D1.4 – Security, safety & legal issues and plans for the 2nd cycle

Project Number:	690705
Classification	Public
Deliverable No.:	D1.4
Work Package(s):	WP1
Milestone	M3
Document Version:	Vs. 1.0
Issue Date:	31.08.2017
Document Timescale:	Project Start Date: September 1, 2016
Start of the Document:	Month 9
Final version due:	Month 12
Deliverable Overview:	**Main document:** Security, safety & legal issues for the 2nd cycle
Compiled by:	Fabio Tango, CRF Stefania Vacca, REL
Authors:	Iolande Vingiano-Viricel, VEDECOM Myriam Hoeffler, VEDECOM Mohamed-Cherif Rahal, VEDECOM Ivan Dmitriev, VEDECOM Sébastien Glaser, VEDECOM
Technical Approval:	Fabio Tango, CRF
Issue Authorisation:	Andreas Lüdtke, OFFIS

DISTRIBUTION LIST		
Copy type[1]	Company and Location	Recipient
E	AutoMate Consortium	All AutoMate partners

[1] Copy types: E=Email, C=Controlled copy (paper), D=electronic copy on Disk or other medium, T=Team site (Sharepoint)

RECORD OF REVISION		
Date	Status Description	Author
07/06/2017	Deliverable v01: structure and request of contributions	Fabio Tango
30/06/2017	Contributions from partners	All authors
31/08/2017	Final version, ready for submission	Stefania Vacca

Table of Contents

Abbreviations

AVs	Automated and autonomous vehicles
ADAS	Advanced Driver Assistance Systems
NHTSA	National Highway Traffic Safety Administration
OEM	Original Equipment Manufacturer
SAE	Society of Automotive Engineers
UNECE	United Nation Economic Commission for Europe

List of figures

List of tables

Executive summary

One of the main question – if not "The Main" – in the current automotive research is: "What form of autonomous driving do we need"? As explained in D1.2, automotive industry has much more difficult problems to solve, for many reasons, but – in particular – because the world is much less structured and more complex, thus the perception of artificial agent can be not so accurate.

For more details, see also the web-site of AdaptiVe European co-funded project (https://www.adaptive-ip.eu/). In this Integrated Project, the sub-project RESPONSE 4, whose main objective are the legal questions resulting from automation, will focus on product liability, road traffic law, regulatory law, data privacy and data security. During the AdaptiVe Final Event partners from AutoMate Project, in particular Fabio Tango from CRF and Stefania Vacca from REL, have participated to the Legal aspects presentation of Prof. Eric Hilgendorf from University of Würzburg and interact with the different interlocutors present at the RESPONSE 4 booth, in order to understand the most important results reached by the European project from the legal point of view.

Today legal framework for automated driving is based on the prerequisite that safe driving is the sole responsibility of the driver. However, with a move towards automation in driving, controllability by the driver at all times might no longer be a basic design criterion.

System limits and safety validation have always been considered during the development of driving functions, especially with regard to the development of Advanced Driver Assistance Systems (ADAS). With level 3 and 4 driving

automation the driving task will be shared and transferred between driver and driving function. This raises several questions: Are there new system limits which have to be handled in particular? Is there a need to change safety validation methodologies?

AutoMate aims at using both the real-cars and the driving simulators for the final demonstrators, in order to investigate and explore different aspects. With demonstrator-cars, as sensor technologies are a key element for the driving tasks, we can consider its technical limits, thus addressing the situations that can be solved in this context and also providing possible requirements about what can be expected from the sensor development in the upcoming years. By using driving simulator, we can assume to have a full-system functionality and address those aspects more related to the interaction between human-agent and machine-agent, in particular the transition strategies from one to another.
AutoMate recommends an integrated approach covering the whole process of function development and safety validation leading to a robust and reliable automated driving function.

Introduction

Deliverable 1.4 aims to analyse the legal framework and the guidelines currently present at International and European level, providing also inputs for exploitation, dissemination and communication in order to support to overcome the existing legal barriers.

Chapter 1 will regard the legal framework in general, both from International point of view, underlying in particular the amendment of the Vienna Convention and the activities of existing bodies of United Nations. Furthermore, it will be indicated the most relevant acts at European Level, as some of them have been already enounced and analysed on deliverable 1.2.

Chapter 2 analyses the liability topic, which is one of the most discussed and relevant issue from a legal point of view in AVs. This session is focused in particular on the responsibility of the manufacturers and on product liability, with the Directive 85/374/ECC and its interpretation in the context of the judgment of the European Court of Justice (joined cause C-503/13 and C-504/13).

Chapter 3 regards cybersecurity and data collection, providing the most important guidelines for carmakers, established from NHTSA and from SAE J3061.

Similarly as for chapter 4, the following session will shortly analyse the current guidelines for privacy sector.

Finally, chapter 5 regards the inputs for exploitation and dissemination, summarizing the best practices for OEMs and describing the activities that AutoMate project intends to realize in order to overcome the legal barriers.

1 Legal Framework

"*Automation technology is intended to partially or completely replace the driver; this has created a new situation, where the requirements for car automation systems overlap with the rules for driver behaviour. Close coordination is therefore needed between the work on the two (…) of road traffic legislation: the vehicle and the driver*" (GEAR 2030 DISCUSSION PAPER).

The quote reported above, from GEAR 2030, well express the situation in which the current framework is. Automated vehicles will be a revolution, but important consequences will take place and must be considered in the development of automated systems. This revolution in automotive will have a lot of positive aspects to be considered, that will improve the way of life the overall society; but every change involves also negative consequences that have to be envisaged in order to control and manage them.

The Table 1, taken by the Joint Research Centre Science for Policy Report "*The r-evolution of driving: from Connected Vehicles to Coordinated Automated Road Transport (C-ART)*" of European Commission, reported the different consequences to take into account about automated vehicles.

Table 1: Advantages and disadvantages related to autonomous driving (sources Joint Research Centre)

POSITIVE	NEGATIVE
Safety (↓ crashes due to human error)	**Safety** (↑ crashes due to new risk situations e.g. human factors issues in SAE level 3 systems, risk compensation, system failures)
Environment (↓ energy use / fuel consumption due to increased fuel efficiency and ↓ pollution due to reduced fuel consumption)*	**Environment** (↑ energy use / fuel consumption and ↑ pollution due to increased traffic)
Mobility (↓ congestion due to e.g. less delays that result from accidents, ↑ road capacity due to platooning, ↑ users e.g. young, elderly, disabled)	**Mobility** (↑ congestion due to increased travel demand, ↓ public transport)
Security (↓ criminal and terrorist activities thanks to vehicle control)	**Security** (↑ criminal and terrorist activities through hacking) **and privacy** (↑ risks of access to personal data)
Value of time (↑ leisure time) **and comfort** (↓ driver stress, possibility to rest or work)	**Flexibility/joy/skills** (↓ flexibility to take instantaneous journey decisions, ↓ joy of driving, ↓ driving skills)
Costs (↓ labour costs of taxis and commercial vehicles as drivers are no longer needed, ↓ crash costs if crashes are reduced, ↓ insurance costs if crashes are reduced, ↓ parking costs if cars can be parked in less space and located in less expensive land, ↓ car ownership costs)	**Costs** (↑ vehicle equipment costs, ↑ infrastructure equipment needed, ↑ maintenance costs) **and revenues** (↓ parking revenues for cities)
Business (↑ new business opportunities based on e.g. new mobility services, ↑ productivity)	**Jobs** (↓ jobs like taxi/truck/bus drivers and crash economy, ↓ vehicle repair demands if crash rates reduce)
Land use (↓ parking spaces and they can be located outside city centres, ↑ green spaces)	**Land use** (↑ sprawled development patterns as a result of lower Value of Travel Time)

In the current scenario, legal issues related to automated vehicles do not have a simple a clear definition. Indeed, we do not have a well-defined legal framework as in other different sectors. The legal aspects and all the consequences in the society must be taken into account when an innovation, as automated vehicles, is introduced in the market. Furthermore, the AutoMate project cannot underestimate these aspects in the design and during the implementation of the system.

The aim of this chapter is to define the legal framework at International and European level, whilst adding the topics and the legal issues already analysed in the deliverable 1.2.

1.1 The International framework

At International level, one of the most important actor in the sector is the UNECE (United Nation Economic Commission for Europe) which, with the UNECE Inland Transport Committee (ITC) and its two permanent subsidiary bodies, meaning the Working Party on Road Traffic Safety (WP.1) and the World Forum for Harmonisation of Vehicle Regulations (WP.29), is particularly active for the introduction on automated driving (M. Alonso Raposo et al., 2017).

In Figure 1, reported also in the Joint Research Science for Policy Report of European Commission, it is described the planned activity of UN bodies in the automated vehicles sector.

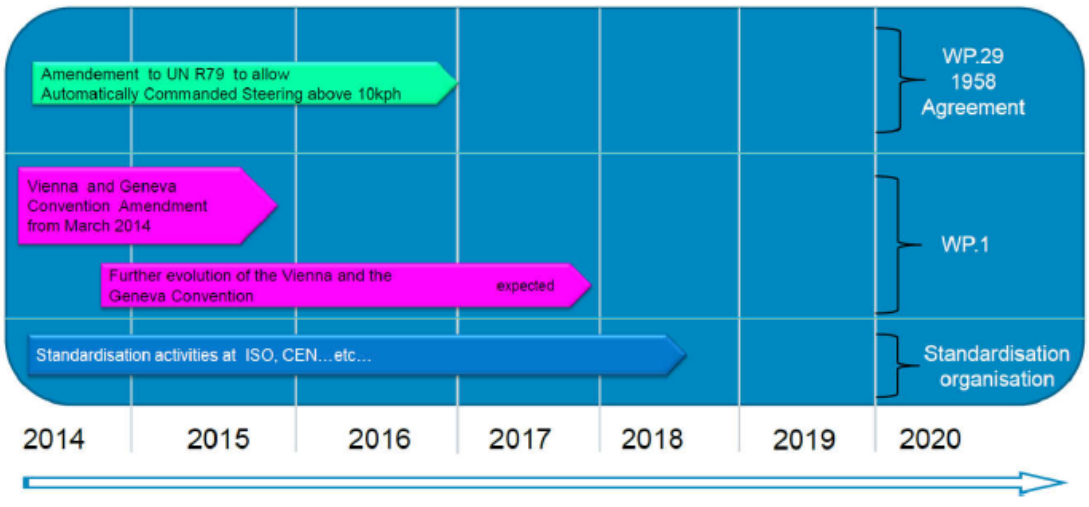

Figure 1: Planned activity in automated vehicle domain (sources Joint Research Centre).

As already mentioned in AutoMate Deliverable 1.2, Vienna Convention on Road Traffic (1968) is the starting point for the definition of the legal framework on automated driving. The Convention, ratified by 73 Countries, has the main goal to simplify the international road traffic, increasing the safety on road (S. Pillath, 2016).

This international Convention has been recently amended (March 2016), with the introduction of the article 8.5bis, which states that *"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 drive".*

Indeed, paragraph 5 of art 8 states that "*Every driver shall at all times be able to control his vehicle or to guide his animals"*.

While paragraph 1 of article 13 established that "*Every driver of a vehicle shall in all circumstances have his vehicle under control so as to be able to exercise due and proper care and to be at all times in a position to perform all manoeuvres required of him. He shall, when adjusting the speed of his vehicle, pay constant regard to the circumstances, in particular the lie of the land, the state of the road, the condition and load of his vehicle, the weather conditions and the density of traffic, so as to be able to stop his vehicle*

within his range of forward vision and short of any foreseeable obstruction. He shall slow down and if necessary stop whenever circumstances so require, and particularly when visibility is not good".

In other words, the amendment of Vienna Convention realized on March 2016 provides that every vehicle shall be equipped with a person who is controlling the vehicle itself, as the driver shall have, in every circumstance, the situation under control. This provision, as already mentioned in the deliverable 1.2, is important because one of the most important Convention at International level provides the possibility that a system is influencing the way vehicles are driven. Consequently, the role of the driver could be reduced, even if the article explicitly established that the driver has to be present and able to intervene, having the situation under control.

Nevertheless, it is clear that the Vienna Convention is, at the moment, not compatible with vehicles characterized by level 3, 4 or level 5 of automation systems (meaning with high or full automation) and the WP.29 has started a discussion with the other ITC permanent body WP.1 in order to tackle the divergences between Convention and WP.29 regulations (A. Raposo et al., 2017).

1.2 The European framework

Automated and connected vehicles are cross-cutting issues in the European Union. The European legislative framework related to these topic is quite wide; in the following it will be indicated the main existing EU legal and policy frameworks, as reported in the JRC Science for Policy Report of the European Commission:

Act	Topic
1949 Geneva Convention on Road Traffic	Convention on Road Traffic
1968 Vienna Convention on International road traffic	Convention on International road traffic
UN Regulation No.79	Steering equipment
UN Regulation No.116	Anti-theft devices
UN Regulation No.131	Technical requirements for the approval of Advanced Emergency Breaking Systems (AEBS) fitted on trucks and coaches
Directive 85/374/EEC	Product liability
Directive 95/46/EC	Data protection
Directive 2002/58/EC	Privacy in electronic communications
Directive 2003/59/EC	Training and initial qualifications of professional drivers
Directive 2006/126/EC	Driving license
Directive 2007/46/EC	Vehicle approval

Directive 2008/96/EC	Infrastructure safety management
Directive 2009/103/EC	Motor insurance
Directive 2014/45/EU	Roadworthiness

Table 2 European Legislative Framework on AVs

In addition, as analysed in the deliverable 1.2, it is extremely relevant the regulation 679/2016 on 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).

2 Liability

Automated vehicles will have an essential impact in our society, as they will introduce many positive and relevant aspects, in particular the reduction of the road traffic accidents, as 90% of accidents are caused by human mistakes and misconducts (M. Maggi, 2017). However, this means that fatalities will be significantly reduced, but unfortunately not eliminated. For this reason, liability is probably one of the most relevant issues related to autonomous vehicle, as it is interesting for different categories which participate in the production of the vehicles.

In case of accidents, it is necessary to understand who is responsible of the damage, and there is the possibility that the system, the car may be responsible for it. In order to limit the negative circumstances, the percentage of accidents on roads, the system must be designed following the requirements defined in particular at international level.

As the dynamic of the incidents and the situations may be very articulated and it could be difficult to understand what is happened and who was driving at the moment of the collision, and also who is responsible of the accident and have to respond of it, the vehicle should be equipped of a black box that can trace the actions and events.

At the moment, the national legislations (as in France for example) frequently recognize the driver as responsible.

Furthermore, the article 8.5bis of Vienna Convention requires that "*Every driver shall at all times be able to control his vehicle…"* meaning that s/he has to monitor the situation, which does not mean that the responsibility is automatically of the driver, but that the driver shall monitor the vehicle. What happens if the driver is able to control the vehicle? Or in case in which

the system asks to take over, but the driver does not react, which will be the responsible for an eventual fatality?

It is not simple to find a solution for these questions; probably, only with the time, the action of the legislator, both at European and national level, with the Conventions and dispositions at International level and with the essential activity of the jurisprudence, which will analyse the concrete situations, the automated vehicles framework will be more clear. Indeed, the European Parliament Research Service in the 2016 January Briefing reports that "*The new possible causes created by automation might interfere with the very objective of liability regimes to apportion risks, therefore an adaptation of liability law to the new technologies and a European harmonisation of the regimes concerning the liability of owners and/or drivers of automated vehicle seem necessary*" (S. Pillath, 2016).

In regards of product liability, the deliverable 1.2 analyses the Council Directive 85/374/ECC. As mentioned in this deliverable, the producer could be responsible even without negligence or fault; nevertheless, the proof of damage shall lie on the injured person, who, however, has not to demonstrate the producer's negligence or fault. As established in article 4 of Directive 85/374/ECC, the victim has to prove the causal relationship between the defect and the damage.

Furthermore, the European Court of Justice, in the judgment of the joined cases C-503/13 and C-504/13, explicitly provided that "*where it is found that such products belonging to the same group of forming part of the same production series have a potential defect, it is possible to classify as defective all the products in that group series, without there being any need to show that the product in question is defective*"(ECJ judgment, 2015). This means

that a product is defective if it is part of a series characterized by the frequency of defects (E. Helmig, 2016). The application of this principle in automated vehicles is very important, because it means that it is not necessary to prove the causal relationship between the defect and the damage when the damage is been caused by a vehicle whose series have a potential defect.

3 Cybersecurity and data protection

The management of data that the system will be able to collect in order to collaborate with the driver and enhance the safety in the car is relevant topic for AutoMate. As reported in the Automotive cyber security dedicated Ebook for the Cyber Security Professional, "*the introduction of connectivity into the auto environment brings with it the responsibility of ensuring security, not only by manufacturers but also owners of these vehicles*". Manufacturers must understand, predict and manage the risks of possible cyber-attacks into the car environment, but an efficient and concrete action shall be taken only in cooperation with the final user, the consumer, who should be advertised of all the dangers and understand all the precautions that could be taken in order to prevent and avoid the attacks.

The E-book for the cybersecurity provides that, while managing the safety and security of a system, some essential elements measures reported below shall be taken in particular consideration:

- Inclusion of cybersecurity as risk element in the hazard and risk analysis;
- Implementation of measures which respect the security standards to ISO 26262;
- Provide a step for the consolidation of requirement;
- Inclusion of security during the validation of safety definition, taking also in consideration during the overall process the security concept (Automotive iQ, 2017).

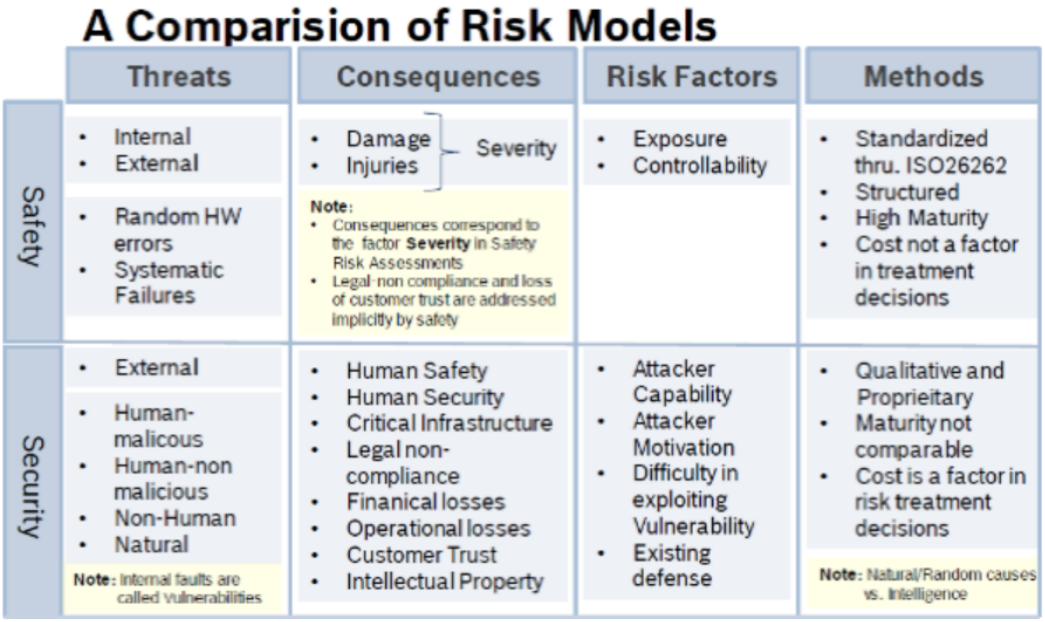

Figure 2: A Comparison of Risk Models (sources Automotive iQ)

A first and essential step in order to guarantee the implementation of the cybersecurity in the system is formed of the National Highway Traffic Safety Administration (NHTSA) best practices, which must be taken into account from OEMs. As reported in the Cybersecurity Best Practices for Modern Vehicles, "*the automotive industry should follow a robust product development process based on a system-engineering approach with the goal of designing systems free of unreasonable the risks*" (NHTSA). Furthermore, industries should take cybersecurity as a priority, with a defined process for risk assessment. This process must regard not only the final stage of the realization of the vehicle, but all the different steps of production (conception, design, manufacture, sale, use, maintenance, resale and decommissioning) (NHTSA).

The process could be divided in the following steps:

1. Definition of priorities;

2. Information sharing, meaning to "share information related to cybersecurity risks and incidents and collaborate in as close to real time as possible" (Executive Order No. 13691).
3. Vulnerability Reporting/Disclosure Policy;
4. Incident Response Process, meaning that each company must have a well-defined process in order to respond to incidents and vulnerabilities;
5. Self-Auditing: the automotive industries should also have a clear and detailed documentation on cybersecurity process, which should include the risk assessment phase, the penetration test results and the organizational decisions.

3.1 SAE J3061

The SAE J3061 is the recommended practice established by the SAE Vehicle Electrical System Security Committee which provided the most relevant guidelines in the sector. It is important to note the difference between the system safety, meaning when the system does not cause harm to life, property or environment (SAE J3061), while a "*system cybersecurity is the state of a system that does not allow exploitation of vulnerabilities to lead to losses, such as financial, operational, privacy or safety losses*" (SAE J3061).

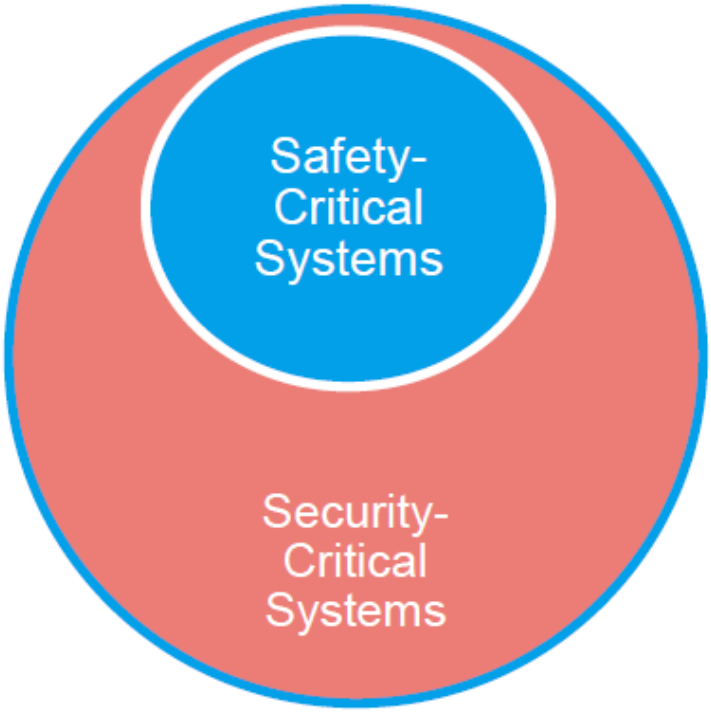

Figure 3 Safety- and Security-critical Systems according to SAE J3061(sources SAE J3061 Cybersecurity guidebook).

3.1.1 Application of the J3061

The J3061 supports the provision of a cybersecurity process for the automotive systems responsible for functions that are Automotive Safety Integrity Level rated to ISO 26262 or responsible for functions associated with propulsion, breaking, steering, security and safety (SAE J3061). Furthermore, this type of process is strongly encouraged for automotive systems that handle Personally Identifiable Information (SAE J3061).

3.1.2 Guidelines

J3061 provides important principles in order to guarantee the cybersecurity on vehicles.

Firstly, it is essential to know and understand which are the possible cybersecurity risks, in particular which will be the consequences (for example

if there are sensitive data or Personally Identifiable Information, or which are the external communication or connection that the system will have) (SAE J3061, for more information consult the cybersecurity guidebook mentioned above).

Secondly, it is very important to have a clear vision of the use that the final user will do, in particular in order to minimize the data collection (SAE J3061).

Thirdly, as provided by the principle enounced in the EU regulation 679/2016 for the privacy, meaning privacy by design, cybersecurity shall be taken in consideration during the different phase of realization of the system, starting with the concept and design phases.

Finally, cybersecurity should be implemented in during the Development and Validation and in Incident Response (SAE J3061, for more information consult the cybersecurity guidebook mentioned above).

In Figure 4, taken from the Cybersecurity guidebook for cyber-physical vehicle systems, are described the activities which analyse the cybersecurity process overview in the product development at the system level.

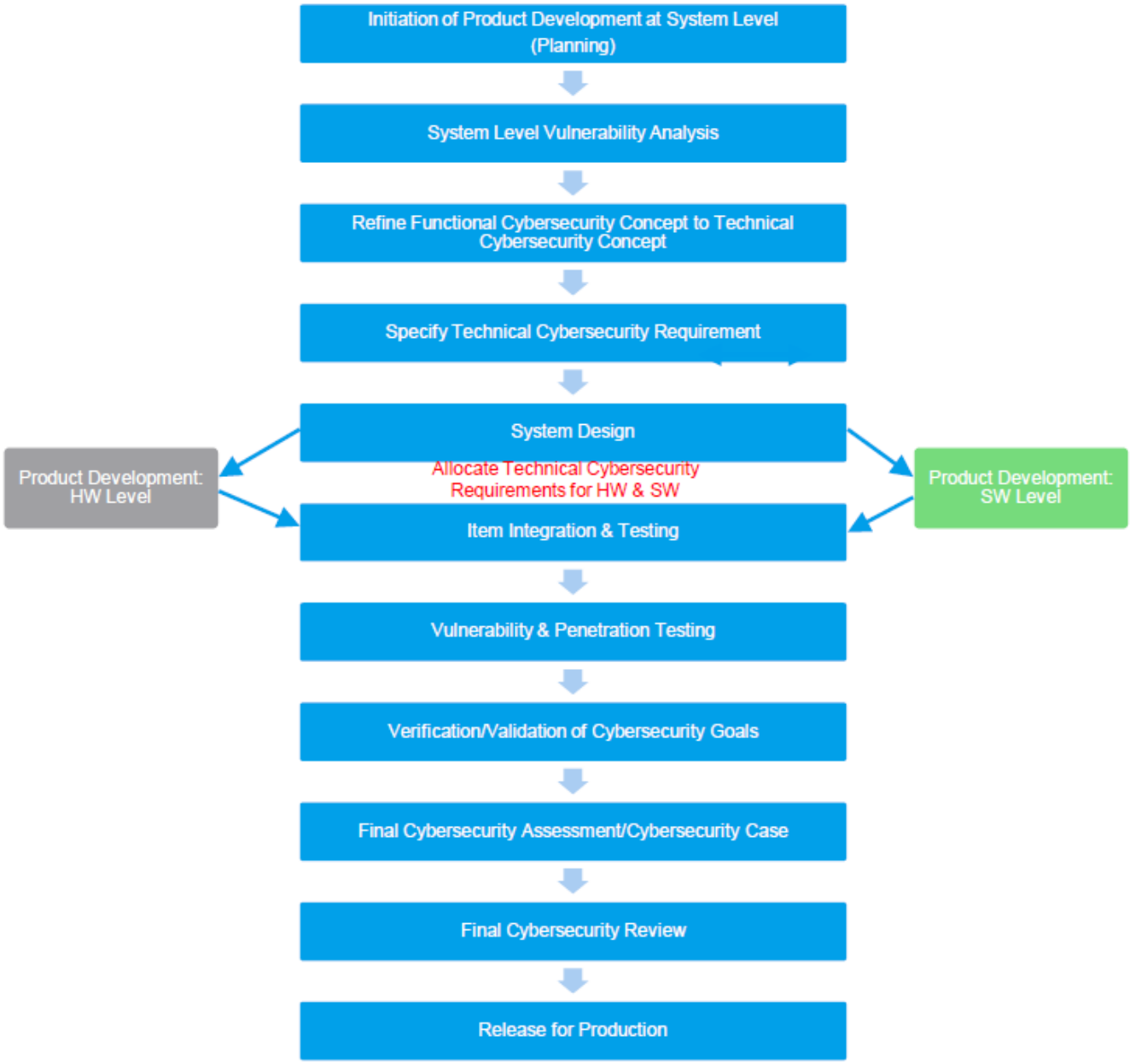

Figure 4 Cybersecurity Process Overview - Product development: Systems level (sources SAE J3061 Cybersecurity guidebook).

4 Privacy

Deliverable 1.2 has already analysed the legal framework regarding privacy in the European Union, with the EU regulation 679/2016. The aim of this paragraph is to examine the existing guidelines for OEMs, in order to guarantee the respect of privacy in the automated vehicles.

The NHTSA, with his Federal Automated Vehicle Policy, has provided different elements that should be ensured by car-makers:

- Transparency: guarantee the clear access to data privacy and security notice agreements;
- Choice: drivers should have the possibility of choice in relation of the use, sharing, retention, deconstruction and collection of data;
- Respect for context: respect the function in order to which the data have been collected;
- Minimization, de-identification and retention: collect the data only for "*the minimum amount of personal data required to achieve legitimate business purposes*" (NHTSA, 2016);
- Data security: the carmakers should provide measures to guarantee the protection of data;
- Integrity and access: provide measures aimed to guarantee the accuracy of personal data and allow the final user and the vehicle operators to rectify the information when it is collected "*in a way that directly or reasonably links the data to a specific vehicle or person*"(NHTSA, 2016).
- Accountability: make sure that entities that will receive and analyse the data will respect the data privacy and security agreements/notices.

5 Inputs to exploitation, dissemination and communication

In this section it will be provided specific guidelines extracted from the previous parts (and from D1.3) for the AutoMate demonstrator owners to overcome the legal issues and maximize the expected impact (and to actually turn AutoMate into mass-market products). Also, it will be inserted different communication and dissemination activities with the aim to increase the interaction with the public and ensure that people understand the importance of automated vehicles.

5.1 Key legal aspects for AVs

In the following table it has been highlighted the most important points extracting from the existing guidelines and legislative acts for liability, cybersecurity, privacy and safety. These elements could be extremely important for the AVs manufacturers and producers, even in the case in which they are not binding dispositions, because the respect of a standard or a set of guidelines will reduce the responsibility of the producer. Indeed, the Autonomous Vehicles Technology guide for policymakers provides that "*in some scenarios and for some industries, demonstrating that products meet well-accepted industry standards may also provide some liability protection for manufacturers*" (J.M. Anderson et al., 2016).

Table 3: AVs Guidelines

Items	Liability	Cybersecurity	Privacy
Act,	Directive 85/374/EEC	SAE 3061	• Directive 2002/58/EC

Items	Liability	Cybersecurity	Privacy
guidelines			• EU Regulation 679/2016
Critical point	Shift in responsibility from driver to manufacturer	Cyberattacks, which may cause incidents, illegal access to personal data etc.	Diffusion of sensitive and personal data
Best practice	• Respect the existing guidelines in other domains; • Incentive and participate in the process for the definition of standards and regulation.	• understand possible cybersecurity risks; • understand the use of data from users; • minimize the collection of data; • design the systems taking into consideration the cybersecurity; • cybersecurity should be implemented in during the Development and Validation.	Principles that carmakers should respect: • Transparency; • Driver's choice in data management; • Respect for data context; • Reduce the collection of data; • Integrity and access to data for final users; • Accountability.

In particulars sectors, as Human Machine Interaction, which is essential for the AutoMate project, important attention should be given to warnings.

Indeed, a product may be indicated as defected if are not provided precise and accurate warnings to the driver-user(J.M. Anderson et al., 2016).

5.2 Dissemination and communication activities to overcome the legal issue

Automated vehicles are a topic particularly discussed by scientific community and public. As every revolution in automation, society is having and will have an important role in the impact and more rapidly success and acceptance of these type of vehicles.

In accordance with the research conducted by the UCL Transport Institute at the beginning of 2017, legal aspects are one of the most discussed topics in the AVs sector, anticipated only by road safety issues, which is strictly linked to the regulatory matters.

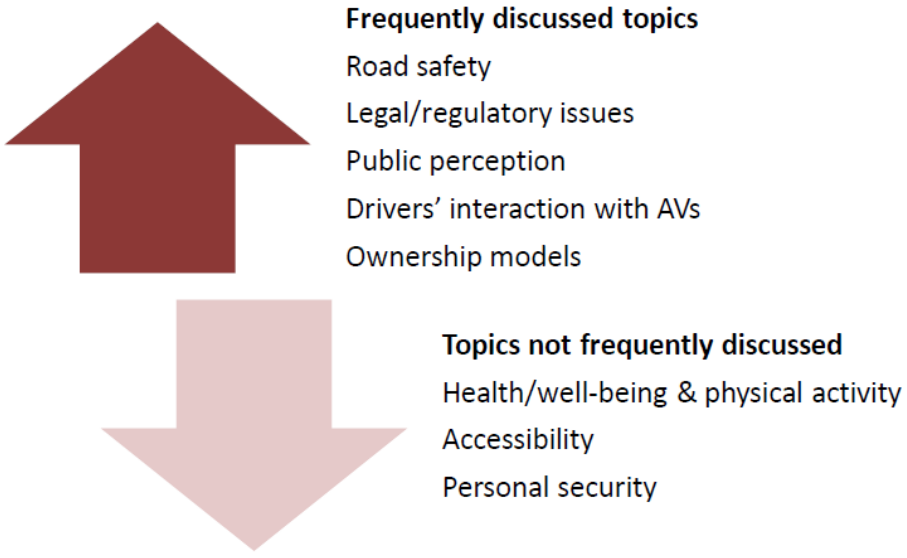

Figure 5: Relevant topics in AVs (sources UCL Transport Institute)

Confirmation that public awareness and acceptance is essential for AVs is provided by the Declaration of Amsterdam – Cooperation in the field of connected and automated driving, an important document signed by the 28 European transport ministers, which recognized the need of a common strategy for connected and automated driving. Indeed, the Declaration affirms that "*It is important to manage societal expectations, to raise awareness and increase acceptance and appreciation of connected and automated vehicles technologies*" (Declaration of Amsterdam, 2016).

In order to accelerate the process, create public confidence and overcome the legal barriers, AutoMate will realize communication activities dedicated to these topics.

Firstly, as one of the most concerned topic is the potential cybersecurity issues, AutoMate consortium will contact the European projects in this field, as for example SAFE COP (http://www.safecop.eu/) or SAFURE (https://safure.eu/), with the aim to realize workshops and public activities together, in which the audience will be informed about criticalities and the way to protect data and guarantee the safety inside the automated vehicle.

Secondly, as the direct involvement of final users from public will increase people's confidence, approaching the drivers to the real experience of automated vehicles, activities which will show directly the functioning of AutoMate will take place before the conclusion of the project.

Finally, the positive impact of AVs will be demonstrated and highlighted by using social media channels.

6 Conclusions and next steps

Currently, the Automated Vehicle (AV) legal framework is very complex and different open questions are still present. The European Union has strongly underlined the importance of a common action and the need of a legislative structure that provide specific dispositions for all the categories that are operating in the sector.

In Deliverable 1.6 will be revised and updated the part related to Safety issues, which has been already analyzed in Deliverable 1.2. At the moment, there are no relevant elements to be added to this part.

In order to guarantee safety and security in AVs, it is essential to include the final users, meaning the driver, in the process. Indeed, as provided by the e-Book for cybersecurity professional, "in the event of a newly discovered vulnerability or security breach, detailed incident response plans provide a quick response to the manufacturer and give confidence to the consumer". Acceptance and trust of people are essential for the evolution of automotive industry, and this element should not be underestimated while planning and defining the legal framework.
For the reasons mentioned above, AutoMate will realize communication and dissemination activities with the intent to bring people closer to the importance of AVs in the society.

References

Alonso Raposo, M., Ciuffo, B., Makridis, M. and Thiel, C. (2017). *The r-evolution of driving: from Connected Vehicles to Coordinated Automated Road Transport (C-ART). Part I: Framework for a safe & efficient Coordinated Automated Road Transport (C-ART) system.* Joint Research Centre, European Commission.

Anderson, J., M., Kalra, N., Stanley K., D., Sorensen, P., Samaras, C., Oluwatola O., A. (2016). *Autonomous Vehicle Technology. A guide for Policymakers*. Rand Corporation.

Automotive iQ. Automotive Cyber Security. *Dedicated eBook for the Cyber Security professional*. (https://www.automotive-iq.com/http%3A//www.automotive-iq.com/electrics-electronics/white-papers/automotive-cyber-security-complete-ebook)

Cavoli, C., Philips, B., Cohen, T., Jones P. (2017). *Social and behavioral questions associated with Automated Vehicles. A Literature Review*. UCL Transport Institute, London: Department for Transport.

Declaration of Amsterdam. *Cooperation in the field of connected and automated driving*. Amsterdam, 14-15 April 2016.

European Court of Justice (2015). *Judgment of the Court (fourth Chamber) in Joined Cases C-503/13 and C-504/13*. ECJ Reports.

GEAR 2030 Discussion Paper (2016). *Roadmap on Highly Automated vehicles*. European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs.

Helmig, E. (2015). *Manufacturer responsibility under European Union Law – prevention and prophylaxis in ECJ jurisprudence.*

Helmig, E. (2016). *Safety Expectations for Automated and Autonomous Vehicles. Liability arising from basic technology vs. future technology*.

Keller, P., Evans, H., Henkel F. (2017). *Autonomous vehicles. The legal landscape of Dedicated Short Range Communication in the US, UK and Germany*. Norton Rose Fulbright.

Maggi, M. (2017). *Driverless Cars: How is Liability in Case of Crash*. AEIT.

National Highway Traffic Safety Administration (2016). *Cybersecurity best practices for modern vehicles*. Report No. DOT HS 812 333. Washington, DC.

National Highway Traffic Safety Administration (2016). *Accelerating the Next Revolution in Roadway Safety*. Washington, DC.

Navetta, D., Segalis, B., Kleiner, K. (2017). *The Privacy Implications of Autonomous Vehicles*. Data Protection Report. Norton Rose Fulbright.

Parker, N., Shandro, A., Cullen, E. (2017). *Autonomous and connected vehicles: navigating the legal issues*. Allen & Overy, London.

Pillath, S. (2016). *Automated vehicles in the EU*. European Parliamentary Research Service.

SAE International (2016). *Cybersecurity Guidebook for Cyber-physical Vehicle Systems*.

Vecere, L. (2016). *Connecting Car e Autonomous Vehicle. Il fenomeno dell'evoluzione del diritto come conseguenza del cambiamento e dell'innovazione tecnologica. II Parte*. Roma.