last accessed on the 23rd of January 2018.

[466] Automated and Electric Vehicles Bill 2018, available at www.legislation.gov.uk/ukpga/2018/18/enacted (last access 20th November 2018).

and the insurer paid for it, they could claim that payment back from the insured person in some circumstances. If damages are suffered by an insured person who is not the holder of the policy, subsection (1)(a) applies only in relation to software alterations which, at the time of the accident, the person knows are prohibited under the policy.
Therefore, if the car is driving automatically, and causes the incident, first instance liability is on the insurer and the (human) driver is also covered. The key policy point in this clause is that extending the insurance system applicable to non-automated-driving is preferable than requiring the consumer to pay damages and then rely on a product liability action which is likely to be costly and long. Insurance companies are left free to regulate the policy market as they prefer, but insurance would be compulsory. According to clauses 2 and 5, when the insurer, or the owner of a vehicle, are bound to a person who has suffered damage as a result of an accident («the injured party»), and (b) the amount is settled – because it has been established by a judgment, a decree, and arbitral award or an enforceable agreement –, any other person liable is also responsible towards the insurer or vehicle owner, to the same amount. Both the insurer and the owner of vehicle can therefore recover from the actual wrongdoer (the driver who has relied on the automated system when it was not appropriate to do so; the manufacturer, in the damages where cause by a defect in the product) the amount paid in compensation.

3.3.3. Reported accidents

No accidents reported in Europe. So far, no accidents involving CADs have been reported within the EU. This scenario reflects the general approach of MS, which either do not allow circulation of CADs on public roads, or allow it only for the purpose of testing. In the latter case, as it was described in §3.2.2.2, companies are required to report any accident occurred during trials. However, no accident-report was found at the time of this report, neither through desk research, nor through interviews.

Accidents reported in other jurisdictions. However, useful insights could indeed be derived from incidents coming from other jurisdictions, since they might help us anticipating the legal problems arising from such situations.

USA. In 2016 a fatal accident was reported in Florida, when a driver of a Tesla Model S crashed into the side of a truck while driving on autopilot mode. According to the first report, it seemed that the autopilot did not recognize the white side of the truck – which was performing a non-authorized turn – against the bright blue sky. Tesla claimed that the car's autonomous software is designed to nudge consumers to keep their hands on the wheels to make sure they're paying attention and remain alert. In that case, instead, the driver might have been fully disengaged with driving related tasks as it was suggested that he was watching a movie. After ongoing homicide investigation into the performance of the autopilot were open, the NHTSA said the driver did not put his hands back on the steering wheel despite instructed to do so several times, set the cruise control at 74 miles (119 km) per hour less than two minutes before the crash — above the 65 mph speed limit – and did not apply the brakes or any other action to avoid collision even though the truck would have been visible for seven seconds before the crash. However, it is worth noting that the Tesla Model S uses a proprietary system to record a vehicle's speed and other data, which authorities cannot access with the commercial tools used to access information from event data recorders in most other cars, thus having to rely on Tesla to provide the relevant data[467].

A non-fatal accident still involving a Tesla automated car – the Model X – occurred in Pennsylvania, where the car was drifted out of the lane, collided with a barrier, overcorrected, crossed both lanes of the highway, struck a median barrier, and rolled over

[467] https://newatlas.com/ntsb-tesla-accident-joshua-brown-report/50136/.

coming to a rest in the middle lane. The driver claimed that the autopilot was on, but Tesla – despite the damage to the vehicle – managed to obtain the car data to show that car's autopilot was turned off during the accident.[468]

In 2018, another fatal accident occurred, involving – for the very first time – an autonomous car with an emergency backup driver, and a pedestrian. As a result of the accident, the company quickly suspended testing in Tempe as well as in Pittsburgh, San Francisco and Toronto. The cause of the accident is still unclear, but it seems that the autopilot did not identify the woman, who was crossing the street in a very dark no-crossing zone, at a very short distance. However, investigations are trying to figure out whether this happened because of a defect or failure in the software, or a non-adequate design, and if there is an exclusive or concurrent responsibility of the backup human driver, as it seems he was not fully engaged in the driving and thus not prompt to resume control to avoid the accident.

China. Outside the USA and EU, two accidents occurred in China, in January and August 2016. In the first fatal case, the footage shows the car driving along a road at speed, seemingly without any problems, until it ploughs into the rear of the road sweeper, with no attempt to slow the car down before the crash. Tesla said it had no way of knowing if its semi-automated Autopilot system was engaged at the time of the accident, since, «because of the damage caused by the collision, the car was physically incapable of transmitting log data to our servers»[469].

In the second case, while on autonomous mode, the car hit a vehicle parked half off the road, shredding off the parked vehicle's side mirror and scraped both cars, but causing no injuries. Tesla commented that «The driver of the Tesla, whose hands were not detected on the steering wheel, did not steer to avoid the parked car and instead scraped against its side». The driver, however said Tesla's sales staff strongly promoted the system as 'self-driving'. with salespeople describing the cars as «self-driving», in Chinese, unlike in English. Moreover, they appeared to demonstrate the car's functioning by leaving their hands off the steering wheel, leading the purchaser to believe the vehicle was capable of operating fully autonomously.

The company reported that they had never described autopilot as an autonomous technology or self-driving car, and that third-party descriptions to this effect are not accurate[470].

From the framework just sketched a series of common problem seem to arise: i) whether or not a consumer expectation of the high performance of the CADs' system justifies qualifying the actual underperformance as a defect, even though no technical failure occurs; and ii) how access to data can be assured for the purpose of ascertaining and apportioning liability, considering that event data recorder might be damaged during the accident and – mostly

---

[468] «We got access to the logs. Data from the vehicle shows that Autosteer was not engaged at the time of this collision. Prior to the collision, Autosteer was in use periodically throughout the approximately 50-minute trip. The most recent such use ended when, approximately 40 seconds prior to the collision, the vehicle did not detect the driver's hands on the wheel and began a rapidly escalating set of visual and audible alerts to ensure the driver took proper control. When the driver failed to respond to 15 seconds of visual warnings and audible tones, Autosteer began a graceful abort procedure in which the music is muted, the vehicle begins to slow and the driver is instructed both visually and audibly to place their hands on the wheel. Approximately 11 seconds prior to the collision, the driver responded and regained control by holding the steering wheel, applying leftward torque to turn it, and pressing the accelerator pedal to 42%. Over 10 seconds and approximately 300m later and while under manual steering control, the driver drifted out of the lane, collided with a barrier, overcorrected, crossed both lanes of the highway, struck a median barrier, and rolled the vehicle».
https://electrek.co/2016/07/14/autopilot-tesla-model-x-crash-pa-elon-prevented-accident/
http://www.businessinsider.com/tesla-model-x-crash-autopilot-2016-7
http://money.cnn.com/2016/07/14/technology/tesla-autopilot-crash-pennsylvania/

[469] http://www.dailymail.co.uk/news/article-3790176/Shocking-dashcam-footage-shows-Tesla-Autopilot-crash-killed-Chinese-driver-futuristic-electric-car-smashed-parked-lorry.html

[470] http://www.reuters.com/article/us-tesla-china-crash-idUSKCN10L0P4
http://jalopnik.com/driver-in-chinese-tesla-crash-was-using-his-phone-1785112290

for commercial reasons – might be developed according to a proprietary scheme, thus preventing access from the victim or the court. The claimant faces as a consequence thereof such a high burden of proof that access to justice could be profoundly impaired (see §3.3.4 below).

3.3.4. Assessment

The European commission reports and staff working document. The PLD has recently been subject to assessment by the European Commission through reports[471] the results of which are also summarized in the Staff Working document[472] and are subject to further discussion by an Expert Group appointed on June 8th, 2018 that works in two formations, one dealing with the directive itself, the other with new technologies. Purpose of the expert groups is to produce a report that addresses the applicability of the PLD to traditional products and new technologies, and the development of «guiding principles for possible adaptations of applicable laws related to new technologies».

The reports as well as the Staff Working document highlight some issues that emerge both theoretically and empirically from the application of the PLD observed in the period between 2000 and 2016 across all MSs. Some of these aspects are of relevance for all applications of the directive, irrespective of the field of application – technologically advanced products or more traditional ones – others are of particular importance when robotics, IoT and AI are taken into account.

Remaining problems. The overall conclusion reached is that the PLD is adequate also to face the challenges posed by existing products[473]. However, some aspects might deserve further clarification.

Incidents of out of court settlement. The report affirms the out-of-court-settlement for claims regarding defective products. The conclusion, however, is reached through a Computer Assisted Telephone Interview CATI[474] survey and confirmed by some interviewees, namely IT representatives, legal experts, and large producers[475]. On the one hand, thence, objective – direct or indirect – data with respect to the actual numbers of cases settled, also within just some of the considered jurisdictions, is absent.

On the other hand, respondents confirming the conclusions appear to primarily belong to those groups who benefit from the limited number of claims brought about under the current framework.

Finally, it shall be stressed how other bodies of regulation – such as the directive on sales of consumers goods (henceforth, SCGD) legislation[476] –, that structurally offer a remedy for

---

[471] Ernst&Young, Technopolis, and VVA.

[472] *Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the Approximation of the Laws, Regulations, and Administrative Provisions of the Member States Concerning Liability for Defective Products (85/374/Eec)* (Brussels: European Commission, 2018).

[473] It shall be noted that the study only identified one single case where a claim was brought regarding a technologically advanced product, namely a computer storage unit, which caused a loss of information. The case, however, does not appear significant for the analysis here conducted and any consideration with respect to the adequacy of the PLD to address technologically advanced products. Not only does it lack statistical value, but also appears not to be representative of the same category of products as those here addressed, CADs and advanced robotics, whose technical complexity largely exceeds that of a computer and of its operating software. No relevant conclusions about the adequacy of the PLD when applied to emerging technologies can therefore be drawn from that example. For further information, see Ernst&Young, Technopolis, and VVA. See especially pp. 24-25.

[474] Ibid. p. 19, nt. 57.

[475] Ibid.p. 19.

[476] Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees, OJ L 171, 7.7.1999.

the user without the need to resort to in-court litigation[477], are at times erroneously overlapped with the PLD. Indeed, the cited report highlights that

> «even if the Product Liability Directive and the contractual liability legislation have different but complementary scopes, often clients do not know the difference between the Product Liability Directive and the guarantee»[478].

Therefore, considerations about the relevance of out-of-court settlements in the solutions of product liability cases, granted exclusively on stakeholders' opinions, might also suffer from a certain degree of ambiguity.

Notion of product. As per the notion of product, it is as of today disputable whether software could be included[479]. This could *per se* represent a major issue when CADs and any other technologically advanced product is considered, where the software and hardware element are tightly connected in their functioning, and most likely the former – such as in the case of CADs – represents the novel aspect of the application, differentiating it from the technology it intends to replace – traditional vehicles, in the current hypothesis –.

The ascertainment of the causal nexus. The ascertainment of the causal nexus between the defect and the damage appears then to be another aspect that burdens the claimant, preventing litigation or its success[480]. Determining that harm is the consequence of a defect in the functioning of the device requires an in-depth analysis of the product, of its functioning – eventually of its design – that presupposes relevant technical expertise, acquiring which might represent a non-viable cost for the user.

The development risk defense. Finally, defenses, such as the development risk defense (art. 7, let. E, PLD) might allow manufacturers to escape liability, leaving the burden of the economic consequences of the accident on the victim, and ultimately modifying the strict standard of liability theoretically put forth by art. 2, PLD. The rationale underpinning such a defense is typical of a rule of negligence. Indeed, the manufacturer who met the state of the art of scientific development and technological advancement may not be blamed when, nonetheless a harmful event resulted from the use of his product. Theoretically, no additional safety investment could be demanded of him[481], thence no further deterrence could be provided by an objective standard of liability holding him liable even in such cases where he could not be blamed. However, as indicated by recitals n° 1 and 2, PLD respectively, said rules are intended to ensure

> « […] a differing degree of protection of the consumer against damage caused by a defective product to his health or property», and
>
> «liability without fault on the part of the producer is the sole means of adequately solving the problem»

Therefore, in the perspective of ensuring victim's compensation the circumstance that the agent may not be reprehended for the standard of behaviour he conformed to appears secondary. **The risk of unexpected and unforeseeable outcomes – or unknown unknowns – is better borne by the party who derives economic benefits from the activity overall, rather than the occasional harmed party**. The former might insure against such events – assessing the statistical possibility of their occurrence – and on the one hand could provide needed compensation, and on the other hand could manage such

---

[477] Primarily the repairing and/or substitution of the non-conforming good (see art. 3, SCGD)
[478] Ernst&Young, Technopolis, and VVA., p. 56.
[479] Bernhard A. Koch, "Product Liability in Austria," in *Product Liability. An Analysis of the State of the Art in the Era of New Technologies*, ed. Piotr Machnikowski (Cambridge: Intersentia, 2016). See Forste and Graf von Westphalen. See in particular §47.
[480] Ernst&Young, Technopolis, and VVA. See especially p. 28.
[481] See also Richard Posner, *Economic Analysis of Law*, Seventh ed. (Wolters Kluwer, 2007).; Castronovo.

costs by spreading them onto all users of the same product. Such an approach is part of an alternative methodology – not entirely foreign to the PLD and current legislation – that might be called a Risk-Management Approach or RMA (see §3.3.4.2 below).

Further problems brought about by advanced technologies. Some of those criticalities are most certainly exacerbated by products such as CADs, for the reasons – discussed in greater details below (see §3.3.4.1) – that on the one hand technological complexity causes the material ascertainment of the defect to become ever more complex, as well as the exact establishment of a causal nexus, and, on the other hand, **human-machine cooperation causes different bodies of rules to overlap**. When a highly-automated vehicle is to be used by a human being who retains some control, at least under certain conditions, any accident might require the application of both the PLD and national regulation on traffic accidents, primarily tort law rules, as described above.

A study for the European Parliament has concluded that while of great importance, «pre-emptive legislation of the Product Liability Directive (PLD) to encourage deployment of connected and autonomous vehicles is not required at this time»[482] as there is a significant push to introduce connected vehicles and as manufacturers are likely to introduce their products in markets outside the EU as well and have to comply with different liability rules. The analysis for the European Parliament argues that while the current regulatory framework of the PLD seems to provide a well-balanced system, if not refined to reflect the changing system incorporating autonomous driving, the «application of the PLD to AVs will have a significant negative impact on consumer protection»[483].

3.3.4.1. Contd.: the problem of liability assessment and apportionment

The PLD is applicable across all MS, having been enacted, at times with some variations that cannot be fully detailed for the purposes of the current analysis. The PLD is certainly applicable to driverless cars, theoretically holding manufacturers liable in all cases where the accident can be traced back to a defect in the vehicle. However, demonstrating the existence of a defect in design, and determining that this was the cause of the accident might be extremely problematic for the victim and, depending on the value of the claim, economically inefficient. Even in the case of serious accidents, where substantial bodily injuries are suffered, the cost of evidentiary acquisition might exceed the amount of damages to be liquidated. The risk associated with losing in court litigation – despite attempts are made to acquire necessary evidence – might further discourage actions from being brought against manufacturers.

In the above-reported accidents it is highlighted how the data recorded for it uses the manufacturer' proprietary system, is impossible for the user to autonomously interpret. Such a material limitation would further exacerbate the evidentiary burden for the claimant.

Assessment and apportionment of liability in accidents involving traditional vehicles. As anticipated above, accidents involving the use of a partially autonomous vehicle might be due to human intervention or misuse of the vehicle and of its autonomous functions. In such a perspective, it shall suffice to recall how each MS provides for tort law rules that, primarily grounded on a notion of fault, hold the driver liable, who caused the accident, and in some cases the owner of the vehicle, jointly and severally, in an objective fashion.

When an accident involving traditional vehicles occurs the liability has to be apportioned among the drivers, based on material observations of the accident's dynamics. This entails determining which is responsible, having violated the street code, norms of prudence and

---

[482] Evas. See esp. p. 138.
[483] Ibid. See esp. p. 24.

diligence, ultimately failing to comply with a desirable conduct that theoretically may be identified.

Assessment and apportionment of liability in accidents involving at least one CAD. When even just one partially autonomous vehicle is involved, instead, the possibility that the accident is due to a malfunctioning of the device needs to be considered. This might be the case when the accident occurs while the autonomous function is being utilized – which would not always be the case when level 2-4 SAE are considered –, yet the very decision to activate such a function in the given circumstances might in and by itself be deemed erratic, that being once again the responsibility of the human driver. Moreover, if the interaction takes into account the possibility that the crash is a consequence of a failure of the various systems – connection and infrastructure – involved in the management of the driving task, the picture is further complicated.

As a result, liability apportionment might become extremely complex and costly, requiring substantial litigation, which ultimately might be – inefficiently – prevented leaving the economic burden of damage compensation either upon the user – even in cases where he is not responsible – or the owner. They, indeed might have no sufficient economic incentives and resources to ascertain the liability of the other parties, and thence pursue actions in recourse against them.

If service providers and infrastructure providers are considered – and increasing automation will involve connected vehicles and smart infrastructures tightly cooperating in the handling of the driving task – liability apportionment will become even more complex for the claimant, who would theoretically be required to determine whether the accident is to be traced back to the malfunctioning of the device – and whether it could be deemed defective – or to a failure in the other relevant systems – providing connecting services, data, or inputs from the road –.

The effect of extant regulation on the roll out of CADs. A recent study[484] – through a basic game-theoretical analysis of the interaction between two vehicles involved in a crash – attempts to show the effect of extant regulation and evidentiary burdens when all these different players are taken into account. According to the study, the likely outcome is that vehicles' owners, in all systems that provide for their joint and several liability, will be primarily targeted in case an accident occurs, irrespective of the reason that caused it. At the same time, and for the considerations already briefly sketched above, the cost of ascertainment of a defect or system failure would be such as to radically discourage any possible action in recourse towards potentially responsible professional parties. The overall outcome, absent legal reform, would be that of placing a relevant burden, in particular on the earlier adopters of more technologically advanced vehicles, that at the same time would not entail the full internalization of costs that producers and service providers would generate.

Such burden would be anticipated by the rational agent when considering purchasing an increasingly autonomous vehicle over a traditional one, leading to choosing the latter unless the performance of the – semi-autonomous – vehicle largely exceeds that of the average human driver. Such a result would be profoundly inefficient. Indeed, from a purely technological standpoint, the alternative between a traditional vehicle and an autonomous one ought to be indifferent as soon as the performance of the latter equals that of the specific driver[485]. In fact, the benefits of autonomous driving are most commonly described as relevant for society as a whole, ideally reshaping traffic and modern cities structures,

---

[484] See Bertolini and Riccaboni.

[485] Of the average driver in all cases that an average agent is considered, should instead the user possess superior driving capabilities, as soon as the vehicles meets them.

reducing accidents, primarily fatal ones[486]. Transition towards automation will necessarily occur over time, also due to technological constraints as well as market mechanisms, since typically vehicles are expensive and long-lasting goods, with a slower replacement rate compared to other technologically advanced products. The pace at which it happens is also relevant[487], and by delaying early adoption liability rules could substantially stretch these transition phase, with all costs associated.

3.3.4.2. Alternative approaches to liability assessment and apportionment

First alternative: no intervention. The first option is to leave the European framework unaltered, primarily with respect to the PLD. In such a scenario, owners of increasingly autonomous vehicles could be burdened with the responsibility for accidents they do not manage to demonstrate are due to a malfunctioning of the vehicle or of any of the related services. This would delay the uptake of CADs, in particular by early adopters stretching the transition phase towards higher levels of automation (SAE level 3 and above).

Consequence: reliance on MSs' legislation. Absent European intervention, some MSs have already taken action towards the adoption of ad-hoc liability rules for CADs. This, however, produces several side effects. On the one hand, national initiatives cause fragmentation that not only affects the creation of a level playing field for European manufacturers, but might also determine different incentives towards alternative technological solutions. Liability rules that primarily burden the manufacturer could favor solutions of full automation that do not allow the user to retain control and decide when to activate the driverless function. To the contrary, should the owner or user be responsible the opposite solution is expected to prevail[488]. Different approaches among MSs would provide diverging incentives among manufacturers, to the detriment of European industry.

On the other hand, solutions adopted so far do not appear radically solving the above-described issue. Primarily, they do not eliminate the need for complex factual assessments, still requiring the apportionment of liability between the manufacturer and the user, under certain conditions that vary.

In this sense, the UK and German reforms present both commonalities and differences. The UK model is based on the assumption that extending the insurance system applicable to non-automated-driving is preferable than requiring the user to pay damages, and then rely on a product liability action, for that is likely to be time-consuming and costly.

In this sense, a first- and third-party insurance scheme the owner of the vehicle is required to purchase ensures the victim obtains prompt and certain compensation, clearly identifying the subject to be sued, resting liability on the party best position to pay (the insurance company itself), irrespectively of any ascertainment about the details of the accident and, more specifically, the mode – traditional or autonomous – in which the vehicle was driving. From the victim's perspective, the solution thus appears to set an efficient compensatory scheme.

However, the apportionment of liability between the insurer and the user is problematic, and might trigger substantial litigation, thence partially – if not completely – vanishing the theoretical advantages of the insurance scheme just sketched.

Indeed, the possibility for the company to escape liability in case the use of the autonomous mode was *ex post* ascertained as being inappropriate – in light of the overall circumstances –, despite intended to discourage morally hazardous behaviour on the side of the user, will ultimately elicit litigation in most – if not all – cases when an accident occurs while the

---

[486] Alberto Broggi et al., "Intelligent Vehicles," in *Handbook of Robotics*, ed. Bruno Siciliano and Oussama Khatib (Springer, 2008). Over 90% of accidents are deemed due to human error.
[487] For further discussion, see Bertolini and Riccaboni.
[488] For a more detailed discussion, see ibid.

driverless function is activated. Therefore, as soon as a claim is brought by the victim to the insurer, the latter will most likely attempt to show the choice to relinquish control to the vehicle was unreasonable, causing the overall ascertainment to become complex, and costly. The economic incentives are, in fact, substantial, for, should it succeed, it would be able to recover the amounts liquidated to the third party, by suing the user in recourse, or radically denying compensation to the user himself.

Moreover, the UK regulation burdens the user for all safety-critical software updates, excluding the liability of the insurer towards the insured person in case they are not installed[489].

The very duty to update is rested on the party that is not best suited to ensure compliance. It may be easily observed how individuals fail to install even safety-critical patches to applications and software to be used on their hand-held devices or computers. Distraction, as well as failure to understand the nature, urgency, and importance of the single update, or the frequently untimely fashion in which the request is prompted to the user – forcing an interruption of the activity carried out at the moment, eventually, in the case considered, the driving task itself – determine the decision to postpone installation. Thence, if the legislator intended to ensure that all vehicles circulating had the most updated software installed it ought to burden the manufacturer, holding him responsible. Indeed, he would be best positioned to minimize the risk associated with users' negligence, by conceiving its vehicles in a way that software is always installed when necessary – if possible overnight and when it is not in use, minimizing inconveniences – eventually forcing a halt unless it was safe to proceed.

The UK legislation thence fails to meet both criteria of a risk-management approach, for it does not ensure risks are managed by the party best positioned to do so, namely the insurance company, nor that the party is burdened who is capable of minimizing it, the manufacturer.

Moreover, by allowing for the possibility of the insurer to escape the duty to compensate the victim in the first instance, it would not reduce or ease litigation substantially, and eventually expose the victim to the possibility of failing to obtain due compensation, if not discouraging a claim on her side in the first place. One could expect the system to require the creation of an additional fund for those victims[490], that would ultimately produce that socialization of damage the conceived solution fails to directly pursue[491].

Overall, the legislation does not substantially depart from the current system, still resting on the ascertainment of some form of fault – in choosing which mode to activate, or in failing to update software –, despite adopting a strategy that primarily aims at victims' compensation through compulsory insurance schemes.

Similar conclusions can be reached for the model set out by German legislation, whereby liability primarily rests upon the user and owner. In such a perspective, the duty to remain vigilant, clearly implies a fault-centered rationale, demanding a diligent behaviour on the side of the user while the autonomous function is activated.

---

[489] Clause 4(1).

[490] That could be similar to the Italian «Fondo di Garanzia per le Vittime della Strada», regulated by the Code of Private Insurance (D. Lgs 209/2005, art. 283 ff.). The fund, which is administrated by a public controlled entity (Consap) under the vigilance of the Ministry for the Economic Development, is designed to compensate damaged caused in a variety of cases exceeding ordinary circumstances, such as those caused by non-identified vehicles (for personal damages and, in some cases, property damages), non-insured vehicles (for both personal and property damages) and vehicles circulating against the will of the owner. Although specific caps apply to each category, a general cap of € 6.070.000,00 for personal damages, and of €1.220.000,00 for damage to property applies. The Fund is financed through a percentage of the premium payed by policy holders for the compulsory car insurance.

[491] Bertolini and Riccaboni.

However, one of the major criticalities automated driving aims at solving is precisely human incapability in maintaining adequate levels of attention, itself one of the main causes of current traffic accidents. This very aspect could also lead to further litigation on the ground that design that failed to consider such human constraints, could be deemed defective[492].

It shall be noted that even compulsory insurance schemes, such as those provided for by the MID (see §3.3.2.3), without a preceding clarification of the liability framework, would prove insufficient. Indeed, uncertainty with respect to liability apportionment reflects upon the very possibility of identifying *ex ante* whom shall insure and against which risks.

Reform of the PLD. A second option would entail a reform of the PLD, despite the conclusions reached in the above mentioned studies, in light of the criticalities nonetheless here highlighted. In particular, the burden of proof with respect to the causal nexus could be reshaped so as to ease the position of the claimant, eventually with respect to possible actions in recourse against the manufacturer. The extension of the notion of product could also clearly encompass software applications.

However, threefold considerations can be derived from a similar approach. Firstly, the revision of the PLD is broader an issue than the mere regulation of CADs. In particular, the very general nature of the directive, conceived to address all products irrespective of their characteristics, might require attentive considerations for the implications in other fields. Because of that, secondly, it might further delay the adoption of EU regulation on CADs. Thirdly, the reversal of the burden of proof with respect to the causal nexus would represent a radical modification of current legislation and of its underlying rationale, leading towards the adoption of – almost – absolute liability rules, such as those that pertain to a Risk-Management Approach (henceforth RMA), as that described below.

3.3.5. Conclusions and recommendations

Applicable legislation – PLD, MID, national traffic rules. CADs are regulated at EU level by the PLD and MID. Both the PLD and the MID were subject to official evaluation to consider possible revision, also in light of technological development. As of now, the Commission decided not to modify the PLD, while a proposal of reform for the MID was developed, which, however, does not address CADs.

Applicable legislation – national traffic rules. Since CADs could fall – in most cases (§3.1.1.1) – under the definition of vehicle, MSs' legislation on traffic accidents and corresponding insurance requirements applies, when ad-hoc legislation is lacking. As of now, only Germany and the UK have adopted a binding law regulating civil liability for CADs.

Traffic liability for traditional vehicles. Although MSs generally hold the driver and/or owner responsible, often jointly and severally, national traffic liability rules offer a highly heterogeneous scenario. As showed by a recent study[493] – MSs adopt different models of liability, ranging from fault-based rules to semi-strict and strict liability schemes and automatic compensation solutions. Different exceptions, limits, and criteria for the assessment of the award are set.

Traffic liability for CADs. Under German law, only driving systems up to level 4 SAE are allowed, and the driver of a highly automated vehicle is under a duty to supervise the driving task, and resume control when indicated by the system, or when objective circumstances require him to do so. Should he fail to do that, he would be liable for the accident.

The UK bill, on the contrary, addresses liability issues by primarily extending to CADs the same insurance duties that have been already enacted for traditional vehicles. Despite

[492] Ibid.
[493] Evas.

tending towards the automatic-compensation scheme, UK legislation still displays fault-based elements, as it burdens the owner of the vehicle with a duty to install safety-critical updates, thus denying compensation to him, or allowing insurance companies to act in recourse, should he fail to do that, in case an accident results as a consequence thereof.

Overlap of different legal frameworks. The legal framework applicable to CADs shows how increasing automation in the driving task causes different bodies of legislation to overlap. The PLD and traffic liability rules – either ad-hoc, or designed for traditional vehicles – will simultaneously apply to the same accident, so long as the vehicle is not fully autonomous and the driving task is shared between the human driver and the autonomous system (up to level 4 SAE).

Difficult ascertainment and apportionment of liability. Apportioning liability in such cases becomes problematic, and exacerbates the major criticalities that current EU legislation (namely the PLD) displays. In particular, it will be difficult for victims to demonstrate that the system was defective, both because of technological complexity and limited access to data – since the recording system of the vehicle is mostly based on a proprietary scheme, allowing only the manufacturer to retrieve and interpret data –. As a result, victims may be discouraged to bring litigation towards manufacturers, to the disadvantage of the human user or owner, or even hindering access to justice.

Against this background, imposing duties to insure – although theoretically positive – is *per se* insufficient, so long as it is not clarified which party bears what risk, and thence who is to be held liable for each kind of accident.

Alternative approaches. These issues can be managed through three alternative approaches, namely: (i) no action; (ii) reform of the PLD; (iii) adopting ad-hoc legislation;

No action. Leaving the *status quo*, without adopting any action, is not advisable, since it will lead MSs to adopt CADs-specific legislation at national level – as it is already happening –, causing the fragmentation of the EU legal system and market.

Reform of the PLD. However, reform of the PLD also might be deemed sub-optimal, as it might require more complex ascertainments due to its broad field of application – theoretically any product –, and might exceed the purpose of easing market penetration by CADs, also requiring excessive time for its completion. Therefore, the same problems arising from option (i) above also apply here.

Ad-hoc legislation. On the contrary, ad-hoc legislation at European level, setting uniform rules which could provide the right incentives to all the subjects involved, could ease the penetration of CADs in the market with relevant economic and social benefits.

Recommended solution: ad-hoc European legislation, pursuant to RMA. For this purpose, such ad-hoc legislation should favor a Risk Management Approach (RMA) – as defined in §1.4 –, thus primarily aiming at ensuring prompt and adequate compensation to the victims, and burdening the party who is best positioned to insure and minimize risks (or ensure compliance).

More specifically, strict liability rules identifying one clearly responsible party towards the victim – pursuant to a one-stop-shop solution – should be favored, since they limit litigation costs, ease access to justice by a wider share of potential victims, providing very clear criteria for the ascertainment of liability.

The duty to update software, for example, should be rested on the manufacturer, to increase the probability of correct compliance, and ultimately easing compensation of the victim, should an accident occur.

Lastly, uniformity of rules is not only required to create a level playing field, in a legal perspective, but also to avoid market and technological fragmentation. Indeed, since liability rules influence which kind of technological solution will prevail, differing rules may favor diverging approaches to automation, limiting the possibility of a vehicle conceived to operate under a given legal framework to function and/or be used in a different one.

4. BIBLIOGRAPHY

A Pathway to Driverless Cars: A Code of Practice for Testing. London: Department for Transport, 2015.

The "Blue Guide" on the Implementation of Eu Products Rules. Brussels: European Commission, 2016.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Europe's Next Leaders: The Start-up and Scale-up Initiative. Strasbourg: European Commission, 2016.

Communication. A European Strategy on Cooperative Intelligent Transport Systems, a Milestone Towards Cooperative, Connected and Automated Mobility. Brussels: European Commission, 2016.

Communication Investing in a Smart, Innovative and Sustainable Industry. A Renewed Eu Industrial Policy Strategy. European Commission, 2017.

European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(Inl)). European Parliament, 2017.

Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building Strong Cybersecurity for the Eu Brussels: European Commission, 2017.

Ppe Guidelines Guide to Application of the Ppe Directive 89/686/Eec. European Commission, 2017.

Commission Staff Working Document. Evaluation of Council Directive 85/374/Eec of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products. Brussels: European Commission, 2018.

Commission Staff Working Document. Liability for Emerging Digital Technologies. Brussels: European Commission, 2018.

Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions. Fintech Action Plan: For a More Competitive and Innovative European Financial Sector. Brussels: European Commission, 2018.

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Artificial Intelligence for Europe. Brussels: European Commission, 2018.

Cybersecurity for Connected Products. Position Paper. Brussels: ANEC-BEUC, 2018.

Frequently Asked Questions: Financial Technology (Fintech) Action Plan. Brussels: European Commission, 2018.

Position Paper on Policy and Regulatory Needs, European Harmonisation Munich: CARTRE - Coordination of Automated Road Transport Deployment for Europe, 2018.

Position Paper on Safety Validation and Roadworthiness Testing. Munich: CARTRE - Connected and Automated Road and Transportation Deployment for Europe, 2018.

Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the Approximation of the Laws, Regulations, and Administrative Provisions of the Member States Concerning Liability for Defective Products (85/374/Eec). Brussels: European Commission, 2018.

Adaptive. *Legal Aspects on Automated Driving*. 2017.

Alemzedah, H. and al. *Targeted Attacks on Tele-Operated Surgical Robots: Dynamic Model-Based Detection and Mitigation*. 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016.

Amigoni, F. and V. Schiaffonati. "Good Experimental Methodologies and Simulation in Autonomous Mobile Robotics." In *Model-Based Reasoning in Science and Technology. Studies in Computational Intelligence*, edited by L. Magnani, W. Carnielli, and C. Pizzi. Berlin, Heidelberg: Springer, 2010.

Amigoni, Francesco, Monica Reggiani, and Viola Schiaffonati. "An Insightful Comparison between Experiments in Mobile Robotics and in Science." *Autonomous Robots* 27 (2009): 313.

Andersen, Rasmus Eckholdt, Emil Blixt Hansen, David Cerny, Steffen Madsen, Biranavan Pulendralingam, Simon Bøgh, and Dimitrios Chrysostomou. "Integration of a Skill-Based Collaborative Mobile Robot in a Smart Cyber-Physical Environment." *Procedia Manufacturing*, no. 11 (2017): 114.

Arosh, S., S. Prakash, S. K. Nayak, and S. P. Duttagupta. "Fitness Function Based Sensor Degradation Estimating Using Hoo Filter." *Procedia Computer Science* 58, (2015): 172-77. http://creativecommons.org/licenses/by-nc-nd/4.0/.

Atain Kouadio, Jean-Jacques and Adel Sghaier. *Les Robots Et Dispositifs D'assistance Physique: Etat Des Lieux Et Enjeux Pour La Prévention*. Paris: Institut National de Recherche et de Securité, 2017.

Barnard, Y., F. Fischer, and M. Flament. "Field Operational Tests and Deployment Plans." In *Vehicular Ad Hoc Networks*, edited by C. Campolo, A. Molinaro, and R. Scopigno. Cham: Springer, 2015.

Bauer, W., M. Bender, M. Braun, P. Rally, and O. Scholtz. *Leichtbauroboter in Der Manuellen Montage - Einfach Einfach Anfangen. Erste Erfahrungen Von Anwenderunternehmen*. 2016.

Bellisario, Elena. "Il Danno Da Prodotto Conforme Tra Regole Preventive E Regole Risarcitorie." *Europa e diritto privato*, no. 3 (2016): 841.

Bertolini, Andrea. "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules." *Law Innovation and Technology* 5, no. 2 (2013): 214.

Bertolini, Andrea. "Insurance and Risk Management for Robotic Devices: Identifying the Problems." *Global Jurist*, no. 2 (2016): 1-24.

Bertolini, Andrea and Giuseppe Aiello. "Robot Companions: A Legal and Ethical Analysis." *The Information Society. An International Journal* 34, no. 3 (2018): 130-40.

Bertolini, Andrea and Massimo Riccaboni. *The Regulation of Connected and Automated Driving. A Law and Economics Analysis of Liability Rules*. Edited by Working Paper, 2018.

Bonsignorio, Fabio and Angel P. del Pobil. "Toward Replicable and Measurable Robotics Research." *IEEE Robotics & Automation Magazine*, no. 9 (2015): 32.

Bonsignorio, Fabio, John Hallam, and Angel P. Del Pobil. *Gem Guidelines*. EURON - GEM SIG, 2008.

Bonsignorio, Fabio, Elena Messina, and Angel P. del Pobil. "Fostering Progress in Performance Evaluation and Benchmarking of Robotic and Automation Systems." *IEEE Robotics & Automation Magazine*, no. 3 (2014): 22.

Borghetti, Jean-Sébastien. "Product Liability in France." In *European Product Liability. An Analysis of the State of the Art in the Era of New Technologies*, edited by Piotr Machnikowski, 205-36. Cambridge: Intersentia, 2016.

Bougrain, L. and B. Le Golvan. "Les Neuroprothèses." *L'Évolution psychiatrique* 81, no. 2 (2016): 353.

Broggi, Alberto, Alexander Zelinsky, Michel Parent, and Charles E. Torpe. "Intelligent Vehicles." In *Handbook of Robotics*, edited by Bruno Siciliano and Oussama Khatib: Springer, 2008.

Castronovo, Carlo. *La Nuova Responsabilità Civile*. Milano: Giuffrè, 2006.

Cerrudo, C. and L. Apa. *Hacking Robots before Skynet*. IOACTIVE, 2017.

Cerrudo, C. and L. Apa. *Hacking Robots before Skynet – Technical Appendix*. IOACTIVE, 2017.

Chan, J. and al. "On the Benefits and Pitfalls of Analogies for Innovative Design: Ideation Performance Based on Analogical Distance, Commonness, and Modality of Examples." *Journal of Mechanical Design* 133, no. 8 (2011). http://dx.doi.org/doi:10.1115/1.4004396.

Chaumette, François and Seth Hutchinson. "Visual Servoing and Visual Tracking." In *Springer Handbook of Robotics*, edited by Bruno Siciliano and Oussama Khatib, 563-83. Berlin: Springer, 2008.

Chinchkhede, N. D. and A. T. Shende. "Automated Guided Vehicle as an Office Boy." *International Journal of Scientific Research in Science and Technology* 4, no. 3 (2018): 18.

Coeuret, Alain. *Droit Pénal Du Travail*. Paris: LexisNexis, 2008.

Cuccuru, Pierluigi. "European Standards at the Bar: Routes Towards a Meaningful Involvement of the Court of Justice in Technical Standardisation." *European Law Journal* (2018 (forthcoming)).

Davies, Ron. *Industry 4.0 Digitalisation for Productivity and Growth*. European Parliament, 2015.

De Looze, Michiel P., Tim Bosch, Frank Krause, Konrad S. Stadler, and Leonard W. O'Sullivan. "Exoskeletons for Industrial Application and Their Potential Effects on Physical Work Load." *Ergonomics* (2015): 3.

Dhillon, B. S. "Robot Testing and Information Related to Robots." In *Robot Reliability and Safety*, 210-25. New York: Springer, 1990.

Dudek, Gregory and Michael Jenkin. *Computational Principles of Mobile Robotics'*. New York: Cambridge University Press, 2010.

Duffy, Austen C. "Where Do Computational Mathematics and Computational Statistics Converge? ." *Wiley Interdisciplinary Reviews: Computational Statistics* 6, no. 5 (2014): 341-51.

Eliantonio, Mariolina and Carlo Colombo. "Harmonized Technical Standards as Part of Eu Law: Juridification with a Number of Unresolved Legitimacy Concerns?" *Maastricht Journal of European and Comparative Law* 24, no. 2 (2017): 323.

Ernst&Young, Technopolis, and VVA. *Evaluation of Council Directive 85/374/Eec on the Approximation of Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products*. Brussels: European Commission, 2018.

Evas, Tatjana. *A Common Eu Approach to Liability Rules and Insurance for Connected and Autonomous Vehicles. European Added Value Assessment Accompanying the European Parliament's Legislative Own-Initiative Report (Rapporteur: Mady Delvaux)*. EPRS European Parliamentary Research Service, 2018.

Faccio, F. and G. Cervelli. "Radiation-Induced Edge Effects in Deep Submicron Cmos Transistors." *IEEE Trans. Nucl. Sci.* 52 (2015): 2413-20. http://dx.doi.org/DOI: 10.1109/TNS.2005.860698.

Fleer, David. "Human-Like Room Segmentation for Domestic Cleaning Robots." *Robotics* 6, no. 4 (2017): 35.

Forge, Simon and Colin Blackman. *A Helping Hand for Europe. The Competitive Outlook for the Eu Robotics Industry*. European Commission, Joint Research Centre, Institute for Prospective Technological Studies, 2010.

Forste, Ulrich and Friedrich Graf von Westphalen. *Produkthaftungshandbuch*. Munich: Beck, 2012.

Gonzalez, Carlos. "7 Common Applications for Cobots." Last modified 2018. Accessed. http://www.machinedesign.com/motion-control/7-common-applications-cobots.

Greenbaum, Dov. "Ethical, Legal and Social Concerns Relating to Exoskeletons." *SIGCAS Computers & Society* 45 (2015): 3.

GWS, Cair, and Ricardo. *Gear 2030 Strategy 2015-2017. Comparative Analysis of the Competitive Position of the Eu Automotive Industry and the Impact of the Introduction of Autonomous Vehicles: Final Report - Study* European Commission, 2017.

Hagele, Martin, Klas Nilsson, and J. Norberto Pires. "Industrial Robotics." In *Springer Handbook of Robotics*, edited by B. Siciliano and O. Khatib, 964. Berlin: Springer, 2008.

Hickman, Frank. "Application of A.I. Techniques to Formulation in Mathematical Modelling " *Mathematical Modelling* 8 (1987): 43-47.

Jamil, M. and Yang X-S. "A Literature Survey for Benchmark Functions for Global Optimization Problems." *Int. Journal of Mathematical Modelling and Numerical Optimisation* 4, no. 2 (2013): 150-94. http://dx.doi.org/DOI: 10.1504/IJMMNO.2013.055204.

Jansen, Anne, Dolf van der Beek, Anita Cremers, Mark Neerincx, and Johan van Middelaar. *Opkomende Risico's Voor Arbeidsveiligheid: Werken in Dezelfde Ruimte Als Een Cobot ('Emerging Risks for Safety at Work: Working in the Same Space as a Cobot').* TNO, 2017.

Kalra, Nidhi and Susan M Paddock. *Driving to Safety. How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?* : Rand, 2016.

Kao, H.-A., n W. Ji, D. Siegel, and J. Lee. "A Cyber-Physical Interface for Automation Systems." *Machines* 3, no. 2 (2015): 93-106. https://doi.org/10.3390/machines3020093 (last accessed 7 November 2018).

Kazerooni, H. "Exoskeletons for Human Performance Augmentation." In *Springer Handbook of Robotics*, edited by B. Siciliano and O. Khatib, 775. Berlin: Springer, 2008.

Khaitan, S.K and J.D. McCallen. "Design Techniques and Applications of Cyberphysical Systems: A Survey." *IEEE Systems Journal* 9, no. 2 (2015): 350-65.

Kishore Kumar, K., M.S. Krishna, D. Ravitej, and D. Bhavana. " Design of Automatic Guided Vehicles." *International Journal of Mechanical Engineering and Technology* 3, no. 1 (2012): 24.

Koch, Bernhard A. "Product Liability in Austria." In *Product Liability. An Analysis of the State of the Art in the Era of New Technologies*, edited by Piotr Machnikowski, 121. Cambridge: Intersentia, 2016.

Kong, L. and al. "Adasharing: Adaptive Data Sharing in Collaborative Robots." *IEEE Transactions on Industrial Electronics* 64, no. 12 (2017): 9569-79.

Kortenkamp, David and Reid Simmons. "Robotic Systemic Architectures and Programming." In *Springer Handbook of Robotics*, edited by Bruno Siciliano and Oussama Khatib, 187. Wien: Springer, 2008.

KPMG. *Autonomous Vehicles Readiness Index. Assessing Countries' Openness and Preparedness for Autonomous Vehicles*. 2017.

Kwek, Phey Sia , Zhan Wei Siew, Chen How Wong, Bih Lii Chua, and Kenneth Tze Kin Teo. *Development of a Wireless Device Control Based Mobile Robot Navigation System*. IEEE Global High Tech Congress on Electronics, 2012.

Laval, J., L. Fabresse, and N. Bouraqadi. *A Methodology for Testing Mobile Autonomous Robots.* IEEE/RSJ International Conference on Intelligent Robots and Systems, 2013.

Lee, E.A. *Cyber Physical Systems: Design Challenges*. IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), 2008.

Lee, S. Y. and H. W. Yang. "Navigation of Automated Guided Vehicles Using Magnet Spot Guidance Method." *Robotics and Computer-integrated Manufacturing* 28 (2012): 425.

Leenes, Ronald, Erica Palmerini, Bert-Jaap Koops, Andrea Bertolini, Pericle Salvini, and Federica Lucivero. "Regulatory Challenges of Robotics: Some Guidelines for

Addressing Legal and Ethical Issues." *Law Innovation and Technology* 9 (2017): 1-44.

Magnus, Ulrich. "Product Liability in Germany." In *European Product Liability. An Analysis of the State of the Art in the Era of New Technologies*, edited by Piotr Machnikowski, 237-74. Cambridge: Intersentia, 2016.

Marinov, Bobby. "22 Exoskeletons for Work and Industry into 6 Categories." Last modified 2016. Accessed. 22 Exoskeletons For Work and Industry Into 6 Categories.

Marques, Lino, "Good Experimental Methodologies for Mobile Robot Olfaction." Workshop on Good Experimental Methodology in Robotics, part of the Robotics: Science and Systems Conference, 2009.

Mazzotta, Oronzo. *Diritto Del Lavoro*. Milan: Giuffrè, 2013.

McClean, J., C. Stull, C. Farrar, and Mascareñas D. *A Preliminary Cyber-Physical Security Assessment of the Robot Operating System (Ros)*. Proc. SPIE 8741. Unmanned Systems Technology XV, 2013.

Menzies, Tim. "Beyond Data Mining." *IEEE Software,* 30, no. 3 (2013): 92.

Mohanty, M. and A. Bhardwaj. *An Exploration of Robot Utilization for Vehicles in Tracking Shortest Route*. International MultiConference of Engineers and Computer Scientists. Hong Kong, 2014.

Moore, C. A., M. A. Peshkin, and J. E. Colgate. *Cobot Implementation of 3d Virtual Surfaces*. Proceedings 2002 IEEE International Conference on Robotics and Automation (Cat. No.02CH37292). Washington, D.C., 2002.

Muller, S. L., S. Stiehm, S. Jeschke, and A. Richert. "Subjective Stress in Hybrid Collaboration." In *Social Robotics*, edited by A. Kheddar, 597. Cham: Springer, 2017.

Negri, E., L. Fumagalli, and Macchi. M. "A Review of the Roles of Digital Twins in Cps-Based Production Systems." *Procedia Manufacturing*, no. 11 (2017): 939-48.

Niño-Suarez, Paola Andrea, Eduardo Aranda-Bricaire, and Martin Velasco-Villa. *Discrete-Time Sliding Mode Path-Tracking Control for a Wheeled Mobile Robot*. 45th IEEE Conference on Decision & Control. San Diego, 2015.

Oakley, J.P. and B.L. Satherley. "Improving Image Quality in Poor Visibility Conditions Using a Physical Model for Contrast Degradation." *IEEE Transactions on Image Processing* 7, no. 2 (1998): 167-79.

Oftadeh, R., M.M Aref, R. Ghabcheloo, and J. Mattila. *Mechatronic Design of a Four Wheel Steering Mobile Robot with Fault-Tolerant Odometry Feedback*. l6th IFAC Symposium on Mechatronic Systems. Hangzhou, 2013.

Palmerini, Erica, Federico Azzarri, Fiorella Battaglia, Andrea Bertolini, Antonio Carnevale, Jacopo Carpaneto, Filippo Cavallo, Angela Di Carlo, Marco Cempini, Marco Controzzi, Bert-Jaap Koops, Federica Lucivero, Nikil Mukerji, Luca Nocco, Alberto Pirni, Humah Shah, Pericle Salvini, Maurice Schellekens, and Kevin Warwick. *Guidelines on Regulating Robotics*. 2014.

Perry, J. C., J. Rosen, and S. Burns. "Upper-Limb Powered Exoskeleton Design." *IEEE/ASME Transactions on Mechatronics* 4 (2007): 408.

Pittman, Kagan. "Automating Material Transportation with Mobile Industrial Robots." Last modified 2017. Accessed. https://www.engineering.com/AdvancedManufacturing/ArticleID/14627/Automating-Material-Transportation-with-Mobile-Industrial-Robots.aspx.

Posner, Richard. *Economic Analysis of Law*. Seventh ed.: Wolters Kluwer, 2007.

Prattichizzo, Domenico and Jeffrey C. Trinkle. "Grasping." In *Springer Handbook of Robotics*, edited by Bruno Siciliano and Oussama Khatib, 671-700. Berlin: Springer, 2008.

Rivest, Chantal. "France: From a Minimalist Transposition to a Full Scale Reform of the Ohs System." In *Regulating Health and Safety Management in the European Union*, edited by David Walters, 81. Bruxelles: PIE, 2002.

Samuel, A. "Some Studies in Machine Learning Using the Game of Checkers." *IBM Journal of Research and Development* 3, no. 3 (1959): 210–29.

Sanislav, T. and L. Micla. "Cyber-Physical Systems – Concepts, Challenges and Research Areas." *Control Engineering and Applied Informatics* 14, no. 2 (2012): 28-33.

Schaapman, Marian. "Germany: Occupational Health and Safety Discourse and the Implementation of the Framework Directive." In *Regulating Health and Safety Management in the European Union*, edited by David Walters, 110. Brussels: PIE, 2002.

Schepel, Harm. *The Constitution of Private Governance. Product Standards in the Regulation of Integrating Markets*. Oxford: Hart, 2005.

Schlusse, M. and J. Rossmann. *From Simulation to Experimentable Digital Twins: Simulation-Based Development and Operation of Complex Technical Systems*. IEEE International Symposium on Systems Engineering (ISSE), 2016.

Scordamaglia, Irene. "Malfunzionamento Delle Macchine E Delle Attrezzature Di Lavoro: Le Concorrenti Responsabilità Penali Del Datore Di Lavoro, Del Fabbricante E Del Fornitore." *Cassazione penale*, no. 4 (2014): 1340.

Shavell, Steven. "Liability for Accidents." In *Handbook of Law and Economics*, edited by A. Mitchell Polinsky and Steven Shavell, 142. Amsterdam: Elsevier, 2007.

Shiravi, A., H. Shiravi, M. Tavallaee, and A. Ghorbani. "Toward Developing a Systematic Approach to Generate Benchmark Datasets for Intrusion Detection." *Computers & Security* 31, no. 3 (2013): 357-74. http://dx.doi.org/https://doi.org/10.1016/j.cose.2011.12.012.

Shneier, M. and R. Bostelman. *Literature Review of Mobile Robots for Manufacturing*. National Institute for Standards and Technology, 2015.

Siciliano, B. and O. Khatib, eds. *Springer Handbook of Robotics*. Berlin: Springer, 2008.

Smit, Jan, Stephan Kreutzer, Carolin Moeller, and Malin Carlberg. *Industry 4.0*. European Parliament, 2016.

Steijn, Wouter, Johan van der Vorm, Eric Luiijff, Raphaël Gallis, and Dolf van der Beek. *Opkomende Risico's Voor Arbeidsveiligheid Als Gevolg Van It-Koppelingen Van En Tussen Arbeidsmiddelen (Emerging Risks for Safety at Work Because of It-Coupling from and between Work Machinery)*. TNO, 2016.

Stoelen, Martin F., Virginia Fernández de Tejada, Alberto Jardon Huete, Carlos Balaguer, and Fabio Paolo Bonsignorio. "Distributed and Adaptive Shared Control Systems. Methodology for the Replication of Experiments." *IEEE Robotics & Automation Magazine*, no. 12 (2015): 137.

Sutcliffe, A. and P. Sawyer. *Requirements Elicitation: Towards the Unknown Unknowns*. 21st IEEE International Requirements Engineering Conference, 2013.

Taleb, Nassim Nicholas. *Antifragile: Things That Gain from Disorder*. London: Penguin, 2012.

Theurel, Jean, Jean-Jacques Atain Kouadio, Kevin Desbrosses, Laurent Kerangueven, and Cèdric Duval. *10 Idées Reçues Sur Les Exosquelettes*. Institut National de Recherche et de Securité, 2018.

Till, Alexander Leopold, Saadia Zahidi, and Vesselina Ratcheva. *The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution*. World Economic Forum, 2016.

Tripathi, G. N. and V. Rihani. "Motion Planning of an Autonomous Mobile Robot Using Artificial Neural Network." *CS&IT-CSCP* (2012): 367.

Van der Vorma, J., R. Nugent, and L. O'Sullivan. *Safety and Risk Management in Designing for the Lifecycle of an Exoskeleton: A Novel Process Developed in the Robo-Mate Project*. 6th International Conference on Applied Human Factors and Ergonomics.

Vanderborght, Bram. "On Reproducible Research." *Robotics and Automation*, no. 4 (2018).

Various. *Utilisation Des Robots D'assistance Physique À L'horizon 2030 En France*. Institut National de Recherche et de Securité, 2015.

Various. *Digitising European Industry - Digital Industrial Platforms*. European Union, 2017.

Verzijl, D., K. Dervojeda, J. Sjauw-Koen-Fa, F. Nagtegaal, L. Probst, and L. Frideres. *Smart Factories - Capacity Optimisation*. European Commission, 2014.

VVA, SSSA, and TNO. *Scenarios and Conditions for the Implementation of Cad and Proactive Mapping of Policy Measures. Interim Report 2*. European Commission, 2018.

Walters, David. "United Kingdom: From a Piecemeal Transposition to a Third Way." In *Regulating Health and Safety Management in the European Union*, edited by David Walters, 235. Brussels: PIE, 2002.

Weng, Yueh-Hsuan, Yusuke Sugahara, Kenji Hashimoto, and Atsuo Takanishi. "Intersection of "Tokku" Special Zone, Robots, and the Law: A Case Study on Legal Impacts to Humanoid Robots." *International Journal of Social Robotics*, no. 7 (2015): 841-57.

Zhang, Y., Qian. C., J. Lv, and Y. Liu. "Agent and Cyber-Physical System Based Self-Organising and Self-Adaptive Intelligent Shopfloor." *IEEE Transactions on Industrial Informatics* 13, no. 2 (2017). http://dx.doi.org/DOI: 10.1109/TII.2016.2618892.

European Commission

Title
SafeNES, Third Interim Report, Part A; Task 3 & 4, A prospective foresight study on testing, certification, liability and insurance of advanced robots, autonomous and AI-based systems including connected and automated vehicles

Luxembourg, Publications Office of the European Union

2019–162 pages

ISBN number: 978-92-79-99495-1
DOI number: 10.2759/448974

European Commission

Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems

SMART 2016/0071

Annex 4, Part B

Task 5: Prospective foresight study on specifications of event data recorders

TNO 2019 R10095

A study prepared for the European Commission
DG Communications Networks, Content & Technology
by:

TNO innovation for life
VVA CONSULTING
Sant'Anna Scuola Universitaria Superiore Pisa

Digital Single Market

This study was carried out for the European Commission by

Authors:

- Ron Snijders (TNO)
- Rino Brouwer (TNO)
- Arturo Tejada (TNO)
- Sjef van Montfort (TNO)
- Sven Jansen (TNO)

Internal identification

Contract number: 30-CE-0887241/00-16

SMART number: 2016/0071

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN number 978-92-79-99495-1

DOI:number 10.2759/448974

Catalogue number: KK-04-19-076-EN-N

Table of Contents

List of Tables

List of Figures

List of abbreviations

Acronyms	Definition
AI	Artificial Intelligence
XAI	Explainable Artificial Intelligence
ML	Machine Learning
ECU	Electronic Control Unit
EDR	Event Data Recorder
OS	Operating System
IR	Industrial Robots
CCAM	Cooperative and Connected Automated Mobility
CAD	Connected and Automated Driving
ADAS	Advanced Driving Assistance Systems
ATA	American Trucking Association
ISO	International Organization for Standardization
IEEE	Institute of Electrical and Electronics Engineers
SAE	Society of Automotive Engineers
VANET	Vehicle Ad hoc NETwork
RSU	Road Side Unit
V2V	Vehicle to Vehicle communication.
V2I	Vehicle to Infrastructure communication.
V2X	Vehicle to everything communication.
SR	Service Robots
DSR	Domestic Service Robots
HMT	Human Machine Teaming
ROS	Robot Operating System
IDS	International Data Space

1. INTRODUCTION

This third interim report, part B describes results of task 5 of the Study on Safety of non-embedded software (SafeNES); part A of the third interim report describes the results of task 3 and 4.

Task 5 of SafeNES focuses on specifications for Event Data Recorders (EDRs), popularly known as "black boxes". EDRs are devices that record and process information from a vehicle or system while it is in operation. The recorded data can be used for multiple purposes, for instance, training, safety assessment, surveillance, vehicle diagnostics, testing and development. The use of EDRs benefits accident reconstruction, future road safety, vehicle design and legal proceedings (Hynd & McCarthy, 2014) . Feedback from the EDR may also be used to improve driver behaviour and reduce fuel consumption (G. Toledo & Shiftan, 2016).

One important use of EDRs is to determine event causation and contributing factors, for example for legal liability after accidents occur. In particular, this report will focus on EDRs for road vehicles that make use of Artificial Intelligence (AI)-based algorithms and will present a recommendation on the data and information that an EDR might need to record to help establish liability. In future cases, the EDR should help to trace and explain the decision-making processes of AI-based algorithms.

This study focuses mainly on application of Event Data Recorders in the field of Connected and Automated Driving (CAD). However, many of these findings (especially those related to AI-based systems) can also be relevant to other (semi-) autonomous systems in fields such as Industrial Robots (IR), Medical and Service Robots (Bleuler et al., 2016) and Autonomous Shipping (Jalonen, Tuominen, & Wahlström, 2017).

The subtasks of task 5 described in the Inception report related to the following chapters as described in Table 20 and Figure 10. Chapter 2 provides a State of the Art description of existing event data recorders and suitable data sharing frameworks. Chapter 3 provides a general discussion on AI-based systems and its effects on the recommended requirements stated in Chapter 4. Chapter 5 summarizes the future innovation requirements needed to support the requirements stated in Chapter 4. Finally, a conclusion is provided in Chapter 6.

Table 20: Relation between the chapters and the subtasks mentioned in the Inception report.

Chapter/Section:	**Description:**	**Relation to Inception report:**
Chapter 2	State of the Art	Subtask 5.1 Subtask 5.2
Chapter 3	Provides a general discussion to support the requirements stated in Chapter 4	
Chapter 4	Recommended Requirements	Subtask 5.1 Subtask 5.2
Chapter 5	Innovation Requirements	Subtask 5.3

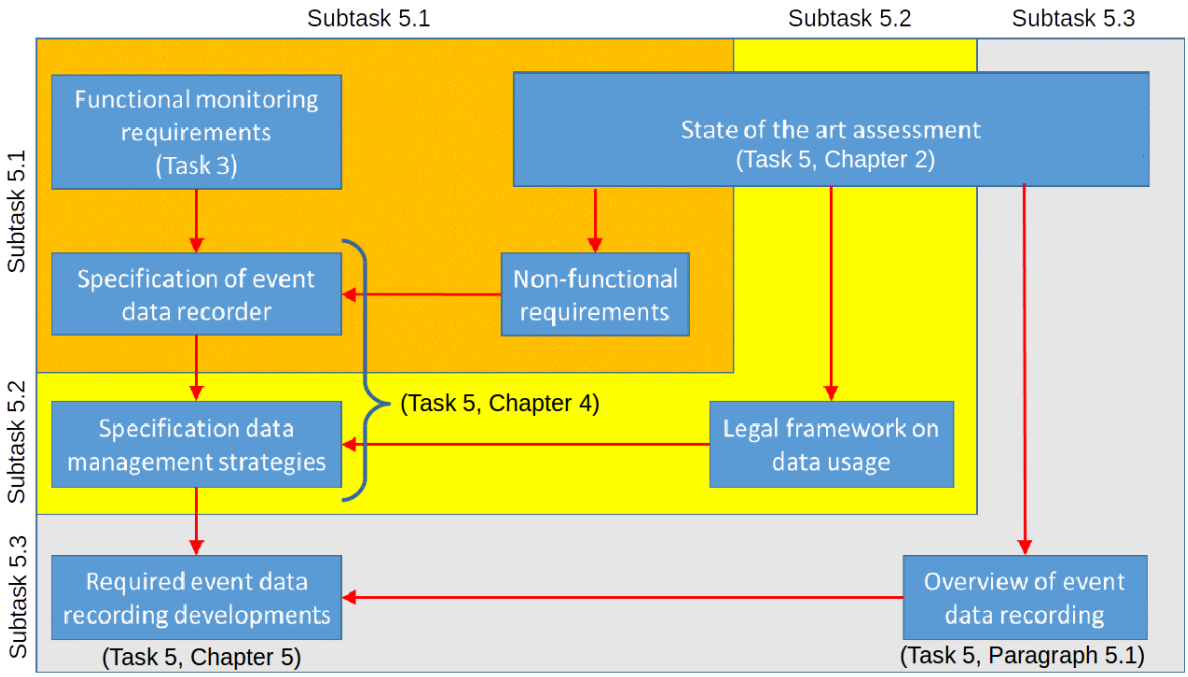


Figure 10 Overview of subtasks in relation to the chapters of this report and Task 3. Modified from the Inception report.

2. STATE OF THE ART

This chapter provides a short state of the art overview on the use of Event Data Recorders mainly within the field of Cooperative and Connected Automated Mobility (CCAM), existing and suggested requirements in literature and relevant data sharing frameworks related to the use of EDRs.

2.1. Event Data Recorders

EDRs have been applied for passenger vehicles for over 40 years and typically originates in the early airbag control module which registered some sensory information relevant for the collision such as acceleration and impact speed (Lange & Wilson, 2017; Marco P. daSilva, 2008). Since then the EDRs have become more advanced in both the diversity in the type of sensory information it records, the total duration it records around events, its resolution and the quality of the data itself.

2.1.1. Available Event Data Recorders

Today's event data recorder in the automotive sector is either a recording device that is retrofitted or is part of an on-board unit. Car manufacturers record a lot of data of their sensors and systems for maintenance purposes. Adding software that records specific data right before and after a specific event can then be seen as an event data recorder.

Many different types of EDRs[715] [716] exist and almost all new cars have an EDR installed (Hynd & McCarthy, 2014). Some generic EDRs exist (such as made by TTechAuto[717] or Squarrel[718]), but most of the on-board EDRs are developed by car manufacturers or their suppliers (see, e.g., Continental[719], Landrover[720]).

An alternative to a factory-installed EDR is a Data Acquisition System (DAS) that can be used to collect data from a vehicle. Usually these DASs are not used as EDRs but function to collect continuously driving related data and sometimes also video data for testing purposes. However, they can also be used as EDRs. A list of providers of DASs is presented in **APPENDIX A**.

[715] https://www.boschdiagnostics.com/cdr/sites/cdr/files/CDR_v16.6_Vehicle_Coverage_List_R1_0_0.pdf
[716] https://rimkus.com/media/pdfs/Event_Data_Recorder.pdf

[717] https://www.tttech-auto.com/products/testing-tools/pm-200/

[718] https://squarell.com/nl/oplossingen/event-data-recorder/

[719] https://www.continental-automotive.com/en-gl/Passenger-Cars/Chassis-Safety/Software-Functions/Function-Modules/Event-Data-Recorder-(EDR)
[720] http://www.ownerinfo.landrover.com/document/3B/2018/T19930/27015_en_GBR/proc/G1806813

2.1.2. Related Tools

Bosch and Global Information Technology provide tools to retrieve the data from most EDRs (Hynd & McCarthy, 2014). Bosch developed a data extraction kit that can be used to extract data from the EDR which they named Crash Data Retrieval kit (CDR)[721]. The documentation page of this kit lists all models that have an EDR, but it is unclear from this list who developed the EDR itself.

In addition, many alternative tools exist to collect and retrieve data from cars (see[722] for a list of data acquisition tools as used in the FOT-Net project). However, these tools are mainly used for testing purposes and fall beyond the scope of this chapter.

2.1.3. 49 CFR Part 563

The National Highway Traffic Safety Administration (NHTSA), an agency of the U.S. government, passed a regulation in 2012 describing what an EDR must log if present in a vehicle (e.g., speed, acceleration, seat belt use, braking etc., see Appendix B; see Docket-ID NHTSA-2012-0099[723]).

This Code of Federal Regulation (CFR) applies to "voluntarily installed data event recorders" and is often referred to as simply "Part 563" in literature. Many of the new N1/M1[724] vehicles in Europe have an EDR installed that comply to this 49 CFR Part 563 rule (Hynd & McCarthy, 2014).

2.1.4. Related Standards

Several relevant SAE/IEEE/ISO/ATA standards exist that specify best practises in the design and application of Event Data Recorders and tools to extract and secure its data. These includes SAE J1698, SAE J2728, SAE J196, IEEE 1616, IEEE 1616a, ISO 15031-3, ISO/TR 12353-3, ATA RP 1210 and ATA RP 1214 (see (Hynd & McCarthy, 2014) for an in depth discussion on these standards).

In addition to these standards, it is also important to take the (functional) safety standards into account that are related to the application domain in which an EDR is used. In case of the automotive sector, ISO 26262[725] provides a specification on the functional safety definitions, practises and requirements that one should adhere to during the design, production, operation and service of automobiles. Likewise, for other fields such as Service Robots, standards such as ISO 13482:2014[726] are relevant. The information recorded in the

---

[721] https://www.boschdiagnostics.com/cdr/

[722] http://wiki.fot-net.eu/index.php/Tool_Catalogue

[723] https://www.federalregister.gov/documents/2012/08/09/2012-19580/event-data-recorders#sectno-citation-%E2%80%89563.8

[724] http://www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29classification.html

[725] https://www.iso.org/standard/43464.html

EDR during an event, should help to establish a conclusion as to whether all manufacturers and suppliers adhered to standards such as these.

Furthermore, as the EDR becomes an integral part as the main witness of the behaviour of many (AI-based) systems, its integrity in terms of being tamper-proof should be considered. Cybersecurity standards, such as the SAE J3061[727], should therefore be taken into account as well.

2.1.5. EDRs and eCall

In April 2015 the European Parliament voted in favour of the eCall regulation[728] which requires all car manufacturers to implement the eCall technology in all new models starting from April 2018. In case of a serious event, the eCall technology automatically calls the European emergency telephone number 112.

Since the EDR and the eCall technology register similar information and typically trigger at the same event (e.g., a serious car accident), it is logical to assume that both functionalities might be implemented by the same device. As such, care should be taken in the design of new EDRs such that they comply to the new eCall regulations.

The need for mandatory installation of EDRs and its relation with the eCall technology is further emphasized by a recent draft report on autonomous driving in European transport[729] by the European Committee on Transport and Tourism, which underlines the following:

"Underlines the need for clear legislation obligating the installation of event data recorders in line with the eCall Regulation in order to clarify and enable the tackling, as soon as possible, of issues of liability."

2.2. Data Sharing Frameworks for Event Data recorders

The following sections provide examples of frameworks and techniques related to data management. See (Jarke & Quix, 2017) for an overview of the evolution from the traditional database designs, to data warehouse integrations, to data lake architectures and finally to the more recent data spaces. During this evolution, data sovereignty becomes increasingly more important in which an organization or entity decides for itself how it wants its data to be used and shared.

2.2.1. FOT-Net – Data Sharing Framework

FOT-Net is a networking platform for researchers who are interested in Field Operational Tests (FOTs).[730] It started in 2008 as a European support action to provide a platform for FOT researchers to share their experiences and knowledge through different workshops and newsletters. One important aspect of work done in the FOT-Net project was to promote and

---

[727] https://www.sae.org/standards/content/j3061/

[728] https://ec.europa.eu/digital-single-market/en/news/ecall-all-new-cars-april-2018

[729] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-623.787+01+DOC+PDF+V0//EN&language=EN

[730] http://fot-net.eu/

update the work of the EU project FESTA.[731] The FESTA project covered "issues concerning all aspects of the time-line and administration of a FOT, such that advice will be provided regarding aspects from needs analysis at the commencement of a FOT all the way through to the integration of the acquired data and estimation of socio-economic benefits at the end."

FOTs collect data in huge quantities and under normal daily driving conditions with 'normal' drivers (meaning not specifically trained drivers). FOTs are naturalistic driving studies (NDs) but with the focus on investigating the effects of a specific system whereas NDs focus on driving behaviour irrespective of safety functions on-board. FOT-Net Data was the third successor of the FOT-Net projects and developed a data sharing framework to share data collected by different FOTs.[732] This framework consists of:

- Project agreement content
- Data and metadata description recommendations to facilitate the understanding of the context in which the data was collected and the validity of the data.
- Data protection recommendations, focusing on personal and confidential data issues.
- Security and human subject protection training for all involved personnel.
- Support and research services
- Financial models to provide funding for the data to be maintained and available, and data access services.
- Application procedures.

(summarised from the report (Gellerman et al., 2017))

This data sharing framework covers topics that are outside the scope of this report. The main overlap is on 'Data protection recommendations'.

The report also classifies collected data in four categories:

- personal data
- sensitive personal data
- confidential commercial data
- non-sensitive data

The EU Regulation 2016/679 Art. 2 defines personal data 'as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[733] The same regulation in Art. 9 paragraph 1 indicates which personal data may not be processed and can be seen as sensitive data: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.". Exceptions apply however (see paragraph 2 of Art.

[731] http://www.its.leeds.ac.uk/festa/

[732] http://fot-net.eu/Documents/d3-1-data-sharing-framework/

[733] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

9). Confidential commercial data "is information which an organisation has taken steps to protect from disclosure" and "The definition of non-sensitive data is data that are completely anonymised and do not include any confidential commercial elements" (Gellerman et al., 2017).

With respect to EDRs all four categories of data may apply. With exception of non-sensitive data policies have to be developed how to treat the three other categories of data. Part of this policy is to determine which data is stored by the EDR and who has access to it.

2.2.2. International Data Space

Another interesting initiative is the International Data Spaces (IDS) Association which aims at:

> "*open, federated data ecosystems and marketplaces ensuring data sovereignty for the creator of the data.*" [734]

Furthermore, its specification forms:

> *"the strategic link between the creation of data in the internet of things on the one hand side and the use of this data in machine learning (ML) and artificial intelligence (AI) algorithms on the other hand side."*[735]

The IDS reference architecture (see footnote[736] for an overview) is based on European values such as data privacy and security and forms the basis for data ecosystems and market places. The architecture, interfaces and open source sample code provided by the association allows data creators to keep in control over who is using the data, for how long, for what purpose and under what kind of conditions.

2.2.3. EDR Data Distribution and Scalability

The information stored inside an EDR can help to investigate an incident only *if* the EDR actually survives the incident. For several reasons (e.g., the EDR was destroyed or its data interface malfunctioned) the data might not be able to be retrieved from the EDR (Gabauer, Newell, & Neill, 2005).

Data communicated wirelessly using systems such as Vehicle Ad hoc NETwork (VANET) could therefor also help to investigate the incident (Al-Sultan, Al-Doori, Al-Bayatti, & Zedan, 2014), especially in cases in which an EDR malfunctioned. This way, the data is distributed over multiple vehicles and infrastructures (also known as Road Site Unit's (RSU)). Sending and storing data from EDRs to RSUs periodically allows to store a backup of the EDR data in a distributed manner, but does pose privacy and integrity risks that should be taken care of (Yeung et al., 2014).

---

[734] https://www.internationaldataspaces.org/

[735] https://www.internationaldataspaces.org/publications/sharing-data-while-keeping-data-ownership-the-potential-of-ids-for-the-data-economy/

[736] https://www.internationaldataspaces.org/the-principles/#overview

New developments in Blockchain technology may also help to establish a more tamperproof accountability of road users using distributed V2X communication (van der Heijden, Engelmann, Mödinger, Schönig, & Kargl, 2017).

3. EVENT DATA RECORDERS FOR AI

3.1. Elements of a AI-based Vehicular System

In the most basic sense, any autonomous (AI-based) system, including current and future (self-driving) vehicles, are in essence robots and operate by repeatedly executing the so-called sense-think-act (or sense-plan-act) cycle (Tobergte & Curtis, 2013) shown in ***Figure 11***.

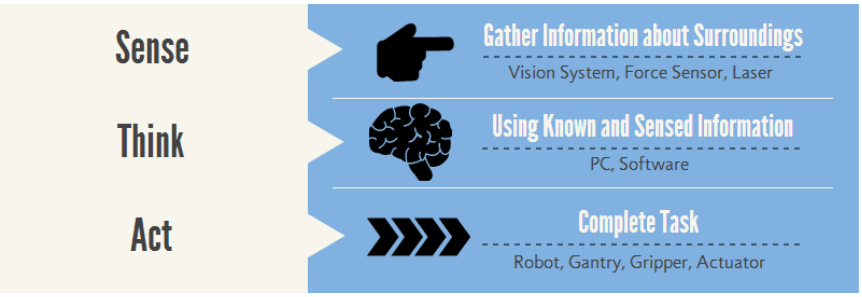


Figure 11: Sense-think-act cycle for self-directing, AI-based, systems. Image source: https://www.crossco.com/blog/what-flexible-automation

During the 'sense"' part of the cycle, the system captures and processes information about itself, its environment and its surroundings (in the case of self-driving vehicles, this information includes the position and speed of other road users, conditions of the road, etc.). This information is then combined, during the 'think' part of the cycle, with known and *a priori* information to estimate the behaviour of other road users, take a decision, reach a conclusion, or to plan what to do next (e.g., whether to turn the vehicle left or right or to keep it going straight). Finally, during the 'act' portion of the cycle, this decision or tasks are executed (e.g., the wheels of the vehicle are turned in the right direction).

In self-driving vehicles (or vehicles with Advanced Driving Assistance Systems (ADAS)), AI-based algorithms are generally involved in the 'sense' and 'think' parts of the cycle. They generally either process vehicle sensor data (see ***Figure 12*** for an overview of vehicle sensors), or help the ADAS systems to take decisions based on processed sensor data.

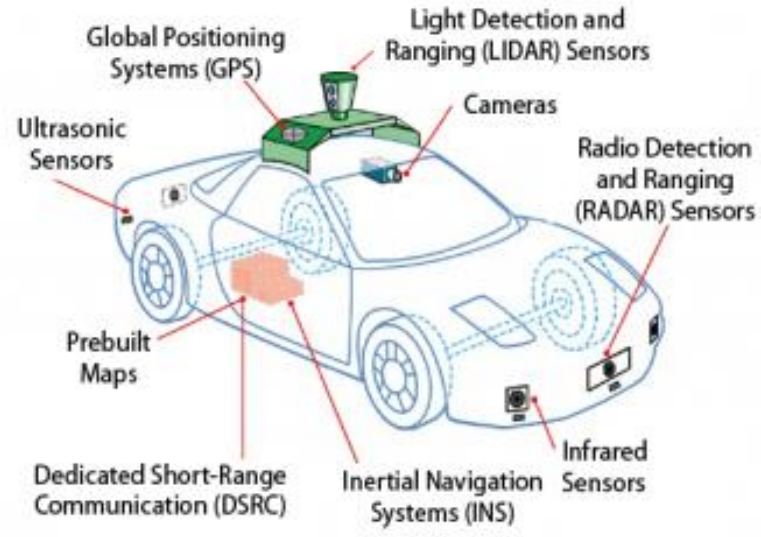


Figure 12: Example of possible sensors associated with a self-driving vehicle. Image source: CRS, based on "Autonomous Vehicles" fact sheet, Center for Sustainable Systems, University of Michigan. https://fas.org/sgp/crs/misc/R44940.pdf

The AI-algorithm itself is programmed and executed in one of the vehicle's computers (known as Electronic Control Unit or ECU) as either a single program or as part of an interconnected network of programs. In the former case, the algorithm's outcome is either transmitted to another ECU or to a set of actuators (brakes, throttle, etc.). In the latter case, the outcome is directly consumed by other algorithms. All these elements are depicted in ***Figure 13***.

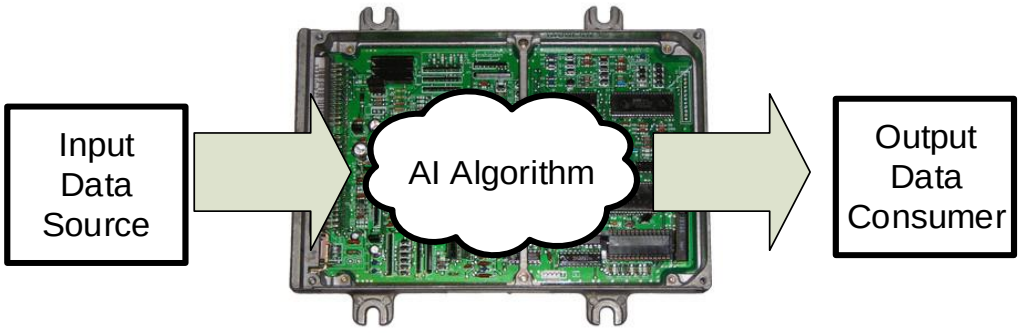


Figure 13: Typical architecture of an AI-based component. Image source: Modified from: http://www.locashdyno.com/store2/index.php?main_page=index&cPath=69

One or more AI-based algorithms may run on a single ECU or a combination of interconnected ECUs. In some cases, the (AI-based) algorithm may be embedded as part of a sensor (for example to classify objects or obstructions) rather than inside a dedicated ECU.

Figure 13 suggests that besides the input data for the algorithm, the output data produced by the algorithm and the algorithm itself, there are other elements that influence the behaviour of an AI-based component. These include, notably, the hardware over which the algorithm is deployed, the operating system and middleware running on the hardware, the training data used to create the algorithm, the software process used to develop the algorithm and the algorithms' software version.

It is important to point out that in automotive systems, AI algorithms are used for a wide variety of tasks, such as vehicle perception (most notably, video processing), behaviour prediction, decision making, noise reduction and filtering, motion planning and human-machine interaction. For each of these tasks, the specifics of each AI algorithm, input/output data and training sets can vary significantly. Furthermore, a single ADAS functionality consist of a complex system of systems with many dependencies, this makes it harder to trace any problems and reproduce the same result afterwards during analysis.

3.2. Non-Embedded Software and AI

This paragraph discusses the relation between 'Non-Embedded Software' and its development, testing and deployment life-cycle of AI-based systems. ***Figure 14*** provides an example of such a deployment lifecycle and can be summarized as follows:

1. Different versions of the software (cV) are developed, by many different authors.

2. This AI-based software is then (re)trained using a specific version of the dataset (dV).

3. The trained AI-based software is tested on a set of scenarios (sV) (and likely modified and retrained to meet the requirements).

4. The final version for deployment (dV, as a combination of cV + dV, tested on sV), is deployed (likely in phases) to the autonomous systems.

5. These autonomous systems (cars) are then used by different users in different locations.

6. The usage of these new systems generate data which is gathered to extend the dataset used in subsequent updates of the (re)trained software.

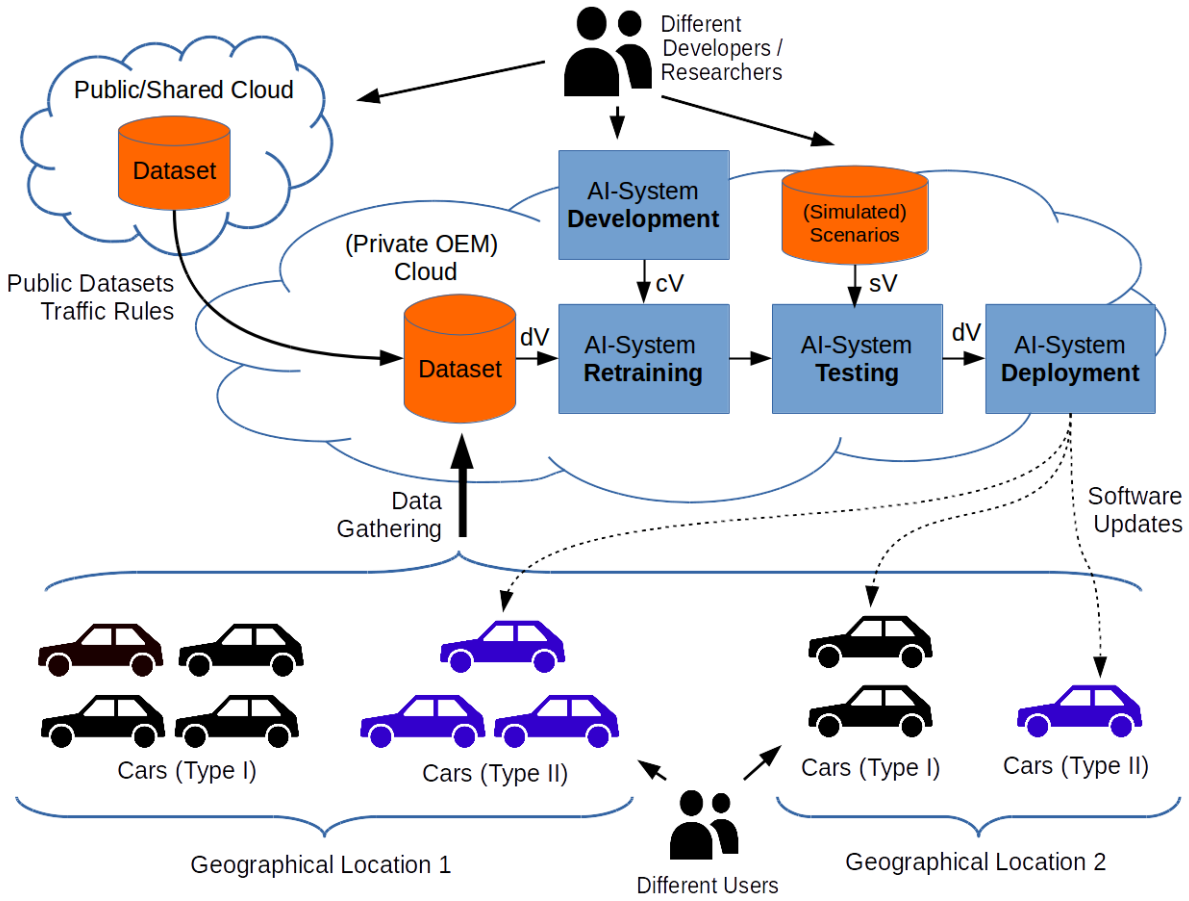


Figure 14 An example overview of a typical AI-based deployment lifecycle. See text for more details.

From the illustration in ***Figure 14*** it is clear that the EDR should not simply store the version of the code (cV) but also the version of the dataset used for training (dsV) and preferably the version of the test scenarios used (sV) in order to answer a range of liability questions such as:

- Was the dataset used for retraining representative for the real-life situations in which AI-based systems were used?
- Was the set of test scenarios representative for the real-life situations in which the AI-based systems were used?

Please also refer to (Walta, 2011) for a general discussion on the deployment of ADAS systems on the road and (Falcini & Lami, 2017) for a possible lifecycle deployment procedure for Deep Learning based technology in the Automotive sector.

3.3. Context-Aware AI

The exact sensor input and internal state of an AI-based system is never the same. And no matter how much training data is used, an AI-based system will always experience new situations (e.g., new roads, weather conditions or unpredictive road users) which it has never seen before.

Therefore, AI-based systems (or some other governing software or hardware component) should be aware of the context in which they run and be able to judge by themselves whether this context corresponds to what is expected during the intendent operation. This context, and especially the change in context, should be stored by the EDR in the form of events.

3.4. Traceability and AI

It is important to realize that the EDR should store sufficient information in a way that the root-cause of an incident can be backtracked. However, this backtracking can be done offline combined with extra (OEM) information from some (Private) Cloud, not solely by the information stored in the EDR.

For example, the EDR might only record the input and output data and the version used for deployment (see "dV" in ***Figure 14*** from Paragraph 3.2). While the actual root-cause might require to actually look at the training data itself to see if the situation during the incident was representative for the situation that the AI-based system was trained for to be used in.

Especially AI-based methods which face poor explainability, it is important to be aware of the kind of conditions the AI-based system was trained for and the context that it has been operating in in real-life (see Paragraph 0).

3.5. Basics on AI Liability

This section summarizes the basics of legal liability as described in (Kingston, 2016). The goal is not to provide in-depth details on the subject, but to motivate which kind of data could be necessary to collect in order to establish liability in case an event occurs. ***Figure 15*** shows the basic aspects of legal liability. It could be divided into two basic types: criminal and civil liability.

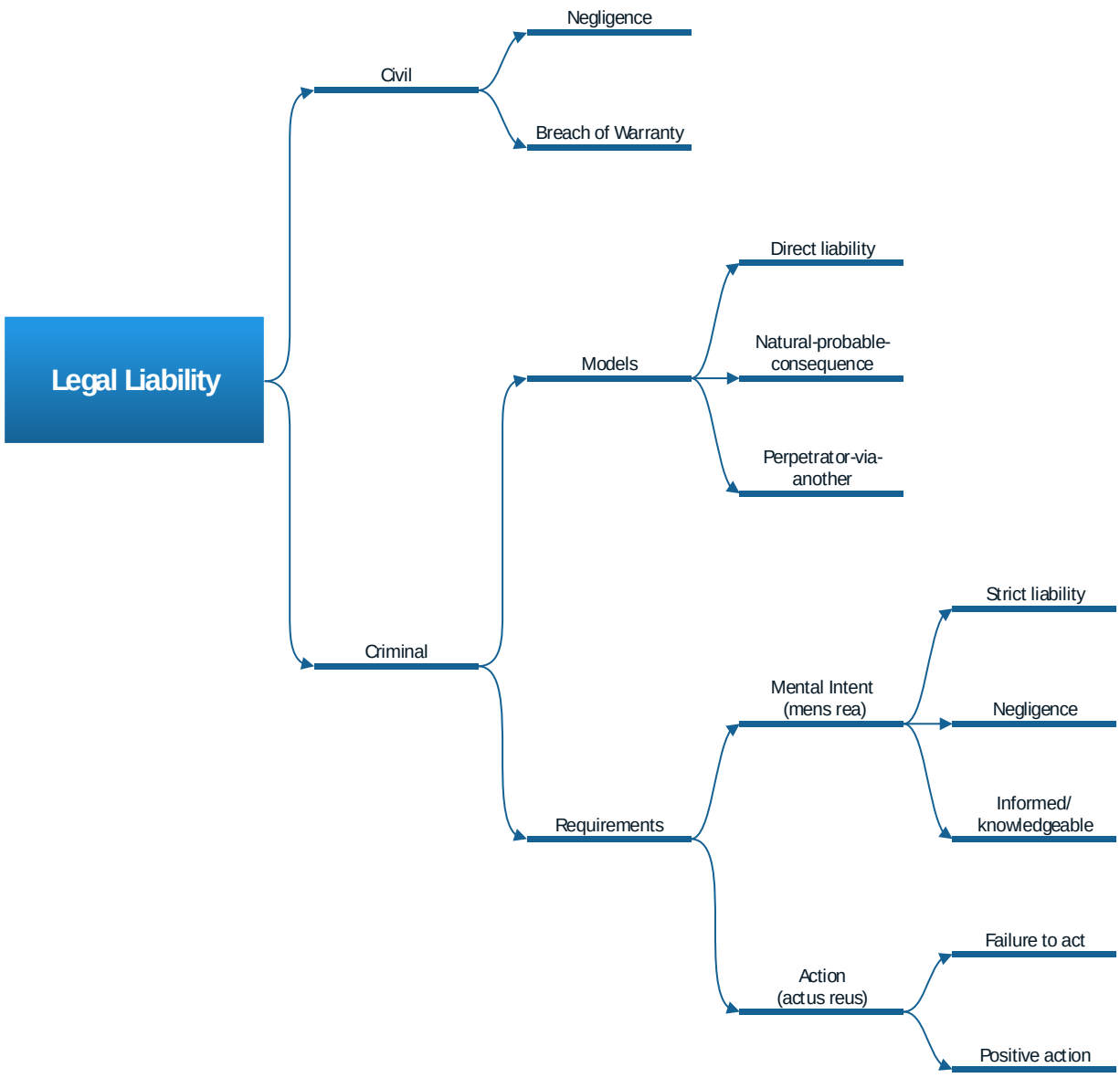


***Figure 15: Elements of legal liability taken from* (Kingston, 2016).**

3.5.1. Criminal Liability

To assign criminal liability to a defendant, one must fulfil two basic requirements: 1) to prove *actus reus*, that is, to prove that an action by the defendant (or a failure to act when it was needed) produced the criminal offense; 2) to prove *mens rea*, that is, that the defendant had the mental intend to commit the offense. The latter requirement can be split in one of three types: offenses that require knowledge or being informed in order to be committed, offenses that require only negligence (e.g., "a reasonable person would have known"), or those for which no intend needs to be shown (these are called strict liability offenses, like traffic violations).

These basic elements lead to three legal models by which **criminal liability** could be assigned to an AI-based system:

Perpetrator-via-another: The AI-based system is considered akin to a mentally deficient person, a child or animal, that lacks the mental capacity for *mens rea*. The system, however, is instructed by a person or another agent to commit an offense (e.g., a dog is commanded by its owner to attack another person). In such case, the person or agent is held criminally liable.

In terms of an AI-based vehicle, either the vehicle's programmer[737], user, or (possibly) a hacker could be considered the offense's perpetrator. To establish this, an EDR should collect data that helps to determine misuse or tampering with the AI-based systems of the vehicle.

Natural-probable-consequence. In this model, part of the AI program which was intended for good purposes is activated inappropriately and performs a criminal action. For instance, a camera-based perception AI inappropriately detects an object in front of the vehicle and triggers an emergency stop, resulting in an impact.

To aid establishing liability in this case, an EDR should collect data that helps to determine what triggered the inappropriate detection by the AI algorithm.

Direct liability: This model attributes both *actus reus* and *mens rea* to an AI system. In the former case, the AI system is liable if it takes an action that results in a criminal act (e.g., run over a pedestrian on purpose) or if it fails to act when it should (e.g. not applying the brakes). The assignment of *mens rea* to an AI system is much harder. Focus could be given to only strict liability situations where no *mens rea* is required to be assigned liability. Examples of these situation are an AI-based vehicle exceeding the legal speed limit or driving in the wrong direction on single direction road.

To aid establishing liability in this case, an EDR should collect data that helps to determine whether traffic infractions were committed, or whether other direct-liability offenses were committed.

3.5.2. Civil Liability

This encompasses two types of offenses: negligence and breach of warranty. Here only the former will be covered.

The basic steps to prove an AI system was negligent are: 1) Prove the AI system had duty of care; 2) Prove it breached that duty; 3) Prove that breach resulted in an injury to a third party. In the context of EDRs, only points 2 and 3 seem to apply (Kingston, 2016).

Breach the duty of could be sustained in numerous ways: "errors in the program's function that could have been detected by the developer after thorough investigation and testing; an incorrect or inadequate knowledge base; incorrect or inadequate documentation or warnings; not keeping the knowledge up to date; the user supplying faulty input; the user relying unduly on the output or using the program for an incorrect purpose."

To aid establishing liability in this case, an EDR should collect data that helps to determine the AI program's version (which is related to its 'knowledge'), warnings provided to the user and his/her response to them, input provided to the AI system

[737] Almost all AI-based systems are written by a large group of developers. It may therefore be very difficult to track down one or more persons who wrote the piece of code that was responsible for the incident.

by the user, and context of use of the AI system (e.g., a highway autopilot used in urban situations).

To prove point 3, the key question is whether the AI system recommends an action in a given situation, or takes an action (as self-driving and safety-equipped cars do).

To aid establishing liability in this case, an EDR should collect data that helps to determine the vehicle's driving context, recommended actions, and actions taken.

4. RECOMMENDED REQUIREMENTS

As part of Subtask 5.1, this paragraph provides the recommended requirements for future Event Data Recorders. These results are based on the State of the Art research from Chapter 2 and the result from Tasks 3 (***Figure 16***).

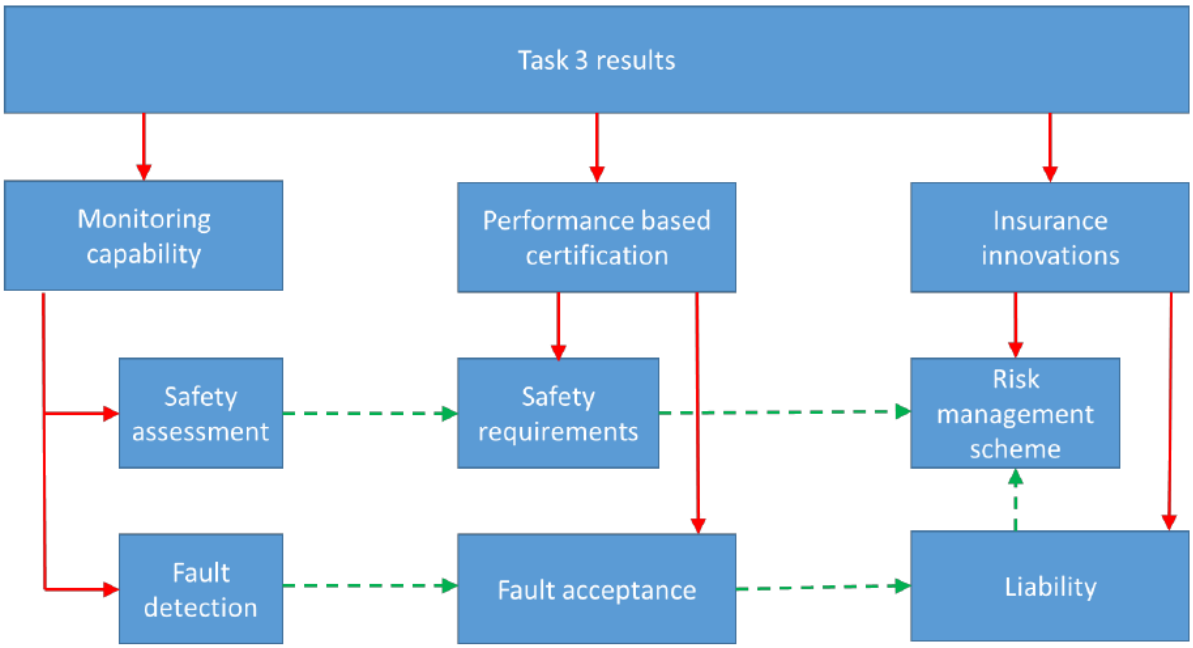


Figure 16 Relationship between testing, certification and insurance as obtained from task 3 (copied from Inception report).

This section presents a suggested list of data that a generic EDR should collect to aid establishing liability. Note that many of these items are also relevant for recording the events of non-AI based systems.

In keeping the recommendations generic, the tables specify data categories instead of specific signals or physical variables. It is assumed that this data is recorded using the internal sensors of the "ego vehicle" (i.e., the vehicle carrying the EDR) or it is received by the ego vehicle from other traffic participants (including the road infrastructure). Please also refer to section 2.1.3 and 2.1.4 for a summary on existing requirements and standards for EDR's that should be considered in addition to the recommended requirements stated here.

4.1. Automotive Specific Requirements

Table 21 summarizes the recommended data categories related to the application of autonomous cars. Many of these categories might contain information as specified in ***Table 22***.

Table 21 Recommended EDR requirements for storing automotive specific data.

Data category	Purpose
Ego vehicle dynamic data	To establish the ego vehicle's behaviour with respect to the road. This includes steering wheel angle, position, brake activation, heading, speed, location, etc..
Ego vehicle interaction data	To establish the ego vehicle's interaction with other road users. This includes for example indicator lights and brake lights.
V2X Communication	All wireless communication to and from the vehicle (known as Vehicle-to-Everything (V2X) communication (5G Automotive Association, 2017; Nguyen et al., 2018)) should be recorded just prior, during and after an event of interest.
Other road user dynamic data	To establish the behaviour of other road users with respect to the road. Both based on sensory information perception and tracking algorithms (Koch, 2014) and as acquired through V2X communication.
Environmental conditions	To establish the context of operation of the traffic participants and the vehicle itself. This includes weather, road layout, inclination, road-surface conditions, light conditions, time of day, local road maps, etc.
User state	To determine the state of the driver and its passengers. This may include seat position, seatbelt status, face tracking, eye tracking and other data to help ascertain what the user was doing prior, during and after an event of interest.

4.2. AI-Based Requirements

Table 22 summarizes the recommended data categories related to AI-based components in autonomous systems. Please note that it might not always be feasible to store all input, internal and output data for on AI-algorithm inside the EDR. The amount might simply be too much (such as retrieved from a high-resolution colour camera or LIDAR system) or application-specific (which might require dedicated hardware or software to read) for it to be practical to (also) store it inside the EDR (next to the ECU) itself. Depending on the capabilities of the ECUs and EDR, only parts of the input and output (in the form of so called `features` or in some other aggregated summarized form) maybe be feasible to be stored on the EDR (or ECU as an extension of the EDR).

Table 22 Recommended EDR requirements for storing information about AI-based systems.

Data category	Purpose
AI-algorithm input data	To establish the data received and processed by the AI algorithm of interest prior/during/after an event of interest.
AI-algorithm output data	To establish the decisions, outcomes, etc., generated by the AI algorithm of interest prior/during/after an event of interest.
AI-algorithm local memory, databases, heat maps	To establish the mental state' of the AI algorithm (what was it paying attention to, what did it know, how up to date its knowledge was, etc.).
AI-algorithm update frequency and latency.	To determine whether the 'mental state' of the AI algorithm (see above) was updated within the designed frequency and latency constrains.
AI-algorithm dataset versions.	The versions of the datasets being used to train the AI algorithms. This so that one can judge whether the training set was representative for the situation in which the AI algorithm was used.
AI-algorithm seed used for random number generation.	This so that the result for a stochastic algorithm (such random sampling in Monte Carlo methods) can be reproduced afterwards.
(Sub-) Context	The state or context identified by the AI-based system (or some governing software or hardware component). See Paragraph 0 for more information.

4.3. Generic Requirements

Summarizes the recommended data categories for an EDR to store. Most of these categories also apply to non-AI-based systems.

Table 23 Recommended EDR requirements for storing generic system information.

Data category	Purpose
Software/middleware data	To establish which (AI-)algorithm version was installed in the ECU executing the algorithm. This includes firmware versions for OS/middleware/AI algorithms, OS system logs, update logs, checksums, etc.

OS security logs and checksums of the (permanently stored) data.	To establish whether the (AI) software was tampered with.
User interface data	To establish which information exchange occurred between the user and the (AI) system prior/during/after an event of interest. This includes warnings to the user, user input to the system, etc.
Hardware (ECU) Performance Indicators	Hardware resources usage (such as CPU, RAM, Memory, IO and Network Bandwidth) of the ECU might reveal situations in which the system was overloaded. Once one or more systems get overloaded, the update frequency and latency of the AI-algorithms might drop below an acceptable limit.

5. INNOVATION REQUIREMENTS

This chapter relates to Subtask 5.3 "Innovation requirements for event data recording" of the Inception report. It also covers the innovation requirements for Data Management Strategies as discussed in Subtask 5.2 of the Inception report.

The aim of this chapter is to provide a general summary of topics required to be researched in future times to meet the requirements as stated previously in chapter 4. Furthermore, a transition of event recorder requirements are suggested. See ***Figure 17*** for an overview.

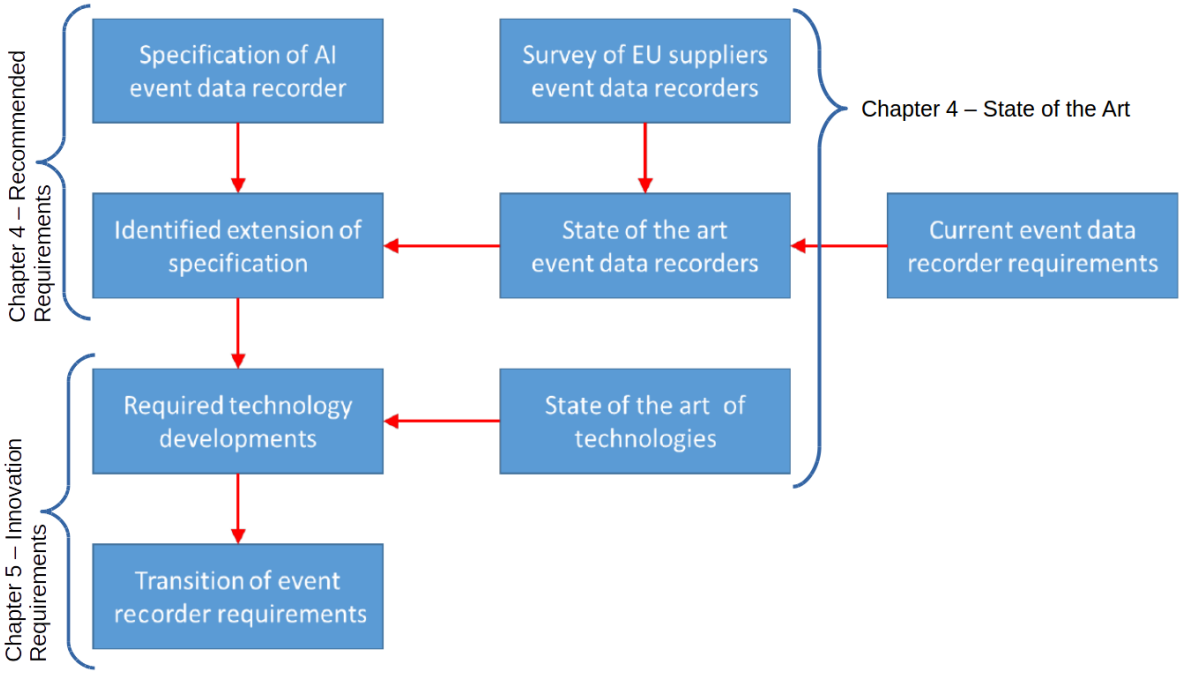


Figure 17 Methodology for identification of innovation for event data recording (modified from Inception report).

5.1. AI-based Systems

This section provides an overview of topics relevant to be researched in future times in order to better keep track of the reasoning and data analytics of AI-based systems with the use of an Event Data Recorder.

5.1.1. Explainable Artificial Intelligence

With the rise of more complex Artificial Intelligence methods such as deep learning (Deng & Yu, 2014; Lecun, Bengio, & Hinton, 2015), it becomes increasingly more important for these methods to be explainable. This so that it becomes easier to backtrack the reasoning behind any mistakes that might happen for an AI-based algorithm. These explanations (or ways to infer them) should be stored in the EDR at critical moments.

Existing solutions and initiatives exist (Core et al., 2006; "Explainable Artificial Intelligence (XAI)," 2016), for example to visualize the state of a Deep Learning network (Samek, Wiegand, & Müller, 2017) or by learning an interpretable model locally around the prediction (Ribeiro & Guestrin, 2016). Also, from an external view, an existing model could be made more insightful by learning the characteristics and accuracy of the model using other methods.

However, making AI-based systems more explainable and insightful should be an integral part of its design, rather than an after-thought. At design time one should be able to provide answers to questions such as:

- Why did the AI algorithm pick for a specific answer and not another? Can this be expressed in a certain confidence level or probability? How does this confidence level or probability relate to what was learned and tested before?
- Can the AI algorithm explain its abductive, deductive or inductive reasoning? Was it sound and based on valid premises?
- Was the answer that the AI-based algorithm gave valid provided the context it was in (see also section 3.3).

5.1.2. Traceable and Reproducible AI

In addition to its explainability as discussed in the previous section, it is also important for an AI-based system to be traceable, so that most of its reasoning and results can be reproduced. This allows for better investigation as to what led to a specific event and whether it is the AI-based system to blame.

5.1.3. Human Machine Teaming

It should be noted that future AI-based systems will often operate in close collaboration with humans. In such cases, AI-based systems become like team members who interact with their users to gain and provide more information in order to fulfil its responsibilities. In cases where the AI-based system is uncertain about its perception (or the context it runs in, see paragraph 0), it may ask a human to take over control (for example to cross a dangerous road or to dock in a busy harbour). Human Machine Teaming (HMT) (Parasuraman, Barnes, Cosenzo, & Mulgund, 2007; van der Vecht, van Diggelen, Peeters, Barnhoorn, & van der Waa, 2018) is a promising paradigm that allows autonomous systems to interact with humans while allowing humans to stay in control.

An EDR should store sufficient information about the interaction between the AI-based systems and humans. This in order to reconstruct the collaboration that took place to see if both the AI system as well as the user took the right amount of responsibility.

5.2. Design and Legislation Considerations

Ideally, an EDR would be able to store all raw sensor information and the complete internal state of all software and hardware components in order to reconstruct any event. However, this is not practically feasible, since the memory and bandwidth interfacing capabilities of the EDR are limited. Furthermore, privacy regulations such as the General Data Protection Regulation (GDPR)[738] may restrict the type or duration of (personal) data being recorded.

The following sections describe topics to take into account when designing or legislating the (mandatory) use or installation of EDR's in combination with AI-based systems.

5.2.1. The kind of data to record

Traditional EDRs typically record low-bandwidth time series data such as velocity and acceleration (see **APPENDIX B** for a list of mandatory data elements in the US).

[738] https://eur-lex.europa.eu/eli/reg/2016/679/oj

However, high-bandwidth sensors such as lidars used in ADAS systems may help to reconstruct incidents in more detail (Zolock, Senatore, Yee, Larson, & Curry, 2016).

Furthermore, as the development in ADAS and AI-based systems advances, it is likely that more types of sensors and other types of (external) information sources will be used (Bengler et al., 2014).These future types of data should be taken into account when legislating the (mandatory) use of EDRs.

5.2.2. When to record the data

Since the memory capabilities of an EDR are limited, it is restricted in the duration and amount of data it can store. One may consider the following criteria when limiting the amount of data being stored inside an EDR:

- A fixed duration (e.g., the last 2 minutes) before the system that the EDR observes was turned off or became idle.
- A severe incident (e.g., a collision) which requires the EDR to be read by authorities.
- A dangerous event (e.g., a near collision or sudden braking) which may indicate abnormal or unsafe use by the user or (AI-based) systems that (start to) malfunction.
- Continuously (such as average speed, breaking force, etc.) for diagnostic purposes and predictive maintenance.

5.2.3. Where to record the data

Traditionally, EDRs consist of a single device (e.g., an airbag control module, see section 2.1). However, as more sensors are being used and more AI-based algorithms being implemented, it is likely that more information is processed in a distributed way using several interconnected systems (e.g., ECUs connected to a CAN-Bus (Avatefipour & Milik, 2017)). Sensors might be able to store data locally before processing it and sending it to other components.

Connecting all these devices to a single EDR seems infeasible if this involves high-bandwidth (raw sensor) data. It is more likely that future EDRs will exist out of many different locally distributed components in which the main EDR provides only a summary of the data and a common interface (or at least a reference) to other (locally) distributed data elements.

As mentioned before in section 2.2.3, an alternative solution would be to store the EDR data in a distributed way outside the system being observed. Here, the data of the EDR could be stored in some cloud environment (He, Yan, & Xu, 2014) or in the environment of the event itself (e.g., infrastructure RSU's).

5.2.4. Data privacy concerns

Storing data for a long duration inside the EDR helps with predictive maintenance and may help to predict and improve the behaviour of the driver (Scanlon, Kusano, & Gabler, 2015; Toledo, Musicant, & Lotan, 2008). However, this also poses privacy concerns especially since the data might end up in many different locations (see section 5.2.3). See also section 0.

5.2.5. The cost of recording data

The more data the EDR needs to record, the higher the costs of installing EDRs. However, it is not simply the amount of data that influences the price, but also the complexity that it

takes to bring all this data together into a single device or common interface while protecting it from tampering or unauthorized retrieval (for sake of evidence and privacy).

Setting very high requirements on the type and amount of data that needs to be recorded for AI-based systems, might hinder the technological advances and application of these systems.

5.3. Interoperability Frameworks and Standards

Open standards and readily available interoperability frameworks could ease the data retrieval and interpretation of the data stored in EDRs for autonomous systems.

An example of such an interoperability framework is the Robot Operating Systems (ROS) (Quigley et al., 2009), a framework used for autonomous systems which eases the collaboration and interoperability of third-party modules and communication between AI-based systems. ROS is widely used in science and provides a tool called "rosbag"[739] which allows to store and replay sensor data and intermediate results of AI-based algorithms to reproduce specific scenario's (possibly in combination with environment simulators such as the Gazebo simulator (Koenig & Howard, 2004)[740]).

See also section 2.2.2 about the International Data Space (IDS) association for a related interoperability initiative that can be used to design a trustworthy architecture to share data in a controlled way.

5.4. Data Management Innovation Requirements

The recommended innovation requirements for data management can be summarised as follows:

1. **Data Ownership:** Better regulation on the issue of who owns the data is needed. It is at this moment unclear whether the data stored inside EDRs and RSUs is owned by the manufacturer, the owner of the car or the driver of the car.

2. **Privacy, Data Sharing and Protection:** How to protect the privacy and validity of the data inside and outside the EDR while allowing access to researchers and authorities? Please also refer to section 2.2.2 for a reference architecture as a possible solution.

Please also refer to section 5.2 for more innovation requirements related to data management.

[739] https://wiki.ros.org/rosbag

[740] http://gazebosim.org/

6. CONCLUSIONS

The use of EDRs is very common in the automotive sector. Almost all new vehicles have an EDR installed. However, these EDRs often only measure basic sensory information such seat belt status, acceleration and speed. Storage of high-bandwidth information and decision-making processes from advanced (AI-based) systems inside existing EDRs is limited (or at least not publicly known).

Future EDRs should record relevant information from these AI-based systems. Which allows researchers to investigate a) whether or not the system was used in the right (environmental) conditions and b) how the relevant AI-based algorithms were trained and tested and c) whether or not the datasets used for training and testing were representative for the situation in which the event occurred. Furthermore, AI-based systems should be designed with explainability and situational awareness in mind. Basic information about decision making processes (the what, where, why and why-not) of AI-based systems should be stored inside the EDR itself.

However, in the possible future legislation of EDRs, cost-effectiviness and the rapid advances in AI-based systems should be taken into account. Setting too high demands on the amount and type of information required to be stored, might hinder the advancement and application of AI-based systems. Alternative solutions might involve storing the event data in a distributed way, using cloud solutions or storing the data in the frastructure itself.

Better regulation on the issue of who owns the data and how the privacy of the user is protected is needed. Initiatives such as the International Data Space (IDS) association can be useful to setup a trustworthy architecture to share data in a controlled way.

REFERENCES

5G Automotive Association. (2017). An assessment of direct communications technologies for improved road safety in the EU, (December), 1–80. Retrieved from http://5gaa.org/wp-content/uploads/2017/12/5GAA-Road-safety-FINAL2017-12-05.pdf

Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., & Zedan, H. (2014). A comprehensive survey on vehicular Ad Hoc network. *Journal of Network and Computer Applications*, *37*(1), 380–392. https://doi.org/10.1016/j.jnca.2013.02.036

Avatefipour, O., & Milik, H. (2017). State-of-the-Art Survey on In-Vehicle Network Communication "CAN-Bus" Security and Vulnerabilities. *International Journal of Computer Science and Network*, *6*(6), 720–727. Retrieved from http://ijcsn.org/articles/0606/State-of-the-Art-Survey-on-In-Vehicle-Network-Communication-CAN-Bus-Security-and-Vulnerabilities.html

Bengler, K., Dietmayer, K., Färber, B., Maurer, M., Stiller, C., & Winner, H. (2014). Three Decades of Driver Assistance Systems, Review and Future Perspectives. *IEEE Intelligent Transportation Systems Magazine*, *6*(4), 6–22. https://doi.org/10.1109/MITS.2014.2336271

Core, M. G., Lane, H. C., Van Lent, M., Gomboc, D., Solomon, S., Rosenberg, M., & TECHNOLOGIES., U. O. S. C. M. D. R. C. I. F. C. (2006). Building explainable artificial intelligence systems. *Proceedings of the National Conference on Artificial Intelligence*, *21*(2), 1766–1773. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Building+Explainable+Artificial+Intelligence+Systems#0

Deng, L., & Yu, D. (2014). Deep Learning: Methods and Applications. *Foundations and Trends® in Signal Processing*, *7*(3–4), 197–387. https://doi.org/10.1561/2000000039

Explainable Artificial Intelligence (XAI). (2016). *Defense Advanced Research Projects Agency*.

Falcini, F., & Lami, G. (2017). *Deep Learning in Automotive: Challenges and Opportunities* (Vol. 155). https://doi.org/10.1007/978-3-642-21233-8

Gabauer, D. J., Newell, H. L., & Neill, M. E. O. (2005). Use of Event Data Recorder (EDR) Technology for Highway Crash Data Analysis, *75*(December). https://doi.org/10.17226/23303

He, W., Yan, G., & Xu, L. Da. (2014). Developing vehicular data cloud services in the IoT environment. *IEEE Transactions on Industrial Informatics*, *10*(2), 1587–1595. https://doi.org/10.1109/TII.2014.2299233

Helena Gellerman, Erik Svanberg, Riku Kotiranta and Ines Heinig (SAFER), Clement Val (CEESAR), Sami Koskinen and Satu Innamaa (VTT), A. Z. (IKA) and J. B. (Daimler). (2017). FOT-Net Data Field Operational Test Networking and Data Sharing Support, (European Commission, 7th

Framework Program). Retrieved from http://fot-net.eu/Documents/d3-1-data-sharing-framework/

Hynd, D., & McCarthy, M. (2014). *Study on the benefits resulting from the installation of Event Data Recorders*. *European Commission* (European C). European Commission.

Jarke, M., & Quix, C. (2017). *On Warehouses, Lakes, and Spaces: The Changing Role of Conceptual Modeling for Data Integration*. *Springer* (Conceptual). Springer International Publishing. https://doi.org/10.1007/978-3-319-45654-6_9

Kingston, J. K. C. (2016). Artificial Intelligence and Legal Liability. In M. Bramer & M. Petridis (Eds.), *Research and Development in Intelligent Systems XXXIII* (pp. 269–279). Cham: Springer International Publishing.

Koch, W. (2014). *Tracking and Sensor Data Fusion*. https://doi.org/10.1007/978-3-642-39271-9

Koenig, N. P., & Howard, A. (2004). Design and use paradigms for Gazebo, an open-source multi-robot simulator. In *IROS* (Vol. 4, pp. 2149–2154).

Lange, R., & Wilson, J. (2017). Data Requirements for Post-Crash Analyses of Collisions Involving Collision Avoidance Technology Equipped, Automated, and Connected Vehicles.

Lecun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436–444. https://doi.org/10.1038/nature14539

Marco P. daSilva. (2008). Analysis of Event Data Recorder Data for Vehicle Safety Improvement. *Nhtsa*, (April), 1–147.

Nguyen, T. V., Shailesh, P., Sudhir, B., Kapil, G., Jiang, L., Wu, Z., … Li, J. (2018). A comparison of cellular vehicle-to-everything and dedicated short range communication. *IEEE Vehicular Networking Conference, VNC*, *2018–Janua*, 101–108. https://doi.org/10.1109/VNC.2017.8275618

Parasuraman, R., Barnes, M., Cosenzo, K., & Mulgund, S. (2007). Adaptive Automation for Human-Robot Teaming in Future Command and Control Systems. *The International C2 Journal*, *1*(2), 43–68. https://doi.org/10.1017/CBO9781107415324.004

Quigley, M., Conley, K., Gerkey, B., Faust, J., Foote, T., Leibs, J., … Ng, A. Y. (2009). ROS: an open-source Robot Operating System. In *ICRA workshop on open source software* (Vol. 3, p. 5).

Ribeiro, M. T., & Guestrin, C. (2016). " Why Should I Trust You ?" Explaining the Predictions of Any Classifier.

Samek, W., Wiegand, T., & Müller, K.-R. (2017). Explainable Artificial Intelligence: Understanding, Visualizing and Interpreting Deep Learning Models. https://doi.org/10.1109/DSAA.2015.7344858

Scanlon, J. M., Kusano, K. D., & Gabler, H. C. (2015). Analysis of Driver Evasive Maneuvering Prior

to Intersection Crashes Using Event Data Recorders. *Traffic Injury Prevention*. https://doi.org/10.1080/15389588.2015.1066500

Tobergte, D. R., & Curtis, S. (2013). *Handbook of Robotics*. *Journal of Chemical Information and Modeling* (Vol. 53). https://doi.org/10.1017/CBO9781107415324.004

Toledo, T., Musicant, O., & Lotan, T. (2008). In-vehicle data recorders for monitoring and feedback on drivers' behavior. *Transportation Research Part C: Emerging Technologies*, *16*(3), 320–331. https://doi.org/10.1016/j.trc.2008.01.001

van der Heijden, R. W., Engelmann, F., Mödinger, D., Schönig, F., & Kargl, F. (2017). Blackchain: Scalability for Resource-Constrained Accountable Vehicle-to-X Communication, (Dl). https://doi.org/10.1145/3152824.3152828

van der Vecht, B., van Diggelen, J., Peeters, M., Barnhoorn, J., & van der Waa, J. (2018). Sail: A social artificial intelligence layer for human-machine teaming. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10978 LNAI*, 262–274. https://doi.org/10.1007/978-3-319-94580-4_21

Walta, L. (2011). *Getting ADAS on the Road Actors ' Interactions in Advanced Driver Assistance Systems Deployment*. PhD Dissertation, Technische Universiteit Delft. Retrieved from https://repository.tudelft.nl/islandora/object/uuid:158bb71b-5dfb-424e-a842-f648fe589872?collection=research

Yeung, C. Y., Law, W. C., Chim, T. W., Yiu, S. M., Li, V. O. K., & Hui, L. C. K. (2014). Distributing blackbox data to multiple vehicles in a secure and privacy-preserving manner. *2014 International Conference on Connected Vehicles and Expo, ICCVE 2014 - Proceedings*, 804–809. https://doi.org/10.1109/ICCVE.2014.7297663

Zolock, J., Senatore, C., Yee, R., Larson, R., & Curry, B. (2016). The Use of Stationary Object Radar Sensor Data from Advanced Driver Assistance Systems (ADAS) in Accident Reconstruction. In *SAE Technical Paper*. SAE International. https://doi.org/10.4271/2016-01-1465

APPENDIX A

List of suppliers of Event Data Recorders and Data Acquisition Systems.

Company	URL
B-Plus	https://www.b-plus.com/en/products/automotive/measurement-logging/brick-the-system.html
TTTechAuto	https://www.tttech-auto.com/products/testing-tools/pm-200/
Vigem	https://www.vigem.de/en/home
Squarell Technology	https://squarell.com/nl/oplossingen/event-data-recorder/
Caetec	https://www.caetec.com/en/
MAF Europe	http://www.mafeurope.it/index.php?ln=uk&gclid=EAIaIQobChMIm4-Lr9zS2wIVEJ0bCh3IBwbCEAMYAyAAEgLC7vD_BwE
Dewesoft	https://dewesoft.com/
IMC	https://www.imc-tm.com/
Elektrobit	https://www.elektrobit.com/products/eb-assist/car-box/
Zuragon	https://www.zuragon.com/what-is-vicando/
IPETRONIK	https://www.ipetronik.com/home.html
Denso	https://www.denso-ten.com/business/safety/

See also http://wiki.fot-net.eu/index.php/Tool_Catalogue with an additional list of DAS's / EDR's and manufacturers.

APPENDIX B

Data elements required to be recorder by an Event Data Recorder as specified by the National Highway Traffic Safety Administration, published in 2012. Copied from NHTSA-2012-0099[741].

Data element	Minimum range	Accuracy[742]	Resolution
Lateral acceleration	At option of manufacturer	At option of manufacturer	At option of manufacturer.
Longitudinal acceleration	At option of manufacturer	At option of manufacturer	At option of manufacturer.
Normal Acceleration	At option of manufacturer	At option of manufacturer	At option of manufacturer.
Longitudinal delta-V	−100 km/h to +100 km/h	± 10%	1 km/h.
Lateral delta-V	−100 km/h to +100 km/h	± 10%	1 km/h.
Maximum delta-V, longitudinal	−100 km/h to +100 km/h	± 10%	1 km/h.
Maximum delta-V, lateral	−100 km/h to +100 km/h	± 10%	1 km/h.
Time, maximum delta-V, longitudinal	0-300 ms, or 0−End of Event Time plus 30 ms, whichever is shorter	± 3 ms	2.5 ms.
Time, maximum delta-V, lateral	0-300 ms, or 0−End of Event Time plus 30 ms, whichever is shorter	± 3 ms	2.5 ms.

[741] https://www.federalregister.gov/documents/2012/08/09/2012-19580/event-data-recorders#sectno-citation-%E2%80%89563.8

[742] Accuracy requirement only applies within the range of the physical sensor. For vehicles manufactured after September 1, 2014, if measurements captured by a sensor exceed the design range of the sensor, the reported element must indicate when the measurement first exceeded the design range of the sensor.

Time, maximum delta-V, resultant	0-300 ms, or 0−End of Event Time plus 30 ms, whichever is shorter	± 3 ms	2.5 ms.
Vehicle Roll Angle	−1080 deg to +1080 deg	± 10%	10 deg.
Speed, vehicle indicated	0 km/h to 200 km/h	± 1 km/h	1 km/h.
Engine throttle, percent full (accelerator pedal percent full)	0 to 100%	± 5%	1%.
Engine rpm	0 to 10,000 rpm	± 100 rpm	100 rpm.
Service brake	On or Off	N/A	On or Off.
ABS activity	On or Off	N/A	On or Off.
Stability control	On, Off, or Engaged	N/A	On, Off, or Engaged.
Steering input	−250 deg CW to + 250 deg CCW	± 5%	± 1%.
Ignition cycle, crash	0 to 60,000	± 1 cycle	1 cycle.
Ignition cycle, download	0 to 60,000	± 1 cycle	1 cycle.
Safety belt status, driver	On or Off	N/A	On or Off.
Safety belt status, right front passenger	On or Off	N/A	On or Off.
Frontal air bag warning lamp	On or Off	N/A	On or Off.
Frontal air bag suppression switch status, right front passenger	On, Off, or Auto	N/A	On, Off, or Auto.
Frontal air bag deployment, time to deploy/first stage, driver	0 to 250 ms	±ms	1 ms.
Frontal air bag deployment, time to	0 to 250 ms	± 2 ms	1 ms.

deploy/first stage, right front passenger			
Frontal air bag deployment, time to nth stage, driver	0 to 250 ms	± 2 ms	1 ms.
Frontal air bag deployment, time to nth stage, right front passenger	0 to 250 ms	± 2 ms	1 ms.
Frontal air bag deployment, nth stage disposal, driver	Yes or No	N/A	Yes or No.
Frontal air bag deployment, nth stage disposal, right front passenger	Yes or No	N/A	Yes or No.
Side air bag deployment, time to deploy, driver	0 to 250 ms	± 2 ms	1 ms.
Side air bag deployment, time to deploy, right front passenger	0 to 250 ms	± 2 ms	1 ms.
Side curtain/tube air bag deployment, time to deploy, driver side	0 to 250 ms	± 2 ms	1 ms.
Side curtain/tube air bag deployment, time to deploy, right side	0 to 250 ms	± 2 ms	1 ms.
Pretensioner deployment, time to fire, driver	0 to 250 ms	± 2 ms	1 ms.
Pretensioner deployment, time to fire, right front passenger	0 to 250 ms	± 2 ms	1 ms.
Seat track position switch, foremost, status, driver	Yes or No	N/A	Yes or No.
Seat track position switch, foremost, status, right front passenger	Yes or No	N/A	Yes or No.
Occupant size classification, driver	5th percentile female or larger	N/A	Yes or No.

European Commission

Study on Safety of non-embedded software; Service, data access, and legal issues of advanced robots, autonomous, connected, and AI-based vehicles and systems

Luxembourg, Publications Office of the European Union

2019 – 39 pages

ISBN 978-92-79-99495-1
doi: 10.2759/448974

KK-04-19-076-EN-N

doi: 10.2759/448974 ISBN 978-92-79-99495-1