

D6.4

Plan and preliminary report on EU policies and regulations recommendations

Dissemination level	Public (PU)	
Work package	WP6: Deployment enablers	
Deliverable number	D6.4	
Version	V3.0	
Submission date	11/11/2020	
Due date	30/10/2020	
Resubmission date	12/05/2023	



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 825496.

www.5g-mobix.com





Authors

Authors in alphabetical order		
Name	Organisation	Author or Co-Author
Janie Baños	DEKRA	3.2.12, 3.4
Oscar Castañeda	DEKRA	3.2.12, 3.4
Carmen	FRAUN	2.1; 2.2
Constantinescu		
Aitor Fernandez	AEVAC	4.4, 4.8, 4.9
Diana Blanco Pérez	CTAG	Questionnaire comments.
Jose Antonio	CTAG	5.3. Recommendations from the car industry.
Fernández Núñez		
Chris Hobbs	CATAPULT	6.2
Akrivi-Vivian Kiousi	INTRA	
Jorge Alfonso Kurano	UPM	6 Conclusions
Pedro Llorens	AEVAC	4, 4.1, 4.2, 4.4, 4.5, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12
José Manuel	UPM	6 Conclusions
Menéndez		
Pieter Nooren	TNO	Co-author 3.2.6, 3.2.8
lván Pérez Piñeiro	CTAG	5.3. Recommendations from the car industry.
Moustafa Roshdi	FRAUN	1.2
Olga E. Segou	INTRA	1.3, 3.2.1, 3.2.2 , 3.2.3, 3.2.4, 3.2.6, 3.2.7, 3.2.8, 3.2.9,
		3.2.10, 3.4.2, 4.1, 4.2 , 4.3, 4.6, 5.1.
Claudiu Alin Rusu	FRAUN	2.1,2.2, review and cleanup
Tahir Sari	FORD	3.2.5, 5.3
Alexander Schletz	FRAUN	5.4
Martin Speitel	FRAUN	ES; 2.1.3 , review and cleanup

Control sheet

Version history			
Version	Date	Modified by	Summary of changes
0.1	29/10/2019	Carmen Constantinescu,	Initial Version
		Elke Roth-Mandutz,	
		Martin Speitel,	
		Bernhard Niemann	
		Claudiu-Alin Rusu	
0.2	18/12/2019	Martin Speitel	Update for Telco 19.12.2019
0.3	29/01/2020	Martin Speitel	Clean-up after telco



0.4	10/02/2020	Martin Speitel	Added reference to WP2.1
			Tables of issues already defined in WP2.1
0.5	24/02/2020	Martin Speitel	Added chapter 4.2 (contribution DEKRA)
0.6	27/02/2020	Carmen Constantinescu	Add Ch. Methodology and Ford
		Claudiu-Alin Rusu	contribution, additionally the
			questionnaire
0.7	08/04/2020	Martin Speitel	Including contributions from partners:
		Claudiu-Alin Rusu	1.3: INTRA
			4.1 TNO
			4.2.4 DEKRA
			4.3.4. TNO
			6.3 CTAG (Table)
			6.3 FORD (Text)
			2.3 ERTICO
0.9	27/10/2020	Fraunhofer Team	Compiling all input together, add input
		Claudiu-Alin Rusu	from review, clean-up formatting
0.10	06/11/2020	Olga Segou	Finalisation of draft
		Akrivi Kiousi	
		Alain Renault	
1.0	09/11/2020	Martin Speitel	Clean-up document and removing last
		Claudiu-Alin Rusu	typos and comments
1.1		Martin Speitel	Update after Review
		Claudiu-Alin Rusu	
		Olga Segou	
1.2	9/05/2021	Martin Speitel	Update after Review
		Claudiu-Alin Rusu	
		Pieter Nooren	
		Olga Segou	
		Tahir Sarı	
		Jose Fernandez	
		Oscar Agustín Castañeda	
		Aguadero	
		Diana Blanco	
1.3	14/05/2021	Martin Speitel	Delivered for review
		Claudiu-Alin Rusu	
1.4	25/5/2021	Martin Speitel	Update after quality review
		Claudiu-Alin Rusu	
2.0	27/5/2021	Martin Speitel	Final version for delivery
		Claudiu-Alin Rusu	
3.0	12/5/2023	Claudiu-Alin Rusu	Update and fixed references



Peer review		
	Reviewer name	Date
Reviewer 1	Doruk Sahinel	15/10/2020
Reviewer 2	Johan Scholliers	18/10/2020

Legal disclaimer

The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The 5G-MOBIX Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. Copyright © 5G-MOBIX Consortium, 2018.



Table of contents

С	ontents	
LI	ST OF FIGURES	8
LI	ST OF TABLES	9
E)	(ECUTIVE SUMMARY	. 13
1.	INTRODUCTION	. 15
	 1.1. 5G-MOBIX concept and approach	15 15 16 16
2.	PLAN AND METHODOLOGY	. 17
	 2.1. Plan	17 17 18 19 20 21 24
3.	REGULATION AND CERTIFICATION	. 27
	 3.1. Cross-border issues identified in D2.1. 3.2. Overview of existing regulatory frameworks	27 28 28 ility
	related applications	29
	3.2.4. Non-discrimination	31
	3.2.5. Car Safety	33
	3.2.6. European Electronic Communications Code	34
	3.2.7. Roaming	35
	3.2.8. Open Internet	36
	3.2.9. Critical Infrastructures & Law Enforcement	38
	3.2.10. UN Regulations on Cybersecurity and Software Updates	39
	3.2.11. Radio equipment	41





	3.2.12.	Certification	
	3.3. Ove	rview of existing certifications	
	3.4. Reg	ulatory certification	
	3.4.1. Ce	ertification according to CE marking	
	3.4.2. FC	CC – Federal communication commission	
	3.4.3. Pr	ivacy certifications	
4.	CURRE	ENT POLICY STATE-OF-PLAY	50
	4.1. 5G f	or Europe Action Plan	
	4.2. Eur	opean 5G Observatory	
	4.3. 5G (Cybersecurity toolbox	
	4.4. Eur	ope on the Move: Third Mobility Package	
	4.5. Cro	ss-border corridors for Connected and Automated Mobility	
	4.5.1. Eu	Jrope's 5G Corridors	55
	4.5.2. In	itiatives for 5G cross-border corridors large-scale testing	56
	4.6. 5G S	Strategic Deployment Agenda for Connected & Automated Mobility	
	4.7. 5G I	nfrastructure Public Private Partnership (5G PPP)	
	4.8.Con	necting Europe Facility (CEF)	
	4.8.1. CI	EF Telecom	59
	4.8.2. CI	EF Transport	59
	4.9. Con	necting Europe Facility (CEF2) Digital	60
	4.10.	C-ITS Platform	60
	4.11.	Other initiatives	61
	4.11.1.	European Automotive – Telecom Alliance (EATA)	61
	4.11.2.	5G Automotive Alliance	61
	4.11.3.	C-ROADS Platform	61
	4.11.4.	CAR2CAR Consortium	62
	4.12.	Post-Covid-19 Releases	62
	4.12.1.	State of the Union 2020	63
	4.12.2.	Spanish Connected, Safe and Sustainable Mobility Strategy 2030	63
	4.12.3.	France – Spain cooperation in CAM	64
5.	PRELI	MINARY RESULTS	65
	5.1. Rec	ommendations from ICT Sector	65
	5.2. Rec	ommendations from road operators	66
	5.3. Rec	ommendations from car industry	69
	5.4. Que	estionnaire Results	
	5.5. Fou	r Questions to Stakeholders	82



6. CONCLUSIONS	85
REFERENCES	89





LIST OF FIGURES

Figure 1: Methodology to collect requirements from partners and stakeholders
Figure 2: Project plan including subtasks 20
Figure 3: Screenshot from the questionnaire asking about barriers
Figure 4: High-level overview of Stakeholder ecosystem 25
Figure 5: Services and applications need to comply with the rules for Internet Access Services (IAS) and the rules for Specialized Services (SpS)
Figure 6: Certification schemes for V2X radio equipment43
Figure 7: 5G Cross-border Corridors for Connected and Automated Mobility
Figure 8: The 5G SDA common principles58
Figure 9: Online survey: Start screen
Figure 10: Online survey: General question (Type of stakeholder, company size, the main area of expertise and country)





Table 1: Communication tools utilized to reach stakeholders for the purpose of this Study	26
Table 2: Issues relevant for regulation from D2.1.	27
Table 3: RED requirements and harmonized standards for ITS radio equipment.	44
Table 4: FCC requirements for ITS radio equipment.	46
Table 5: Contribution to the questionnaire per stakeholder	74
Table 6: Contribution to the questionnaire per company size	74
Table 7: Contribution to the questionnaire per area of expertise	74
Table 8: Contribution to the questionnaire per working country, multiple answers were possible via	"other". 75
Table 9: Technical/scientific challenges foreseen by the "Academia/R&D-experts"	76
Table 10: Main motivation by the "Academia/R&D-experts".	78
Table 11: Main gains expected from research in 5G/CAM by the "Academia/R&D-experts"	
Table 12: Main barriers in 5G/CAM research by the "Academia/R&D-experts"	79
Table 13: Cooperation with other stakeholders by the "Academia/R&D-experts"	79
Table 14: Status of cross-border scenarios in research by the "Academia/R&D-experts"	80





ABBREVIATIONS

Abbreviation	Definition	
5G PPP	5G Infrastructure Public Private Partnership	
5GAA	5G Automotive Association	
5G-PPP	5G-Public Private Partnership	
ACEA	European Automobile Manufacturers' Association	
AD	Automated Driving	
ADAS	Advanced Driver Assistance Systems	
ARCADE	Aligning Research & Innovation for Connected and Automated Driving in Europe	
ASECAP	European Association of Operators of Toll Road Infrastructures	
AV	Autonomous Vehicle	
BEREC	Body of European Regulators for Electronic Communications	
CAD	Connected and Automated Driving	
CAM	Connected and Automated Mobility	
CARTRE	Coordination of Automated Road Transport Deployment for Europe	
CE	Conformité Europënne	
CEDR	Centre for Effective Dispute Resolution	
CEF	Connecting Europe Facility	
CEN	European Committee for Standardisation	
DSIs	Digital service infrastructures	
DSRC	Dedicated Short-Range Communications	
EATA	European Automotive and Telecom Alliance	
EC	European Commission	
EC DGs	European Commission Directorates-General	
ECHR	European Charter of Human Rights	
ECN/ECS	Electronic Communications Networks or Services	



EDPB	European Data Protection Board	
EEA	European Economic Area	
EMC	Electromagnetic Compatibility	
ENISA	European Union Agency for Cybersecurity	
ENSEMBLE	ENabling SafE Multi-Brand platooning for Europe	
ETNO	European Telecommunications Network Operators' Association	
ETSI	European Telecommunications Standards Institute	
EU	European Union	
Euro NCAP	European New Car Assessment Programme	
FCC	Federal Communications Commission	
FDI	Foreign Direct Investment	
GCF	Global Certification Forum	
GDPR	General Data Protection Regulation	
GSA	Global mobile Suppliers Association	
GSM	Global System for Mobile Communications	
HITRUST	Health Information Trust Alliance	
ICT	Information and Communications Technology	
IoT/M2M	Internet of Things / Machine to Machine	
ITS	Intelligent Transport Systems	
JRC	Joint Research Centre	
KETs	Key Enabling Technologies	
LTE	Long Term Evolution	
MITMA	The Spanish Ministry of Transports, Mobility and Urban Agenda	
MNOs	Mobile Network Operators	
MoU	Memorandum of Understanding	
MS	Members States	







NFC	Near-field communication
NIS	Network and Information Systems
NRAs	National Regulatory Authorities
OBU	On-Board Unit
OEM	Original Equipment Manufacturer
ΟΤΑ	Over-the-air
PCS	Process Control Systems
QoS	Quality of Service
RE	Radio equipment
RED	Radio Equipment Directive
RF	Radio frequency
RSUs	Road-Side Units
SAE L4	Semi-autonomous vehicles LEVEL 4: No human interaction required
SIM	Subscriber identity module
SLA	Service-Level Agreement
SMEs	Small and Medium-sized Enterprises
UNECE	United Nations Economic Commission for Europe
V2X	Vehicle-to-everything wireless communications
VRUs	Vulnerable Road Users
WLAN	Wireless Local Area Network
WP	Work Package
X-border	Cross-border





EXECUTIVE SUMMARY

Deliverable *D6.4* "*Plan and preliminary report on EU policies and regulations recommendations*" presents a complete cycle of requirements gathering, analysis, target group and framework identification, and finally a synthesis exercise. This has resulted in a first step in a comprehensive overall view on the major issues that are of concern to the relevant stakeholders in deployment of 5G CAM solutions, such as the Automotive Industry, Road Operators, the ICT sector and more. As a result, the following short-term (2020) regulatory needs were identified:

- A common European understanding on necessary digital infrastructure quality/coverage for Level 3;
- Joint approach between telecom and vehicle industries to support CAD;
- Common European understanding on safety & security validation (when are the systems safe enough);
- Coordinated European and Member State programs to support global competitiveness;
- Adaption of road traffic rules in Member States;
- Align General Data Protection Regulation within the European member states to ensure privacy.

To achieve that, it is crucial that existing and future policies are implemented in order to:

- Align roadmaps and priorities for a coordinated 5G deployment across all EU Member states;
- Promote early deployment in major urban areas and along major transport paths;
- Unite leading actors in working towards the promotion of global standards;
- National strategies and plans by EU Member States, available national data on 5G deployment including coverage and quality;
- Preparation and execution of spectrum assignments by public authorities as well as 5G public funding for network deployment and R&I;
- Reduce the cost and increase the speed of deployment of very high-capacity networks, notably by removing unnecessary administrative hurdles;
- Common message sets/protocols dedicated to police interactions shall be standardized at international level for suspicious events;
- Roaming, and the obvious implication for Cross Border 5G CAM applications and scenarios;

Furthermore, this document presents results on the first 5G-MOBIX Stakeholder Survey. The related questionnaire was distributed inside the 5G-MOBIX consortium first and second among external partners and email lists like the ERTICO newsletter. This document presents the feedback collected from 52 participants with 28 coming from academia and R&D centres.

A short analysis of the answers to the questionnaire and additional questions to selected stakeholders, as well as input and analysis from ongoing and recent initiatives have resulted in the identification of the following challenges, and mainly the lack of a regulatory framework for CAM solutions and vehicles, involving a common European understanding on necessary digital infrastructure, a joint telecom/vehicle





industry approach on supporting CAD, awareness on interoperability issues and cross-border items, a common European Security & Safety validation, and the need for a progressive adaptation of road traffic rules in Member States.

The major technical aspects being addressed by the 8 participants coming from the automotive sector include V₂X communication technologies and performance items, service and application requirements, and most importantly, Cybersecurity, Privacy and Digital infrastructure aspects for CAM. This document intends to get an update after the X-Border trials, if new aspects or issues arise in the ongoing tests.





1. INTRODUCTION

1.1. 5G-MOBIX concept and approach

5G-MOBIX aims to showcase the added value of 5G technology for advanced Connected and Automated Mobility (CAM) use cases and validate the viability of the technology to bring automated driving to the next level of vehicle automation (SAE L4 and above). To do this, 5G-MOBIX demonstrates the potential of different 5G features on real European roads and highways, create, and use sustainable business models to develop 5G corridors. 5G-MOBIX also utilizes and upgrades existing key assets (infrastructure, vehicles, components) and the smooth operation and co-existence of 5G within a heterogeneous environment comprised of multiple incumbent technologies such as ITS-G5 and C-V2X.

5G-MOBIX executes CAM trials along cross-border (x-border) and urban corridors using 5G core technological innovations to qualify the 5G infrastructure and evaluate its benefits in the CAM context. The Project defines deployment scenarios, identifies and responds to standardization and spectrum gaps.

5G-MOBIX first defines critical scenarios needing advanced connectivity provided by 5G, and the required features to enable some advanced CAM use cases. The matching of these advanced CAM use cases and the expected benefits of 5G are tested during trials on 5G corridors in different EU countries as well as in Turkey, China and Korea.

The trials will also allow 5G-MOBIX to conduct evaluations and impact assessments and to define business impacts and cost/benefit analysis. As a result of these evaluations and international consultations with the public and industry stakeholders, 5G-MOBIX identifies new business opportunities for the 5G enabled CAM and proposes recommendations and options for its deployment.

Through its findings on technical requirements and operational conditions, 5G-MOBIX consortium expects to actively contribute to standardization and spectrum allocation activities.

1.2. Purpose of the deliverable

The purpose of the deliverable is to:

- Monitor specification, deployment, trial and evaluation activities to identify challenges relating to deployment and x-border issues to:
 - Transform the expression of issues into topics of discussions with the related organizations;
 - Assess key emerging topics in 5G topics springing with direct interaction with stakeholders (authorities and service providers);
 - Provide corresponding recommendation to policy makers and regulators;



- Analyse the issues detected to transform them first in topics of discussions pushed to the relevant EU bodies (private or public) to provide recommendations to those bodies.
 - Expound and push 5G-MOBIX issues and recommendations and follow up the discussions to get concrete results provide topics of discussions on real x-border issues and resulting recommendations to EU-wide policy makers and regulators to:
 - Ensure liaison with the EU policy and regulation platforms and the related EC DGs (MOVE, CONNECT, JRC);
 - Liaison with the industry associations regarding automotive and telecommunications;
 - Guidance of the national legislative procedures, as well as contribution to the EU regulative processes, is the main target;
 - Monitor and provide inputs to the discussion about spectrum allocation in the EU and beyond.

1.3. Intended audience

The current document is publicly disseminated and is available as a free download on the 5G-MOBIX website [1]. It is meant primarily as a handbook that introduces 5G for CAM stakeholder opinions and discusses challenges that can be addressed by proposed recommendations at regulatory and policy level. Thus, this document aims to serve not just as an internal guideline and reference for all 5G-MOBIX beneficiaries but also for the larger communities of 5G and CAM development, as well as national and EU regulators and other policy makers.

Interested readers may also refer to:

- D6.1 "Plan and Preliminary Report on deployment enablers" for discussion on the current state and evolution of 5G for CAM;
- D6.2 "Plan and Preliminary Report on the business models for cross border 5G deployment enabling CAM" for an analytical discussion on business models, covering the entire 5G CAM value chain;
- D6.3 "Plan and Preliminary Report on the standardisation and spectrum allocation needs" for an extensive analysis of standardisation and spectrum allocation.

These documents are also available as a free download on the 5G-MOBIX website.

1.4. Covid-19 impact

As of 2020, an internal monthly update is done and a bi-weekly assessment in PMT is performed to monitor the COVID-19 pandemic impacts on the project (quality). Besides, a COVID-19 section numbered 1.5 shall be added in any deliverable submitted after November 1st, 2020 else the Quality Management is not affected further by the COVID-19 pandemic. Moreover, a general description of the post COVID-19 releases of documents and deliverables can be found in chapter Current Policy State-of-Play (subsection 4.12).





2. PLAN AND METHODOLOGY

2.1. Plan

In this section, we give an overview of the devised plan to meet the aforementioned objectives. We divided our plan into four phases with the main purpose of monitoring and assessing in the first one, and sharing the outcomes in the fourth one with multiple underlying subtasks, as illustrated in Figure 1.

2.1.1. Methodology of the 5G-MOBIX regulation recommendations

Deliverable 6.4 workplan is based on four phases to identify the issues of 5G-enabled CAM, including crossborder prospects, to generate detailed analyses on the means of overcoming the previously stated issues, and providing recommendations for policymakers and regulators as well as valuable feedback for the industry.

The first phase of the work consists of monitoring specifications and issues that are related to the deployment of the Trial Sites and in the Cross-Border Corridors that relate to policy, cooperation and regulatory matters. The issues previously mentioned are clustered according to the specific domain of research and expertise from which it derived. The provided questionnaire will provide impartial feedback on the issues and potential means of creating the fundamental legislative and regulatory background necessary for the further development of 5G supported autonomous vehicles.

The second phase consists on the survey and the internal review of the questionnaire, improvements, and development of the wording which is used to improve the understanding and clearance of the ambiguous questions of the questionnaire while keeping the support for all types of stakeholders implied in 5G-MOBIX and other like projects domains of expertise essential inquiries.

The further aspect that is considered in the second phase is the research and documentation of other related projects, which work with the 5G and autonomous vehicles, to accomplish the overall view regarding the issues, areas of implementation, and domains of integrations of the technology in the real world. The output of this phase will provide the preliminary conclusions regarding the data gathered from the stakeholders through the questionnaire and the elaboration of the first online version of the survey.

The third phase of the deliverable has the purpose to identify a list of EU-wide policy makers and regulators to develop a dialogue, which will improve the pre-existing regulations and create the fundamental standardization regarding future laws over telecommunications, road operations, and network existing and future infrastructure. The relevant CAD and 5G projects are identified and the means of communication with the representatives are done for data exchange and external improvements and feedback. The phase is also strongly correlated with the external roll of the survey which permits unbiased feedback and data gathering will improve the overall transparency of the process while targeting the indispensable information.

The main output for the third phase consists of the validation of the gathered data internally, and confirmation/information of the final survey feedback; the final part of this phase will coincide with the analyses of the external roll gathered information. The results are shared and are transposed as



recommendations and suggestions from the industry, academy and other entities to the EU-wide policy makers and regulators in the fourth and final phase of the Deliverable 6.4.

PHASE 1: Monitoring and assessment distribution	PHASE 3: Validate & Exchange Views on emerging topics with the stakeholders focus groups at targeted events
Activities: Monitor specification, deployment, trial and evaluation activities. Output: Questionnaire realized and approved by the WP 6 partners.	Activities: Identify the list of EU-wide policy makers to be addressed and contact partners to these organizations and core external stakeholders. Output: Final Survey distributed to external core stakeholders for validation; Preliminary recommendations list for EU policies and regulation bodies and industry associations.
Delivera Metho	able 6.4 dology
Activities: Analysis of the survey; Elaboration of preliminary internal conclusions. Output: Final survey improve after internal consultations to rG-Mohiy Consortium distributed	Activities: Align WP 6 task results Provide topics of discussions on x-border issues and resulting recommendations to EU-wide policy makers, create liaison with EU policy platforms Output: Guidance of the national legislative procedures; Topic of discussions and recommendations
PHASE 2:	for EU policy makers, formalized and prepared for liaison and communication. PHASE 4:
Self-assessment	Share outcomes with policy community and let policy makers decide the optio

Figure 1: Methodology to collect requirements from partners and stakeholders.

2.1.2. Participatory Collection of Requirements

This step is mainly concerned with collecting all the information and challenges from the different stakeholder audiences involved while facing deployment and x-border coordination. This step is divided into the following individual subtasks performed in T6.4:

- Using the cross-border issues identified in WP2 as a starting point, 5G-MOBIX further examines the current regulatory frameworks across the EU and identify the gaps that need to be addressed. An overview of the current regulatory frameworks can be found in Section 3.2.
- Classifying of potential issues by clusters, e.g., regulation, certification, etc. An overview of this classification can be found in Sections 3.2 and 3.3.
- Designing and realizing an online questionnaire to collect inputs from the identified stakeholders and groups of relevance to the project, on the prioritization of clustered issues and barriers. The design and contents of the questionnaire are explained in more details in subsection Monitoring Instruments (2.2)
- Distribution of the questionnaire to 5GMOBIX partners to collect initial inputs from internal and external stakeholders.



- Update the questionnaire after the initial feedback and distribute it to a wide range of stakeholders outside the consortium.
- Analysis of the results from the second round of inputs to the questionnaire.

Results are then presented in Stakeholder engagement activities such as:

- WP6 presentation in Infocom World 2020 (November 4th 2020, online)
- Presentation to the 5G-MOBIX advisory board (November 18th 2020, online)
- WP6 organised workshop titled "Workshop on the Deployment Methodology of 5G for CAM on Cross-Border Corridors" (March 26th 2021, online), with more than 50 invited attendees.

2.1.3. Providing recommendations for policy makers and regulatory entities

The objective of this step is to analyse the collected data and provide recommendations for the appropriate regulatory bodies. This step is divided into the following subtasks:

- Analysis of the internal survey results to conclude the requirements for addressing the issues raised through the partners' initial analysis. This is the first step towards analysing the issues into topics and transposing them into recommendations.
- A summary of the recommendations from different clusters of stakeholders is present in sections 5.1-5.3. Moreover, sections 5.4-5.5 add the results of questionnaires to stakeholders.
- During the latter stages of communication and validation of our outputs, T6.4 plans to:
 - Identify the first candidate list of EU policy makers and regulators to be addressed.
 - Identify contact partners to these bodies and organizations, and ensure liaison with the EU policy and regulation platforms and the related EC DGs (MOVE, CONNECT, JRC).
- Interaction with the relevant bodies to push 5G-MOBIX issues and recommendations and follow up the discussions to accomplish concrete results.





Figure 2: Project plan including subtasks.

2.2. Monitoring instruments

As the main instrument of monitoring the demands in matters of infrastructure, protocols of telecommunications, automotive base, and road operating means, the purpose of the questionnaire is to facilitate the communication between the experts in the above areas and regulatory authorities. Thus, by improving the link between the demands of the industry and the provided legislative background in the area of telecommunications and road infrastructure and sharing of such platforms, networks and assets, as well as the bases for autonomous driving and international telco protocols for such purposes, will increase the rate of integration and adaptability of the technology within the existing infrastructure and will enable the future use and implementation in real-life scenarios. The questionnaire is divided into multiple pages, starting from the area of expertise of the questioned company or individual, following through the questions directly related to their domain of expertise. This is meant to keep the context and specialist speech content and to avoid eventual confusion regarding the questions and answers of the stakeholders.

The first page describes the participant domain of expertise, the group of stakeholders, the interest and expectations regarding the results and further development of CAM, 5G and autonomous vehicle technology, the country of origin for the company which is also required for the international purpose of the 5G-MOBIX project. The current document is publicly disseminated and is available as a summary on the 5G-MOBIX website. It is meant primarily as a research instrument for an overall view of the technology, infrastructure, laws, regulations and business models for the CAM and 5G technology. Secondly, this document aims to serve not just as an internal guideline and reference for all 5G-MOBIX beneficiaries but also for the larger communities of 5G and CAM development, as well as national and EU regulators and other policy makers. The questionnaire is disseminated among the consortium members, in the liaison projects



5GCroCo, 5G-CARMEN, 5G-EVE, 5GENESIS, 5G-VINNI, 5G-DRIVE, C-ROADS, CONCORDA, ICT4CART, INFRAMIX, AUTOPILOT, 5G!PAGODA, ONE5G, 5G-TOURS, 5GROWTH, 5G-HEART and 5G IA. In addition, it is disseminated in the ERTICO newsletter with more than 4000 subscribers.

What are the important barriers hindering 5G/CCAM research?					
	1 - not a factor	2	3	4	5 - major barrier
Cooperation with other stakeholders	0	0	\bigcirc	\bigcirc	\bigcirc
Access to experimentation data	0	0	\bigcirc	\bigcirc	\bigcirc
Access to experimentation facilities (vehicle testing sites, etc)	0	0	\bigcirc	\bigcirc	\bigcirc
Access to experimentation infrastructures (5G, Cloud, High Performance Computing etc.)	0	0	\bigcirc	0	0
High costs for vehicle/hardware/software procure- ment	\bigcirc	0	\bigcirc	\bigcirc	\bigcirc
End-to-end experimentation requires varied skills	0	\bigcirc	\bigcirc	\bigcirc	\bigcirc
Skills/Knowledge not present in my organisation	0	0	0	0	0
Acquiring licenses (spectrum, use of road etc.)	0	0	0	0	0
Other (please indicate)	0	0	0	0	0

Figure 3: Screenshot from the questionnaire asking about barriers.

2.3. Data and gap analysis

ERTICO ITS Europe has conducted a relevant analysis of the EU policy and regulatory landscape for several current and previous projects, which will be part of the comprehensive literature review to be conducted providing input into the final report. This research will be built upon and updated to reflect the most recent steps forward in autonomous vehicle regulation at UN, EU and member state levels.

The European Commission has published in 2016 a series of strategies and action plans to support the deployment of key enabling technologies and in particular, the connectivity infrastructure paving the way for automated vehicles: the Communications on "5G for Europe: An Action Plan" (COM(2016) 588), the European C-ITS Strategy and "A Space Strategy for Europe" (COM(2016) 705). The Commission's 5G Action Plan laid down an ambitious deployment timeline with an early roll-out in at least one major city in each member state in 2020 and uninterrupted coverage over all urban areas and major transport paths by 2025. The Action Plan aims at fostering the competitiveness of the European industry by supporting the deployment and take-up of 5G networks, enabling among other things the timely assignment and availability of radio spectrum, creating more favourable conditions. "Mission-critical services" for transport and vehicles will become feasible thanks to the higher performances achievable by 5G, including advanced services based on cloud, edge computing, vehicle-to-vehicle and vehicle-to-infrastructure connectivity that are important for automation. Standardisation, spectrum and regulatory work for 5G are being carried out







through the 5G-PPP, an initiative between the ICT industry and the European Commission, and the 5G Automotive Association (5GAA).

Under the EU funded Coordination and Support Action CARTRE (Coordination of Automated Road Transport Deployment for Europe, 2016 - 2018) [2] coordinated by ERTICO, project partners conducted an exploration of the policy environment for automated and autonomous vehicles, published in October 2018 under the form of a position paper [3].

Key obstacles the CARTRE team and stakeholder network identified for the development of autonomous vehicles included non-existent, incomplete or different national legislative approaches across countries. This is a major obstacle on the path to the market introduction of automated and especially autonomous vehicles. It was recommended to create a regulatory framework that is as unified as possible for the benefit of the European internal market. Type approval regulation is a key area for regulatory development.

The risks of both over-regulating, in terms of stifling innovation, and in under regulating, including having unsafe and environmentally damaging motorized vehicles on the roads were highlighted. The report further highlights the difference between the directions of EU, Japanese, Chinese and US policy approaches to the regulation of autonomous vehicles.

The following short-term (2020) regulatory needs were identified:

- A common European understanding of necessary digital infrastructure quality/coverage for Level 3.
- Joint approach between telecom and vehicle industries to support CAD.
- Need for cross-border pilot operation projects for a quick rollout of Level 3.
- Common European understanding on safety & security validation (when are the systems safe enough).
- European push in setting up the framework for a safe level 4 series development (new UN Regulation, so-called horizontal regulation on accelerator, brakes, steering, lighting, vehicle access).
- Coordinated European and Member State programs to support global competitiveness.
- Adaption of road traffic rules in Member States.

Long term (2040) vision on policy and regulatory requirements for European harmonization identified were as follows:

- Pan-European approach on overall mobility solutions for cities including electric autonomous shared mobility.
- Political framework for the rollout of electric autonomous shared mobility into rural areas (mobility for all).
- Clear common approach for cities to coordinate private and public transport.
- Role of traffic management.
- Safe coexistence of automated vehicles and non-motorized road users.





Issues identified included reducing obstacles to foster introduction of enabling regulations; development of a common EU perspective; updates and harmonization of traffic rules; addressing data sharing and privacy issues; and addressing liability, especially insurance issues. More specifically for connectivity, the CARTRE position paper dedicated to this topic recommended the development of "flexible regulatory approaches to allow industry and public bodies to generate the considerable investments needed to deploy V₂X connectivity in vehicles and infrastructure (road and telecoms) sustainably, in line with public policy priorities".

The ARCADE project (Aligning Research & Innovation for Connected and Automated Driving in Europe), successor of CARTRE which started in October 2018, is currently looking further into Policy and Regulations related to Connected and Automated Driving across Members States and in particular European harmonization. Information on the status in Member States, future regulatory needs as well as guidelines for projects are being gathered in the Knowledgebase [4], which the project is maintaining. ARCADE develops and updates a roadmap for Connected Automated Driving which has provided key input to the ERTRAC CAD roadmap 2019 [5], the STRIA CAT 2.0 [6] and is providing input to the Single Platform for Open Road Testing and Pre-deployment of CAM.

The ARCADE roadmap and ERTRAC CAD roadmap conclude that the focus for the coming 10-year period in the development paths will be on highly automated vehicles (SAE L4) in mixed traffic. A selection of use cases has been identified to illustrate this development in the roadmap. Key priorities have been identified by the thematic areas within ARCADE together with the ARCADE stakeholder network.

While the ARCADE roadmap is principally focusing on future research needs, some of the identified challenges and requirements for R&I are related to policy and regulatory aspects. The roadmap report reiterates the need to define flexible regulation for Automated Driving, enabling different solutions, within the boundaries of safety, to build a common framework for connected automated vehicles for Europe and to make cross-border testing easy. Regarding connectivity in general, the following key priorities that need to be supported by policy and regulatory measures, have been identified:

- Definition of connectivity requirements for AD functions (performance, Quality of Service, resilience, etc.).
- Standardisation and further deployment of V2X technologies.
- (Cyber) secure and safe communications respecting privacy and various levels of trust.
- Interoperability of communication technologies / hybrid connectivity solutions.
- Correctness and latency for multiband configuration. Common communication specifications and standardization will be required for multiband exchange for freight vehicles.
- Specification of Day 2 and Day 3 C-ITS services.

The Single Platform for Open Road Testing and Pre-deployment of CAM launched by the European Commission in 2019 comprises two Working Groups focusing on connectivity related topics:

• WG 5: Cybersecurity and access to in-vehicle data linked to CAM.





• WG 6: Connectivity and digital infrastructure for CAM.

Working Group 6 in particular has as main objectives to promote collaboration between the various actors of the CAM community regarding communication technology, to establish an interoperable connectivity framework, and to coordinate testing and pre-deployment activities. Activities include gathering and exchanging experiences, best practices and knowledge on how spectrum can be efficiently allocated to various technologies; and addressing technical and legal issues that are relevant to data storage and cloud access in the testing and pre-deployment phase. The group identified as priority the need to have an updated inventory and mapping of current, relevant, initiatives and standards. Inventory on Priority Road Transport Services [7] An important work item thus consists in categorizing the communication technologies/issues for services (day category, communication type, possible provision with cellular technology, availability of the service, critical for road safety, latency needs...).

The EU project HEADSTART has developed two complementary studies regarding user needs and technical and functional requirements for autonomous vehicle adoption, which provide useful insights for this study. HEADSTART Report D.1.2. "Stakeholders and user group needs", [8] provides a brief overview of the current standards and regulations concerning safety for testing CAD at the national and international level as well as relevant standards.

HEADSTART Report D1.3 "Technical and functional requirements for Key Enabling Technologies (KETs [8]) which include Connectivity, Cybersecurity and Positioning, looks at the policy framework regarding cybersecurity requirements. It highlights as key sources the US Department of Transportation voluntary guidance, best practices and design principles for cyber vehicle physical systems, the SAE J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" and the work ongoing as part of the UNECE World Forum for the harmonization of vehicle regulations (WP.29). The "Proposal for a Recommendation on Cyber Security [9] includes some cybersecurity requirements for over-the-air (OTA) update use cases. Included, as Annex A is a draft regulation on cyber security.

Research undertaken in the EU project CARTRE has analysed the needs in short and long term to enable the deployment of highly automated vehicles. The EU project ENSEMBLE (Enabling Safe Multi-Brand platooning for Europe) built upon the work of the CARTRE project to develop a report which provides an overview of the regulatory framework for truck platooning, including elements relevant for autonomous truck platoons (D6.10 ENSEMBLE regulatory framework – state of the art, 2019) [10]. The report presents a Regulatory Matrix to provide a classification of all regulations, directives and standards that might need a revision or modification to make the type-approval of platoons possible. This matrix has been shared with several OEMs to align ideas and concepts and to detect possible missing items or gaps.

2.4. Stakeholder engagement

Mitchell, Agle et al.[11] were among the first that attempted to formalize stakeholder analysis and provide the basis for stakeholder theory, which they describe as a "popular heuristic for describing the management





environment". They proposed a classification of stakeholders based on three characteristics, namely: (a) their power to influence, (b) the legitimacy of each stakeholder's relationship with the organization, and (c) the urgency of the stakeholder's claim on the organization. Other factors used to estimate salience include Power, Influence, Interest, Closeness, etc. 5G-MOBIX bases its stakeholder engagement on the well-known classification method.

Figure 4 presents a preliminary stakeholder analysis for 5G for CAM, which will be further elaborated during the Study to address specific stakeholders per CBC (Cross Border Corridors).



Figure 4: High-level overview of Stakeholder ecosystem.

The precise objective of the stakeholder engagement strategy will be:

- To introduce 5G-MOBIX WP6 results to the relevant parties as identified both by the project partners and the wider EC business and research communities, by using traditional dissemination channels and in collaboration with the communication manager since it will follow the project dissemination roadmap.
- To receive stakeholder feedback regarding the methodology of WP6, using data collection activities (such as a Survey, direct contact etc.) both external and internal to the project consortium.
- To validate key results of WP6 and discuss the results from the stakeholders' point of view, by holding at least one online workshop.

With respect to receiving stakeholder feedback and validating our results, the communication strategy compiled with the cooperation of WP7 will be focused on classification of stakeholders stating which stakeholders to monitor, manage closely, keep informed and choosing appropriate channels to do so (see Table 1). At a minimum, 5G-MOBIX intends to collect inputs through direct contact, the first 5G-MOBIX Survey launched in Q3 2020 and analysed in Q4 2020, as well as an online workshop during Q4 2020. If a stakeholder is under-represented in the results of WP6, more activities with more targeted scope will be scheduled within the project lifetime. Dissemination material (such as infographics, blog posts etc.) will also



be planned within 2021 to provide a brief overview of the issues and recommendations identified in T6.4, so they can be easily communicated while avoiding the use of jargon.

Table 1: Communication tools utilized to reach stakeholders for the purpose of this Study.

Activity	Communication tools	Target Audience	
Кеер	5G-MOBIX website, newsletter, social media, blog posts,	All	
Informed	Infographics etc.		
Manage	Invitation to 5G-MOBIX online workshop	Stakeholders that are under-	
Closely	Invitation to participate to 5G-MOBIX survey (questionnaire)	represented in the 5G-MOBIX	
	Direct contact more activities with smaller participation but CBCs (Cross border Corric		
	more targeted can be envisioned (e.g., under personal		
	invitations etc.)		
Monitor	Direct contact	Stakeholders that are well-	
	Input requests with key CBC (Cross border Corridors)	represented in the 5G-MOBIX	
	participants	CBCs	
	Invitation to participate to 5G-MOBIX survey (questionnaire)		
	Invitation to 5G-MOBIX online workshop		





3. REGULATION AND CERTIFICATION

3.1. Cross-border issues identified in D2.1

During the development and detailing of the 5G-MOBIX use cases, an initial set of cross-border issues related to several types of regulation has been identified. The table below reproduces the relevant issues from the wider overview that also includes non-regulatory issues in D2.1 [12]. The analysis in this section goes beyond these identified issues and takes a look at existing regulations and public policies that can affect 5G/CAM, following in subsection 3.2.

ID	Issue name	Short description
SDPo	Personal data processing under different data protection regulations	Different data protection regulations apply when processing personal data of data subject in Europe, Turkey, China and Korea. Therefore, many legal, organisational and technical challenges need to be overcome for lawful processing of this data. This is the general case of SP1 and SP2.
SDP1	Legal	Without a proper legal basis, lawful processing of personal data could not be achieved. Indeed, legal issues arise at the enforcement of the GDPR to CAM. For example, CAM and DENM messages (and other CAM messages) are considered personal data but are required for the normal functioning of the CAM systems.
RC1	Autonomous Vehicle regulation Compliance	GDPR and homologated systems for ADAS are properly implemented and applied, also to support difficulties of identifying AVs from Non-AVs on roads
RC2	Road & traffic regulation Compliance	Traffic signs and rules have a different regulation requiring different computer vision training or application of different operative limits to vehicles' dynamics
RC3	Sensor Compliance	Heterogeneous homologation of sensors
RG1	Geo-dependent spectrum	Neighbouring countries can have different radio frequency spectrum
RL1	Law enforcement interaction	Absence of procedures for law enforcement interaction with AVs
RN1	Neutrality regulation	Incompatibility of Network Neutrality directives with applied traffic prioritization techniques

Table 2: Issues relevant for regulation from D2.1.





3.2. Overview of existing regulatory frameworks

This section provides a brief overview of the existing legal framework in the EU and how it applies to 5G for CAM. Some aspects we look into include:

- The applicability of the GDPR and the need for data portability.
- The possible effect of the upcoming ePrivacy regulation.
- The need for safeguards against profiling and discrimination.
- The need to clarify the legal framework surrounding M2M Roaming.
- The possibility of exhaustion of numbering resources.
- Ensuring net neutrality within the context of slicing in 5G networks.
- Ensuring car safety for autonomous vehicles.
- Safety and cybersecurity of critical infrastructures.

3.2.1. General Data Protection Regulation

General Data Protection Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)[13]. Some important considerations need to be made for the case of 5G CAM:

The data for each vehicle or driver that are being processed by CAM services may include personal data in the form of IP addresses, credentials and other communication metadata such as position, which could also fall under the new ePrivacy Regulation. 5G-MOBIX services may collect personal data, however, they do not profile a natural person's behaviour. 5G-MOBIX does not inspect the contents of communications to assess personal aspects of a natural person's behaviour (e.g., driving patterns, health etc.).

Processing for the explicit purpose of providing CAM features (as defined in the Commission Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility applications, also see section 3.2.2) can be considered lawful. Article 7 of the GDPR also states that when consent is given in the context of a written declaration that also concerns other matters (e.g., a contract) it must be presented in a form that is easily distinguishable and comprehensible, otherwise the declaration will not be considered binding. This means that the consent of the buyer of 5G for CAM services must be clear and informed.

GDPR dedicates Articles 12-23 to the description of the Rights of the Data Subject and how they shall be exercised, including the right for access, erasure, restriction, rectification, portability and the right to be forgotten. It further specifies, that if the stored information is not identifiable, then the data subject is responsible to provide additional information to identify their data. Portability is another important aspect since it is aligned with the EU's competition law. If a person's data are not portable among different CAM providers, then customer lock-in conditions are created as the customer might not able to freely change providers. The data subject rights however, do not apply if a component does not retain any data [14].





Articles 24-43 relate to the responsibilities of the data controller, the data processor, and establishes the role of the Data Protection Officer. This information should be transparent to the user as well. The data subject should be able to contact the DPO (Data Protection Officer) or the Data Processor regarding their data. Article 26 describes the case for Joint Controllers. This case could be applicable to 5G/CAM if the telco provider is operating third party services for CAM, e.g., if a telco provider is deploying an ITS service on behalf of a road operator that collect driver information under the consent of the driver, joint Controllers from the road operator and telco side are needed. The text also includes rules on data sharing (Articles 44-50). If data are shared with third parties (or monetized) the data subject should consent. Sharing data with Law Enforcement or CERTs (Computer emergency response team) should be enabled for alignment with other Directives as well. Other issues covered in the GDPR include the role of independent supervisory authorities (Articles 51-59), Liabilities and penalties (Articles 77-84) etc.

An important aspect that applies to 5G-MOBIX is the exchange of data with third countries. GDPR dedicates Art.44-50 to cross-border sharing of information. Any country within the EEA applies the GDPR. For countries outside the EEA, the first important step is to assess whether there is a standing Adequacy Decision. The European Commission has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679 whether a country outside the EU offers an adequate level of data protection. At the proposal of the European Commission, the European Data Protection Board provides an opinion on the status of personal data protection in a specific country. If representatives of EU countries provide their approval, the EC adopts the Adequacy Decision.

The effect of such a decision is that personal data can flow from the EEA to that third country without any further safeguard being necessary. Transfers to the country in question will be assimilated to intra-EU transmissions of data. At any time, the European Parliament and the Council may request the European Commission to maintain, amend or withdraw the adequacy decision. These adequacy decisions do not cover data exchanges in the law enforcement sector, which are governed by the "Police Directive" (article 36 of Directive (EU) 2016/680). In the case of the GR-TR trial, which features a hard border, there is no adequacy decision yet regarding data exchange with Turkey. Chapter 5 of the GDPR states other cases where exchange of information might be considered legitimate such as binding corporate rules and derogations. Unless a data exchange can fall under any of the cases explained in Chapter 5 of the GDPR, it will not be legitimate.

3.2.2. Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

The European Data Protection Board, adopted in January 2020, a set of "Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications"[15]. The document makes the following definitions and recommendations regarding the applicable laws.

According to the "Commission Directive 2008/63/ECof 20 June 2008 on competition in the markets in telecommunications terminal equipment (Text with EEA relevance)"[16] the definition of "terminal





equipment is given as follows: "equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network; (b) satellite earth station equipment". The recommendations of the EDPB consider that **the connected vehicle can be considered as "terminal equipment"** under that definition and as such, related provisions of the ePrivacy Directive need apply.

Personal data can be collected through several means, including vehicle sensors, telematics boxes or mobile applications (e.g., accessed from a device belonging to a driver). In order to fall within the scope of the document the EDPB considers that applications need to be related to the environment of driving, such as:

- **Mobility management:** functions that allow drivers to reach a destination quickly, and in a costefficient manner, (e.g., GPS navigation, traffic information etc.).
- Vehicle management: functions that are supposed to aid drivers in reducing operating costs and improving ease of use (e.g., such as notification of vehicle condition and service reminders).
- **Road safety:** functions that warn the driver of external hazards and internal responses, (e.g., collision protection, hazard warnings, emergency calls etc).
- Entertainment: functions providing information to and involving the entertainment of the driver and passengers, (e.g., hands-free phone calls, voice generated text messages, music, video, etc).
- **Driver assistance**: functions involving partially or fully automated driving, (e.g., operational assistance or autopilot etc.).
- **Well-being:** functions monitoring the driver's comfort, ability and fitness to drive (e.g., fatigue detection or medical assistance).

Examples of applications that don't fall within the scope of the document are:

- Applications that suggest places of interest (restaurants, historic monument, etc.) to the user.
- Applications provided by an employer to monitor a company owned vehicle fleet.
- Applications for video capture (e.g., dash cams).
- Applications for C-ITS, as the data collection needs to be extensive and there are still on-going discussions[17].

The Guidelines list the main risks to privacy and security with respect to:

- **Control and asymmetry of data protection:** there is the risk that adequate controls are not available to the driver, and that the driver might not always be the vehicle owner and have the same amount of access. Communications could also be triggered automatically or by default, without the user always being aware of the exact data exchanges that take place.
- **Quality of user consent:** classic mechanisms used to obtain individuals' consent may be difficult to apply resulting in a "low-quality" consent based on a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals. Consent might





also be difficult to obtain for drivers and passengers who are not related to the vehicle's owner in the case of second-hand, leased, rented or borrowed vehicles.

- Additional Processing & Extensive Data Collection: when data are collected on the basis of consent, no additional processing for further purposes is legitimate as consent needs to be specific and informed to be valid. Furthermore, there are risks introduced by extensive data collection that could be required in some cases, e.g., Artificial Intelligence etc.
- Security of personal data: given the multitude of vastly different components and technologies, as well as the dynamic nature of service-oriented infrastructures in the CAM ecosystem, there is a large attack surface and a lot of opportunities for an attacker to gain unauthorised access or otherwise compromise CAM security.

However, the guidelines also suggest a few best practices per type of data (e.g., biometric, geolocation etc.) and summarise some general best practices as follows (Guideline #74):

- Users should be able to control how their data are collected and processed in the vehicle,
- Information regarding the processing must be provided in the driver's language (manual, settings, etc.),
- The EDPB recommends that only data strictly necessary for the vehicle functioning are processed by default, and data subjects should have the possibility to activate or deactivate the data processing for each other purpose and controller/processor and have the possibility to delete the data concerned
- Data should not be transmitted to any third parties (i.e., the user has sole access to the data),
- Data should be retained only for as long as is necessary for the provision of the service or otherwise required by Union or member state law,
- Data subjects should be able to delete permanently any personal data before the vehicles are put up for sale
- Data subjects should, where feasible, have direct access to the data generated by these applications.

3.2.3. ePrivacy

The ePrivacy Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, also known as the EU Cookie Law, sets the rules for the collection of cookies and ensures the confidentiality of electronic communications [12]. At the moment, there is a proposal [18] for a revision of the ePrivacy Directive, to better align it with the GDPR, take into account continuing technical innovation, and transform it into a Regulation. This would mean that the EU Member States would implement the Regulation as-is, as opposed to a Directive, which can be implemented in any way, considered suitable by the Member States. The proposal for the Regulation was released in January 2017. Regarding the applicability of the ePrivacy Directive and the future ePrivacy regulation, 5G-MOBIX makes the following considerations:





Profiling of a user's behaviour through cookies is not considered in any 5G-MOBIX User Stories. Otherwise, consent and additional safeguards to ensure the data subject's rights and non-discrimination should be in place.

Protection of communication contents under the new regulation will apply to telco traffic (e.g., SMS), as well as other digital communications providers (e.g., Skype, WhatsApp etc.). The new regulation might apply to CAM services.

A new component is the protection not only of communications content but also of communication metadata, including location. Pending finalisation of the ePrivacy Regulation, additional protections can be considered.

3.2.4. Non-discrimination

Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation.[19]

European Charter of Fundamental Human Rights [20], esp. Article 8(1) on the protection of personal data Treaty of Amsterdam[21] (1997/1999 establishing the protected grounds against discrimination) & Treaty of Lisbon[22] (2007/2009 making the ECHR Bill of Rights legally binding)

Council of Europe recommendations on profiling: Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling[23].

Although the non-discrimination body of law in the EU regards to access to employment, education etc. that are out of the scope of 5G-MOBIX, we can consider some basic principles and definitions to be freestanding. Access to the Internet can be regarded as a basic service that should be available to all citizens and any discriminatory practices should be abolished. Some key definitions should be in place, for future reference:

- The entry into force of the Treaty of Amsterdam in 1997 enabled the European Commission to legislate on non-discrimination based on defined protected grounds, which include gender, age, race, ethnicity, religion, belief, age, disability and sexual orientation. The GDPR considers data that may expose these aspects of the data subject as "special category" data.
- Protection against discrimination is not only present in EU Law but also within the European Charter of Human Rights (ECHR) that was proclaimed by the European Union and the Member States in 2000. The ECHR declared the fundamental human rights to be protected and became legally binding after the 2009 Treaty of Lisbon.
- Most definitions in EU law and ECHR regard cases of direct discrimination. The EU Agency of Fundamental Rights (FRA), however, further defines indirect discrimination, when a rule that appears to be neutral affects a specific group of citizens in a significantly more negative way, by comparison to others





in a similar situation. It also defines harassment and instruction to discriminate as violating the dignity of a person.

Hence, any data processing CAM component that profiles aspects of the data subject concerning these protected grounds should have safeguards in place to ensure that processing is lawful and that such information cannot be misused and lead to discriminatory practices. The Council of Europe has published a recommendation on safeguards for processing that leads to profiling, although this predates the GDPR and there was no legal definition of profiling at the time.

3.2.5. Car Safety

The lack of 5G-CAM regulations represents a challenge for automotive OEMs. As an OEM, you need to know your limits, how to design a CAM feature etc. Especially for those features that trust connectivity like 5G, it is important to have a common sense of development on the market, for all vehicles to be able to "speak the same language" on the road. This "speaking" must be safe. OEMs need to ensure that vehicles are safe, before delivering them to their customers, and this is an essential aspect. For this purpose, Cybersecurity step in to prevent unauthorized access to vehicle controllers and communication units. The United Nations Economic Commission for Europe (UNECE) works for related regulations. These regulations are listed below and at the time of this article deliverable, they have not been published yet:

- UN ECE Regulation No. 155 ECE/TRANS/WP.29/2020/79 as amended by 2020/94 and 2020/97.
- UN ECE Regulation No. 156 ECE/TRANS/WP.29/2020/80.

For conventional vehicle safety, "ISO 26262-1:2018 Road vehicles — Functional safety" standard has been published. This document is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles, excluding mopeds. This document does not address unique E/E systems in special vehicles such as E/E systems designed for drivers with disabilities [24].

For autonomous vehicle safety, "ISO/PAS 21448:2019 Road vehicles — Safety of the intended functionality" standard has been published. This document is intended to be applied to intended functionality where proper situational awareness is critical to safety, and where that situational awareness is derived from complex sensors and processing algorithms; especially emergency intervention systems (e.g., emergency braking systems) and Advanced Driver Assistance Systems (ADAS) with levels 1 and 2 on the OICA/SAE standard J3016 automation scales. This edition of the document can be considered for higher levels of automation; however, additional measures might be necessary. This document is not intended for functions of existing systems for which well-established and well-trusted design, verification and validation (V&V) measures exist at the time of publication (e.g., Dynamic Stability Control (DSC) systems, airbag, etc.).

A Delegated Act "ITS Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport" has been published on 9th January 2018 and various related associations such as 5GAA, ETNO, GSMA, GSA stated their concerns about Delegated Act that is not being technology-neutral by ruling out C-V2X technology. On 8th





July 2019, the Council of the European Union adopted a decision to object to the proposal for Delegated Regulation on Cooperative Intelligent Transport Systems and currently this study is ongoing.

To see highly automated and connected vehicles on the public road standards and regulations must be finalized. So far, there has not been any published standard or regulation that covers highly automated and connected vehicle safety.

3.2.6. European Electronic Communications Code

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) Text with EEA relevance.

The European Electronic Communications Code is an EU Directive that regulates electronic communications networks and services. It was adopted in December 2018 to reform the existing regulatory framework and is to be adapted by the Member States by 2020. For the mobile operators that provide the 5G networks for CAM, the European Electronic Communications Code (ECCC) is a central piece of regulation. The EECC contains, among many other things, stipulations on service and network interoperability and the role of specifications and standards, planning and coordination of radio spectrum policy, and the handling of personal data. BEREC, national ministries and NRAs base their policies and oversight of network operators on this key legislation.

In this section, the focus is on the legislation of numbering resources in the EECC, which is an important topic for CAM services as the large number of devices involved will require substantial numbering resources for network routing and identification. Taking into account the need of IoT/M2M service providers and with the view to create competitive market entry conditions (aligned with the EU Digital Single Market), the EU has legislated the use of numbering resources. The EECC aims to:

- Allow the possibility to assign numbers to undertakings other than providers of electronic communications networks or services;
- Enable an extraterritorial use of non-geographic numbers within the EU for the provision of noninterpersonal communications services;
- Promote, where technically feasible, the over-the-air (OTA) provisioning of numbers for easier switching;
- Ensure the efficient use of numbering resources.

As the demand for CAM services and M2M/IoT communications, in general, appears to be increasing, there is a worldwide concern that it might consequently cause a scarcity of numbering resources. The International Telecommunication Union (ITU) standardizes such resources (such as telephone numbers, operator identifiers, SIM identifiers and more). The European Electronic Communications Code permits Members States to grant rights of use for numbering resources on a non-discriminatory basis to undertakings other than providers of Electronic Communications Networks or Services (ECN/ECS entities) under Article 93(2) if adequate numbering resources are available to satisfy current and foreseeable future demand. This possibility of assignment is also to support the development of cross-border services in the case of non-interpersonal communications services (Recitals 246 and Article 93(4)). Non-ECN/ECS entities





shall demonstrate their ability to manage the numbering resources and to comply with any relevant requirements set out under Article 94. These conditions are, in fact, pre-conditions that non-ECN/ECS entities have to meet to be eligible to receive the right to use numbering resources. This will allow non-ECN/ECS entities (e.g., truck fleets or connected cars services, i.e. with potentially a huge customer base). However, this is not obligatory, as member states are still free to decide whether to allow or restrict the assignment of numbering resources to non-ECN/ECS entities nationally.

According to a recent BEREC survey in 2019, NRAs from 12 Member States were already assigning or planning to assign numbering resources to stakeholders other than providers of electronic communications services, in specific categories of (mostly E.164) resources such as:

- Special rate services (Freephone, Shared cost numbers, Premium rate numbers);
- Short codes (directory enquiry services, European 116 numbers, public interest numbers);
- Specific services (private network, maritime or aeronautical services, direct dialling or collect call services);
- Personal numbers;
- Technical resources (Mobile network codes (E. 212) such as private networks with dedicated frequencies or providers of fixed wireless internet access services -, Signalling point codes).

These assignments are done as a rule-based on a single number or a block of few numbers and refer mostly to E.164 numbering resources. Non-ECN/ECS entities use the directly assigned resources for their purposes and a sub-assignment to third parties is explicitly forbidden by the conditions attached to the rights of use. The ECN/ECS providers do the implementation and activation of numbering resources in the network. The characteristic that the assignment is done based on a single number or a block of few numbers implies that there is no need to assess the risk of exhaustion of numbering resources.

3.2.7. Roaming

Regulation (EU) No 531/2012 of the European Parliament and of the Council of 13 June 2012 on roaming on public mobile communications networks within the Union

Amended by:

Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Text with EEA relevance)

• Regulation (EU) 2016/2286 of 15 December 2016 laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges and on the application to be submitted by a roaming provider for that assessment





- Regulation (EU) 2017/920 of the European Parliament and the Council of 17 May 2017 amending Regulation (EU) No 531/2012 as regards rules for wholesale roaming markets Text with EEA relevance.
- Regulation (EU) 2019/2116 of 28 November 2019 setting the weighted average of maximum mobile termination rates across the Union and repealing Implementing Regulation (EU) 2018/1979 (Text with EEA relevance)

The regulation of roaming prices and fair use policies is the subject of several regulations in force. The EU has been taking steps since 2006 to reduce roaming charges, culminating with "Roam Like At Home" rules entering into force in 2017, thus ending subscribers' roaming charges. This work starts with the Roaming Regulation (531/2012), also known as the Eurotariff law, which regulates the imposition of roaming charges in the European Economic Area (EU Member States, Iceland, Liechtenstein, and Norway). It regulates the charges that can be imposed on subscribers by the telco operators, as well as the wholesale rates operators can charge each other to allow their subscribers to access another provider's network while roaming. It also provides a "fair use policy" under which the use of roaming without extra charges is limited to business and leisure, to prevent misuse and add costs to operators. Although the mechanisms to enforce fair use are not entirely clear, the EU has stated that it should be based on the "a principle of residence or stable links EU consumers may have with any EU Member State", where a stable link can be defined as "work commuters, expats who are frequently present in their home country or Erasmus students".

As a consequence of the current legislation, mobile operators still have to pay for wholesale charges while subscriber roaming fees are abolished; this has led to a rise in subscription prices across many operators in many member states. Furthermore, while the Roaming Regulation disallows operators charging extra for roaming, it does not force them to make roaming available in the first place (i.e. Telcos are allowed to have national-only subscription plans without roaming). Since the Roaming Regulation is set to expire in 2022, the EU is launching[24] to assess its impact with the view to prolong the Roaming Regulation.

Thus, in the case of 5G CAM roaming many questions are formed:

- How will 5G CAM roaming fees be taxed and regulated?
- Does CAM or M₂M roaming in general, necessitate new regulation or should the current regulation be amended?
- What would constitute "fair use" for 5G CAM roaming?
- How can consumers be protected and enjoy absolute transparency in terms of roaming charges?
- How can we ensure international cooperation and a fair roaming policy across hard EU borders?

3.2.8. Open Internet

Open Internet Regulation: Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within




the Union (Text with EEA relevance) [24].

The Open Internet Regulation establishes the circumstances where traffic classification and management are legitimate. It lays down specific net neutrality rules and governs the way ISPs may choose to manage the traffic that passes through their networks while ensuring equal and non-discriminatory treatment of traffic. Specifically, the following aspects are particularly relevant to 5G-MOBIX:

- When providing internet access services, providers of those services should treat all traffic equally, without discrimination, restriction or interference, independently of its sender or receiver, content, application or service, or terminal equipment. According to general principles of Union law and settled case law, comparable situations should not be treated differently, and different situations should not be treated in the same way unless such treatment is objectively justified.
- Reasonable internet traffic management (this refers to the traffic management of network packets, not to be confused with road traffic management) does not require techniques that monitor the specific content of data traffic transmitted via the internet access service.
- Traffic management measures that go beyond such reasonable traffic management measures may only be applied as necessary and for as long as necessary to comply with the three justified exceptions laid down in this Regulation.
 - 1. First, situations may arise in which providers of internet access services are subject to Union legislative acts, or national legislation that complies with Union law (for example, related to the lawfulness of content, applications or services, or public safety), including criminal law, requiring, for example, blocking of specific content, applications or services.
 - 2. Second, traffic management measures going beyond such reasonable traffic management measures might be necessary to protect the integrity and security of the network, for example by preventing cyber-attacks that occur through the spread of malicious software or identity theft of end-users that occurs as a result of spyware.
 - 3. Third, measures going beyond such reasonable traffic management measures might also be necessary to prevent impending network congestion, that is, situations where congestion is about to materialise and to mitigate the effects of network congestion, where such congestion occurs only temporarily or in exceptional circumstances.

Article 3 further states that traffic management must be reasonable, transparent, non-discriminatory and proportionate. Article 4 details how providers of internet access services shall be transparent in their contracts about traffic management; hence, traffic management through 5G-MOBIX for cybersecurity purposes should be included. Article 5 also mentions that national authorities should be able to monitor compliance with this Directive and record their findings.

A key technical advancement of 5G is the existence of slicing. This allows dedicated "slices" of resources to be shared to different verticals or users the use of slicing technology in a mobile operator network can bring in the rules for Internet Access Service, for Specialised Services or both, depending on the services and applications that are supported. It is not possible to come to an overall assessment with a single outcome on the alignment of slicing with net neutrality rules. This is because the topics that are encountered in the





assessment and the outcome depend not only on the 5G technology but also on the specific combination of services, applications and network architecture. A consequence is that mobile operators and CAM application providers and national regulatory authorities will need to do further analysis to evaluate whether a particular type of (tailored) connectivity complies with the net neutrality rules. Another point that needs to be clarified how the National Regulating Authorities will be able to monitor operators for breaches of the Open Internet Regulation in the case of slicing and CAM.

In the follow-up work after this deliverable, we will explore the relation between 5G in CAM and net neutrality in more detail, including the analysis of the network slicing. From the 5G-MOBIX architecture designs, we will have a good technical view of how the CAM services will be built on 5G slicing and edge computing. We will use that technical view, and the network level requirements, to make a detailed analysis of how these CAM services map to the net neutrality rules for Internet Access Services and Specialised Services. This analysis will be based on an earlier study on 5G and net neutrality[25], see Figure 5.



- 1. Multiple IASs with different traffic management settings in one network
- 2. QoS differentiation within IAS
- 3. Local access to the internet
- 4. Public and private services and associated networks
- 5. Objective need for optimisation in SpS
- 6. Impact of SpS on IASs
- 7. SpS and connections to the internet
- 8. Connectivity to limited number of internet end points
- 9. Access control

Figure 5: Services and applications need to comply with the rules for Internet Access Services (IAS) and the rules for Specialized Services (SpS).

3.2.9. Critical Infrastructures & Law Enforcement

Data protection in criminal investigations: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.





Network Information Security (NIS) Directive: 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.

Although these directives do not apply directly to 5G-MOBIX, they are relevant as service providers may be required to cooperate with law enforcement in a criminal investigation or with appropriate cybersecurity agencies in case of a cyberattack. A CAM service may expose APIs for the exchange of information with relevant third parties under these directives, although the exact use of such APIs would be defined by the provider and their internal policies regarding the statutory process (unless access is court-mandated).

Specifically, the NIS Directive aims to develop the principles for European cyber-crisis cooperation. Since it is a Directive, the Member States can select the specific of its implementation, leading to concerns on fragmentation and disparities among the Member States. NIS states that a certain level of cooperation and cyber security readiness is expected from operators of critical services, defined as (Article 4):

- (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.

This applies to critical infrastructures (including banking, health, transport etc.), providers of telecommunication basic services (DNS providers etc.), digital service providers (e.g., marketplaces), cloud infrastructure providers etc. As the effects of a cyberattack against critical $_5$ G/CAM infrastructure could be extremely destructive, cyber-crisis cooperation is a critical capability that needs to be fostered among the $_5$ G/CAM actors.

3.2.10. UN Regulations on Cybersecurity and Software Updates

UN Regulation on Cybersecurity and Cyber Security Management Systems UN Regulation on Software Updates and Software Updates Management Systems

The UN Regulation on Cybersecurity and Cybersecurity Management Systems[26] provides a framework for the automotive sector to put in place the necessary processes to:

- Identify and manage cyber security risks in vehicle design;
- Verify that the risks are managed, including testing;
- Ensure that risk assessments are kept current;
- Monitor cyber-attacks and effectively respond to them;
- Support analysis of successful or attempted attacks;
- Assess if cyber security measures remain effective in light of new threats and vulnerabilities;





• All of these will be audited by national technical services or homologation authorities.

The UN Regulation on Software Updates and Software Update Management Systems provides a framework for the automotive sector to put in place the necessary processes for:

- Recording the hardware and software versions relevant to a vehicle type;
- Identifying software relevant for type-approval;
- Verifying that the software on a component is what it should be;
- Identifying interdependencies, especially with regards to software updates;
- Identifying vehicle targets and verifying their compatibility with an update;
- Assessing if a software update affects the type approval or legally defined parameters (including adding or removing a function);
- Assessing if an update affects safety or safe driving;
- Informing vehicle owners of updates;
- Documenting all the above.

All of these will be audited by national technical services or homologation authorities.

These Regulations were adopted on June 2020 by UNECE's World Forum for Harmonization of Vehicle Regulations, require that measures be implemented across 4 distinct disciplines:

- Managing vehicle cyber risks;
- Securing vehicles by design to mitigate risks along the value chain;
- Detecting and responding to security incidents across vehicle fleet;
- Providing safe and secure software updates and ensuring vehicle safety is not compromised, introducing a legal basis for so-called "Over-the-Air" (O.T.A.) updates to onboard vehicle software.

According to UNECE's press release, the regulations will apply to passenger cars, vans, trucks and buses. They will enter into force in January 2021. Japan has indicated that it plans to apply these regulations upon entry into force. The Republic of Korea has adopted a stepwise approach, introducing the provisions of the regulation on Cybersecurity in a national guideline in the second half of 2020, and proceeding with the implementation of the regulation in a second step. In the European Union, the new regulation on cyber security will be mandatory for all new vehicle types from July 2022 and will become mandatory for all new vehicles produced from July 2024. Together, the EU, the Republic of Korea and Japan accounted for some 32 million vehicles produced in 2018, representing just over one-third of global production.





3.2.11. Radio equipment

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 (Text with EEA relevance)

Directive 2014/30/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 electromagnetic compatibility (recast) Text with EEA relevance

Directive 2014/53/EU focuses on the harmonisation of laws across the EU relating to Radio Equipment (RE). It is complemented by the EECC and applies to radio equipment available in the market, excluding RE exclusively used for public security, defence and State Security. It requires that RE will be constructed to ensure the protection of health and safety of persons and domestic animals, including the protection of property and that an adequate level of electromagnetic compatibility (as set out in Directive 2014/30/EU). It states that RE within certain categories or classes must comply with the following essential requirements:

- a) Radio equipment interworks with accessories, in particular with common chargers;
- b) Radio equipment interworks via networks with other radio equipment;
- c) Radio equipment can be connected to interfaces of the appropriate type throughout the Union;
- d) Radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;
- e) Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and the subscriber are protected;
- f) Radio equipment supports certain features ensuring protection from fraud;
- g) Radio equipment supports certain features ensuring access to emergency services;
- h) Radio equipment supports certain features to facilitate its use by users with a disability;
- i) Radio equipment supports certain features to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated.

According to the Directive: "The Commission shall be empowered to adopt delegated acts in accordance with Article 44 specifying which categories or classes of radio equipment are concerned by each of the requirements set out in points (a) to (i)."

Furthermore, it states that MS shall not impede the free movement of radio equipment and sets out various obligations for the manufacturers such as drawing up technical documentation, assessing conformity and compliance (e.g., affixing the CE marking), ensuring that it can be operated in at least one Member State without infringing applicable requirements for the use of spectrum and many more.

In the context of 5G-MOBIX this directive should also apply not only to 5G equipment but to radio-enabled On-Board Units utilised in automated vehicles as well as to road-side units (OBUs/RSUs). Importers and





distributors are also under the obligation to place only compliant radio equipment on the market and ensure that the conformity assessment has been carried out (more information on this procedure is provided in Section 3.3.2). Thus, the Directive imposes obligations to all members of the related supply chain.

3.2.12. Certification

This section describes the certification requirements applicable to radio equipment that enables ITS functionality inside the vehicle (i.e. On-Board Units -OBUs) or as part of road infrastructure (i.e. Road Side Units – RSUs).

In the context of 5G-MOBIX, radio equipment will usually be equipped with cellular technology (LTE or 5G) and/or DSRC technology (ITS-G5). Other radio technologies that may be used in vehicles/road infrastructure, and so, subject to be certified are Wireless LAN (WLAN – including Wi-Fi-, Bluetooth, NFC, wireless charging, etc.).

There are two major certification schemas applicable to products in general and radio equipment in particular, regulatory certification schemas and private certification schemas. Regulatory certification schemes are mandatory and are defined and controlled by local authorities (i.e. governments). Private certification schemes are normally set by the industry or by specific telecom operators, or automotive players.

In general, any radio equipment needs to fulfil certain regulatory requirements before it can be placed on the market. These requirements intend to ensure that the equipment fills essential requirements in terms of health, safety, electromagnetic compatibility, and use of the radio spectrum.

Each government sets its own requirements, and they may be different in different countries or areas. The European regulatory framework (CE marking) and the U.S regulatory framework (FCC) have become reference regulatory frameworks in the world and most radio equipment fulfils these requirements before going to market.

Private certification schemes focus on requirements not covered by regulatory requirements. These certifications are carried out after regulatory certification is complete (as failing regulatory certification may imply design changes in the product). The fulfilment of private requirements usually gives the right to use a logo that shows compliance to those requirements.

Commonly, cellular devices undergo industry private certifications GCF and/or PTCRB CERTIFICATION, as these schemes are usually an entry requirement for the majority of network operators. Additionally, network operators have their own homologation programs where additional tests are performed, mainly testing the behaviour of the telecom devices with the network operator network equipment and configurations.





Figure 6 shows an example of well-known regulatory and private certification schemes around the world. In the case of ITS radio equipment, the applicable private certification schemes are industry certification, network operator's homologation and vehicle manufacturer's homologation.



Figure 6: Certification schemes for V2X radio equipment.

3.3. Overview of existing certifications

An important aspect to address at this point is the difference between compliance and certification. Certification requires the existence of a trusted third party (e.g., an accredited organization) that audits a 5G or CAM system and, upon a successful inspection, grants a certification mark. This section describes the most relevant existing certifications of regulatory compliance.

3.4. Regulatory certification

3.4.1. Certification according to CE marking

Telecommunication products must be CE marked before they can be sold in the European Economic Area (EEA) market. CE marking requirements are covered by a number of directives. CE marking shows that a product had been assessed and meets EU safety, health and environmental protection requirements.





The product's manufacturer takes sole responsibility for declaring the product conformity with all CE marking requirements. The manufacturer must elaborate a technical dossier proving that the product fulfils all the EU-wide requirements.

The CE marking requirements are defined in directives that cover different products or product sectors.

The Radio Equipment Directive (RED), directive 2014/53/EU, establishes the regulatory framework for radio equipment to be made available in the market and put into service in the Union. RED Directive applies to equipment that uses the radio frequency spectrum, (i.e., which intentionally transmits or receives radio waves for communications or radio-determination and operating below 3 GHz - no lowest frequency limit is defined -).

The RED directive principles for product compliance are:

- Compliance with essential requirements.
- Procedures for Conformity assessment.
- Presumption of conformity with essential requirements provided by Harmonised Standards.
- Participation of a Notified Body if there are no radio Harmonised Standard.

A harmonised standard is a standard created upon a request from the European Commission to a recognised European Standards Organisation: CEN, CENELEC (European Committee for Electrotechnical Standardization), or ETSI to demonstrate that products, services, or processes comply with relevant EU legislation. The table below list the conformance requirements established for radio equipment by the RED directive that needs to be fulfilled by any telecom equipment to be used as part of ITS systems and the related harmonized standards that may be used as a test method to show compliance. The technologies covered are cellular (5G, 4G, 3G, 3G and 2G), Bluetooth, Wireless LAN (WLAN) -including Wi-Fi-, NFC and Wireless Charging.

Requirement	Technology	Harmonized standard	Description
Electrical Safety (RED, Article 3.1a)	All	EN 62368-1:2014 / EN 60950-1:2006 + A11:2009 + A12:2011 + A1:2010 + AC:2011 + A2:2013	Information technology equipment - Safety - Part 1: General requirements.
Health (RED, Article 3.1a)	All	EN 50360:2001 + AC:2006 + A1:2012	Product standard to demonstrate the compliance of mobile phones with the basic restrictions related to human exposure to electromagnetic fields (300 MHz - 3 GHz).
		EN 62311:2008	Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (o Hz - 300 GHz).

Table 3: RED requirements and harmonized standards for ITS radio equipment.





	Bluetooth, NFC, Wireless charging	EN 62479 2010 (if power less than 20 mW)	Assessment of the compliance of low-power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz).
5146			
EMC (RED, Article 3.1b)	All	EN 301 489-1 V2.1.1	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements.
	Cellular	EN 301 489-52 v12.1.1	Part 52: Specific conditions for Cellular Communication Mobile and portable (UE) radio and ancillary equipment.
	NFC, Wireless charging	EN 301 489-3 v2.1.1	Specific conditions for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 246 GHz.
	Bluetooth, WLAN	EN 301 489-17 v3.1.1	Part 17: Specific conditions for Broadband Data Transmission Systems.
Radio Spectrum	2G	EN 301 511 v12.5.1	Global System for Mobile communications (GSM); Harmonized EN for mobile stations in the GSM 900 and GSM 1800 bands.
(RED, Article 3.2)	3G & LTE	EN 301 908-1 V11.1.1 EN 301 908-2 V11.1.1 EN 301 908-11 V11.1.2 EN 301 908-13 V11.1.2 EN 301 908-14 V13.1.1 EN 301 908-15 V11.1.2	IMT cellular networks; EN 301 908-11 (Repeaters supporting 3G/LTE) EN 301 908-14 (Base Stations supporting LTE only) EN 301 908-15 (Repeaters supporting LTE only) EN 301 908-18 (Base Stations supporting LTE and (2G/3G)).
	DSRC, PC5	EN 302 571 v2.1.1	Intelligent Transport Systems (ITS); Radio communications equipment operating in the 5 855 MHz to 5 925 MHz frequency band;
	Bluetooth, WLAN 2.4GHz	ETSI EN 300 328 V2.2.2	Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz Industrial, scientific, and Medical band and using wide band modulation techniques.
	WLAN 5GHz	ETSI EN 301 893 v1.7.1	Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN.
	NFC	ETSI EN 300 330 v2.1.1	Short Range Devices (SRD); Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz
	Wireless charging	ETSI EN 303 417 V1.1.1	Wireless power transmission systems, using technologies other than radio frequency beam, in the 19 - 21 kHz, 59 - 61 kHz, 79 - 90 kHz, 100 - 300 kHz, 6 765 - 6 795 kHz ranges.





3.4.2. FCC – Federal communication commission

The Code of Federal Regulations, Telecommunications (title 47 of the United States Code of Federal Regulations) holds the U.S. federal regulations for telecommunications.

The Government Printing Office (GPO) publishes and maintains the official rules in the Federal Register.

The FCC regulates radio frequency (RF) devices in electronic -electrical products capable of emitting radio frequency energy by radiation, conduction, or other means in the range of 9 kHz to 3 GHz.

Equipment needs to comply with the requirements established in the FCC rules, independently of the technology it uses.

The table below details the FCC requirements that need to be fulfilled by telecommunication devices to be used in vehicles and Road Side Units, to enable ITS communication. Related technologies are cellular (5G, 4G, 3G, 3G and 2G), Bluetooth, Wireless LAN (WLAN) - including Wi-Fi-, NFC and Wireless Charging.

RQMT	47 CFR Regulation	Section	Description	Band
ЕМС	Part 2	2.950 (h)	Measurements for unintentional radiators	Any
	Part 15 Subpart B	15.107	Unintentional radiators. Conducted limits	Any
		15.109	Unintentional radiators. Radiated emission limits	
		15.111	Unintentional radiators. Antenna power conduction limits for receivers	Band 17 / XVII Band 05 / V / GSM850 Band 12 / XII Band 13 / XIII Band 14 / XIV
Radio	Part 2	2.950 (g)	Measurements for intentional radiators	Any
		2.1041	Measurement procedure - Certification	-
		2.1046	RF power output	
		2.1047	Modulation characteristics	
		2.1049	Occupied bandwidth	
		2.1051	Spurious emissions at antenna terminals	
		2.1053	Field strength of spurious radiation	
		2.1055	Frequency stability	
		2.1057	Frequency spectrum to be investigated	
	Part 15 Subpart C	15.204	External radio frequency power amplifiers and antenna	Any

Table 4: FCC requirements for ITS radio equipment.





		modifications. For WLAN, Bluetooth and NFC devices	
	15.209	Radiated emission limits - General requirements. For WLAN, Bluetooth and NFC devices	2.4 GHz 5.1 GHz 5.2 GHz 5.4 GHz 5.8 GHz 13.56 MHz (NFC)
	15.212	Modular transmitters. For WLAN, Bluetooth, NFC and Wireless charging devices	Any
	15.215	Occupied bandwidth. For WLAN and NFC devices	2.4 GHz 5.8 GHz 13.56 MHz (NFC)
	15.217	Operation in the band 160-190 KHz (Only applicable to equipment operated according to "Intentional radiators - Alternative conditions"). For wireless charging devices	148.5-300 kHz
	15.225	Intentional radiators. For NFC devices.	13.56 MHz (NFC)
	15.247	Intentional radiators. Operations within the bands (for WLAN devices and Bluetooth devices)	2.4 GHz
	15.249	Operation within the 5725- 5875 MHz band. For WLAN and Bluetooth devices	5.8 GHz
Part 15 Subpart E	15.407	Unlicensed National Information Infrastructure Devices: General technical requirements. For bands: For WLAN devices	5150-5250 MHz, 5250-5350 MHz, 5470-5725 MHz & 5725-5850 MHz
Part 22 Subpart H	22.335	Frequency stability	869-894 paired
	22.913	Effective radiated power	with
	22.917	limits Emission limitations	824-849 MHz GSM850; 3G & LTE band 5
Part 24 Subpart E	24.232	Power and antenna height limits	1850-1910 MHz & 1930-1990 MHz
	24.235	Frequency stability	PCS1900; 3G &
	24.238	Emission limitations for Broadband PCS equipment	LTE bands 2 and 25
Part 27	27.5	Frequencies	Band o7 / VII
	27.50	Power limits and Duty Cycle	Band 17 / XVII
	27.53	Emission Limits	Band 04 / IV
	27.54	Frequency Stability	Band 12 / XII
	27.55	Power Strength Limits	Band 38 / D Band 40 / E





				Band 41 n71
		27.75	Basic interoperability requirement	n71
	Part 18	18.301	Operating frequencies (Only required for equipment operated according to "ISM Equipment" conditions)	Wireless charging: 100-300 KHz 6.78 MHz
		18.305	Field strength limits (Only required for equipment operated according to "ISM Equipment" conditions)	
		18.309	Frequency range of measurements (Only required for equipment operated according to "ISM Equipment" conditions)	
	Part 30	30.4 (C)	Frequencies	5G: n257, n258,
		30.202	Power limits	n260
		30.203	Emission limits	
		30.208	Operability	
	Part 90	90.210	Emission masks	n79
		90.213	Frequency Stability	
		90.1213	Band plan	
		90.1215	Power limits	
		90.531(g)	Band plan	Band 14 / XIV
		90.539(e)	Frequency Stability	
		90.542	Broadband transmitting	
			power limits	
		90.543:	Emission Limitations	
	Part 90 Subpart M	90.375	DSRC RSU. RSU license areas, communication zones and registrations	5850-5925 MHz (DSRC)
		90.377	DSRC RSU. Frequencies available; maximum EIRP and antenna height, and priority	
		90.379	DSRC RSU ASTM E2213-03 DSRC Standard (ASTM-DSRC Standard).	
	Part 95	95.3159	DSRC OBU. OBU channel sharing and priority of use.	
	Subpart L	95.3161	DSRC OBU. OBU transmitter certification.	
		95.3167	DSRC OBU. OBU transmit power limit.	
Health/ SAR	Part 27 Section 27.52	1.1307	Actions that may have a significant environmental effect	Band 07 / VII Band 17 / XVII Band 04 / IV
		1.1310	RF radiation exposure limits	Band o5 / V / GSM850
		2.1091	RF radiation exposure	
		<u> </u>	evaluation. Mobile devices	Band 12 /XII





Electrical Safety	No requirements // U	L mark or equivalent		
		KDB Publication 941225	evaluation: Portable devices SAR test procedures for devices incorporating Long Term Evolution (LTE) capabilities	Band 38 / D Band 25 / XXV Band 40 / E Band 41 Band 02 / II / PCS1900- WLAN: 5.1 GHz 5.2 GHz 5.4 GHz 5.8 GHz
		2.1093	RF radiation exposure	Band 13 / XIII

3.4.3. Privacy certifications

Some operational examples of successful privacy certifications in various domains include:

- **PrivacyTrust** (formerly eTrust) [27]: a private company that provides privacy certifications for websites and online businesses. A PrivacyTrust certification indicates that a website has been reviewed by the company and is aligned with their privacy and data protection requirements. Similar certifications are available by other providers such as WebTrust, etc. although they are not focused on GDPR or software-oriented architectures.
- The Health Information Trust Alliance (HITRUST) is a US-based association of organisations, that certifies products for compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [28]. HIPAA sets rules for the handling of medical data in the US. HITRUST, therefore, is able to certify products for HIPAA compliance. It is therefore a case where an appropriate body certifies legal compliance for data protection, although its scope is not as broad as the EU GDPR.

In 5G-MOBIX's case, certification requires the existence of a trusted third party that inspects the CAM service and verifies that it is compliant with GDPR and that the information provided in its specifications are accurate. According to the GDPR Article 42:

"the Member States, the supervisory authorities, the Board and the Commission shall encourage the establishment of data protection certification mechanisms and of data protection seals and marks".

The certification should be voluntary and transparent, and the certification body should be granted cooperation and access to the processing. **Article 43** of the GDPR states **that certification bodies should be accredited** (ISO 17065). As GDPR is implemented in each Member State, it is expected that multiple data protection certification providers will be accredited with the relevant national authorities. Thus, it will be possible in the future for CAM service developers to get their products certified for GDPR compliance. At this time, it is uncertain if certifications will be available across all member states by the date of the project's completion.





4. CURRENT POLICY STATE-OF-PLAY

5G-enabled CAM presents a complex ecosystem of stakeholders and technical innovations. This section focuses on existing public policy frameworks that affect 5G CAM.

The EU's strategy is developed and translated into policies and initiatives by the European Commission, which organizes that strategy around six priorities. One of these EC's priorities is "A European fit for the digital age". This European approach to digital transformation is based on three pillars:

- Technology that works for the people.
- A fair and competitive digital economy.
- An open, democratic and sustainable society.

Europe will aim to become a global role model for the digital economy; support developing economies into going digital and develop digital standards and promote them internationally, with a clear focus on data, technology, and infrastructure. Connectivity is one of the fundamental actions required by digital transformation. The deployment of fibre and 5G networks offers economic opportunities and supports digital transition, enabling innovation in all relevant sectors. One of those sectors is connected transport and mobility.

EC is collaborating to achieve the EU's ambitious vision for connected and automated mobility in a Digital Single Market. The evolution in digital technologies is quickly changing vehicles, so policies related to digital technology, including cybersecurity, radio communications, data use, liability, privacy, etc. are becoming more relevant for the transport sector. The EC is supporting the deployment of CAM with:

- Developing policies, initiatives and roadmaps.
- Developing European standards.
- Co-funding research and innovation projects and pilots.
- Introducing European legislation.

Connectivity and in particular the deployment of 5G networks, is enabling and driving those efforts. This chapter discusses some of the existing public policy, funding frameworks and other initiatives with relevance to 5G for CAM. This section includes an extract of information available on the EU website, where more detailed information can be found:

- 5G policies and initiatives resulting from connectivity strategies follow the roadmap defined in the "5G for Europe Action Plan", while the mobility strategy is compiled in the "Europe on the Move" sets of initiatives with special focus in Cross Border Corridors.
- The progress of Europe's 5G Action Plan is assessed and monitored by the European 5G Observatory.



- The softwarised, cloud-native nature of 5G make it an attractive target for cyberattacks. Policies should be in place to minimise such risks.
 - **5GPPP** is launching R&I projects like 5GMOBIX funded by the Horizon 2020 programme. Horizon Europe will continue funding R&I projects from 2021.
 - **CEF** (2014-2019) and **CEF2** (2021-2027) are instruments funding infrastructure investments in Europe.
- Some of these policies and initiatives have been presented in detail at events or in publications like the **"5G Strategic Deployment Agenda for Connected Automated Mobility".**

4.1. 5G for Europe Action Plan

The 5G Action Plan [29] is a strategic initiative, which concerns all stakeholders, private and public, small and large, in all Member States of EU, to meet the challenge of making 5G a reality for all citizens and businesses by the end of 2020. A very high-capacity network like 5G will be a key asset for Europe to compete in the Global market, with worldwide 5G revenues for mobile operators expected to reach €225 billion annually by 2025. On 14 September 2016, the Commission launched a plan to boost EU efforts for the deployment of 5G infrastructures and services across the Digital Single Market by 2020. The action plan set out a clear roadmap, for public and private investment on 5G infrastructure in the EU.

To achieve that, the Commission proposed the following measures:

- Align roadmaps and priorities for a coordinated 5G deployment across all EU Member states, targeting early network introduction by 2018, and moving towards commercial large-scale introduction by the end of 2020 at the latest;
- Make provisional spectrum bands available for 5G ahead of the 2019 World Radio Communication Conference (WRC-19), to be complemented by additional bands as quickly as possible, and work towards a recommended approach for the authorisation of the specific 5G spectrum bands above 6GHz;
- Promote early deployment in major urban areas and along major transport paths;
- Promote pan-European multi-stakeholder trials as catalysts to turn technological innovation into full business solutions;
- Facilitate the implementation of an industry-led venture fund in support of 5G-based innovation;
- Unite leading actors in working towards the promotion of global standards.

The EU Public-Private Partnership (5G-PPP) launched in 2013 put Europe clearly at the forefront of the current research phase, as compared to other regions. The research results are now feeding the global standardisation process and is used to prepare the first large scale trials and demonstrators in Europe, in cooperation with several key sectors. The 5G Action Plan is leveraging these initial research successes.

The new European Electronic Communications Code [30] and the 5G action plan are closely related: they are both aimed at fostering the competitiveness of our industry in the Digital Single Market. They will both





support the deployment and take-up of 5G networks, notably as regards the timely assignment and availability of radio spectrum, more favourable conditions for small cell deployment or sectorial issues preventing the deployment of particular services, investment incentives and favourable framework conditions, while the recently adopted rules on Open Internet provide legal certainty as regards the deployment of 5G applications.

5G will enable:

- Industrial transformation through wireless broadband services provided at Gigabit speeds. 5G should offer data connections well above 10 Gigabits per second, latency below 5 milliseconds and the capability to exploit any available wireless resources (from Wi-Fi to 4G) and to handle millions of connected devices simultaneously).
- The support of new types of applications connecting devices and objects (the Internet of Things) and versatility, by way of software virtualisation allowing innovative business models across multiple sectors (e.g., transport, health, manufacturing, logistics, energy, media and entertainment).

It opens up prospects for new pervasive mobile virtual services, important for the economy and society ranging from virtual reality for remote collaboration to online health monitoring or connected cars, and possibly drone delivery or automated driving.

4.2. European 5G Observatory

The European 5G Observatory monitors market developments and preparatory actions taken by industry stakeholders and EU's members in the context of 5G rollout in Europe and beyond. The Observatory enables the EC to assess the progress of Europe's 5G Action Plan and take action to fully implement it [31].

As 5G gets closer to market deployment, the European 5G Observatory provides updates on all market developments, including actions undertaken by the private and public sectors, in the field of 5G. All developments will be analysed given their strategic implications on the objectives of the 5G Action Plan and other public policy objectives. The Observatory focuses primarily on developments in Europe, along with major international developments that could influence the European market.

The Observatory monitors the following developments:

- Main 5G market developments including planning and commercial launch of 5G products and services with major impact.
 - New developments regarding key 5G products and components as well as technology choices made by key actors including regarding standards and use of spectrum bands.
 - 5G pre-commercial trials and partnerships between actors of the 5G value chain.
 - National strategies and plans by EU Member States, available national data on 5G deployment including coverage and quality.



• Preparation and execution of spectrum assignments by public authorities as well as 5G public funding for network deployment and R&I.

Plans to establish the European 5G Observatory were announced in February 2018, to closely monitor the progress of the European 5G Connectivity objectives for a competitive Digital Single Market by 2025. The observatory provides regular updates of the latest trends in 5G deployment and publishes quarterly reports on the 5G progress.

In line with the 5G Action Plan for Europe, EU countries have already agreed on a 5G roadmap to coordinate the availability of new 5G frequencies. Several Member States have published national strategies on 5G in the context of national broadband plans (NBPs).

IDATE DigiWorld has been selected to carry out the 5G European observatory for the European Commission.

4.3. 5G Cybersecurity toolbox

5G is expected to be a major enabler for multiple digital services, including CAM. 5G can be a key factor towards the development of a digital economy in the coming years, affecting many citizens' lives. However, due to the less centralised architecture and its cloud-native, softwarised nature, it can offer a valuable target to attackers. Thus, it is crucial to ensure a secure roll-out with built-in security and robustness features using a coordinated approach at the national and EU level.

Thus, the NIS Cooperation Group has worked on a 5G Cybersecurity toolbox containing a common set of measures to mitigate cybersecurity risks and achieve a level of resilience. The toolbox proposes a set of Strategic and Technical Measures to ensure the deployment of secure 5G networks [32].

Key measures include:

- Strengthening security requirements for Mobile Network Operators (MNOs) at Member State level.
- Assessing the risk profile of suppliers and applying restrictions in terms of key assets such as the exclusion of a high-risk supplier.
- Ensuring that MNOs adopt a multi-vendor strategy and avoiding dependency on a single supplier.
- Maintaining a diverse and sustainable 5G supply chain.
- Using relevant EU programs and funding.
- Facilitating standardization and certification.
- Making use of other existing frameworks, e.g., relating to the screening of Foreign Direct Investment (FDI) etc.

In July 2020 ENISA [33] issued a report on "Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity". The report concludes that most Member States (MS) have been taking important steps to implement the Toolbox. Most MS carried out gap analyses and launched processes to review and upgrade existing security measures, as well as advanced in the preparation of more advanced security measures.





Work is still ongoing, however, in order to properly define the scope of the measures and many political and regulatory decisions still need to be made. Although most Member States do not share specific details for national security reasons, the report presents a high-level analysis:

- Most MS are in the process of strengthening power for regulatory authorities, to allow powers to regulate the procurement of equipment, based on security-related grounds.
- There is still a need to address how cybersecurity audits will be conducted.
- Regarding the restriction on suppliers based on their risk profile, the identification of criteria is
 ongoing in many MS, although it is a complex and sensitive matter. It is recommended that the
 assessment takes into account the international trade context and prioritises specific key assets (such
 as MANO). Another issue to be considered is the transition period as operators might already use
 equipment from high-risk vendors, particularly during the upgrade cycle from non-standalone to
 standalone 5G.
- Several MS has not yet adopted measures to limit the ability of MNOs to outsource particular functions and activities.
- Many MS are facing challenges in defining the process to impose multi-vendor strategies for individual MNOs or at the national level.
- Several Member States have recently taken steps to introduce or reinforce existing national Foreign Direct Investment (FDI) screening mechanisms. FDI screening is not yet in place in 13 MS, and steps should be taken to introduce it in view of the approaching application of the EU screening framework as of October 2020. FDI screening should be applied in cases where the 5G supply chain is involved.
- The process of reviewing and reinforcing network security requirements for operators is welladvanced. Progress is slower when defining security requirements and technical measures since the development of many technologies is still ongoing. The role of standardisation is instrumental in this respect and European participation in relevant SDOs (Standards Developing Organizations) is a necessity
- It is crucial that MS exchange information and best practices regarding 5G cybersecurity and ensure the cooperation of the Commission and ENISA towards the monitoring of the implementation of the Toolbox as well as the implementation of EU-wide actions.
- Ensuring that 5G projects supported by public funding take into account cybersecurity.

4.4. Europe on the Move: Third Mobility Package

The EC launched Europe on the Move in 2017, a set of initiatives aimed to modernise European transport and mobility in a transition to digitalisation and clean energy. It is based on three pillars: Socially fair & Competitive; Clean; and Connected Transport and Mobility. Actions were taken in three phases. The third package of measures, presented in May of 2018, is related to connected and autonomous mobility. It included proposals about safe mobility, clean mobility, and connected & automated mobility [34].

The proposal about automated mobility [On the road to automated mobility: An EU strategy for mobility of the future COM/2018/283 [35] describes CAM as a new opportunity for Europe and gives the EU's vision. It





introduces the funding options: Horizon 2020 programme for R&I projects and CEF for deployment initiatives. It emphasises aspects like innovation, safety, liability issues, connectivity, cybersecurity, and data protection [35]–[37].

4.5. Cross-border corridors for Connected and Automated Mobility

Within the European 5G vertical strategy, Connected and Automated Driving (CAD) is considered as a flagship use case for 5G deployment along European transport paths, in view of creating complete ecosystems around vehicles, beyond the safety services targeted by the Cooperative-Intelligent Transport System (C-ITS) roadmap of Europe [38].



Figure 7: 5G Cross-border Corridors for Connected and Automated Mobility.

29 European countries are committed to the development of large-scale testing sites of connected and automated driving on European motorways in the form of cross-border corridors.

4.5.1. Europe's 5G Corridors

A collaborative network of cross-border corridors between European countries will enable a better environment for the testing and deployment of 5G technology.





Member States and industry first agreed to establish cross-border corridors in September 2017, during the round table on Connected and Automated Driving (CAD) in Frankfurt. Several Member States have gone on to sign and/or announce bilateral agreements among themselves for more test corridors.

Thanks to these 5G corridors, Europe is currently the biggest experiment area in 5G technology. This affirms Europe's ambition to lead in large-scale testing and early deployment of 5G infrastructure, enabling connected and automated driving (or mobility). Only a pan-European effort will create a secure and safe environment for citizens to enjoy the benefits of connected and automated mobility.

4.5.2. Initiatives for 5G cross-border corridors large-scale testing

As part of the European Commission's 5G Public Private Partnership (5G PPP), the EU supports and co-funds three 5G cross-border corridor projects for large-scale testing of connected and automated mobility (CAM), which are co-funded under Horizon 2020 and include 5G MOBIX. The three projects, launched in November 2018, trial 5G technology applied to CAM over more than one thousand kilometres of highways across four borders:

- 5G-CARMEN: 600 km of roads across an important north-south corridor from Bologna to Munich via the Brenner Pass.
- 5GCROCO: over highways between Metz, Merzig and Luxembourg, crossing the borders of France, Germany and Luxembourg.
- 5G MOBIX: along two cross-border corridors, one between Spain and Portugal and the other between Greece and Turkey.

Further funding opportunities are currently planned by the Commission both under the last phase of Horizon 2020 and the next EU budget proposal. In particular, as part of the next Connecting Europe Facility programme (CEF2 Digital) for 2021-2027. There are also several important initiatives/projects[39] and cooperation agreements in place among Member States:

- France, Germany and Luxembourg have announced a joint corridor between Luxembourg, Metz and Merzig.
- Norway, Finland and Sweden with the E8 corridor between Tromsø (Norway) and Oulu (Finland) and the E18 corridor between Helsinki, Stockholm and Oslo.
- The **Netherlands and Belgium** have agreed to the Rotterdam Antwerp Eindhoven corridor.
- **Spain and Portugal** signed a letter of intent to have two joint corridors between Vigo and Porto and between Evora and Mérida, allowing connected automated driving to be tested across borders.
- **Slovenia, Hungary and Austria** signed a memorandum of understanding on cross-border cooperation in developing and testing electric, integrated and autonomous vehicles.
- Bulgaria, Greece and Serbia signed a letter of intent on the corridor Thessaloniki Sofia Belgrade to develop experimental 5G cross-border corridors that will allow for the testing of driverless vehicles.





- **Poland and Lithuania** signed a letter of intent on 5/9/2018 to cooperate on technical, legal and policy of the cross-border CAD corridor 'via Baltica' (Warsaw, Kaunas, Vilnius).
- Lithuania, Latvia and Estonia signed a memorandum of understanding for the 'Via Baltica North'.
- Italy and the three presidents of Euroregion Tirol-Südtirol-Trentino have confirmed their intention to work, in cooperation with other interested Member States, on the development of the 5G Corridor on the Brenner-pass motorway.

Overall, thanks to the support of enhanced cross-border cooperation and the support of EU Research and Innovation funding, a new map of 5G cross-border corridors is progressively taking shape in Europe [38].

4.6. 5G Strategic Deployment Agenda for Connected & Automated Mobility

The "**5G Strategic Deployment Agenda for Connected Automated Mobility"** sets the "shared view of a wide group of industry stakeholders supporting the objectives of the 5G Strategic Deployment Agenda (SDA)". The aim is to support Connected and Automated Mobility (CAM) in Europe and set the basis for "future-proof 5G infrastructure, technologies and vehicles".

The current proposal for the SDA envisions that deployment of 5G is a major enabler for commercial (e.g., infotainment) as well as safety services, due to improved speed and reliability. In addition, the service-based approach is expected to transform vertical industries and spark economic growth. The 5G SDA for CAM revolves around the **deployment objectives, cooperation models and regulatory innovations** as its main elements [40]. These were defined during the first open stakeholder workshop that took place in February 2019. The common principles that underline the SDA were hence defined:

- **Deployment of 5G should follow an evolutionary path:** In order to account for future market needs and technical developments, the deployment of 5G should follow an evolutionary path. 5G should co-exist and be interoperable with other networks like 4G LTE.
- Service Continuity across borders and actors: As many CAM services (e.g., guidance, autoovertake etc.) can be considered "mission-critical", there needs to be reliable, uninterrupted connectivity and coverage, with service continuity across borders and actors.
- End-to-end cybersecurity: A high level of end-to-end cybersecurity is necessary to ensure trust in CAM services, but it also needs to be held to high performance and reliability criteria.
- 5G for CAM needs to be a **Multi-service/Multi-application platform** with standardised interfaces and data formats.
- **Coordination among public & private actors in V2X** for the deployment of 5G infrastructure is necessary. Starting from major corridors and highways, the benefits of 5G for CAM can be demonstrated. Coverage can then be extended to secondary roads and urban areas.
- **Public authorities and administrations** in charge of roads should collaborate for the deployment of connectivity along major corridors.
- **Cooperative planning & cost optimisation** is necessary to deliver improved networks costeffectively.





• Digital transformation for industry verticals must be accelerated [41].

لم	Deployment of 5G should follow an evolutionary path
۲	Service continuity across borders and actors: e.g. Mobile Network Operations, road operators etc.
8	End-to-End cybersecurity, privacy and trust.
4 <u>1</u> 4	Coordination among public & private actors in V2X in order to move from 5G-enabled highways, to secondary roads etc.
8	Multi-service/Multi-application platform with standardized data formats and interfaces and "mutualization" of costs across actors
Â	Coordination with public authorities (e.g. road operators) to simplify deployment
٠	Cooperative Planning to support innovative deployments with optimised network economics
3	Digital transformation and automation of industry processes

Figure 8: The 5G SDA common principles.

4.7. 5G Infrastructure Public Private Partnership (5G PPP)

The 5G Infrastructure Public Private Partnership (5G PPP) is a joint initiative between the European Commission and European ICT industry (ICT manufacturers, telecommunications operators, service providers, SMEs and researcher Institutions). The 5G-PPP is now in its third phase where many new projects were launched in Brussels in June 2018. 5G MOBIX with 5GCroCo and 5GCARMEN were the projects selected in part 2, automotive projects, of that third phase.

The 5G PPP will deliver solutions, architectures, technologies and standards for the ubiquitous nextgeneration communication infrastructures of the coming decade. The challenge for the 5G Public Private Partnership (5G PPP) is to secure Europe's leadership in the particular areas where Europe is strong or where there is potential for creating new markets such as smart cities, e-health, intelligent transport, education or entertainment & media. The 5G PPP initiative will reinforce the European industry to successfully compete on global markets and open innovation opportunities. It will "open a platform that helps us reach our common goal to maintain and strengthen the global technological lead" [42].

The key challenges for the 5G Infrastructure PPP are:

- Providing 1000 times higher wireless area capacity and more varied service capabilities compared to 2010.
- Saving up to 90% of energy per service provided. The main focus will be on mobile communication networks where the dominating energy consumption comes from the radio access network.





- Reducing the average service creation time cycle from 90 hours to 90 minutes.
- Creating a secure, reliable and dependable Internet with a "zero perceived" downtime for services provision.
- Facilitating very dense deployments of wireless communication links to connect over 7 trillion wireless devices serving over 7 billion people.
- Ensuring for everyone and everywhere access to a wider panel of services and applications at lower cost [42].

4.8. Connecting Europe Facility (CEF)

The Connecting Europe Facility (CEF) is a key EU funding instrument to promote growth, jobs and competitiveness through targeted infrastructure investment at European level. It supports the development of high performing, sustainable and efficiently interconnected trans-European networks in the fields of transport, energy and digital services. CEF investments fill the missing links in Europe's energy, transport and digital backbone.

The CEF benefits people across all Member States, as it makes travel easier and more sustainable, it enhances Europe's energy security while enabling wider use of renewables, and it facilitates cross-border interaction between public administrations, businesses and citizens.

In addition to grants, the CEF offers financial support to projects through innovative financial instruments such as guarantees and project bonds. These instruments create significant leverage in their use of EU budget and act as a catalyst to attract further funding from the private sector and other public sector actors.

The CEF is divided into three sectors: Energy, Telecom and Transport.

4.8.1. CEF Telecom

The Connecting Europe Facility (CEF) in Telecom is a key EU instrument to facilitate cross-border interaction between public administrations, businesses and citizens, by deploying digital service infrastructures (DSIs) and broadband networks. Supported projects will contribute to the creation of a European ecosystem of interoperable and interconnected digital services that sustain the Digital Single Market.

4.8.2. CEF Transport

The Connecting Europe Facility (CEF) [43] for Transport is the funding instrument to realise European transport infrastructure policy during the period 2014-2020. It aims at supporting investments in building new transport infrastructure in Europe or rehabilitating and upgrading the existing one.

CEF Transport focuses on cross-border projects and projects aiming at removing bottlenecks or bridging missing links in various sections of the Core Network and on the Comprehensive Network (link), as well as for horizontal priorities such as traffic management systems.





CEF Transport also supports innovation in the transport system to improve the use of infrastructure, reduce the environmental impact of transport, enhance energy efficiency and increase safety [44].

4.9. Connecting Europe Facility (CEF₂) Digital

The Connecting Europe Facility (CEF2) Digital programme aims to support and catalyse investments in digital connectivity infrastructures of common interest during the period 2021-2027.

Europe can fully reap the benefits of the digital transformation if high-quality access to Gigabit networks is made available to all people, businesses and "socioeconomic drivers" such as schools, universities, hospitals, transport hubs and public administrations.

The Connecting Europe Facility (CEF₂) Digital programme will support and catalyse investments in digital connectivity infrastructures of common interest, during the period 2021-2027.

Actions foreseen under the programme include:

- The deployment of and access to very high-capacity networks, including 5G systems, capable of providing Gigabit connectivity in areas where socioeconomic drivers are located.
- The provision of very high-quality local wireless connectivity in local communities that is free of charge and without discriminatory conditions.
- Uninterrupted coverage with 5G systems of all major transport paths, including the trans-European transport networks.
- Deployment of a new or significant upgrade of existing backbone networks including submarine cables, within and between Member States and between the Union and third countries.
- Implementing digital connectivity infrastructures related to cross-border projects in the areas of transport or energy and/or supporting operational digital platforms directly associated with transport or energy infrastructures [45], [46].

4.10. C-ITS Platform

Following 2010 ITS EU Directive and its subsequent regulation on issue like road safety, real-time-traffic and multimodal travel information, providing the necessary legal and technical framework to steer and ensure the interoperability of deployed ITS services, the EC decided in 2014 to take a more prominent role in the deployment of connected driving, setting up a C-ITS Deployment Platform. The Platform was conceived as a cooperative framework including national authorities, C-ITS stakeholders and the Commission, in view to develop a shared vision on the interoperable deployment of C-ITS in the EU. Hence, it was expected to provide policy recommendations for the development of a roadmap and a deployment strategy for C-ITS in the EU and identify potential solutions to some critical issues.





After the first phase towards its first milestones in connected and autonomous vehicles in the EU, the second phase developed a shared vision on the interoperable deployment of Cooperative Intelligent Transport Systems (C-ITS) towards connected and automated mobility (CAM) in the European Union.

This included making tangible progress in topics like security, data protection, compliance assessment and hybrid communication, essential to the interoperability of C-ITS deployment and relevant for the preparation of Delegated Acts on C-ITS. The Platform work was closed in 2017 but the EU rejected the Delegated Act in 2019 after considerations of lack of neutrality from industry telecommunications and automotive stakeholders.

The EC recommendation to make the Wi-Fi-based (802.11p) ITS-G5 standard mandatory requirement for vehicle-to-X (V2X) capabilities, did not leave any room for the Cellular-V2X (C-V2X) technology favoured by the GSMA community. When rejected, this opened the door for C-V2X, that many considered a better option in areas like day one services like VRU safety.

4.11. Other initiatives

4.11.1. European Automotive – Telecom Alliance (EATA)

The EC initiated a number of High-Level Round Table discussions to strengthen the digital dimension of CAM. These discussions brought together the industrial players from the digital and automotive sectors to develop joint road maps and establish cross-border deployment actions. Among the main achievements of the Round Table is the creation of the "European Automotive – Telecom Alliance" (EATA) to promote the wider deployment of connected & automated driving.

The first target of the Alliance was to implement the pre-deployment project for testing CAM in a real setting.

4.11.2. 5G Automotive Alliance

In parallel, the industry joined up to create the 5G Automotive Alliance (5GAA) to specifically promote 5G in the automotive sector. A Memorandum of Understanding amongst EATA and 5GAA was signed at the Mobile World Congress (February 2017).

4.11.3. C-ROADS Platform

Through the C-Roads Platform, funded under CEF, authorities and road operators join together to harmonize the deployment activities of cooperative intelligent transport systems (C-ITS) across Europe. The goal is to achieve the deployment of interoperable cross-border C-ITS services for road users.





According to the C-ROADS main website¹, the governance structure can be described as follows:

- The C-Roads Platform is steered by the C-Roads **Steering Committee** which is composed by Member State representatives. With the support of the **Supporting Secretariat**, decisions for achieving the goal of the implementation of interoperable end-user services are done.
- In this respect specifications, which are proposed and recommended by specific Working Groups, are approved. These specifications are the basis for the single pilot activities. This especially goes with technical decisions, which influence deployment and procurement decisions at pilot sites.
- Working Groups are installed as decision support for the Steering Committee to ensure proper decisions towards interoperable deployments. Individual experts participating in the single pilots work together in these Working Groups to prepare proposals and recommendations.
- Also, members of the single-pilot activities as well as of the C-Roads-Working Groups actively contribute to the work of the EU-C-ITS-Platform.

Additionally, the European Commission and the Innovation and Networks Executive Agency as well as associated member State representatives are invited to follow and actively participate in discussions at all C-Roads Platform levels. The C-ROADS platform deals with cross-border interoperability of C-ITS services. C-ROADS provides specifications of C-ITS Day 1 I2V services. In addition to ITS-G₅, C-ROADS has defined an IP-based protocol for communication between back ends, allowing service continuity across borders. C-ROADS collaborates with the Car2Car Consortium, in order to assure that the specifications are accepted by the vehicle industry.

4.11.4. CAR2CAR Consortium

The CAR₂CAR consortium focuses on wireless vehicle-to-vehicle (V₂V) communication applications based on ITS-G₅ and concentrates all efforts on creating standards ensuring the interoperability of cooperative systems spanning all vehicles classes, across borders and brands. The Consortium works in close cooperation with the European and international standardisation organisations like the European Telecommunications Standards Institute (ETSI) and European Committee for Standardisation (CEN).

4.12. Post-Covid-19 Releases

Europe is in transition between two long term budgeting periods: from CEF to CEF2 and from Horizon 2020 R&I programme to Horizon Europe, involving new projects' calls. On the other hand, Europe is struggling to overcome the Covid-19 pandemic. The post-COVID era will bring new trends and needs in mobility, transport and communications: Increase in last mile delivery operations due to increased online commerce activity; demand increase of individual and/or driverless transportation of passengers and goods; an increase of use of broadband services for remote work, online meetings, home schooling, TV streaming; etc.





Post-COVID rescue packages and bailout funds will be implemented via projects so we will see new developments and projects during the following years.

This subsection includes some references to updates in the policies and initiatives described in this section and some references to local initiatives in countries where 5G MOBIX is working.

4.12.1. State of the Union 2020

After the <u>State of the Union Address</u> in September 2020, the EC issued a recommendation to boost investment in very high-capacity broadband connectivity infrastructure, including 5G, which is the most fundamental block of the digital transformation and an essential pillar of the recovery. It boosts fast network connectivity and develops a joint approach to 5G rollout. The timely deployment of 5G networks will offer significant economic opportunities for the years to come, as a crucial asset for European competitiveness, sustainability and a major enabler for future digital services.

The recommendation included a toolbox of best practices that should aim to:

- Reduce the cost and increase the speed of deployment of very high-capacity networks, notably by removing unnecessary administrative hurdles.
- Provide timely access to 5G radio spectrum and encourage operators' investments in expanding network infrastructure.
- Establish more cross-border coordination for radio spectrum assignments, to support innovative 5G services, particularly in the industry and transport fields.

The recommendation also sets out guidance for best practices to provide timely access to radio spectrum for 5G as well as ensure stronger coordination of spectrum assignment for 5G cross-border applications. This is particularly important to enable connected and automated mobility, as well as the digitisation of industry and smart factories. Enhanced cross-border coordination will help to provide Europe's main transport paths, particularly road, rail and in-land waterways, with uninterrupted 5G coverage by 2025. However, until mid-September 2020, Member States (and the UK) had assigned on average only 27.5% of the 5G pioneer bands. It is therefore essential that Member States avoid or minimise any delays in granting access to radio spectrum to ensure timely deployment of 5G.

The recommendation also promotes the rollout of sustainable high-speed networks by reducing deployment costs through harmonized measures to ensure network providers and operators can share infrastructure, coordinate civil works and obtain the necessary permits for deployment.

4.12.2. Spanish Connected, Safe and Sustainable Mobility Strategy 2030

The Spanish Ministry of Transports, Mobility and Urban Agenda (MITMA) presented in September of 2020 **es.movilidad**, the Connected, Safe and Sustainable Mobility Strategy 2030 that will guide the next ten years actions in mobility, infrastructure and transport. The strategy is built around nine axes, including smart





mobility, European connectivity, safe mobility, low emissions mobility, and inclusive mobility, among others. The first phase will include a laboratory of ideas to define some of the required initiatives.

The Ministry is working on a new Mobility Law that includes connected and automated mobility.

4.12.3. France – Spain cooperation in CAM

France and Spain ministers of transport signed in September 2020 a Memorandum of Understanding (MoU) on connected and automated driving aimed to develop the collaboration in future driving. The main objectives are:

- Bigger interoperability of systems and standardization.
- Development of the use cases of shared mobility, transport and logistics.
- Adaptation of regulations and infrastructures to new systems of connected mobility.
- Introduction of cooperative communication systems and 5G connectivity in transport [47].

The MoU will boost cooperation between different ongoing research projects and will facilitate autonomous driving cross border tests between both countries.

The Spanish Ministry of Transport is open to autonomous driving tests in open traffic roads and the Spanish Secretary of Telecommunications and Digital Infrastructure has stated that the development of cross border corridors is a key priority [48], [49].





5. PRELIMINARY RESULTS

The following chapters describe recommendations from the stakeholders (road operator, car/truck industry and network operators) to the regulation and policy entities for enabling an X-border traffic with automated vehicles.

5.1. Recommendations from ICT Sector

Although specific recommendations on the ICT side were provided in D6.1 "Plan and Preliminary Report on deployment enablers", some important aspects that touch upon regulation and cooperation can also be presented here. In order to create a fast-growing market of 5G for CAM services, there needs to be improved cooperation when it comes to the **standardisation of interfaces and data formats** to ensure interoperability but also data portability. Furthermore, the specifications for 5G services need to be standardised and include their QoS requirements and the limits under which the services are expected to degrade or fail.

The concerns over the use of data-intensive services based on Artificial Intelligence and highly-automated ITS are highly relevant to the future of CAM. Improved and complex functionalities may require the use of massive data collection over periods of time. This needs to be performed under the confines of the GDPR and the new ePrivacy Regulation. More guidance should be provided by higher-level authorities on **how data should be stored**, transferred, shared etc. Attention should be given to **data Integrity**. Governments should push for regulating stakeholders on the type of data they provide across platforms, ensure that these data are reliable and of good quality, and set requirements regarding data quality.

The need for **ethical data proxies** can be a potential solution to this problem, as data intermediaries that provide encryption, anonymization/pseudonymisation on the fly, and manage who is authorised to access this data and under authenticated access only. This is particularly relevant in the Cross-Border setting, in order to adhere to the principle of data minimisation and becomes even more critical in hard border cases, where GDPR-level protection may not be applicable.

The democratisation of data access can in turn lead to the development of more intelligent CAM services. The next step would be to make these services available through the **creation of a digital marketplace**. This would assume that there are ways to properly specify the deployment requirements of each service (including boundary conditions that can lead to failure) and a way to negotiate **Service Level Agreements** (SLAs) with the service provider. SLA assurance can then be monitored, and a penalisation model can be applied to providers that fail to comply with the SLA contract. Blockchain technology can be applied to Smart Contracts and provide a basis for future SLA negotiations and monitoring.

On the side of the Telco operators, **flexible spectrum licensing and payment methods** seem to be a key concern as these can potentially affect the investment in new infrastructures. A specific plan needs to be in place from any member state prior to the spectrum auctions to enable telco operators to make appropriate





plans for 5G deployments. A flexible mechanism should be in place to enable leasing of additional frequencies and the additional licensing processes for the development of infrastructure (e.g., antenna placement etc.) should be fast.

Particularly in the **cross-border case**, recommendations are focused on **harmonisation and roaming**. Specifically, Cross-border harmonisation issues may arise in cases of countries that do not implement the ECC/DEC/(15)01 decision on "Harmonised technical conditions for mobile/fixed communications networks (MFCN) in the band 694-790 MHz including a paired frequency arrangement (Frequency Division Duplex 2x30 MHz) and an optional unpaired frequency arrangement (Supplemental Downlink)" e.g., Bulgaria. Frequency harmonisation is a necessary component of CAM, otherwise, there is the risk that automated capabilities will not be available across a hard border.

In the case of Roaming:

- It needs to be clarified whether the extent of current Roaming regulation is applicable for M2M communications and what the definition of "fair use" entails. There needs to be harmonisation in the way Roaming is implemented, billed and taxed.
- The negotiation of GRX connections needs to be simplified by the related regulators.
- There needs to be transparency and notification when a vehicle is changing network.
- There need to be technical safeguards against accidental roaming when driving near a border region, as the accidental handover can severely impact vehicle QoS.

5.2. Recommendations from road operators

The introduction of automated vehicles in public road networks presents a new challenge for road operators in the relation between infrastructure and road users. Although the rules and context of vehicle operation is expected to remain the same, the automation of driver tasks must include all the safety and compliance demands a human driver should abide by. Some rules can be computationally modelled, and some others fall into the behavioural and cultural domain.

The road environment community of stakeholders has also evolved to a more shared space, where soft modes and new mobility forms are increasing the complexity of the road and the coexistence of different classes of vehicles and pedestrians. Road Operators are committed to the introduction of high-level automation in both vehicles and infrastructure but given top priority and concern to all matters having an impact on road safety.

Considering the regulatory issues that may have a strong influence in supporting cross-border automated vehicles in the next generation of connected mobility and the policy measures that may be taken to support them, the main issues and suggestions for policy recommendations from a Road Operator perspective are depicted below in detail.





- Higher levels of automation, that have road infrastructure requirements such as surface marking or telecommunications support, should require validation to be active. The validation could be achieved by including AD levels in HD Map information or by broadcasting allowed AD levels in I2V services and are currently under discussion in the C-ROADS platform. A common regulation must exist to define the compliance of vehicles with infrastructure conditions, including cross-border borders.
- Extended sensors allow the increased visibility and awareness of a vehicle's surrounding, shared information measures must be implemented to define the level of trust, reliability and precision of extended sensor information. Policies regarding the handling of Road Infrastructure sourced sensor information and shared vehicle awareness information must define the priority and validity of overlapping or conflicting data.
- Safety and reliability of AV handling and manoeuvre is heavily reliant on global positioning systems and HD Map information, which do not have enough precision for kinetic calculations. For most high precision AV functions, local positioning systems and HD Maps should be adopted, supported by infrastructure location reference services.
- It is not expected that vehicles can include all traffic laws and regulations into their AV functions. Specifications and specific regulations must be developed in a common format to describe the general laws and regulations, as well as the laws and regulations applicable locally for specific conditions. This description should take the Vienna convention and existing standards as a base for a I2V service or HD Map data layer to allow the vehicles to receive traffic law compliance instructions for ADAS systems.
- From a traffic management point of view, platooning is a specific vehicle formation that already
 exists with human driving. The rules for platoons of vehicles, for example in emergency and
 military formations, restricts the flow of traffic for remaining drivers. Specific regulations must
 be created for the existence and limits of automated platooning, and the ADAS for all vehicles
 member of a platoon must comply with manoeuvre enforcement measures that reduce the
 impact for remaining road users.
- Road traffic is based on the principle that each vehicle has the responsibility to perform according to the rules of traffic while ensuring observance to safety conditions in the surrounding. Remote driving allows for an operator to replace the driver, being limited to the capabilities of the vehicle sensors and communications, much like the highest level of SAE driving. Specific regulations must be created to define the conditions in which remote driving is allowed and to assure the liability for operators in case of incident or non-compliance to traffic laws.
- The rise of automated interaction with vehicles driving components, along with the meaningful
 interference of digital telecommunication services in ADAS, shall require the creation of specific
 regulation for black box information and road accident recording. Such information is not only
 required for legal and liability purposes but also as a key factor to improve the resilience and
 reliability of AV.
- The technology of AV for higher levels of SAE autonomous driving and remote driving can and should be, used as additional **safety measures regarding human failure**. Systems such as





detection of illegal substance abuse or sudden illness can be regulated as future mandatory base functions of AV, along with the support for contingency stops and automated malfunction response manoeuvres with or without road infrastructure support.

- The coexistence of AV with other conventional vehicles on the road requires the creation of specific regulation regarding the need to support additional safety measures in AV, prioritization of road traffic, maximizing road safety and performance. Using high-level automated functions in environments with pedestrians or vulnerable road users (VRUs) shall require certification/validation or rating of safety levels for a vehicle to operate in automated mode, similar to the Euro NCAP.
- To reach the full potential of CAM technologies in road vehicles, conventional vehicles must become, more and more, connected vehicles. This technology should not only benefit new vehicles manufactured with specific applications for connected mobility. In particular for awareness and safety functions, there must be a development policy that allows this technology to be available for conventional vehicles by retrofitting them with connected V2X systems.
- The communication in V2V and V2I must safeguard all aspects of **privacy and secure data handling, making available only the relevant data to the involved parties**. Some AV functions rely on the detection and tracking of specific vehicles, by recording and processing data that is needed to remain trackable for a certain span of time. Specific regulation must be developed to handle the ability of automated systems to perform data processing in closed context, assuring the privacy of tracked and recorded data.
- Higher-level functions of CAM like overtaking or lane merging, in mass transit or highperformance roads, may require arbitration between the involved parties depending on the implementation model. Road Operators may provide such arbitration and manoeuvre coordination. For that purpose, it shall be necessary to create specific regulation that provides a framework for infrastructure action and vehicle abidance by ADAS, including the possibility of non-compliance by any party involved.

In the case of **Real-Time Multi-tier Processing and Remote driving**, recommendations include:

- KPI (Key Performance Indicators) verification of sensor operation. Some of the usual KPIs are vehicle manoeuvres, safety measures, environmental impact or network efficiency within the car. Checking the data at the beginning of the process ensures that the system works properly.
- **Raising the level of data processing.** With traditional data storage methods, the results must be stored on a NAS-based (Network-attached storage) system and then transferred to workstations. This process has three drawbacks:
 - Large amounts of data must be moved, which requires considerable bandwidth and operating time.
 - Individual workstations do not offer the massive computing power required to return results quickly enough.





- Employ work environments that allow processing and storage to be scaled to hundreds of petabytes (e.g., open-source Hadoop for programming distributed applications that handle large volumes of data)
- Making the most of advanced analytics. The new analysis tools can read different data formats thrown up by cars and provide appropriate levels of access to metadata (e.g., video recordings valid for both analysing vehicle right-hand drive behaviour and determining the accuracy of a model representing the vehicle's perception of its physical environment). The more sensors that can cover a type of information, the final decision will be based on the action that indicates the largest number of sensors in case of inconsistency. However, much work remains to be done in this regard in terms of ethics and prioritizing actions when lives are at stake. Furthermore, there is a need for further harmonisation in data standards, interoperability and ensuring data quality is still lacking.

In the case of Autonomous Vehicle Regulation Compliance and QoS Support, recommendations include:

- **Definition of an international regulation and an associated set of drivers** who must outperform both the on-road equipment and the ADAS in order to guarantee the quality of the service.
- Definitions, associated measurement methods and guidance objectives for road-centred parameters
- Definition of the exact metrics (e.g., minimum performance, maximum latency, etc.) that information has to transfer during the handover procedure in cross-border environments. This handover must operate independently of the equipment, vehicle and external factors. It must be possible to ensure that the minimum requirements are met in order to be able to switch from assisted driving to manual driving without risk to users.

5.3. Recommendations from car industry

This section aims to describe the requirements of automated vehicles for cross-border operation by identifying the possible regulation issues that automated vehicle may encounter during soft or hard border crossings and then proposing solutions from the perspective of OEMs. In 5G-MOBIX project, we study five different use cases comprised of advanced driving, vehicles platooning, extended sensors, remote driving and vehicle QoS support that classified under 3GPP trail site 22.186 R16. In this section, we provide the regulation issues that are already identified with additional concerns and respective solutions, as discussed with 5G-MOBIX partners.

It should be noted that a correct choice of an appropriate set of extensible standards and rules still should be made in the context of the working objectives and safety criteria for the system/infrastructure. The UN Economics and Social council and the World forum for Harmonization of Vehicle Regulations has approved in June 2020 the resolution (ECE/TRANS/WP.29/2020/79). The two new UN Regulations, adopted



by UNECE's World Forum for Harmonization of Vehicle Regulations, require that measures be implemented across 4 distinct disciplines:

- 1. Managing vehicle cyber risks;
- 2. Securing vehicles by design to mitigate risks along the value chain;
- 3. Detecting and responding to security incidents across vehicle fleet;
- 4. Providing safe and secure software updates and ensuring vehicle safety is not compromised, introducing a legal basis for so-called "Over-the-Air" (O.T.A.) updates to on-board vehicle software.

The regulations will apply to passenger cars, vans, trucks and buses. They entered into force in January 2021. Despite this and having some guidance related to 5G deployment for connected vehicles and data there is still significant work to be done to have a more harmonized set of standards and guidance's on:

GDPR, recommending to develop a standard to ensure all data sharing complies to GDPR, referring to AP-C100-17 Privacy Impact Assessment (PIA) for Cooperative Intelligent Transport System (C-ITS) data messages. Also, development of guidelines to encourage widespread data sharing while complying to GDPR.

Data Structure & Transmission, recommending to investigate the potential to standardise CAM data structure and data transmission format. The China standard 'GB/T 102-2 Automotive intelligent, networked data structure and transmission format' should be reviewed as a potential basis for this.

Ethics, recommending to investigate potential alignment on Ethics of AI in CAM applications, referring to:

- IEEE P2846: Assumptions for Models in Safety-Related Automated Vehicle Behaviour,
- BS 8611: Robots and robotic devices. Guide to the ethical design and application of robots and robotic systems,
- IEEE P7001 Draft Standard for Transparency of Autonomous Systems,
- CAN/CIOSC 101: Ethical design and use of automated decision systems,

Security, strongly recommend to apply existing security standards to CAM across all member states, including but not limited to:

- SAE J2945/5: Service Specific Permissions and Security Guidelines for Connected Vehicle Applications,
- SAE J₃₀₀₅₋₂ Diagnostics: Permanently or Semi-Permanently Installed Diagnostic Communication Devices, Security Guidelines,
- BS EN 17529: Data protection and privacy by design and by default,
- ISO/TR 4804: Road vehicles Safety and cybersecurity for automated driving systems Design, verification and validation,
- ISO/TR 21186-3: Cooperative intelligent transport systems (C-ITS) Guidelines on the usage of standards — Part 3: Security,
- ISO/DAPS 5112: Road vehicles Guidelines for auditing cybersecurity engineering,
- ISO/IEC 27007: Information technology Security techniques Guidelines for information security management systems auditing,
- ISO/IEC 27034: Information technology Security techniques Application security,
- ISO/IEC 19790: Information technology Security techniques Security requirements for cryptographic modules,





- ISO 20828: Road vehicles Security certificate management,
- ISO/TS 21185: Intelligent transport systems Communication profiles for secure connections between trusted devices,
- ISO/TS 21177: Intelligent transport systems ITS station security services for secure session establishment and authentication between trusted devices,
- ETSI TS 102 731: Intelligent Transport Systems (ITS); Security; Security Services and Architecture.

On the other hand, certain detected gaps, for what there are not current global harmonization or standardization frameworks, are recommended to be covered by:

- Digitalization of highway codes (deciding if these should be incorporated with ODD activities or kept separated) and, related to this, digitalization of traffic rules so this information should be made available for vehicles, then knowing the relevant digital highway code, the corresponding traffic rules could be applied.
- Definition of specific standards:
- To avoid any ambiguity about maturity of development or enabling framework for teleoperation of CAM vehicles;
- To specify CAM vehicle in-use monitoring, including sensor performance is needed (ITU Focus Group on AI for autonomous and assisted driving (FG-AI4AD) – Monitoring in use, and others, have identified this gap);
- To establish a trusted perception from off-vehicle sources (V2X, GNSS, HD maps).
- Definition and commissioning of dedicated testbeds for CAM trialling in real world conditions, potentially in tandem with definition of 5G corridors.
- Harmonisation of EU rules and regulations to facilitate the widespread installation of integrated 5G infrastructure.
- Agreement with European public health organisations on EU 5G EMF limits to avoid controversies associated with exposure to radiofrequency electromagnetic fields, including in relation to 5G, so technology deployment is not jeopardized by not counting on a large public support.
- EU policies in support of the reduction of technological expenses in vehicles. Perception and localization related capital expenditures (CAPEX) are standing as an obstacle for autonomous vehicles to be readily available on the market. Road operators may provide this information. Thus, cost/benefit balance can be ensured for OEMs.
- **Compliance with at least FCC and CE marking regulations**. This should guarantee that the vehicle is able to operate legally in most of the countries.
- Definition of an international regulation and an associated set of test cases that an autonomous vehicle has to pass in order to be authorized to drive on public roads. Similar to EuroNcap test protocols that evaluate the performance of ADAS systems.



- Use of **geo-fencing to restrict the AD functions** to operate only on the operational design domain where they have been authorized.
- Regulations allowing Platooning applications in hard-border crossings to be switched to remote driving by an operator or a cloud, because at hard-border settings platooning should be dissolved for security controls.
- Vehicles on-the-road should **share their safety distance level for emergency braking situations** or other applications and corresponding information.
- **Regulations and homologation processes in different countries should be unified.** Compliance to several regulations can be costly from the perspective of OEMs.
- There should be **unified messaging list for each CAM application and each vehicle should transmit and receive these messages among themselves.** Moreover, since not all CAM applications are supported by each vehicle, the ability to support related CAM application should also be provided as a separate message.
- In case of different traffic laws of neighbouring countries, autonomous vehicle should be capable to adapt its driving condition with the help of the information provided by RSUs and HD maps.
- To increase the speed of the security control process in border settings, additional sensors to monitor the goods on vehicles may be mandatory. Sharing related vehicular information in advance may decrease the inspection time.
- Enabling regulation for the use of Autonomous cars for on-demand transport services in a sustainable Mobility-as-a-Service scheme this can alleviate impact of epidemic and pandemic occurrences such as Influenza or COVID-19.
- CAM applications that are **ensuring safety of VRUs should be mandatory** for all vehicles, because in regions where mostly high-level AVs exist, pedestrians tend to expect AVs to brake automatically. Thus, in case of duality, fatal accidents could emerge as expectations of pedestrians would not meet the ability of vehicle.
- All AVs must be able to **perform safe stop in case an unknown environment** is encountered.
- All AVs should be **reachable by traffic management centres** in order to exchange information to optimize traffic and there should be a specific messaging list for this purpose.
- All hardware and software components of AVs **should be compliant in a global manner**. For example, allowed frequencies for radar and LIDAR sensors should not vary from one country to another as vehicles cross the border.
- Common message sets/protocols dedicated to police interactions shall be standardized in international level for suspicious events.
- Align **infrastructure maintenance entities with map providers** so that whenever the first do changes the second can update its database. Add a **certificate to the map information** so that when it is updated in the car the source can be trusted.




5.4. Questionnaire Results

Task 6.4, in cooperation with T6.1-T6.3, created a first Stakeholder survey, provided in the form of a questionnaire, to gather inputs on the stakeholder motivations, status of cooperation with other stakeholders etc. The online questionnaire was set up by Fraunhofer IAO, using the online survey tool "LimeSurvey", hosted on a server of the Fraunhofer IAO to ensure a high level of data security standards. The questionnaire has been disseminated within the 5G-MOBIX consortium in September 2020. The possibility for contributions has been extended to gather more feedback from the project partners. During October 2020, the questionnaire was also disseminated externally:

- On the 5G-MOBIX website and on social media.
- With the sister projects in ICT-18/ICT-53
- With 5G-PPP, 5G-IA and 5GAA.
- Through the <u>http://connectedautomateddriving.eu</u> news and on their social media.

The following screenshots show the implemented online survey:



Figure 9: Online survey: Start screen.

SG MOBIX	
5G-MOBIX: 5G for cooperative & connected automated MOBIility on X-bo	rder corridors
General Questions	
* What type of stakeholder do you represent?	
Automotive Industry	
Telecommunications operators	
O Road operators	
O Hardware/Software suppliers	
O Regulator or Policy maker	
Academia/R&D centres	

Figure 10: Online survey: General question (Type of stakeholder, company size, the main area of expertise and country).





The question "Type of stakeholder" was used to filter the following questions so that each type of stakeholder gets specific questions. So, it was ensured that the questions fit the expertise of the participants but all answers are stored in one data file. In the following, the questions for one stakeholder are shown.

The questionnaire was opened in two phases. The first phase was only for consortium members to get an initial feedback and in a second phase, it was disseminated in a wider range of potentially several thousand contributors. At the time of the delivery of this document, the questionnaire was still open for inputs.

The results are:

Table 5: Contribution to the questionnaire per stakeholder.

Type of Stakeholder	Number of contributors
Automotive Industry	8
Telecommunication operator	3
Road Operator	6
Hardware/Software suppliers	5
Regulator or Policymaker	2
Academia/R&D centre	28
Sum	52

Further details concerning the experts answering the questionnaire are related to company size, area of expertise and "working country".

Table 6: Contribution	n to the q	uestionnaire	per company	/ size.

Company size	Number of contributors
Up to 10	2
Up to 50	9
Up to 250	15
Up to 1.000	3
Up to 5.000	9
Up to 10.000	4
More than 10.000	9
Sum	52

Table 7: Contribution to the questionnaire per area of expertise.

Area of expertise	Number contributors	of
Technological/Scientific aspects	36	
Regulatory & Compliance aspects	5	
Infrastructure aspects	4	
Security and Privacy aspects	2	
Business aspects	5	
Sum	52	





Table 8: Contribution to the questionnaire per working country, multiple answers were possible via "other".

The answers show that 77 % of the experts are located in Europe and 13 % in China.

For a statistical, a minimum of 100 participants should have been reached. Taking this into account, only a few responses of stakeholders can be used to derive recommendations for the policymakers and regulatory entities. Future activities will thus need to focus more on policymakers and national regulators. Nevertheless, some questions for the group of the Academia/R&D centre will be shown in details as this group is that one with the highest representation in the survey. The first question addressed the main research area of the academia/R&D experts. The main areas are "Connected and Automated Mobility (CAM) Application developer" and "Next-generation Network".



Figure 11: Main research areas of "Academia and R&D experts", N=28.





The "other" main research areas mentioned by the participants are:

- Generic ITS.
- Human Factors (2).
- Education.
- Testing.
- 5G non-terrestrial network convergence.
- Intelligent infrastructure for automated vehicles.
- Machine Learning.

The experts were asked: "What technical/scientific challenges do you foresee for 5G-CAM?". The following tables show, that major challenges are seen in Interoperability and Cybersecurity.

Table 9: Technical/scientific challenges foreseen by the "Academia/R&D-experts".

Technical/scientific challenges	o - not a challenge	1	2	3	4	5 - major challenge
Computational complexity	3	1	8	7	6	3
Algorithmic complexity	1	3	7	7	6	4
Hardware complexity	1	3	9	10	3	2
Decision Support	1	2	6	6	8	4
Scalability of the architectures to a massive deployment	0	1	3	5	11	8
Cybersecurity	0	0	2	8	5	12
Interoperability	0	0	2	3	10	12
Standardization	0	2	5	6	6	9
Validation	0	1	3	12	6	6

The experts from the academia and R&D sphere were also asked what kind of funding for research and development in 5G/CAM they are receiving. The following figure shows, that the main funding resources coming from European and national side.





Figure 12.: Funding resources of "Academia and R&D experts", N=28.

Another topic in the survey was concerned with the relation of resources dedicated on the one hand (Question: "What type of resources does your organisation dedicate to research and development in 5G/CAM?") and lacking on the other hand (Question: "What type of resources are lacking in your organisation regarding research and development in 5G/CAM?") regarding research and development in 5G/CAM. The following figure shows the answers:

Resources for Research and Development in 5G/CCAM:





Figure 13.: Dedicated and lacking funding resources of "Academia and R&D experts", N=28.





The experts were asked, "How can the Academia/R&D Centres better provide their contribution to 5G-CAM?". As the following figure shows, participating in projects is the most mentioned option. One expert mentioned an "other" idea which is "Development of Standards".

Three more questions addressing motivation, expectations and barriers of 5G/CAM research in the sphere of academia and R&D.

The top-rated motivation factors are "Scientific interest" followed by "Part of my organisation's research" as the following table shows.

What is the main motivation for being part of 5G/CAM research?	1 - low motivation	2	3	4	5 - high motivation
Profit (N= 25)	10	8	4	3	0
Department/Lab mission statement (N= 26)	1	2	10	8	5
Scientific interest (N= 27)	1	0	2	11	13
National Mandate (N= 25)	6	7	8	4	0
Part of my organisation's Research Strategy (N= 27)	0	1	2	13	11
Networking (N= 26)	0	5	11	5	5

Table 10: Main motivation by the "Academia/R&D-experts".

Under the expected gains of 5G/CAM research Demonstrations get the highest values:

Table 11: Main gains expected from research in 5G/CAM by the "Academia/R&D-experts".

What do you expect to gain from participating in 5G/CAM research?	1 - not likely	2	3	4	5 - very likely
Scientific publications (N= 28)	0	5	9	6	8
Demonstrations (N= 28)	0	1	5	11	11
Dissemination events (N= 26)	0	4	6	8	8
Creation of IP (N= 27)	3	7	9	5	3
Profits resulting from IP, Patents or any other knowledge-based asset (N= 25)	4	9	9	3	0
Creation of spin-off companies (N= 25)	7	9	6	3	0
Attracting more researchers (N= 27)	0	5	12	4	6

Asked about main barriers in the field of 5g/CAM research, procurement costs are mentioned with the highest rate, followed by access to experimentation facilities.





What are the important barriers hindering 5G/CAM research?	1 - not a factor	2	3	4	5 - major barrier
Cooperation with other stakeholders (N= 26)	1	10	7	6	2
Access to experimentation data (N= 27)	4	5	6	11	1
Access to experimentation facilities (vehicle testing sites, etc) (N= 27)	2	6	4	11	4
Access to experimentation infrastructures (5G, Cloud, High Performance Computing etc.) (N= 28)	3	5	7	8	5
High costs for vehicle/hardware/software procurement (N= 26)	1	1	6	8	10
End-to-end experimentation requires varied skills (N= 26)	1	1	12	8	4
Skills/Knowledge not present in my organisation (N= 25)	5	10	8	2	0
Acquiring licenses (spectrum, use of road etc.) (N= 27)	2	9	8	3	5

Table 12: Main barriers in 5G/CAM research by the "Academia/R&D-experts".

Also, the intensity of cooperation of the academic/R&D organisations was part of the survey. The six answer options of the question were single choice, so that "cooperation in major work and projects" had to been understood as the highest form of cooperation, including the other forms. The answers show that the cooperation with the National Regulators has the lowest intensity.

Table 13: Cooperation with other stakeholders by the "Academia/R&D-experts".

Does your organisation cooperate actively with other stakeholders in 5G and/or Connected and Automated Mobility (CAM)?	o - no cooperati on	1 - minimal cooperation and we are interested in increasing communicat ion	2 - active channels of communicat ion	3 - cooperati on in joint policy shaping	4 - active cooperati on through bilateral agreeme nts	5 - cooperati on in major works and projects
Other road operators (N= 27)	3	5	6	2	4	7
Local government (N= 26)	0	6	7	3	4	6





Automotive manufacturers (N= 27)	2	4	6	8	1	6
Mobile Network Operators (telcos) (N= 27)	0	3	5	7	4	8
National Regulators (N= 27)	0	10	6	6	3	2

The question if and how the organisations of the academia and R&D take into account the effects of crossborder scenarios in your research was the last specific question for this stakeholder type. The answers are listed below and show that the status of cross-border scenarios is mainly on second-highest level.

Table 14: Status of cross-border scenarios in research by the "Academia/R&D-experts".

Does your organisation take into account the effects of cross-border scenarios in your research?	o - Does not apply to my organisation	1 - No, we are not taking into account cross- border scenarios	2 - No, but we are aware of the issues	3 - Yes, we are actively researching safeguards for our products	4 - Yes, we already have presented research results
Service Continuity	1	1	7	11	7
Data Protection	4	3	10	4	5
Management and Orchestration	2	1	7	11	4
Service and Data Migration	2	4	6	9	4
Ressource allocation	3	2	8	11	2
Spectrum allocation	6	4	9	5	2
Vehicle development	5	6	9	5	1

The eight experts from the automotive industry answering the survey are the second-largest stakeholder group. Far away from statistical representativeness, a few spotlights to their answers are listed below:

- Asked about the technical maturity of eleven areas, "Remote driving" was the item with the highest
 rating of "least mature". All other areas (Advanced, Automated Driving, Quality of Service, Platooning,
 Continuity of Vehicle-to-Everything (V2X) connectivity, Cybersecurity & Data Protection, Driving
 Safety, Issue Traceability & Accountability, Service continuity, Automated Fleet Management, Device
 Synchronisation) were rated less clear. The areas with the highest rated maturity were "Automated
 Fleet Management" and "Continuity of Vehicle-to-Everything (V2X) connectivity".
- Concerning the **technical priority** of these areas, "Driving safety" get the highest rating, followed by "Cyber Security, DataProtection" and Issue Traceability & Accountability.



- The top **motivation factor** for new investments in CAM development is "New Trends" and "Improving the company's position in the market for automated professional vehicles".
- When asked "What criteria do you think should be **unified between the different countries** to avoid problems for connected and autonomous driving through the different countries?" "Cybersecurity" and "Data Quality and reliability" were highest rated.
- As the most important barriers hindering technical developments in 5G and CAM "Critical/Real-time nature of applications" followed by "Safety" were mentioned.
- To the question "What is the expected role of Artificial Intelligence in the deployment of CAM technology?" the following answers were given by the Automotive Industry experts:
 - Autonomous driving technology.
 - Object recognition is key.
 - Al may have an influence on the quality and the efficiency of realization and deployment.
 - Provides safe options for decisions to driver and vehicles, liberates driver full attention to driving tasks, eliminates human accident factors.
 - Al will be the primary technology in finding solutions and making decisions, but will always need to be backed up by sanity checks based on "classical" algorithms.
- The experts were also asked how their organisations ensure trustworthy Artificial Intelligence by taking measures for privacy, accountability, non-discrimination and fairness. The answers were:
 - No clue yet.
 - We ensure these aspects by incorporating them in the projects and proposals.
 - Through a global certification program.
 - We are actively involved in several research projects to render AI trustworthy and ensure privacy.
- The last questions were about major regulatory gaps and barriers regarding automated vehicles. These are the answers:
 - The main gap we see it the diversity between countries. Bridging this gap means getting regulatory bodies from several countries in one single line which takes time.
 - implementation of 5G in all geographical areas, today is up to the operator to deploy...needs for automotive is just one, not necessarily the 1st priority for them.

At the end of the survey, all the experts of all stakeholder types were asked to give free comments (Question: "If there are any important remarks you would like to make regarding 5G/CAM that have not been addressed in the survey, please leave a comment:"). Six of the 52 experts gave the following answers:

- Great survey, was a pleasure to fill it.
- We see that interoperability is a major issue currently in Europe. As an example, we see that the current C-ITS PKI is limited to short range connectivity, that message types are not properly standardised (e.g.,





not backwards compatible or versioned), no proper standardisation going on for long range message exchange. With the current implementation rate, it will take a long time before we come to a suitable CAM infrastructure.

- We consider it very important to establish a permanent mechanism for the dissemination of best practices, implementations, lessons learned in Europe and internationally.
- The survey does not account for technology companies who are not in the 'regular' CAM eco-system but who are driving a lot of innovation who are driving innovation in CAM as well as the deployment of 5G system. Equally the survey does not address the aspect of 'digital connectivity provider' (as per 5G-PPP vision) that would orchestrate the 5G connectivity through the use of MNO, 5GSA owned by road infrastructure, infrastructure hosted by cities, other non-terrestrial networks. It comes across that MNOs are considered to be the connectivity provider - which is not the case for CAM to scale, resilience and reach.
- Regulation shall apply to data but also on services for sharing, requesting, searching this data.
- I'm concerned about the compatibility between ITS-G5 and the 5G-C2X standards. Standardization bodies are spending too much time articulating a satisfactory solution for both technologies.

5.5. Four Questions to Stakeholders

In addition to the questionnaire for widespread participation, four Questions were selected for dedicated short interviews with stakeholders to supplement the Questionnaire and provide additional feedback from Commercial partners and all the CBC countries. The feedback gave additional 12 contributions for the recommendations with a special focus on the X-border issues and the 5GMobix program.

The four questions are:

- 1. What is your implication in automated driving and the view on 5G in your company or research institutes?
- 2. Which are the most challenging issues related to 5G for CAM in your perspective and which are the one related to your work or research activity?
- 3. How would you prioritize these challenges and what can be done from the policymakers and regulatory entities to overcome these challenges?
- 4. How can 5GMobix influence the regulatory entities and policymakers to overcome these issues?

The main statements are listed in the following part.

A selection of answers to the questions: "Which are the most challenging issues related to 5G for CAM in your perspective and which are the ones related to your work or research activity?"

- 5G coverage and access to the network, also in X-Border (avoid coverage gaps).
- Definition of standards and use cases contributing to improving safety, traffic efficiency and environment.
- Definition of Test Method and Certification Programs for Conformance, Interoperability, Cybersecurity and Applications (use cases).
- Investment in infrastructures (MNO, Road, etc.).





- Achieving trust of final users.
- Possibility to make edge cloud processing of sensor data.
- Including the social and environmental impact.
- Scalability from test to large scale implementations.
- Implementation of security.
- Definition of responsibility boundaries of different stakeholders (e.g., safety-related information management).
- Interoperability of users with different network operators (roaming).
- Business plan behind 5G coverage in non-urban motorways, including X-Border scenarios.
- Service continuity.
- Align Spectrum allocations.
- Alignment of signalling, RSI and road maintenance between countries.
- Establish a common roadmap.

A selection of answers to the questions: "How would you prioritize these challenges and what can be done from the policymakers and regulatory entities to overcome these challenges?"

- Definition of standards and use cases contributing to improving safety, traffic efficiency and environment.
- Definition of Test Method and Certification Programs for Conformance, Interoperability, Cybersecurity and Applications (use cases).
- Align Spectrum allocations.
- Create legislation to not only eliminate the costs of roaming, as well as simplify and encourage the interoperability between network providers.
- Incentivise mechanisms to overcome the challenges of having different network and app providers collaboration.
- Define stakeholder's responsibility.
- provide a landscape rules definition about the operational deployment of roads.
- Automakers should publish a clear development plan, showing their milestones commitment related to technology adoption.
- Definition for rules about the operational deployment (ex: regulatory operational rules, which roads to start to equip, in which time frame, which funding...).
- Definition of liability borders and 5G-CAM service minimum required standards.

A selection of answers to the questions: "How can 5GMobix influence the regulatory entities and policymakers to overcome these issues?"

• 5Gmobix can influence prioritizing the more relevant use cases, defining the architectures and elements involved in real deployment and establishing the test methodology to verify the final objectives across the borders.



- Through the activities carried out in WP6 and 7, the recommendations for deployment will be proposed and communicated by subject matter experts.
- Thanks to the 5G-MOBIX project, policymakers and regulatory entities can become aware of these problems and work in this area can gain momentum.
- 5G-Mobix should communicate the good results in proving 5G technology in CAM use. It is also important to engage the decision makers in this, so they understand what is needed for wide adoption and the potential benefits the technology has in the ODD. Participation in interest groups where lobbying is an activity can be beneficial, so the focus on transport nodes and routes remains high.
- Increasing awareness of the issue and proposal for setting up working groups.
- Should provide studies and solutions to propose for the decision makers, taking into account the relevant aspects of the different sector stakeholders (Regulatory Entities (Transport and Telecom), Road Administrations, Automakers, Telecom Operators, Telecom Industry...).
- 5G-MOBIX can mainly contribute by sharing the knowledge acquired during the deployment of the cross-border solutions and the execution of the trial tests, and also by participating and influencing the work carried out in different working groups and standardization bodies.
- 5G-MOBIX may help to identify required information to be shared for specific use cases and can implement those use cases to test the viability.
- As in many other areas, the regulatory entities should enforce the usage of open standard protocols in order to ensure the interoperability of the different systems.
- 5GMobix should work with the regulatory entities to create the specifications (protocols) that should be mandatory in all EU and to define a rollout timetable.
- The experience and results obtained through the 5GMobix usage of the existing open standards can provide good arguments for their enforcement by policymakers.
- 5G-MOBIX could use its set of CAM use cases (eventually extending it) and determine where the use cases would apply in terms of motorway sections/locations (like intersections, service and rest areas, etc.). It would be important to understand if all motorway locations would need 5G coverage or if it would suffice to cover a small portion at specific critical locations. This would enable planning 5G investments and future endeavours in a much clearer manner.
- The Project should share its development results and challenges that are faced during these development periods with regulatory entities and policymakers in detail. Additionally, try to help to set up a common understanding of developed applications.





6. CONCLUSIONS

The objectives of the deliverable D6.4 were to monitor activities related to deployment and Cross-Border issues to identify challenges and analyse the issues and challenges detected. Then put them into an effective discussion procedure resulting in actions to mitigate and address those challenges for the relevant bodies and organizations. The 5G-MOBIX experiences is used to provide concrete results and recommendations in supporting of issues identified. The project is used as an effective platform for the dissemination of these results, by liaising with relevant organisations and regulation platforms in support of regulatory, legislative, operative and industry processes.

The main instrument for monitoring ongoing activities on cross-border deployment issues was a questionnaire designed to facilitate the communication between experts and professionals in the areas of infrastructure, telecommunications, automotive industry and road operations. It has provided with an overall view of the technology, infrastructure, regulatory framework and business potential for the CAM and 5G technology, thanks to the contributions from consortium members, related 5G projects and project partners' own networks. T6.4 partners also provided their inputs through a participatory process, where they could relate policies and concerns based on their expertise.

Short analysis of the answers to the questionnaire, as well as additional input and analysis from ongoing and recent initiatives have resulted in the identification of the following challenges, and mainly the lack of a regulatory framework for CAM solutions and vehicles, involving a common European understanding on necessary digital infrastructure, a joint telecom/vehicle industry approach on supporting CAD, awareness on interoperability issues and cross-border items, a common European Security & Safety validation, and the need for a progressive adaptation of road traffic rules in Member States. This lack of regulation is identified as being addressed by different initiatives (ARCADE, CAM platform, HEADSTART, CARTRE, and more), focusing on addressing different aspects that could support the transition towards that missing regulatory framework.

The major technical aspects being addressed include V₂X communication technologies and performance items, service and application requirements (coming from C-ITS specifications after Day 1, Day 2 and Day 3 services), and most importantly, Cybersecurity, Privacy and Digital infrastructure aspects for CAM.

A specific analysis on different regulatory items and their potential relation to 5G-MOBIX is carried out as well in the document:

- GDPR, and the implications for cross-border operations.
- Non-discriminatory practices.
- Vehicle safety, or rather the lack-thereof of regulation on this aspect for highly automated and connected vehicles.
- European electronics Communications Code, and specifically, the IoT/M2M service needs.





- Roaming, and the obvious implication for Cross Border 5G CAM applications and scenarios.
- Open Internet, and the implications for Cross Border CAM solutions providers.
- Critical Infrastructures and Law enforcement and the relation with 5G CAM cybersecurity operations and liability.
- Radio Equipment and conformity in wide-spread 5G CAM scenarios.
- Certification as the step following up-regulation and one of the basic mechanisms to ensure interoperability, of particular relevance in Cross Border CAM scenarios.
- CE RED compliance and associated harmonized standards applicable (Electrical Safety, Health, EMC, Radio spectrum).
- Privacy certifications (PrivacyTrust, HITRUST).

Once the major issues and action areas were identified, the entities and frameworks with the potential to address these areas were also identified. In general, the EC is supporting the deployment of CAM with the development of policies, initiatives and roadmaps; supporting the development of European standards, co-funding research and innovation projects and pilots and introducing relevant legislation and regulation.

The specific initiatives by which these actions are articulated are, amongst others, the following:

- The '5G for Europe Action Plan' defining the roadmap for connectivity strategies. It involves all stakeholder, private and public, in all Member States of the EU, to meet the challenge of making 5G a reality by the end of 2020.
- The 'Europe on the Move' for mobility strategies
- The European 5G Observatory for monitorisation on the implementation of the 5 Action Plan
- 5G Cybersecurity toolbox
- 5G Cross-Border corridors for CAM initiatives
- 5G Strategic Deployment Agenda for Connected & Automated Mobility
- 5GPPP as a major R&D framework for 5G initiatives
- CEF/CEF2 as funding instruments for infrastructure investments in Europe
- C-ITS platform, focused in its day in an integral view of the Cooperative ITS environment and solutions, from technologies to business and societal impact, and several of the results are being carried on to current standardization activities and certification procedures.

Finally, as the feedback from the final survey has been collected, some preliminary findings on the challenges and way to address them via the identified mechanisms and frameworks have been developed as guidance on discussion topics and necessary guidelines for future regulation and policy for 5G CAM.

Selected recommendations from OEMs & Software suppliers are considered of relevance in the sense that information and data exchanges and therefore their access and interoperability become increasingly important, and can be seen as valuable by themselves.





Selected recommendations from the road operators are of relevance in the sense that the introduction of automated vehicles in public road networks is a challenge for the operators in the relation between infrastructure and road users. Amongst others, the feedback focused on aspects such as better definition and specification of infrastructure (physical and digital) autonomous-readiness-level. It shall involve also infrastructure-based information and support for AV manoeuvres, support for traffic law compliance dynamic mapping and data exchanges for vehicles, traffic management and safety concerns in different scenarios -platooning, remote driving, human failure, higher AV levels security and privacy issues in an increasingly monitored environment, and support for backwards compatibility of higher-level AV functions.

Selected recommendations from car industry. Of relevance in relation to the requirements of automated vehicles for Cross-Border operation. Amongst others, the feedback focused on aspects such as the cross-border issues from multiple angles, from harmonization of application messages and information exchanges to regulation and homologation processes, to traffic law compliance for cross-border applications, to support for monitoring goods to facilitate border security control. These topics, as well as in-vehicle data access, as well as other sensitive information exchanges, are long-standing discussion issues from the car industry.

Other highlighted results involve selected recommendations from network operators, recommendations related to remote driving, and recommendations related to QoS for the users.

As these recommendations can be seen as requirements and needs from operative entities in the 5G CAM environment, these can be interpreted in the other hand as recommendations for the sanctioning bodies (policy makers and regulatory authorities). As per the requirements identified during the task, it is possible to categorize the recommendations for these bodies in the categories of:

- Telecommunications (e.g., roaming, continuity in mixed coverage scenarios and cross-border interoperability issues).
- Applications (e.g., stability of communications performance, data structures consistency across logical entities, scalability issues, positioning accuracy issues).
- Security and data privacy (e.g., Trusted entities and certification of elements related to information processes).
- Regulation (e.g., AV regulation compliance and neutrality in remote driving, law enforcement for AVs).

Deliverable D6.4 presents a complete cycle of requirements for EU policies and regulations gathering, analysis, target group and framework identification, and finally a synthesis exercise. This has resulted in a first step in a comprehensive overall view on the major issues that are of concern to the relevant stakeholders in the deployment of 5G CAM solutions. In the second step, the main result has been the identification of all those entities that could address in a relevant way these issues and the mechanisms and initiatives by which these are being currently addressed, and the production of recommendations and guidelines that should serve as support for the further development of these mechanisms and initiatives.





This would ensure that the needs and requirements of the stakeholders are met, and all within the proper regulatory and policy frameworks.

As future steps, T6.4 will communicate the results to the related stakeholders, through all available dissemination and communication channels. An update of this recommendations will be given after completion of the trials by including the experience gathered there.





REFERENCES

- [1] "5G Mobix." https://www.5g-mobix.com/ (accessed May 11, 2023).
- [2] "CORDIS." https://cordis.europa.eu/project/id/724086 (accessed May 11, 2023).
- "Position Paper on Policy and regulatory needs." CARTRE, p. 6, 2018, [Online]. Available: https://knowledge-base.connectedautomateddriving.eu/wpcontent/uploads/2019/08/181016_Position-Paper_Policy_Regulatory_Harmonization.pdf (accessed May 11, 2023).
- [4] "Regulations and Policies." https://knowledge-base.connectedautomateddriving.eu/regulationand-policies/ (accessed May 11, 2023).
- [5] E. Working, "Connected Automated Driving Roadmap." p. 56, 2019, [Online]. Available: https://www.ertrac.org/wp-content/uploads/2022/07/ERTRAC-CAD-Roadmap-2019.pdf (accessed May 11, 2023).
- [6] E. Commission, "STRIA Roadmap on Connected and Automated Transport." p. 164, 2019, [Online]. Available: https://trimis.ec.europa.eu/sites/default/files/roadmaps/stria_roadmap_2019connected_and_automated_transport.pdf (accessed May 11, 2023).
- [7] E. Commission, "Transport in the European Union." p. 171, 2019, [Online]. Available: https://trimis.ec.europa.eu/documents/transport-european-union-current-trends-and-issues-o (accessed May 11, 2023).
- [8] "Project Deliverables." https://www.headstart-project.eu/results-to-date/deliverables/ (accessed May 11, 2023).
- [9] A. coalition Experts, "Proposal for a Recommendation on Cyber Security." p. 4, 2020, [Online]. Available: http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/GRVA-05-16e.pdf (accessed May 11, 2023).
- [10] Marta Tobar and E. Martinez, "ENSEMBLE regulatory framework." p. 67, 2020, [Online]. Available: https://platooningensemble.eu/storage/uploads/documents/2023/03/13/ENSEMBLE-D6.10regulatory-framework---state-of-the-art-FINAL.pdf (accessed May 11, 2023).
- [11] A. Crane and T. Ruebottom, "Stakeholder Theory and Social Identity: Rethinking Stakeholder Identification," J. Bus. Ethics, vol. 102, no. 1, pp. 77–87, 2011, doi: 10.1007/s10551-011-1191-4.
- [12] A. Soua *et al.*, "Deliverable D2.1 5G-enabled CCAM use cases specifications." 2019.
- [13] T. E. PARLIAMENT, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 Da. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016.
- [14] "Directive on privacy and electronic communications," 2002. http://eur-lex.europa.eu/legal-





content/EN/TXT/?uri=celex%3A32002L0058 (accessed May 11, 2023).

- [15] *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications.* The European Data Protection Board.
- [16] COMMISSION DIRECTIVE 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment. THE COMMISSION OF THE EUROPEAN COMMUNITIES.
- [17] Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS).
- [18] C. of the E. U. European Parliament, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). European Parliament, Council of the European Union.
- [19] T. C. O. T. E. UNION, Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation.
- [20] E. C. of F. Rights, Article 8 Protection of personal data.
- [21] E. Communitie, "TREATY OF AMSTERDAM AMENDING THE TREATY ON EUROPEAN UNION, THE TREATIES ESTABLISHING THE EUROPEAN COMMUNITIES AND CERTAIN RELATED ACTS," 1997.
- [22] E. C. European Union, TREATY OF LISBON AMENDING THE TREATY ON EUROPEAN UNION AND THE TREATY ESTABLISHING THE EUROPEAN COMMUNITY. European Union and the European Community.
- [23] the C. of M. of the C. of Europe, *The protection of individuals with regard to automatic processing of personal data in the context of profiling.*
- [24] "Public consultation on the review and prolongation of the Roaming Regulation," 2020. https://ec.europa.eu/digital-single-market/en/news/public-consultation-review-and-prolongation-roaming-regulation (accessed May 11, 2023).
- [25] A. H. J. N. P.A. Nooren, N.W. Keesmaat, A.H. van den Ende, "5G and Net Neutrality : a functional analysis to feed the policy discussion," 2018.
- [26] "UN Regulation No. 141 Tyre Pressure Monitoring Systems (TPMS)." https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-141-160 (accessed May 11, 2023).

[27] "Privacy Trust." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010 (accessed Mar. 13, 2023).

[28] "HIPAA Act" 1996 - https://www.cdc.gov/phlp/publications/topic/hipaa.html (accessed May 11, 2023).



- [29] "5G for Europe Action Plan." https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan (accessed May 11, 2023).
- [30] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS." 2016, [Online]. Available: http://data.europa.eu/eli/dir/2018/1972/oj (accessed May 11, 2023).
- [31] "European 5G Observatory," 2019. https://ec.europa.eu/digital-single-market/en/european-5gobservatory (accessed May 11, 2023).
- [32] "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures," 2020. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468 (accessed May 11, 2023).
- [33] "A TRUSTED AND CYBER SECURE EUROPE." p. 24, 2020, [Online]. Available: https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secureeurope-enisa-strategy (accessed May 11, 2023).
- [34] "Europe on the Move: Commission takes action for clean, competitive and connected mobility," 2017. https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1460 (accessed May 11, 2023).
- [35] "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE, THE COMMITTEE OF THE REGIONS On https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0283 (accessed May 11, 2023).
- [36] "Europe on the Move: Commission completes its agenda for safe, clean and connected mobility," 2018. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_18_3708/IP_18_3708_ EN.pdf (accessed May 11, 2023).
- [37] "HARNESSING THE BENEFITS OF AUTOMATION, CONNECTIVITY AND SMART MOBILITY SERVICES." [Online]. Available: https://transport.ec.europa.eu/document/download/d9b415d2-6554-45f1-9d9b-5ecd8e19bf12_en?filename=mobility-package-factsheet-ii.pdf (accessed May. 11, 2023).
- [38] "Cross-border corridors for Connected and Automated Mobility (CAM)." https://ec.europa.eu/digital-single-market/en/cross-border-corridors-connected-and-automatedmobility-cam (accessed May 11, 2023).
- [39] "New 5G cross-border corridors for connected and automated driving announced at the Digital Day 2018." https://digital-strategy.ec.europa.eu/en/news/new-5g-cross-border-corridors-connected-and-automated-driving-announced-digital-day-2018" (accessed May 11, 2023).
- [40] "5G Strategic Deployment Agenda (SDA) for Connected and Automated Mobility (CAM) -Stakeholder workshop report," 2019. https://digital-strategy.ec.europa.eu/en/library/5g-strategicdeployment-agenda-sda-connected-and-automated-mobility-cam-stakeholder-workshop-report (accessed May 11, 2023).





- [42] "5G PPP." https://5g-ppp.eu/wp-content/uploads/2015/10/5GPPP-brochure-final-web.pdf (accessed May 11, 2023).
- [43] "Connecting Europe Facility." https://ec.europa.eu/inea/en/connecting-europe-facility (accessed May 11, 2023).
- [44] "Five years supporting European infrastructure." 2019, [Online]. Available: https://ec.europa.eu/inea/sites/inea/files/cefpub/cef_implementation_brochure_2019.pdf (accessed May 11, 2023).
- [45] "Connecting Europe Facility (CEF2) Digital." https://ec.europa.eu/digital-singlemarket/en/connecting-europe-facility-cef2-digital(accessed May 11, 2023).
- [46] "DRAFT ORIENTATIONS TOWARDS AN IMPLEMENTATION ROADMAP CONNECTING EUROPE FACILITY (CEF2) DIGITAL." 2019, [Online]. Available: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63665 (accessed May 11, 2023).
- [47] "State of the Union: Commission calls on Member States to boost fast network connectivity and develop joint approach to 5G rollout," 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1603 (accessed May 11, 2023).
- [48] "Estrategia de movilidad." https://esmovilidad.mitma.es/ejes-estrategicos (accessed May 11, 2023).
- [49] "Spain and France step up collaboration in development of automated and connected driving," 2020. https://www.lamoncloa.gob.es/lang/en/gobierno/news/Paginas/2020/20200923driverless-car.aspx (accessed May 11, 2023).