Security, safety and legal issues and plans for 3rd cycle

Project Number:	690705
Classification	
Deliverable No.:	1.6
Work Package(s):	1
Document Version:	V1.0
Issue Date:	29.09.2018
Document Timescale:	
Start of the Document:	06/2018
Final version due:	09/2018
Compiled by:	Mohamed Cherif RAHAL
Authors:	Mohamed Cherif Rahal (VED) Adam Knapp (BIT) Stefan Suck (OFF) Daniel Twumasi (HMT) Fabio Tango (CRF)Iolande Vingiano-Viricel (VDC) Thibault Griffon (PSA)
Technical Approval:	Fabio Tango (CRF)
Issue Authorisation:	Andreas Lüdtke, (OFF)

DISTRIBUTION LIST		
Copy type[1]	Company and Location	Recipient
T	AutoMate Consortium	all AutoMate Partners

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

RECORD OF REVISION

Date	Description	Author
July, 15th, 2108	Document structure and first draft	Mohamed Cherif Rahal (VED)
August, 1st, 2018	V2X section	Adam Knapp (BIT)
Sept. 7th, 2018	Architecture explanation	Stefan Suck (OFF) Daniel Twumasi (HMT)
Sept. 18th 2018	Italian Law analysis	Fabio Tango (CRF)
Sept. 18th 2018	Safety and Fault tree analysis	Thibault Griffon (PSA)
Sept. 18th 2018	German Law analysis	Stefan Suck (OFF)

Content table

List of illustrations

List of Tables

Executive summary

This deliverable D1.6 is an update of the previous D1.2 and D1.4 and it is focused on Security, Safety and Legal Issues.

As showed by the Fault-tree analysis, it is necessary to have a redundancy at the top of the architecture, at least for the most critical components, both hardware (e.g. sensors) and software (e.g. multiply the perception algorithms or the trajectory planning algorithms).

In the section dedicated to the legal aspects, we recall the Vienna convention and the side activities dealing with the autonomous driving. In particular, we present an update of the new European law about the data protection and anonymization of personal data in the field of the General Data Protection Regulation (GPRD). Moreover, the situation for different countries is illustrated as well: we analyse the laws of the experimentations in the three countries: Germany, Italy and France.

The security and privacy related issues are handled by the standard. Therefore, in the commercialisation phase of the products developed during the AutoMate project, the solutions, related to these two aspects, have to take into account the possibilities offered by the standards, to be compatible with the already available products on the market. However, during the AutoMate project security and privacy solutions are minimized to ease the development and integration of V2X components.

At the moment, there is no legislation on what a driver can do if is not driving. In addition, there are no changes to Vienna Convention. Thereby, the driver still holds control of his/her vehicle and commands it in any circumstances, being responsible in case of accident.

Finally, for the personal data protection, according to the new law on GPRD all Member States of the European Union must comply with it regarding their data protection policies, in this field, and since the 25th may 2018 all AUTOMATE experiments has to comply with this law.

1 Introduction

This document is an update of the deliverables D1.2 and D1.4 dealing with the Security, safety and legal issues.

As of technical and safety aspects, we explain in the two first sections the overall architecture of AUTOMATE and propose an analysis of the safety using Fault Trees Analysis. Some recommendations are also given to ease the usage of the TeamMate car by non-experimented users. Some methods for encryption and decryption of the transmitted and received data using car2X communication protocols are thus introduced

The last section is dedicated to the legal aspects, we recall the Vienna convention and the side activities dealing with the autonomous driving. We update the new European law about data protection and anonymization of personal data regarding the General Data Protection Regulation (GDPR) which came into force across the European Union on May 25th, 2018. We finally give an update of the legal aspect, we analyse the law of the experimentations in these three following countries: Germany, Italy and France.

2 Safety of the TeamMate System

This section is dedicated to the technical parts concerning the safety and the security of the TeamMate system. First of all the architecture and details of the fault analysis tree of our system is defined. Then the V2X data protection will be addressed.

2.1 Architecture of the TeamMate

In the following we give a brief description of the currently used TeamMate architecture. A detailed description can be found in D5.1. Figure 1 shows the currently used approach to integrate the Automate enablers together with a given demonstrator platform, i.e., vehicle or simulator.
The TeamMate enablers support different functional steps:

- “data processing & fusion”,
- “interpretation”,
- “planning & actions”.

To the enablers most parts of the existing platform are considered as a black box, meaning the simulator or the vehicle might already have modules performing one or more of the aforementioned functional steps. Though the TeamMate system does not have to know how those internal modules of the existing demonstrator platform work or interact with each other.

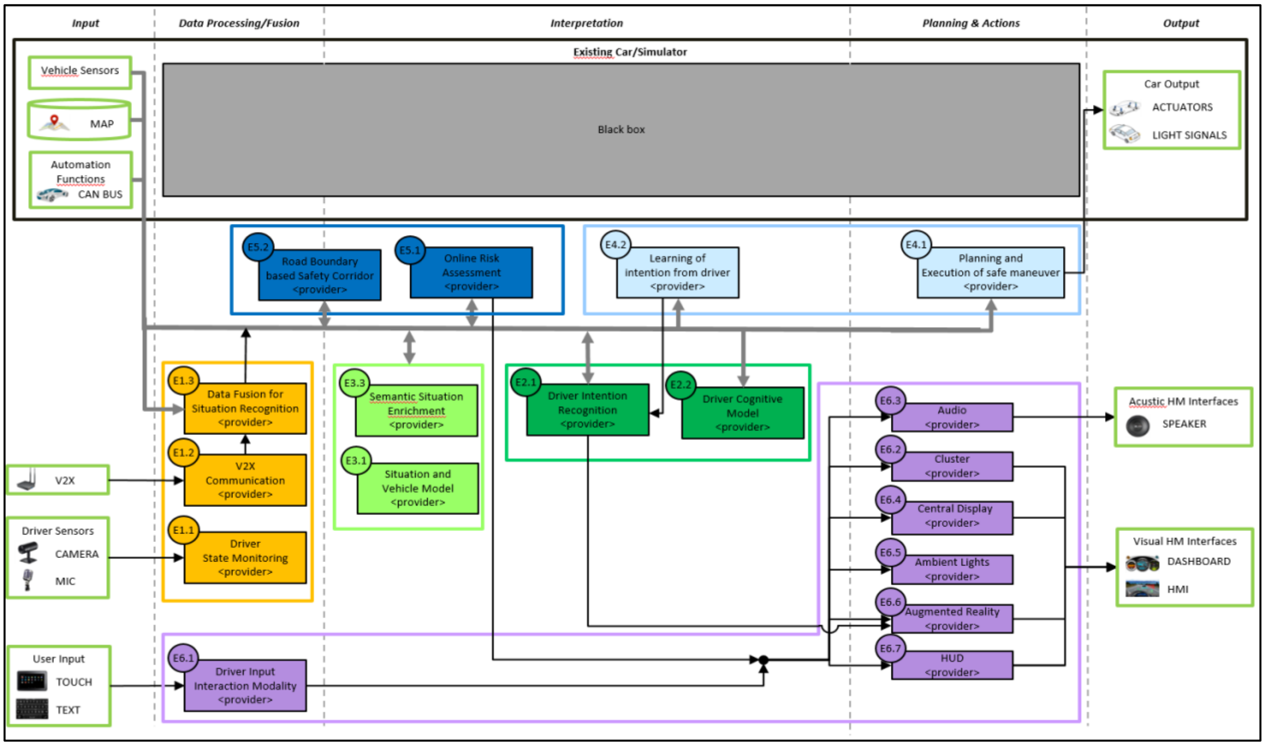
Input
Data Processing/Fusion
Interpretation
Planning & Actions
Output
Existing Car/Simulator
Vehicle Sensors
MAP
Automation Functions
CAN BUS
Black box
Car Output
ACTUATORS
LIGHT SIGNALS
E5.2
Road Boundary based Safety Corridor <provider>
E5.1
Online Risk Assessment <provider>
E4.2
Learning of intention from driver <provider>
E4.1
Planning and Execution of safe maneuver <provider>
E1.3
Data Fusion for Situation Recognition <provider>
E1.2
V2X Communication <provider>
E1.1
Driver State Monitoring <provider>
E3.3
Semantic Situation Enrichment <provider>
E3.1
Situation and Vehicle Model <provider>
E2.1
Driver Intention Recognition <provider>
E2.2
Driver Cognitive Model <provider>
E6.3
Audio <provider>
E6.2
Cluster <provider>
E6.4
Central Display <provider>
E6.5
Ambient Lights <provider>
E6.6
Augmented Reality <provider>
E6.7
HUD <provider>
E6.1
Driver Input Interaction Modality <provider>
V2X
Driver Sensors
CAMERA
MIC
User Input
TOUCH
TEXT
Acustic HM Interfaces
SPEAKER
Visual HM Interfaces
DASHBOARD
HMI

Figure 1: Current TeamMate Architecture

However, for the communication of the TeamMate system with the existing platform it is required that the simulator or the vehicle provides interfaces for certain input and output data.

Input data from automation functions, from maps, and from vehicle sensor are expected to be provided by either the vehicle or the simulator. V2X data, driver sensor data, and user input via touch or text interfaces are further inputs introduced by the TeamMate architecture. The enablers themselves are represented by software components which are dependent on their concerns. A message BUS oriented data exchange between the components is implied to support a communication via one or more channels.

Output interfaces introduced by the TeamMate system are acoustic and visual human-machine interfaces to be delivered to the driver. Furthermore it is required that output interfaces to car actuators and light signals are to be provided by the existing demonstrator platform.

2.2 Fault tree analysis

To build the following Faults Trees, we studied our TeamMate architecture. Three outputs were identified:

- “Car output” with actuators and light signals (Figure1);
- “Acoustic HMI” with the speakers (Figure3);
- “Visual HMI” including dashboard and the HMI in general (Figure5).

Thus, three Faults Trees and three Faults Trees Analysis are brought up.

The first issue "Actuators or Light Signals gives an inopportune or erroneous action" (Figure 2), is directly linked to the box "Planning and execution of safe manoeuvre E4.1". Then there is a series of possible causes, going through several boxes like "Data Fusion for situation recognition" or "Driver Intention recognition", that all come from several inputs that are:

- Erroneous due to the input V2X (5 times)
- Erroneous due to the automation functions CAN BUS (10 times)
- Erroneous due to "Map" (10 times)
- Erroneous due to the vehicle sensors (10 times)

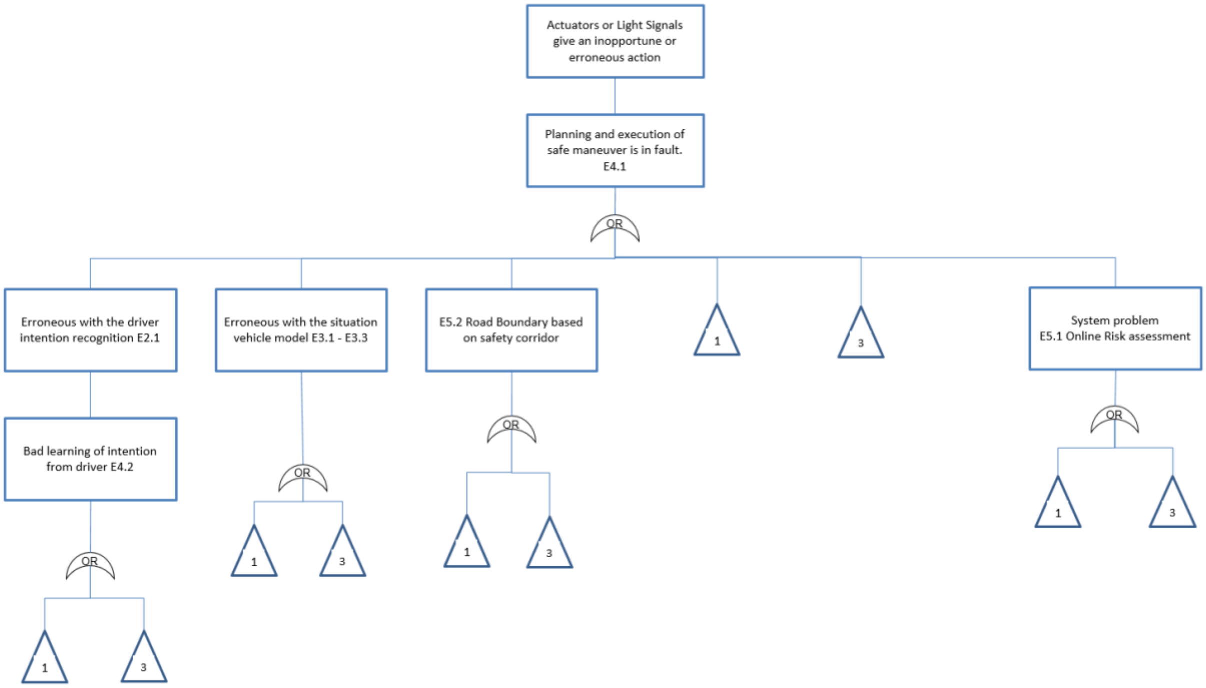
Actuators or Light Signals give an inopportune or erroneous action
Planning and execution of safe maneuver is in fault. E4.1
OR
Erroneous with the driver intention recognition E2.1
Erroneous with the situation vehicle model E3.1 - E3.3
E5.2 Road Boundary based on safety corridor
1
3
System problem E5.1 Online Risk assessment
Bad learning of intention from driver E4.2
OR
OR
OR
OR
1
3
1
3
1
3
1
3

Figure 2, Car output - main part

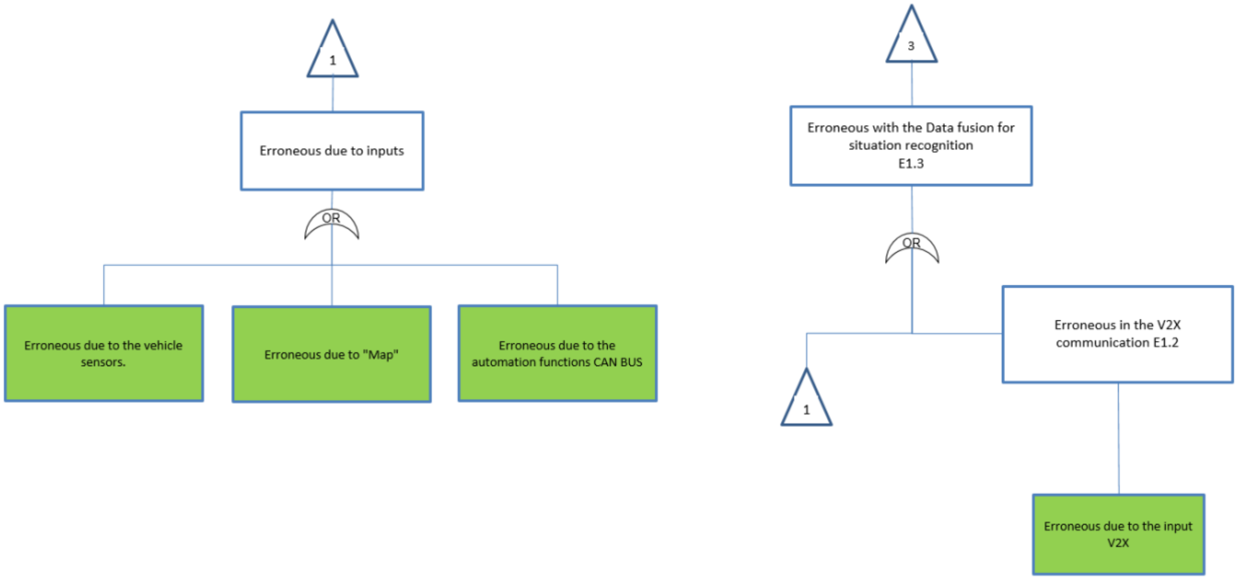
1
Erroneous due to inputs
OR
Erroneous due to the vehicle sensors.
Erroneous due to "Map"
Erroneous due to the automation functions CAN BUS
3
Erroneous with the Data fusion for situation recognition E1.3
OR
1
Erroneous in the V2X communication E1.2
Erroneous due to the input V2X

Figure 3, Car output - subparts

The second issue is related to the "Speaker / acoustic HMI" that does not reflect what it should – Figure 3. This first box is linked to the "Driver input interaction modality" or to the "Online Risk Assessment". Again, there are some boxes to go through to arrive at one of the first inputs, which are the following:

- Erroneous in the transcription of the user's input / text information (1 occurrence)
- Erroneous due to the sensor / touchpad or Keyboard (1 occurrence)
- Erroneous due to the input V2X (1 occurrence)
- Erroneous due to the automation functions CAN BUS (2 occurrences)
- Erroneous due to "Map" (2 occurrences)
- Erroneous due to the vehicle sensors (2 occurrences)

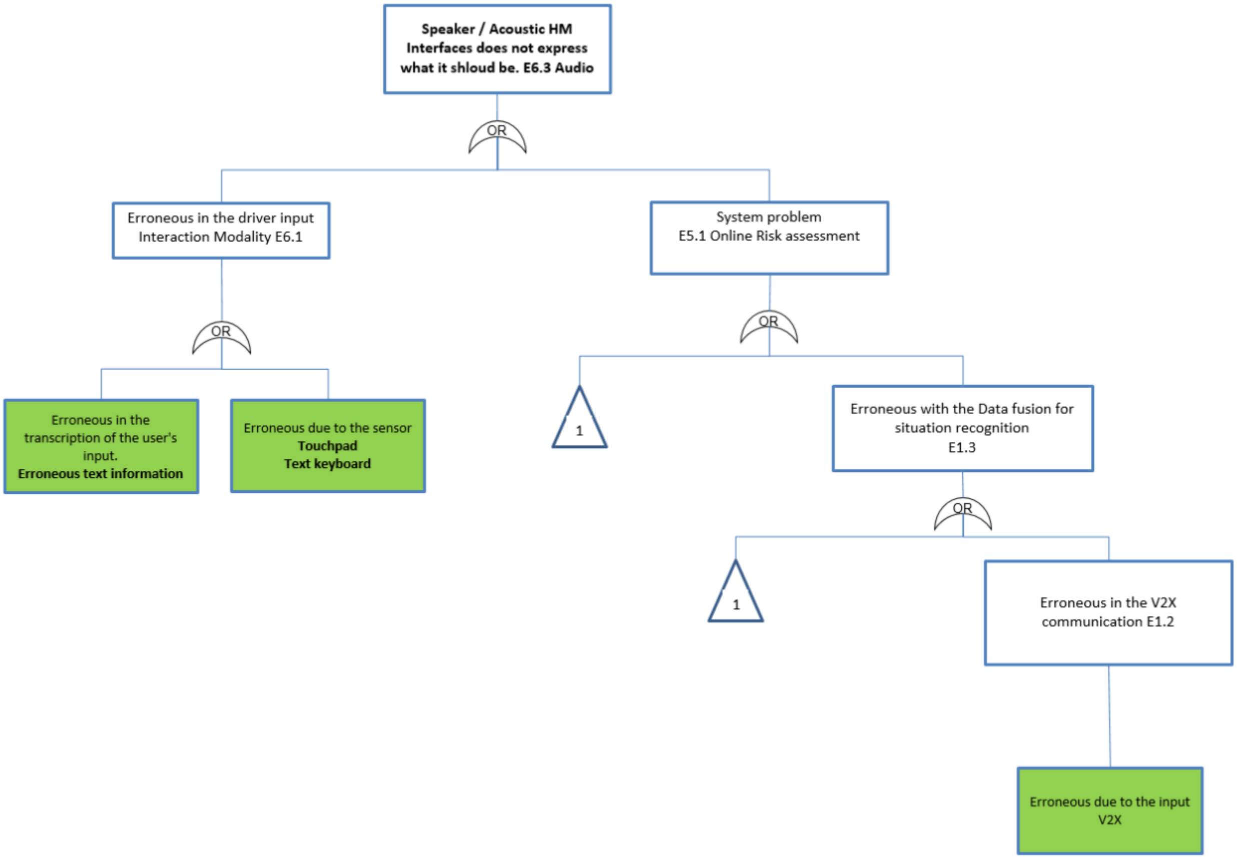
Speaker / Acoustic HM Interfaces does not express what it shloud be. E6.3 Audio
OR
Erroneous in the driver input Interaction Modality E6.1
System problem E5.1 Online Risk assessment
OR
OR
Erroneous in the transcription of the user's input. Erroneous text information
Erroneous due to the sensor Touchpad Text keyboard
1
Erroneous with the Data fusion for situation recognition E1.3
OR
1
Erroneous in the V2X communication E1.2
Erroneous due to the input V2X

Figure 4, Acoustic HMI - main part:

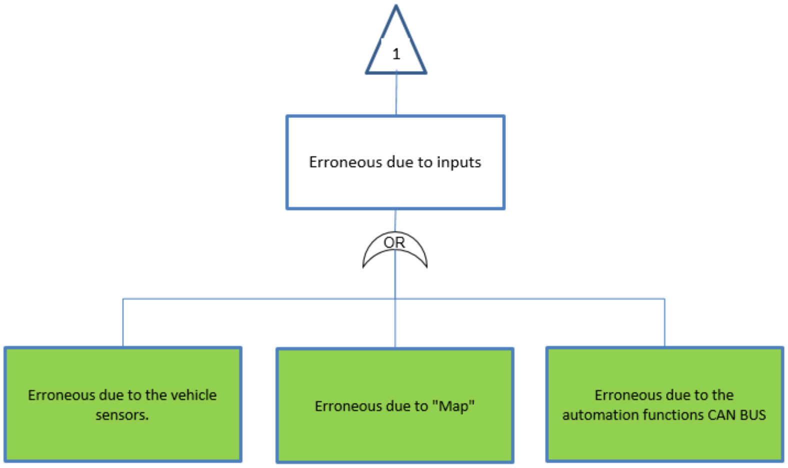
1
Erroneous due to inputs
OR
Erroneous due to the vehicle sensors.
Erroneous due to "Map"
Erroneous due to the automation functions CAN BUS

Figure 5 : Acoustic HMI - subpart 1

Once more, the last issue concerns the “Visual HMI” that does not demonstrate what it should – Figure 5. The tree shows us manifold possible causes. It also ends to the same inputs as the two other trees:

- Erroneous in the transcription of the user’s input / text information (5 times)

- Erroneous due to the sensor / touchpad or Keyboard (5 times)
- Erroneous due to the input V2X (6 times)
- Erroneous due to the automation functions CAN BUS (12 times)
- Erroneous due to “Map” (12 times)
- Erroneous due to the vehicle sensors (12 times)

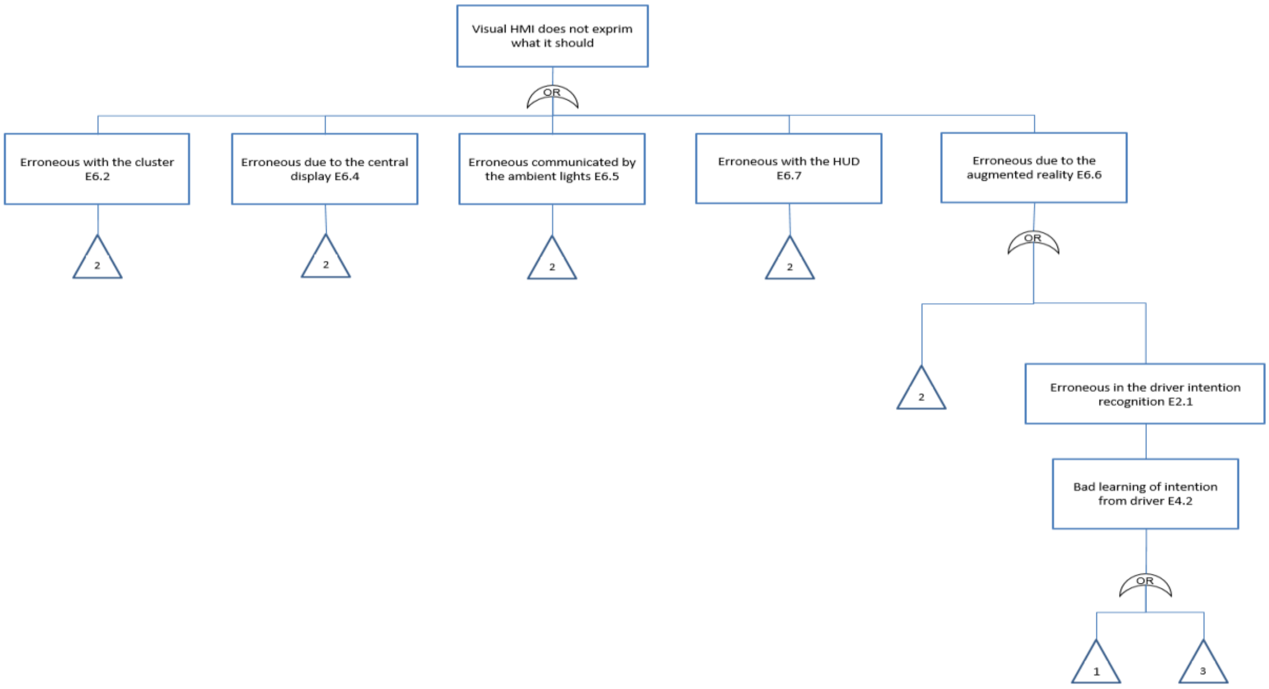
Visual HMI does not exprim what it should
OR
Erroneous with the cluster E6.2
Erroneous due to the central display E6.4
Erroneous communicated by the ambient lights E6.5
Erroneous with the HUD E6.7
Erroneous due to the augmented reality E6.6
2
2
2
2
OR
2
Erroneous in the driver intention recognition E2.1
Bad learning of intention from driver E4.2
OR
1
3

Figure 6 Visual HMI - main part:

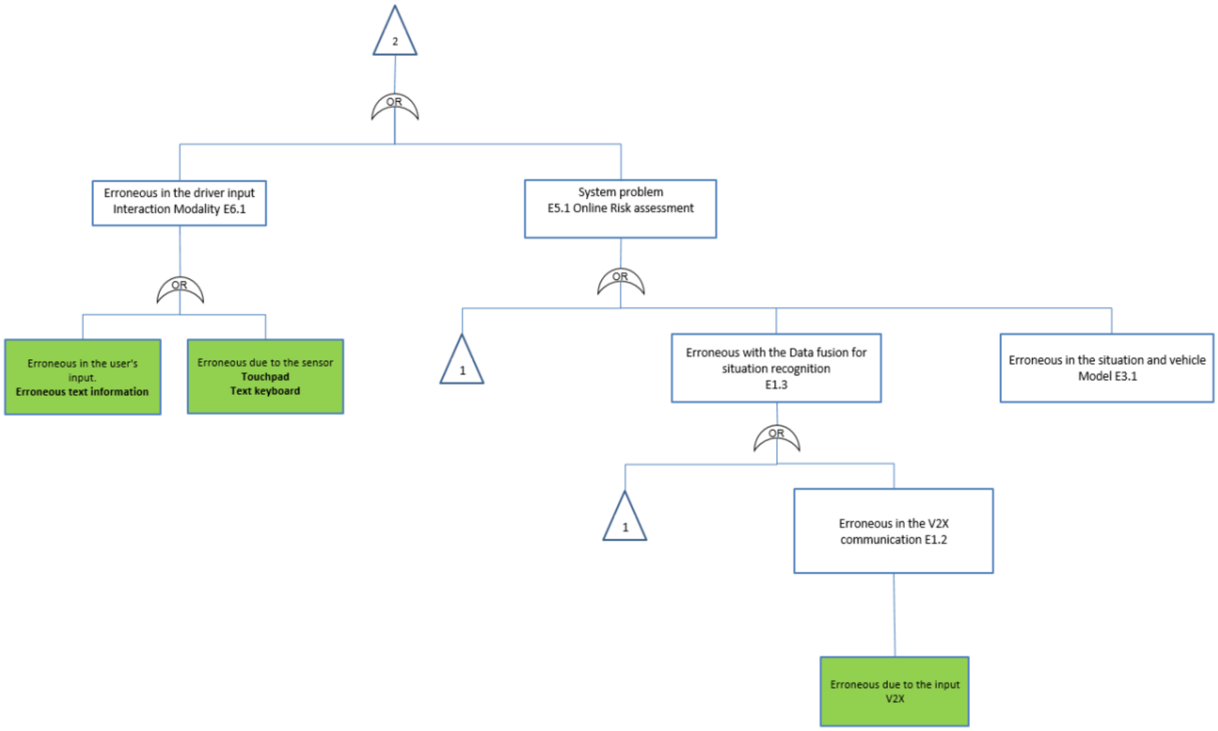
2
OR
Erroneous in the driver input Interaction Modality E6.1
System problem E5.1 Online Risk assessment
OR
OR
Erroneous in the user's input. Erroneous text information
Erroneous due to the sensor Touchpad Text keyboard
1
Erroneous with the Data fusion for situation recognition E1.3
Erroneous in the situation and vehicle Model E3.1
OR
1
Erroneous in the V2X communication E1.2
Erroneous due to the input V2X

Figure 7 : Visual HMI – subpart 2:

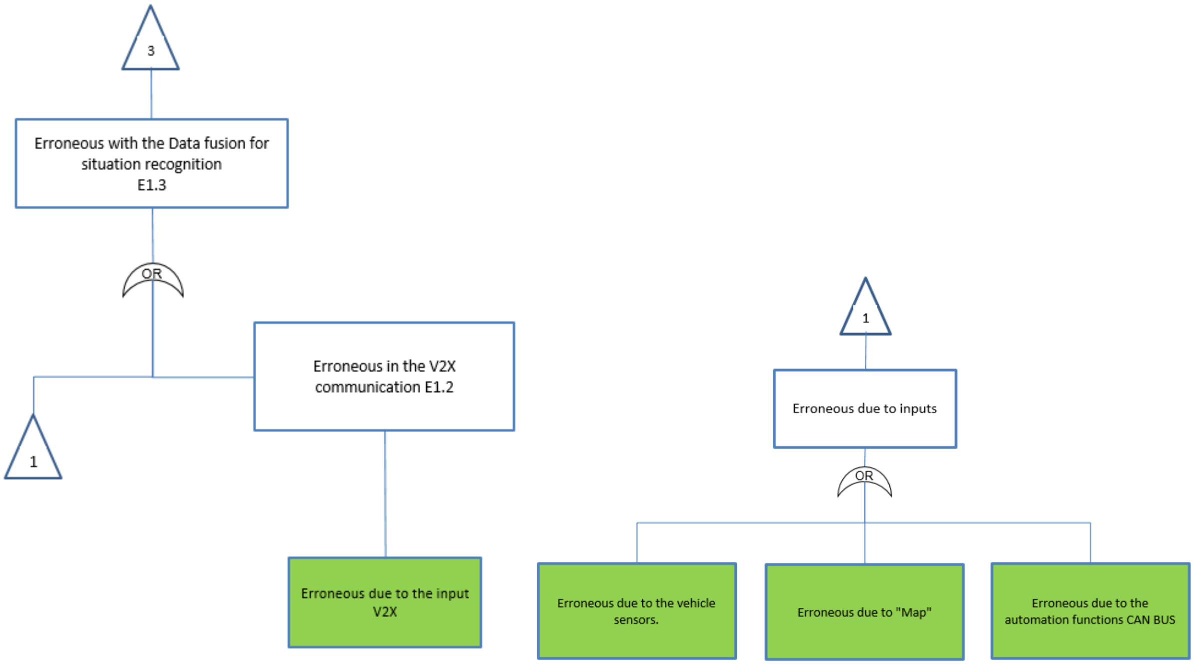
3
Erroneous with the Data fusion for situation recognition E1.3
OR
Erroneous in the V2X communication E1.2
1
Erroneous due to the input V2X
1
Erroneous due to inputs
OR
Erroneous due to the vehicle sensors.
Erroneous due to "Map"
Erroneous due to the automation functions CAN BUS

Figure 8 : Visual HMI - subparts 3 and 1

Regarding safety activities, the most suitable solution is a redundancy at the top of the architecture of the tree. With an “AND” branch it will reduce the risk by two.

Another solution could be to have, at least, control algorithms at the bottom of the trees, for the first inputs, in green in the pictures. The most requested inputs, by occurrences, are the “vehicle sensors”, the “map” and the “automation function / can bus”. Thus, control algorithms should be firstly design for such inputs. If “control algorithms” are not the solution, there is “confirmation frames” or other analysis methods to ensure the safety of the Team Mate architecture.

Besides, such a system failure conditions is a very well established and simple method to make decisions regarding safety validation.

Another part of the architecture is critical regarding occurrences because the “situation and vehicle Model E3.1” is also at the bottom of each tree, as an input can be.

One last concern, regarding safety activities, is the V2X input. This input seems very difficult to control, so cybersecurity and data control should be particularly attentive to this input and should give the appropriate safety barriers.

2.3 Data encryption for V2X system

This section sets forth standards and a state-of-the-art in security and privacy applied to V2X communications. This section is based on the related ETSI standards [1], [2] and a related article [3].

2.3.1 ITS security related concepts

Anonymity is the ability of a user to use a resource or service without disclosing its identity.

Authorization authority provides an ITS-S (Intelligent Transport System Station) with permission to invoke ITS applications and services.

Canonical identifier is a structured identifier who is globally unique, which is similar to the MAC address of a WiFi or Bluetooth device.

Enrolment authority validates that an ITS-S can be trusted and function correctly.

Pseudonymity is the ability of a user to use a resource or service without disclosing its identity while still being accountable for usage.

Unlinkability is the ability of a user to make multiple uses of resources or services without others being able to link these uses together.

Unobservability is the ability of a user to use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

2.3.2 ITS authorities

Trust and privacy management requires secure distribution and maintenance of trust relationships. Public key certificates and Public Key Infrastructure (PKI) are used to establish and maintain trust between the ITS-S and other ITS stations and authorities.

ETSI TS 102 731 [1] defines the following security management roles:

- manufacturers: insert an ITS authoritative identity (canonical identifier) into each ITS-S;
- Enrolment Authorities (EA): verify an ITS Station (ITS-S) as a whole;
- Authorization Authorities (AA): authorize an ITS-S to use a particular application, service, or privilege.

Separation of enrolment (identification and authentication) and authorization has been shown in ETSI TS 102 731 [1] as an essential component of privacy management and provides protection against attacks on a user's privacy. However, it is possible for the EA role to be delegated to the manufacturer and for the EA and AA roles to be assumed by a single authority.

2.3.3 Privacy

ISO/IEC 15408-2 [4] identifies four key attributes that relate to privacy: anonymity, pseudonymity, unlinkability and unobservability.

Anonymity alone is insufficient for protection of an ITS user's privacy and unsuitable as a solution for ITS, as one of the main requirements of ITS is that the ITS-S should be observable in order to provide improved safety. Consequently, pseudonymity and unlinkability offer the appropriate protection of any senders' privacy for basic ITS safety messages (CAM and DENM which are used in the AutoMate project). Pseudonymity shall be provided by using temporary identifiers in ITS safety messages. The station's canonical identifier shall never be transmitted in communications between ITS stations. Unlinkability can be achieved by limiting the amount of detailed immutable (or slowly changing) information carried through ITS safety messages, thus preventing the possible association of transmissions from the same vehicle over a long time period (such as two similar transmissions broadcast on different days).

ITS Privacy is provided in two dimensions:

a) privacy of ITS registration and authorisation signalling:
   - ensured by permitting knowledge of the canonical identifier of an ITS-S to only a limited number of authorities;
   - provided by the separation of the duties and roles of ITS authorities into an entity verifying the canonical identifier known as the Enrolment Authority (EA) and an entity responsible for authorising and managing services known as the Authorization Authority (AA);

b) privacy of communications between ITS stations.

2.3.4 Security of communication patterns and messages

Three V2X communication patterns are defined: broadcast, multicast, unicast. In contrast to the strictly safety-related broadcast applications (CAM and DENM), multicast and unicast applications are supposedly supplied by various providers and can be commercially sensitive. Therefore, the requirements really depend on the specific application and the respective business model.

With the exception of broadcast applications, all other multicast and unicast communications can use either asymmetric or symmetric key systems to provide for Security Association (SA) lifecycle and the related key management (registration, key establishment, updates and removal).

Unicast and multicast applications shall use link layer encryption and regular changes of the ITS MAC addresses to protect the privacy of the ITS-S (and its user) as well as all higher layer information from radio channel eavesdropping.

Broadcast applications such as CAM and DENM require authentication, authorisation and integrity but not confidentiality. Senders of CAM and DENM shall obtain this service by signing with an authorization certificate using the mechanisms of IEEE 1609.2 [5]. Figure **Error! Reference source not found.** illustrates the use of the authorization certificate to sign a CAM or DENM between ITS stations. The "Signer Info" field is a 1609.2 field that contains either the certificate or a reference to it.

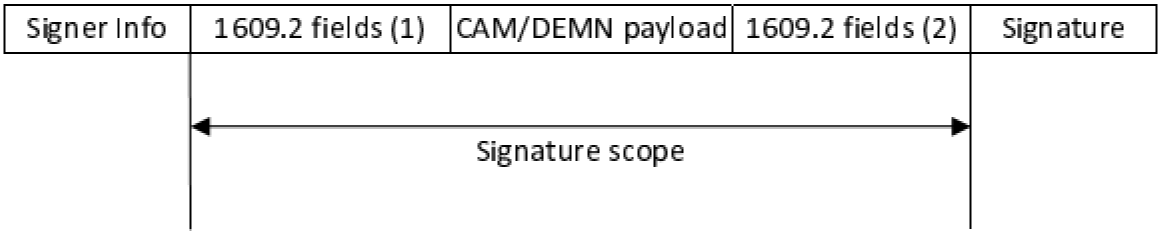

Figure 9 : CAM and DENM signed using authorization certificates [2]

The following table summarizes the security requirements of V2X communication patterns.

Table 1. Security requirements of V2X communication patterns [3]

Security requirement	**Security mechanism**	**Broadcast**	**Unicast**
Confidentiality	Encryption on sensitive messages; randomizing traffic patterns	-	+
Authenticity	Message signature; Trusted hardware module; active detection systems	+	+
Integrity	Message signature and other integrity metrics for content delivery	+	+
Authorization	Certificate accompanying message signature	+	+

Non-repudiation of origin	Message signature	+	+
Anti-replay	Message signature containing verifiable time variant data	+	+
Plausibility verification	Check mechanisms ensured by IEEE P1609.2	+	+
Availability	Pseudo-random frequency hopping; Access control and signature-based authentication	+	+
Privacy	Pseudonymity, unlinkability; ID-based system for user privacy	+	+

3 Legal issues

This section is an update of the recent paper entitled "D1.2 - Security, safety & legal issues" written in December 2016.

3.1Vienna Convention and side activities

There is no important modification to observe in the regulation (national nor international) that requires a review but the three main topics regarding the Vienna Convention (3.1), the European General Data Protection Regulation (hereafter "GDPR") (3.2), and the latest French Decree regarding the testing of automated vehicle on the public roads (3.3).

There is currently no legislation on a driver's distracting activity while driving. Indeed, such actions are allowed by default if the driver still holds control and command of his vehicle in any circumstances.

Still, proceedings in Geneva by the WP1 task force are currently studying the possibility of doing such side activities with an in-vehicle system[2]. Such studies would set two conditions to allow a driver to be hands-free:

1°) those side activities do not stop the driver to take control and command of the vehicle if the in-vehicle system requires it;
2°) those side activities must be compatible with the use and functioning of the in-vehicle system.

The informal paper will be discussed on September 2018 and a report should be published forthwith after.

[2] http://www.unece.org/fileadmin/DAM/trans/doc/2018/wp1/ECE-TRANS-WP1-INF-May-2018-1e.pdf

For now only one activity is strictly forbidden by the Vienna Convention: “the use by a driver of a motor vehicle or moped of a hand-held phone while the vehicle is in motion” (Vienna Convention, art. 8 §6). The Vienna Convention is a minimum requirement to observe and Member States can have a restrictive approach. For example, in France, the use of a mobile phone while driving is ruled in the French Road Code “The use of a hand-held telephone by a driver of a vehicle in traffic is prohibited” (art. 412-6-1).

On January 23rd, 2018, this rule was emphasized by a decision of the French High Court of Justice regarding civil and criminal matters (Cass. Ch. Crim., January 23 2018, n° 17-83.077). It allows further details:

1°) the vehicle must be in motion, for the judge to qualify a breach of the law;

2°) the use of a mobile phone by a driver while stopped (forbidden) and the use of a mobile phone by a driver while parked (allowed if respecting parking's rules) are two distinctive actions and have to be taken separately.

For any of the experimentations with an automated vehicle, we recommend not to use mobile phones at any time.

3.2 Data protection in European law

After four years of discussions, the new European General Data Protection Regulation got into force on May 25th, 2018. All Member States of the European Union must comply with it regarding their data protection policies.

Now all the new rules we presented are effective and have to be applied into all the Member States. We suggest to you all to have a look at the former document for further details.

France made the decision to regulate data protection, even though the GDPR is directly applicable, for three main reasons:

1°) First, France did not want to repeal its first Law or modify its content regarding data protection, considered as pioneering data management of citizens;

2°) Second, France wanted to establish national arrangements when the GDPR is silent or let the Member States free to implement;

3°) At last, France wanted to transpose the European Directive on the protection of individuals with regards to the processing of personal data by competent authorities for purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Directive UE 20176/680, April 26 2018).

Following, a Decree dated August 1st, 2018 fixed the former Law on data protection in France (n° 2018-687).

In this Decree and more specifically “the in-vehicle system”, the question of the data logger remains crucial. Indeed and as a reminder, Article 4 of the GDPR defines a personal data as "any information relating to an identified or identifiable natural person (‘data subject’)". In that way, an "identifiable natural person" is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online ID or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

In France, the National Commission for Data Protection and Liberties (CNIL) published in 2017 a Compliance Pack regarding the automated in-vehicle system, specifying that geo-tracking data, technical data about the vehicle, biometric data or the use of the car by any driver are all personal data.

Thus, those vehicle data are personal data regarding Article 4 of the GDPR and must be anonymized or pseudonymized.

Before these experiments, we recommend to inform the participants not only of the collection of the personal data, but also of the objective and the duration of this collection in order to obtain their free consent before the test.

3.3Experimentations conditions (France point of view)

3.3.1 Analysis of French Decrees and Laws

The main update in France, regarding automated vehicle, is the Decree n° 2018-2011 dated of March 28th, 2018. This Decree details conditions and aims to implement such new engines. The Decree focus on two aspects :

- First, the French Decree spells out the conditions regarding administrative authorization to have automated in-vehicle system(s)? on the road.
- Second, the French Decree details the roll-out, which will be from January 1st, 2019, under a specific Certificate.

Uncertainty remains on the training that any driver must have received before the experiment. It is not clear yet what the appropriate training is.

3.3.2 Analysis of German Decrees and Laws

The main update in Germany, regarding automated vehicles, are §§1a and 1b of the Road Traffic Act (StVG) released in June 2017.

§1a defines conditions when a car is considered as highly or fully automated. In the sense of this Law impose some general requirements for manufactures and drivers.

§1b defines Rights and Obligations for the drivers of automated vehicles in the sense of §1a.

Mostly discussed legal questions are currently still concerning the liability.
Legal questions regarding liabilities are still under discussions.

3.3.3 Analysis of Italian Decrees and Laws

The conditions for experimentations of Automated Driving Functions (ADFs) in Italy is regulated by the administrative Order, called "Smart Roads". All details can be found on this following website: http://www.mit.gov.it/comunicazione/news/nuove-smart-road-e-guida-automatica (in Italian language, of course).
Hereafter is a short summary in which the following articles 2, 3, 4, 9, 10, 11, 14, 16 and 19 have been considered.
"Smart Roads" are defined as ordinary roads which went under digital transformation, in order to adapt to the monitoring and observation of the traffic flow, to the modelling of data and to processing of information, as well as advanced services. The idea is to create a technological eco-system for new generation of both vehicles and infrastructure.
In this context, the experimental phases of automated vehicles (AVs) is authorized on such roads. It can be required by the car-manufacturer, owner of the automated technology, but also by research institutes, universities and public administrations that want to carry out experiments in this field.
The authorization can only be given to approved vehicles (in the version without automated technologies).
Therefore such prototype vehicles have to use test-plate and receive security clearance of the transports and/or roads administrative department to have experimentations on "Smart roads".
This kind of experiments is carried out by a supervisor, who has at least 5-years of valid driving license for the class of the vehicle under test and has passed successfully the exam of a safety-driving course. In addition, this person has to have travelled on a vehicle equipped with automated technology in private test-tracks for at least 1,000 (one thousand) kms and has to have the right knowledge[i] about the vehicle.

All actors who wish to perform these tests, have to present a specific request to the “Ministero delle infrastrutture e dei Trasporti”, indicating – among others – in which scenario and on which road segments the tests will be carried out. The qualifying documentation should always be inside the vehicle and valid for each road segment. Furthermore, the legal entity requiring this authorization must prove to have already done tests in simulation and in private test-track in the same scenario, considering possible variations and sensors' malfunctioning (including risk-analysis and procedure to manage the emergency and critical situations). A list of all the people allowed to drive the prototype vehicle equipped with automated technology has to be available at any time and also provided in the submission phase of the request.
Moreover, the authorizing entity (e.g. “Ministero delle infrastrutture e dei Trasporti”) can require for any further information about the experiments and the automated functions to the entity asking this authorization.
A list of test-scenarios and used road segments must be communicated to the authorities ten days before the starting date of the experimental phase. Data collection, with all the drawbacks and problems related to the performances of the ADFs, have to be available for a certain time (to be defined) and included in a yearly report.

On the insurance side, the requiring entity has to stipulate a third party liability contract specific to automated vehicles with a maximum amount equal to four times of the amount for the same vehicle in its “normal” version.

It is finally worth to keep in mind that a specific agreement for the experimentation of automated vehicles in the city of Turin and nearby has been signed within the following partners: City of Turin, FCA Group, GM Global Propulsion Systems s.r.l., ANFIA, 5T s.r.l., Politecnico of Turin, University of Turin, Foundation Turin Wireless, Tim S.p.A., Open Fiber S.p.A., Italdesign Giugiaro S.p.A., Industrial Union of Turin, FEV Italia and Unipol.

4 Conclusion

In the first part of this document we demonstrated a fault analysis of our architecture and of safety activities. The most suitable solution is to have a redundancy at the top of the architecture of the tree especially for the demo-car, reducing the risk by two. This redundancy can relate to either hardware (sensors) or software (multiply the perception algorithms or the trajectory planning algorithms). Since we have a dedicated enabler to assess the risk (E5.2 Online Risk Assessment) taking as an input the planned trajectory, the boundary of the road and the road participant we can assess in this case several trajectories coming from several algorithms and their control variables.

According to the V2X and the above overview it is obvious that the security and privacy related issues are handled by the Standards. Since the V2X technology is becoming more and more general, the security and privacy aspects are weighting more in research areas. The European Commission now, funds on-going R&D projects related to these topics, e.g., SAFERtec [6], while other efforts have done by researchers and ITS specialists [7]. These projects are monitored during the interval of AutoMate project to see how the V2X communication evolves.

In the commercialization phase of such products developed during the AutoMate project, they have to include security and privacy solutions taking into account the possibilities offered by the Standards to be compatible with available products already on the market. However, during the AutoMate project security and privacy solutions are minimized to ease the development and integration of V2X components.

Since there has been no evolution of the Vienna Convention and no legislation on how a driver can have distractive activities while driving has been acted. Indeed, such actions are allowed by default if a driver still holds control and command of his vehicle in any circumstances and is responsible in case of an accident.

Regarding personal data protection, the new Law on GPRD mandate all Member States of the European Union to comply with regarding their data protection policies. Since May, 25th, 2018 all AUTOMATE experiments have to comply with this Law.

5 References

[1] ETSI TS 102 731 V1.1.1 (2010-09): "Intelligent Transport Systems (ITS); Security; Security Services and Architecture"

[2] ETSI TS 102 941 V1.1.1 (2012-06): "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management"

[3] E. B. Hamida, H. Noura and W. Znaidi, "Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures", Electronics 2015, 4, pp. 380-423

[4] ISO/IEC 15408-2: "Information technology – Security techniques – Evaluation criteria for IT security; Part 2: Security functional components"

[5] IEEE P1609.2/D12 (January 2012): "IEEE Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages".

[6] SAFERtec, https://www.safertec-project.eu/

[7] Car-2-Car Communication Consortium, https://www.car-2-car.org/index.php?id=6

[i] Meaning that s/he can change quickly and appropriately from automated mode to normal mode (and vice-versa).