DRIVE2 THE FUTURE

Needs, wants and behaviour of "Drivers" and automated vehicles users today and into the future

Contract No: 815001

D1.2: Acceptance Risk Assessment

Version 1.0

Work package	WP1
Activity	A1.3
Deliverable	**D1.2 Acceptance Risk Assessment**
Authors	Matina Loukea, Evangelos Bekiaris, Evangelia Gaitanidou, Xanthippi Gkaitatzi, Christos Britsas (CERTH/HIT), Nikolaos Bakalos (INFILI)
Status	Final (F)
Version	1.0
Dissemination Level	PU
Document date	30/04/2019
Delivery due date	30/04/2020
Actual delivery date	30/04/2020
Reviewers	Maria Panou (CERTH/HIT), Marco Ducci (DBL), Brayan González-Hernández (CTL)

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement no 815001.

Version History

Document history			
Version	**Date**	**Modified by**	**Comments**
0.1	2020-03-02	Matina Loukea	Initial draft
0.2	2020-04-06	Matina Loukea, Evangelos Bekiaris	Second draft
0.3	2020-04-08	Evangelia Gaitanidou	Third draft
0.4	2020-04-20	Maria Panou, Marco Ducci, Brayan González-Hernández	Minor Comments
1.0	2020-04-30	Matina Loukea	Final version

Legal Disclaimer

Table of Contents

List of Figures

List of Tables

Abbreviations List

Abbreviation	Definition
5G	5th generation mobile network
API	Application programming interface
AVs	Autonomous Vehicles
ESoP	European Statement of Principles
FMEA	Failure Mode and Effects Analysis
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HD	High Definition
HMI	Human-Machine Interaction
I2V	Infrastructure 2 Vehicle
NDRT	Non-driving-related tasks
OEM	Original Equipment Manufacturer
PT	Public Transport
QoS	Quality of Service
RN	Risk Number
TMC	Traffic Management Centre
UC	Use case
VRU	Vulnerable Road Users

Executive Summary

This report constitutes the Deliverable 1.2 of Drive2TheFuture project, illustrating the work performed in A1.3 (Acceptance Risk Assessment) as part of the WP1 ("Driver", traveller and stakeholder clustering a priori needs and wants and UC's) during the period M1-M12 (May 2019 – April 2020).

The current Deliverable provides a structured approach for the identification of the risks related to the user acceptance of autonomous vehicles (AVs), using a modified extended Failure Mode and Effects Analysis (FMEA) methodology. Even if many risk assessment methodologies exist, in Drive2theFuture we choose to use the extended FMEA methodology, and adapt it according to the needs and the nature of the project, since it allows us to identify relevant risks and to cluster them in categories, capturing all the dimensions of their probable impact. Using extended FMEA methodology allows us to identify risks that are related to behavioural, legal, operational and technical issues related either directly to the project's outcomes, as well as indirectly to its stakeholders, while also prioritise them according to their ***severity, occurrence probability, detectability and recoverability***.

Currently, that the a priori phase of the risk assessment has been finalised, 50 risks have been identified so far, with the majority of them (36%) focusing on operational issues. More specifically, emphasis has been given by the experts to re/upskilling needs and resources, while also to operational changes in Traffic Management Centers (TMC) and logistics chains and the cost of such services. Behavioural risks follow (28%) that mainly concern the overreliance on technology and/or wrong use of AVs technology by the users. The technical risks (20%) focus mainly to communication failures and sensors malfunctions, as well as the fear of cybersecurity attacks, while the legal issues (16%) deal mostly –as expected – with the need for the adaptation of legislation and data protection and data ownership.

An *a posteriori* risk analysis will also follow later in the project (on Month 30), which will provide an update of the already identified risks, based mainly on the analysis of social media, as this is over data already available through relevant APIs, such as the Twitter API, that allows the extraction of content based on specific queries (A2.5), as well as on the results of the project's pilots (WP5).

1. Introduction

Today's vehicles - in all modes of transport - are becoming increasingly connected and cooperative, as well as automated, raising a number of issues about the role of the "driver" of all kinds (i.e. operator, rider, pilot, captain) in such vehicles. Human-machine interaction is becoming increasingly complex in an environment with higher levels of information, both qualitative and quantitative, automated data exchange and increasing levels of automation (systems, operations, etc.). Riding in an autonomous vehicle gives the opportunity to the drivers to exempt from driving tasks and offers them the opportunity to engage in other leisure or productivity non-driving activities, while at the same time AVs provide a new traveling option for people not able to drive conventional vehicles (i.e. persons with disabilities or the elderly), thus promising an improvement of their mobility and independence.

While AVs may offer a wide range of benefits in terms of safety, increased mobility, energy efficiency and environmental protection, these benefits cannot be reached until a significant market penetration of AVs is met. At all cases, the introduction of autonomous vehicles is expected to bring a revolution to the transport system as we know it. However, it is generally suggested that the biggest barrier to this AV penetration does not reside on relevant technology aspects (i.e. maturity), but it is rather mostly on public acceptance issues [1]. Even though technology is almost there, it is a crucial issue whether humans are ready to abandon the driving task and/or even the car ownership – in combination with car sharing/pooling applications - or board a vehicle with no driver present [2].

In this framework, user awareness, acceptance and training formulate the first-priority challenge. Questions related to vehicle taking over control from humans, change of mobility habits and experience, cost of commuting and travelling in the future, ethical decisions of a machine vs. a human, as well as the need of new driver training incentives for adapting to the technological evolution in future vehicles, are some of the key issues that are yet to be investigated. Drive2theFuture project recognises the need for providing measures, tools and procedures in order to prepare “drivers”, travellers and vehicle operators of the future to accept and use connected, cooperative and automated transport modes and the industry of these technologies to understand and meet their needs and wants. More specifically, Drive2theFuture develops training, HMI concepts, incentives policies and other cost efficient measures to promote and then to comparatively assess several alternative connected, shared and automated transport Use Cases for all transport modes and with all types of users (drivers, travellers, pilots, VRUs, fleet operators and other key stakeholders), in order to understand, simulate, regulate and optimize their sustainable market introduction; including societal awareness creation, acceptance enhancement and training on use.

To increase the public’s acceptance of AVs, it is important to understand which factors have significant effects on AV acceptance. Some preliminary attempts have been made. For instance, it has been consistently found that young and male drivers have a more welcome attitude towards AVs and would be more willing to use and buy one [3].

1.1. Purpose of the Document

One of the many aspects of the Drive2theFuture project is to explore and recognise factors affecting users’ acceptance of autonomous vehicles. The purpose of this report is to describe the process that is being followed within the Drive2theFuture project, in order to examine the risks related to AVs user acceptance, as well as the key features and factors that will be taken under consideration. Emphasis is also given on the analysis of these risks, and on the suggestion of specific recommendations for their elimination.

1.2. Intended audience

The Deliverable is public, thus addresses a wide audience of all interested in the risks associated with autonomous vehicles’ acceptance.

1.3. Interrelations

This Deliverable is part of Activity 1.3 of WP1. Input was received from almost all other activities operating in Year 1 (A1.1, A1.4, A2.1, A2.2, A2.5, A3.1, etc.) while it is expected to feed A1.7 (Use Cases), while also A8.5 (Guidelines & Policy Recommendations) and A8.6 (User Acceptance Roadmap).

2. Methodology

Key risks to user acceptance of AVs will be assessed during the project by experts in two phases: ***a priori*** on expected risks and ***a posteriori***, based also on the analysis of social media and project evaluations. The risk assessment within the Drive2TheFuture project is based upon an extended FMEA methodology, whereby for every risk identified, its risk severity, occurrence probability, detectability and recoverability is being estimated and the overall risk level is being calculated.

The FMEA (Failure Mode and Effects Analysis) procedure is a tool that has been adapted in many different ways for many different purposes. It can contribute to improved designs for products and processes, resulting in higher reliability, better quality, increased safety, enhanced customer satisfaction and reduced costs. In Drive2TheFuture the extended FMEA that has been developed at ADVISORS project has been used [4]. The introduction on Autonomous Vehicles will undergo a thorough assessment of risks and barriers regarding the acceptance of the users using this methodology, adequately adopted in order to fit the needs of the project. Relevant risks and barriers are currently being identified during the realisation of the a priori phase of the process and the risks and barriers assessed together with the mitigation strategies are being presented in this report. This assessment is expected to assist on the adoption of Drive2theFuture outcomes, towards the enhancement of the acceptance of the AVs functions.

The **extended FMEA** methodology is based on the classical FMEA methodology, which includes the indicators of *hazard consequence severity, occurrence probability, detectability and recoverability*, and extends it, covering not only technical risk, as done in classical FMEA methodology, but including also *behavioural, legal and operational (organisational)* ones. For the issue of AV acceptance, risks will be first identified and the level of risk will be assessed by considering the number of characteristics, for each risk type (behavioural, legal, operational and technical). The significance of a risk, overall, depends both on its consequences and the probability of its occurrence, but also on how easily the developing risk can be detected. The overall process proposed for the extended FMEA methodology for a specific solution, is summarised in Figure 1 below:

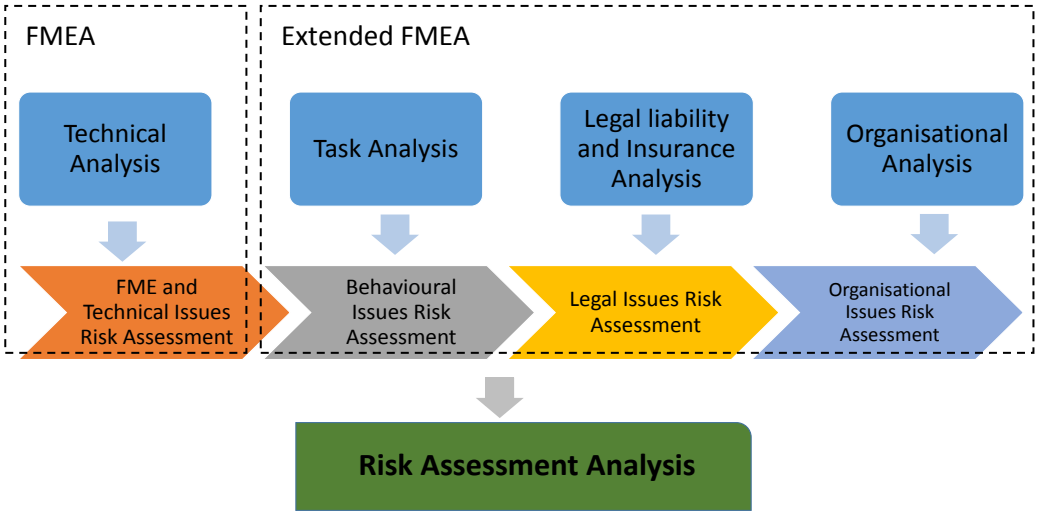

Figure 1: Extended FMEA (proposed by Bekiaris and Stevens 2005)

In general, a risk assessment consists of an analysis of the risks (i.e. the identification of potential hazards and some estimation of their magnitude) and an evaluation of the tolerability of that risk in its anticipated context. The steps that follow the calculation of the risk within the extended FMEA methodology as applied in Drive2theFuture for AV acceptance are depicted in Figure 2.

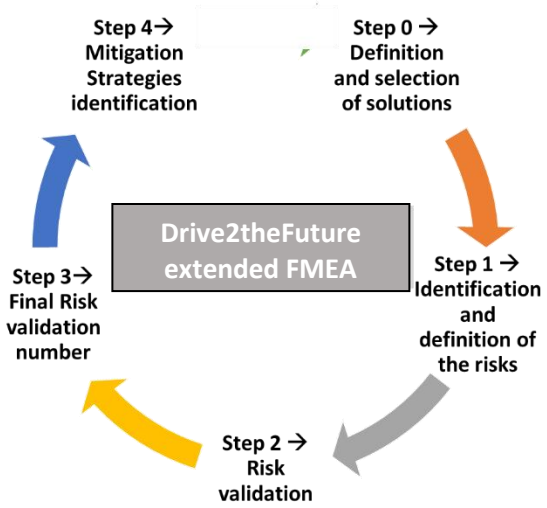

Figure 2: FMEA methodology steps in Drive2TheFuture project for AV Acceptance

Two iterations of risks identification, analysis and assessment will be realised within A1.3. The *a priori* one has already been completed, updating the collection of risks with preliminary findings of the project. Moreover, a Workshop has also taken place in Brussels (6th March 2020), with the participation of more than 40 people (physically and online). During this Workshop, the identified risks haven been presented to the participants, who were asked to rank them according to their perceived importance, for each one of the risks categories (namely behavioural, legal, operational and technical). Then, four boards were placed in the room, again one per risk category, and the attendees were invited to write any additional risks they consider significant and which were not yet identified in the presented list. This was a very fruitful exercise, as about 35 more risks were suggested, which have been considered in the final acceptance risk assessment.

2.1. Drive2TheFuture AV Acceptance risk analysis methodology

For the realisation of the extended FMEA methodology a template (see Table 1) has been defined and filled in from experts within the Drive2theFuture Consortium during the initial assessment, while it will be updated during the second iteration. Each cell of the table is related to the steps of the methodology.

Table 1: Risks assessment methodology template

Risk type (select one)	Problem short description	Relevant WP/ Activity	S*	O*	D*	R*	Risk	Problem severity	Mitigation strategy*	Mitigation possibility
❑Technical ❑Behavioural ❑Legal ❑Operat.										

Based on various criteria (i.e. society readiness, technical aspects, etc.), partners that have expertise within different areas of transport automation, have been asked to identify and prioritise risks stemming from different Drive2theFuture steps, based on their expertise. For every risk identified, the risk severity, occurrence probability, detectability and recoverability has been estimated by three independent experts and the overall risk level has been calculated. Risks are clustered into behavioural (related to HMI and handover strategies acceptance), legal (legal framework and readiness to user acceptance), operational (related to loss of jobs, shift of authority, responsibility or current procedures, shift of work times, etc.) and technical (i.e. related to

potential future technological limitations and accident types). For each one of the risk types (behavioural, legal, operational and technical) a specific validation has been made.

2.1.1. Risk Severity (S)

"Severity" is a ranking number associated with the most serious effect for a given failure mode, based on the criteria from a severity scale. It is a relative ranking within the scope of the specific FMEA. The factors that are examined related to the severity of the risks for the different risks cluster for AV acceptance, are presented in Table 2 below.

Table 2: Examined factors per risks cluster

Risks Cluster	Examined factors
Technical risks analysis	• A technical solution or part of it, is not available, needs further investigation, or is highly complicated. • Cost of the technical solution or part of it would be prohibitive. • The benefits gained from the functionality of the solution are uncertain.
Behavioural Risks Analysis	• A change to human behaviour (reduced human error) is required before the solution can be fully deployed. • The expected cost (training, design changes, time availability) of the deployment of the solution is significant. • The benefits gained from changed human behaviour due to the deployment of the solution are uncertain.
Legal Risks Analysis	• A change to existing law is required before the module can be fully deployed. • The expected legal cost of deployment (including fees and damages) is significant. • There is uncertainty about where large potential liabilities will fall
Operational Risks Analysis	• Occurrence of organisational failures • The roles and responsibilities, as well as processes and communications has presented confusion

The severity levels (S) for risks in all clusters can be ranked as described below.

Table 3: Definition of unmitigated severity levels for risks clusters

Severity of unmitigated risk of issue now	Rate	Definition for technical risks	Definition for behavioural risks	Definition for legal risks	Definition for operational risks
Extremely severe	9-10	The failure could put user safety at risk.	The user error in operating the solution could lead to an incident worseness (i.e. safety effects).	Are there laws in each country that do not allow the solution to be implemented?	Wide and different operational framework is needed, that is completely missing (i.e. new services).
Severe	7-8	The failure implies total loss of the solution availability causing major user's dissatisfaction.	User behavioural error may abort the solution's benefits (i.e. safety effects due to changes in ways of acquiring info).	New laws are required for solution's implementation and no relevant work has been performed yet.	Operational framework adaptation is needed (some initial actions have been taken on this domain).

Severity of unmitigated risk of issue now	Rate	Definition for technical risks	Definition for behavioural risks	Definition for legal risks	Definition for operational risks
Moderate	5-6	Failure implies the partial loss of the solutions' function causing user's dissatisfaction.	User's behavioural changes may significantly reduce the positive effects of the solution.	New laws are required for solution's implementation and work required has already been performed.	Operational framework adaptation is needed which has already started being realised.
Slight	3-4	The failure implies slight dissatisfaction to the user.	User's behavioural changes may somehow influence the positive effects of the solution.	New laws are required for solution's implementation but consensus on them exist.	There is a need for limited and easily realised organisational changes.
Insignificant	1-2	The failure does not imply perceptible effects to the system function and to the user's satisfaction.	User's behaviour is not expected to reduce the solution's benefits significantly, or may even further enhance them.	No new laws are required for implementation.	There is no need at all for organisational changes.

2.1.2. Risk Occurrence Probability (O)

The Occurrence Probability (O) is the probability that all the risk causes related to the risk modes described in the analysis can occur. This is often a qualitative index especially when new technologies are concerned because of the few reliability data available.

Table 4: Occurrence indicator scale of risk analysis methodology

Occurrence Probability (O)	Technical issue	Behavioural issue	Legal issue	Operational issue
9 – 10 (HIGH)	It is certain that some failures will sometimes occur.	It is certain that some behavioural effects will occur (by the users).	It is certain that some legal problems will occur.	It is certain that there will be a need for operational restructuring.
6 - 7 – 8 (MEDIUM)	A failure could occasionally occur.	Some behavioural effects could occasionally occur.	Some legal problems could occasionally occur.	A need for operational restructuring could occasionally occur (depending on the needs of the solution that will arise).
3 - 4 – 5 (SLIGHT)	There is only a slight probability that an error/failure will occur.	There is only a slight probability that some behavioural effects will occur.	There is only a slight probability that some legal problems will occur.	There is only a slight probability that a need for operational restructuring will occur.

Occurrence Probability (O)	Technical issue	Behavioural issue	Legal issue	Operational issue
1 – 2 (IMPROBABLE)	It is unlikely that a fault will occur.	It is unlikely that some behavioural effects will occur.	It is unlikely that some legal problems will occur.	It is unlikely that a need for operational restructuring will occur.

2.1.3. Risk Detectability (D)

Detectability (D) is the probability to detect the occurrence of a risk identified. Detection of a developing risk is an important aspect of overall risk management, as early detection is a prerequisite for the application of mitigation strategies. In the technical, and to some extent behavioural, domains, detection can be facilitated by additional sensors and processing. In the legal and operational domains surveys, monitoring and feedback are important tools. Detectability is assigned a value between 1 and 10 (1 means that it is always perfectly detectable and 10 that it is always undetectable).

Table 5: Detectability indicator scale of risk analysis methodology

Detectability (D)	Technical issue	Behavioural issue	Legal issues	Operational issue
9 – 10 (IMPROBABLE)	It is impossible or improbable that a problematic area will be detected.	It is impossible or improbable that a user's behavioural effect will be detected.	It is impossible or improbable that a legal problem will be detected.	It is impossible or improbable that an operational problem will be detected.
7 – 8 (SLIGHT)	The problematic area is detected only in particular cases.	The user's behavioural effect is detected only in particular cases.	The legal problem is detected only in particular cases.	The operational problem is detected only in particular cases.
5 – 6 (MODERATE)	It is probable that the problem will be detected (depending on the situation).	It is probable that the user's behavioural effect will be detected.	It is probable that the legal problem will be detected.	It is probable that the operational problem will be detected.
3 – 4 (HIGH)	It is very probable that a problem will be detected.	It is very probable that the user's behavioural effect will be detected.	It is very probable that the legal problem will be detected.	It is very probable that the operational problem will be detected.
1 – 2 (VERY HIGH)	It is certain that a problem will be detected.	It is certain that the user's behavioural effect will be detected.	It is certain that the legal problem will be detected.	It is certain that the operational problem will be detected.

2.1.4. Risk Recoverability (R)

Recoverability (R) is an efficacy index of the possible recovery action performed by the risk management procedures implemented in the Scenario. It estimates the ability of the solution to tolerate the risk. The effectiveness is valued in terms of recoverability which is assigned a value between 1 and 10 (10 represents not recoverable and 1 always perfectly recoverable).

Table 6: Recoverability indicator scale of risk analysis methodology

Recoverability (R)	Technical issue	Behavioural issue	Legal issues	Operational issue
9 – 10 (NULL)	No recovery action is provided.	System is inflexible to user's behavioural effects.	System is either accepted or rejected by the legal framework.	System requires a fixed operational environment to operate.
6 - 7 – 8 (LOW)	The user is only advised on the failure.	Behavioural effects are taken into account by the solution.	System may be slightly adapted to meet legal restrictions.	System requires a fixed operational framework with limited adaptations.
3 - 4 – 5 (HIGH)	Effective recovery action is provided.	System customisation might compensate for user's behavioural effects.	System encompasses different versions to meet particular legal demands.	System may operate within various operational frameworks.
1 – 2 (TOTAL)	The failure effect is completely avoided by the recovery action.	System does not allow user's behavioural effects.	System is easily reconfigurable to meet legal demands.	System does not require operational changes.

2.1.5. Final risk validation number

After the risk classification in each of the four domains, an overall relative indication of risk may be useful and for this reason the extended FMEA calculates a risk number (RN) for each risk identified, using the following formula:

$$\textbf{Risk Number (RN)} = S * O * \{[D + R]/2\}$$

This calculation is applied to each risk area (technical, behavioural, etc.) to generate a risk number. The results of this equation may vary from 0 to1000 depending on the validity of the risk each failure mode has. Normally, organisations select a pre-defined range for the RN, i.e. above 500 in the 0-1000 scale for which risks a mitigation strategy should be implemented. This is done in order to optimise use of resources and minimise cost.

The results of the risk number can be translated using the following table, which has been established by the FMEA methodology.

Table 7: Results of the risk number

Overall risk factor	Overall severity	Mitigation possibility
513-1000	I- Extremely severe	Very High
217-512	II- Severe	High
65-216	III - Moderate	Medium

Overall risk factor	Overall severity	Mitigation possibility
9-64	IV - Slight	Low
1-8	V - Insignificant	Improbable

2.1.6. *Mitigation strategies identification*

The issues that will be identified as risks will be further analysed to determine the possibility of mitigating strategies. Risk reduction is an iterative process involving dependencies between the different issues. In terms of mitigation strategies, risk can be reduced in a number of generic ways:

1. reducing the probability of the hazard occurring;
2. increasing failure detection speed and probability;
3. reducing the magnitude (severity) of the consequences of the potential hazard;
4. protecting against the risk - mitigating strategies to compensate for a failure (e.g. back-ups).

One advantage of this approach is its consistency between the different domains (Behavioural, Legal, Operational and Technical).

2.2. Determining Fears through Social Media Sentiment Analysis

During the a posteriori phase of the acceptance risk assessment, the social media analysis will be integrated in the process and the extraction of the final results.

This analysis aims to elicit the main fears and reservations of the general public towards autonomous modes of transportation, using a combination of social media mining and a sentiment analysis framework to classify behaviours expressed in Twitter and Reddit posts. The “negative” opinions are being further analysed, in order to fears and reservations to be identified.

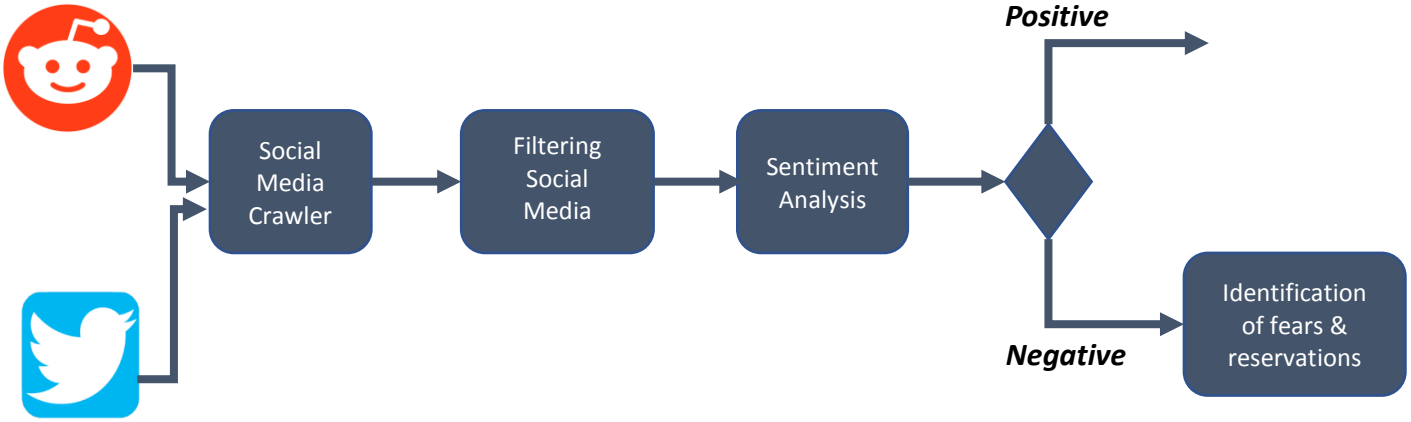

Figure 3: Social Media Sentiment Analysis process

Beyond the statistical breakdown, the negative opinions captured are being further analysed in order to identify the specific fears and reservations. This is an ongoing process during the Drive2theFuture project, which is going to feed the project’s risk assessment in its next steps. More specifically, relevant analysis is performed over social media posts from Twitter and Reddit. To achieve this a specialised lexicon of terms is used to query social media content from the dedicated Application Programming Interfaces (APIs) that

the aforementioned social media platforms provide[1]. In this context, the main fears that have been captured so far, are listed below:

- **Technophobia** ranked higher than all, with **42.55%** of the posts mentioning cyber-security, robotics, and safety concerns
- **Employment issues** were the second reservation identified, with **32.41%** of negative posts mentioning such fears.
- Fears due to the probable **presence of both autonomous and conventional mobility solutions**.
- Issues regarding the **insurance of autonomous cars and liability** in crashes
- **Personal property** and the possible extinction of driving as an everyday task/hobby.

3. Risks identified during the a priori phase

The aim of Activity 1.3 of the Drive2TheFuture project is to perform the assessment of the risk of acceptance of AV technology by their current and future users and related stakeholders. To achieve this, the first step has been the identification of possible related risks, though consultation of the project's Consortium and external experts. Risks have been clustered into behavioural (related to HMI and handover strategies acceptance), legal, operational (related to loss of jobs, shift of authority, responsibility or current procedures, shift of work times, etc.) and technical (i.e. related to potential future technological limitations and accident types). For all risks, mitigation strategies have been proposed (in terms of HMI design, training of incentives provision, suggested policies, necessary certification schemes, etc.) and will be followed throughout the project (when relevant) or included in the final project recommendations.

3.1. Identified risks

The initial list of the risks, coming from the first phase of the assessment can be found in **Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.** below, as they have been identified and evaluated by the Consortium experts.

Table 8: AV Acceptance initial risks identified by the Consortium

Risk Caterogy	Initial risks identified
Behavioural risks	• Overreliance on technology (i.e. AV performance at level 3 or even 4). • Reduced use of AVs due to technophobia and especially safety or security fears. • Mimicking of AV behaviour by non-equipped users (i.e. in platooning scenarios). • Pedestrians or others misuse of AVs autonomous braking in violating priority or for fun. • Misunderstanding by non-equipped users of AV status and operation levels. • Failure of HMI handover strategies for specific driver cohorts or states. • User confusion due to different OEM strategies and AV levels.
Legal risks	• Need to change current conventions (i.e. Vienna Convention). • Liability transfer driver to OEM or/and infrastructure operator and share between them. • Data protection and data ownership issues.

[1] *Read more in Drive2theFuture, D2.2 "Sentiment Analysis in social media"*

Risk Caterogy	Initial risks identified
	• Lack of appropriate insurance schemes. • Share of liability in case of accidents between equipped and non-equipped vehicles or VRUs. • BVLOS height, weight and region regulations UAVs.
Operational risks	• Lack of AV proper infrastructure maintenance. • Job loss at AV operation and especially maintenance / servicing. • Re-skilling/ up-skilling needs of affected workers. • Training needs of all stakeholders. • Workers and unions opposition to AV introduction. • Need of AV operation and planning data sharing with TMC/ logistics chain. • Coordination of mixed flows at TMC and need for new operational algorithms.
Technical risks	• Non-reliable infrastructure (i.e. no clearly visible lane markers). • Adverse weather conditions (i.e. lane markers hidden by snow). • Loss of I2V (G5 or 5G signals or other communication failures). • Critical on-board sensors malfunctions (i.e. GPS accuracy level) • Cybersecurity attacks

3.2. Risk Assessment Workshop

The risks described above, have been presented in an audience of 40 participants who attended the 1st Drive2theFuture Workshop that was held in Brussels, on the 6th of March 2020. With the use of the Mentimeter online tool (https://www.mentimeter.com/), the participants voted using their mobile phones regarding the significance of these risks per category. From the results that came out of this voting, the risks have been ranked, according to the audience's perceived importance.

More specifically, regarding the ***behavioural risks***, the *overreliance on technology* emerged as the most important, followed by the risk of *misunderstanding by non-equipped users of AV status and operation levels* and the risk of *pedestrians or others misusing AVs autonomous braking in violating priority or for fun*. On the other hand, as least important risk in this category was rated the *user confusion due to different OEM strategies and AV levels.*

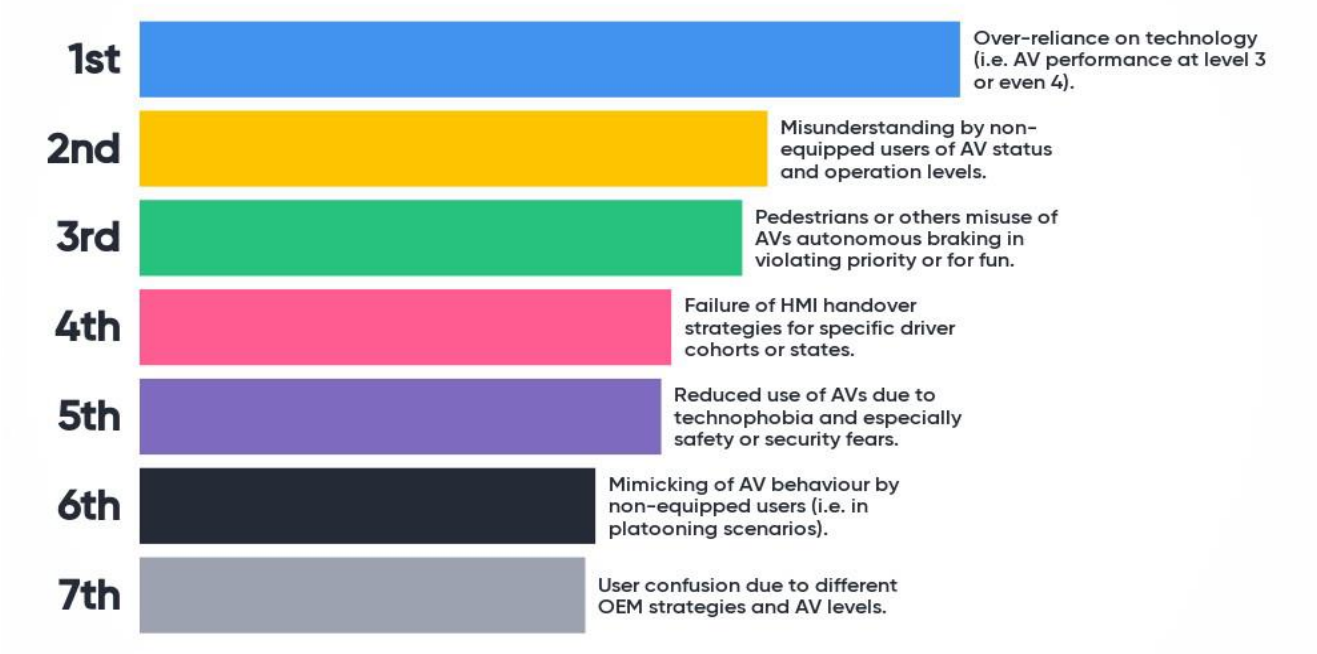

Figure 4: Behavioural risks ranking for AVs user acceptance

Moving on to the **legal risks**, the *data protection and data ownership* issue was identified, as expected, as the major legal risk towards AVs user acceptance, with the *liability risks* following both in case of accidents between equipped and non-equipped vehicles or VRUs but also the transfer from driver to OEM or/and infrastructure operator).

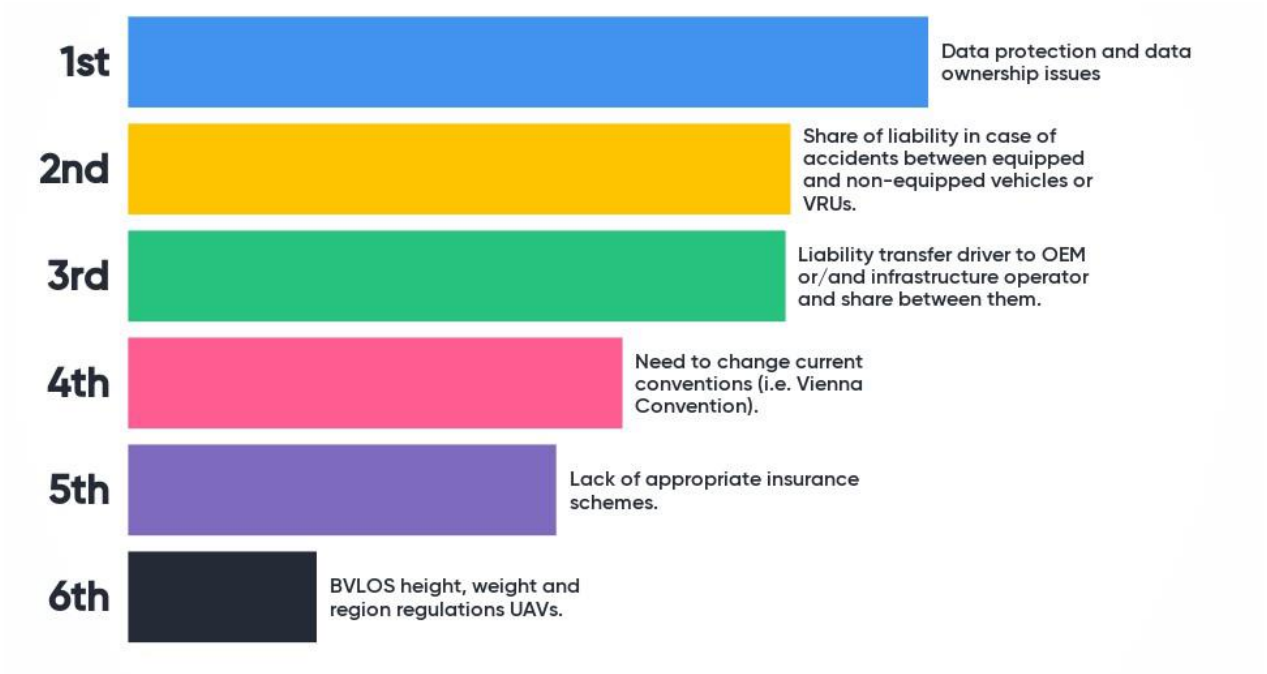

Figure 5: Legal risks ranking for AVs user acceptance

As for the ***operational risks***, the one that was identified as the most significant for the social acceptance of the autonomous vehicles has been the issue of *lacking AV proper infrastructure maintenance,* as well as the

coordination issues of mixed flows at TMC and need for new operational algorithms. Following down the order of risks in this category, although the needs of *re-skilling/ up-skilling of affected workers and training of all stakeholders* ranked in the fourth and fifth places respectively, the risk of *Job loss at AV operation* has been identified as the least critical.

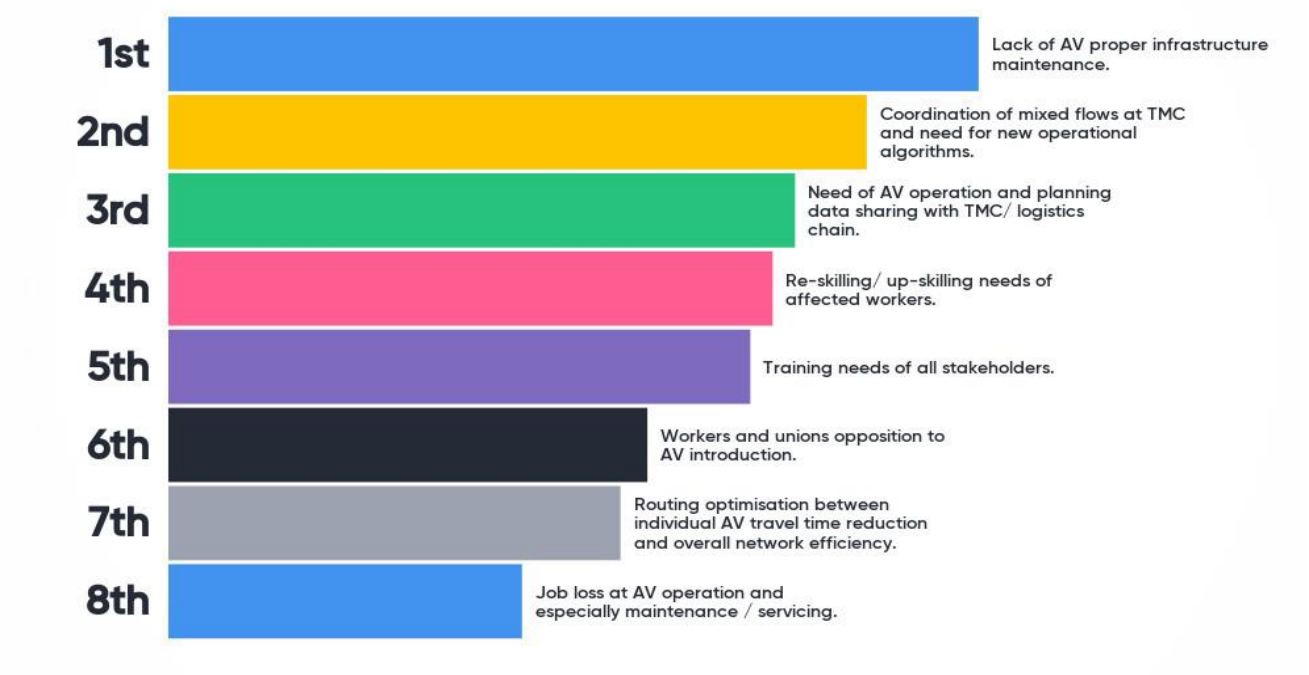

Figure 6: Operational risks ranking for AVs user acceptance

Finally, concerning the ***technical risks***, the issue of *non-reliable infrastructure* emerged as the most important, followed by the *critical on-board sensors' malfunctions,* while the *cybersecurity attacks* have been ranked one place before the last.

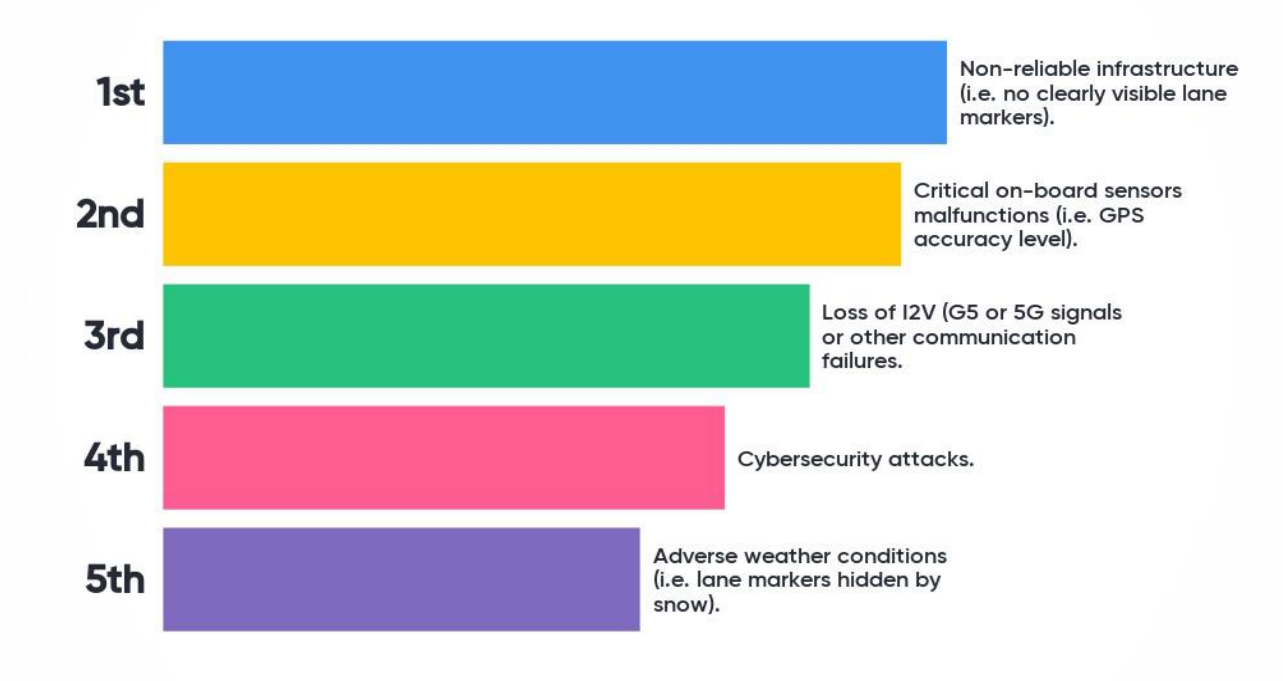

Figure 7: Technical risks ranking for AVs user acceptance

On the second part of the AV Acceptance Risk Assessment session of the Workshop, the Participants were asked to move around the room, where 4 separate boards were set (one for each category) and to suggest additional risks that will, in their opinion, affect the AVs user acceptance.

From this exercise, ***36 new risks*** were proposed, which are presented in Table 9 below.

Table 9: New risks identified during the 1st Drive2theFuture Workshop

Risk Caterogy	New risks suggested
Behavioural risks	▪ Road rage/ angry driving due to over-secure AV driving style. ▪ Misuse or no-use of automated functions because of the "pleasure of driving" ▪ Too many AVs in city centres. ▪ Unaccepted/ false reaction of AVs in emergency situations. ▪ Abuse of alcohol and drugs in AVs ▪ Impression of being in a video game. Loss of awareness. ▪ Specific uses/ group needs, i.e. young children, persons with dementia, persons with disabilities. ▪ AVs sickness ▪ Not comfortable due to technical limitations (i.e. hard braking, etc.)
Legal risks	▪ Lack of regulating the amount of AVs ▪ Risk of focus on technical issues and not on securing the users. ▪ Regulating the industry players, while protecting the competition and intellectual property. ▪ Data linkage/ data abuse ▪ Lack of pressure from population vs other priorities (i.e. climate, immigration, unemployment). ▪ Need for standardisation

Risk Caterogy	New risks suggested
	▪ Accountability issues from infrastructure and mobility operators, in case problems occur.
Operational risks	▪ Users expecting revenue back for the use of their data. ▪ Cost of new services of AVs. ▪ Users' fear of infection in car-sharing schemes. ▪ Lack of HD maps. ▪ Need of vehicles cleaning (inside and outside). ▪ Problems with the power recharge. ▪ Manage of drop-off areas for the delivery trucks. ▪ Lack of route choice. ▪ Integration with emergency services. ▪ Performing automated check-in/ check-out to determine damage responsibility (for insurance companies). ▪ Lack of business case if the driver is not rewarded (i.e. shuttles). ▪ Lack of economic feasibility.
Technical risks	▪ No-human actions (i.e. abrupt braking) and its influence of the vehicle's passengers. ▪ Too slow automated shuttles. ▪ Risk of AV being out of connection (GPS, GNSS, etc.). ▪ Negative impact on the use of Public Transport (PT). ▪ Risk of dealing with no-programmed situations. ▪ More computing power required for higher speeds in shuttles (i.e. space and cooling issues). ▪ Issue of safety in automated shuttles due to the lack of safety belts and/or restraints for wheelchairs. ▪ User perception that the AV occupant protection is not high.

These new risks suggested during the workshop have been adjusted –when needed- and integrated to the initial risk assessment of the project.

3.3. Results of a priori AV Acceptance Risk Analysis

Upon considering the full list of anticipated risks, including also the ones identified during the 1st Workshop, the Consortium experts have performed the evaluation of the overall risks, taking under consideration the feedback from the stakeholders. Moreover, a mitigation strategy for each one of the risks has been proposed. Table 10 below includes the complete a priori Risk Assessment of the project.

Table 10: Drive2theFuture a priori Risk Assessment

Risk type* (select one)	Problem short description *	S*	O*	D*	R*	RN	Problem severity	Mitigation strategy*
Behavioural risks								
❑Technical ✓Behavioural ❑Legal ❑Operat.	Overreliance on technology (considered as level 4).	9	6	3	6	243	Severe	Clear presentation of technology limitations and what each level encompasses to. Clear communication within the OEM sales strategy.
❑Technical ✓Behavioural ❑Legal ❑Operat.	Reduced use of AVs due to technophobia and especially safety or security fears.	8	5	2	6	160	Moderate	Emphasis is put to enhance user experience inside the vehicle as well as the interface towards other travellers and the vehicles; to alleviate safety and security fears. Also, citizen engagement strategies aim to find solutions towards this goal.
❑Technical ✓Behavioural ❑Legal ❑Operat.	Mimicking of AV behaviour by non-equipped users (i.e. in platooning scenarios).	9	8	3	7	360	Severe	Enhance public awareness on the specific risk and its consequences. Also, strong supportive legal framework and enforcement during the transition period.
❑Technical ✓Behavioural ❑Legal ❑Operat.	Pedestrians or others misuse of AVs autonomous braking in violating priority or for fun.	9	8	3	7	360	Severe	Enhance public awareness on the specific risk and its consequences. Also, strong supportive legal framework and enforcement during the transition period.
❑Technical ✓Behavioural ❑Legal	Misunderstanding by non-equipped users of AV status and operation levels.	8	7	2	7	252	Severe	Develop optimal HMI to enhance VRU conspicuity of the AV actions and intentions and vice versa; including AV recognition or not of the specific VRU.

Risk type* (select one)	Problem short description *	S*	O*	D*	R*	RN	Problem severity	Mitigation strategy*
❑Operat.								
❑Technical ✓Behavioural ❑Legal ❑Operat.	Failure of HMI handover strategies for specific driver cohorts or states.	8	7	4	3	196	Moderate	Develop relevant adaptive HMI for specifics driver states and/or cohorts.
❑Technical ✓Behavioural ❑Legal ❑Operat.	User confusion due to different OEM strategies and AV levels.	6	4	2	6	96	Moderate	Emphasis to OEMs to explain simply their strategies at manuals and other communication materials. Also, de juro/ de facto regulation of common principles, i.e. through ESoP for AVs.
❑Technical ✓Behavioural ❑Legal ❑Operat.	Too many AVs in city centres may enhance traffic density, pollution and result also in traffic conflict and incidents/ accidents.	9	5	2	7	203	Moderate	AV use needs to be regulated towards ride/ vehicle sharing/ pooling; at least in major cities.
❑Technical ✓Behavioural ❑Legal ❑Operat.	Unaccepted/ false reaction of AVs in emergency situations.	10	3	9	9	270	Severe	Fail safe design and alternative (back-up) critical sensors/ systems (technical). Also, ethics-based behaviour design (behavioural).
❑Technical ✓Behavioural ❑Legal	Abuse of alcohol and drugs in AVs	5	5	5	5	125	Moderate	May be controlled through the use of in-vehicle cameras; that are needed anyway for security reasons.

Risk type* (select one)	Problem short description *	S*	O*	D*	R*	RN	Problem severity	Mitigation strategy*
❑Operat.								
❑Technical ✓Behavioural ❑Legal ❑Operat.	Impression of being in a video game by "drivers"/ passengers. Loss of awareness.	9	3	8	5	176	Moderate	Need for appropriate driverless campaigns and training schemes for all.
❑Technical ✓Behavioural ❑Legal ❑Operat.	Specific users/ group needs, i.e. young children, persons with dementia, persons with disabilities may not be adequately covered by general purpose AVs	6	5	3	5	120	Moderate	Need for inclusive design, modularity and appropriate design guidelines (i.e. ESoP for AVs)
❑Technical ✓Behavioural ❑Legal ❑Operat.	AVs sickness (motion sickness)	7	3	2	7	95	Moderate	Vehicle behaviour needs to be designed to follow a "normal" driving pattern and not be machine abilities driven.
❑Technical ✓Behavioural ❑Legal ❑Operat.	Not comfortable due to technical limitations (i.e. hard braking, etc.)	8	5	3	7	200	Moderate	Sufficient distances and speed profile need to be kept; following a "conservative" driving style; to avoid as much such event from occurring
Legal Risks								
❑Technical ❑Behavioural	Need to change current conventions (i.e. Vienna Convention).	9	9	2	6	324	Severe	It is an unavoidable process, which, however, takes time.

Risk type* (select one)	Problem short description *	S*	O*	D*	R*	RN	Problem severity	Mitigation strategy*
✓Legal ❑Operat.								
❑Technical ❑Behavioural ✓Legal ❑Operat	Liability transfer from driver to OEM or/and infrastructure operator and share between them.	9	2	9	9	162	Moderate	Clearly must be well defined in a new legal framework and significantly covered by insurance schemes.
❑Technical ❑Behavioural ✓Legal ❑Operat	Data protection and data ownership issues	9	6	7	7	378	Severe	OEMs must provide tools and mechanisms in order to guarantee the privacy of the driver and passengers. This affects not only manufacturers, but also those companies that provide the communication mechanisms between AV and the infrastructure, as well as those that host and store all the information generated. Many AV applications are based on sharing data generated by the vehicle and by the driving mode of the driver. Many of these data could provide critical information about the driver and passengers that should be private and must by anonymized.
❑Technical ❑Behavioural ✓Legal ❑Operat	Lack of appropriate insurance schemes.	9	3	2	5	95	Moderate	They constitute sine qua non condition for AVs introduction in the market. If not voluntarily/market set; they should be legislated.
❑Technical ❑Behavioural ✓Legal ❑Operat	Share of liability in case of accidents between equipped and non-equipped vehicles or VRUs.	9	2	9	9	162	Moderate	Needs to be covered by the new legislative framework and insurance schemes.

Risk type* (select one)	Problem short description *	S*	O*	D*	R*	RN	Problem severity	Mitigation strategy*
❑Technical ❑Behavioural ✓Legal ❑Operat.	BVLOS height, weight and region regulations for UAVs.	8	7	2	6	224	Severe	Need for common standards and legislation Europewide to allow BVLOS use and identify limitations and conditions.
❑Technical ❑Behavioural ✓Legal ❑Operat.	Lack of pressure from population vs other priorities (i.e. climate, immigration, unemployment).	8	6	5	5	240	Severe	A real threat; especially in view of the Coronavirus effect in the economy. Effective Use Cases are required to meet real needs.
❑Technical ❑Behavioural ✓Legal ❑Operat.	Accountability issues from infrastructure and mobility operators, in case problems occur.	9	7	5	5	315	Severe	Needs to be clearly defined and included in the new legislative framework.
Operational Risks								
❑Technical ❑Behavioural ❑Legal ✓Operat.	Lack of AV proper infrastructure maintenance.	9	7	3	6	284	Severe	Specific QoS indicators need to be extracted and included in infrastructure operation and maintenance contracts. They also need to be checked/enforced by audits.
❑Technical ❑Behavioural ❑Legal	Job loss at AV operation and especially maintenance / servicing.	7	7	7	3	245	Severe	Creating additional places for technical maintenance, supervise, and control, analyse the system functionality and market needs

Risk type* (select one)	Problem short description *	S*	O*	D*	R*	RN	Problem severity	Mitigation strategy*
✓Operat.								
❑Technical ❑Behavioural ❑Legal ✓Operat.	Need and resources for re-skilling/ up-skilling of affected workers.	7	7	3	7	245	Severe	Relevant legal and operational schemes need to be in place.
❑Technical ❑Behavioural ❑Legal ✓Operat.	Training needs of all stakeholder may not be met in time or not be synchronised.	6	6	5	7	216	Moderate	Such training schemes need to be developed, piloted and introduced into the future operational schemes.
❑Technical ❑Behavioural ❑Legal ✓Operat.	Workers and unions opposition to AV introduction.	8	6	3	6	216	Moderate	Need to work with the workers' unions early, to get their acceptance, as well as devise appropriate supportive policies for those in risk of job loss.
❑Technical ❑Behavioural ❑Legal ✓Operat.	Need of AV operation and planning data sharing with TMC/ logistics chain.	7	7	3	6	221	Severe	AV fleets management needs to be integrated within the TMCs and with all relevant logistics chains; to operate efficiently and safely.
❑Technical ❑Behavioural ❑Legal	Need for coordination of mixed flows at TMC and need of new operational algorithms.	7	7	3	5	196	Moderate	Relevant s/w and applications (including data analytics and AI) are definitely needed.

Risk type* (select one)	Problem short description *	S*	O*	D*	R*	RN	Problem severity	Mitigation strategy*
✓Operat.								
❑Technical ❑Behavioural ❑Legal ✓Operat.	Users expecting revenue back for the use of their data.	7	3	2	5	74	Moderate	Forms of indirect benefits (i.e. free use of services against provision of data) can be agreed. Minimum data provision for public benefit can be legislated.
❑Technical ❑Behavioural ❑Legal ✓Operat.	High prices of new services of AVs; impact on equity and accessibility of services for all citizens.	7	7	2	6	196	Moderate	Although costs and market conditions will define prices, relevant substitution and social schemes may be initiated by governments to guarantee equity at PT level.
❑Technical ❑Behavioural ❑Legal ✓Operat.	Users' fear of infection in car-sharing schemes.	8	9	3	6	324	Severe	Will hopefully die out with the Coronavirus emergency. Nevertheless, appropriate separation schemes/ apartments may need to be set.
❑Technical ❑Behavioural ❑Legal ✓Operat.	Lack of HD maps.	8	6	2	6	192	Moderate	Relevant maps need to be developed and maintained either by the market or with State intervention.
❑Technical ❑Behavioural ❑Legal	Need of vehicles cleaning (inside and outside).	5	7	2	5	123	Moderate	Such services need to be set and paid for.

Risk type* (select one)	Problem short description *	S*	O*	D*	R*	RN	Problem severity	Mitigation strategy*
✓Operat.								
❑Technical ❑Behavioural ❑Legal ✓Operat.	Problems with power recharge	7	5	2	7	158	Moderate	It may require bigger fleets for the same operation; if not properly solved. Need for spare vehicles/ batteries stock.
❑Technical ❑Behavioural ❑Legal ✓Operat.	Manage of drop-off areas for the AV delivery trucks.	5	7	2	6	140	Moderate	Relevant areas, procedures and technical solutions, used to be set up (relevant UC for AVs' logistics).
❑Technical ❑Behavioural ❑Legal ✓Operat.	Lack of route choice by AVs.	6	5	2	5	105	Moderate	Proper routing/ re-routing may be realised by the connected AV fleet operation centres; optimally with the context of the TMC.
❑Technical ❑Behavioural ❑Legal ✓Operat.	Integration with/ interaction to emergency services.	8	5	2	5	140	Moderate	Should be secured both autonomously by the AV (emergency vehicle detection functionality/ UC) and through its control centre.
❑Technical ❑Behavioural ❑Legal	Performing automated check-in/ check-out to determine damage responsibility (for insurance companies).	6	7	3	7	210	Moderate	Relevant automated function (i.e. based-upon digital all-around plates before and after use) needs to be implemented.

Risk type* (select one)	Problem short description *	S*	O*	D*	R*	RN	Problem severity	Mitigation strategy*
✓Operat.								
❑Technical ❑Behavioural ❑Legal ✓Operat.	Lack of business case if the driver is not totally replaced (i.e. shuttles).	9	8	2	8			Eventually, the operation of some UCs requires SAE level 5.
Technical Risks								
✓Technical ❑Behavioural ❑Legal ❑Operat	Adverse weather conditions (i.e. lane markers hidden by snow).	5	3	5	4	68	Moderate	Need to keep roads clean (QoS corresponding today to airports) or stop the service. Alternatively, other lane markers recognition technologies (i.e. with magnetic markers (can be utilised.
✓Technical ❑Behavioural ❑Legal ❑Operat.	Loss of I2V (G5 or 5G signals) or other communication failures.	9	9	4	8	486	Severe	Alternative communication means and/or use of on-board sensors are crucial to guarantee fail safe operation; also, if/when detected the vehicle should stop.
✓Technical ❑Behavioural ❑Legal ❑Operat.	Critical on-board sensors malfunctions (i.e. GPS accuracy level)	3	2	8	7	45	Slight	Back-up systems, redundant sensors, learning processes based on training phases that allow the AV to anticipate the response of the sensors in these conditions; also, if/when detected the vehicle should stop.
✓Technical ❑Behavioural	Cybersecurity attacks	10	3	7	9	240	Severe	Possible mitigation strategies include: **1) Secure buy-in from Senior leadership.** This is a must! Balance security budget vs. amount of risk your company executives are willing to assume.

Risk type* (select one)	Problem short description *	S*	O*	D*	R*	RN	Problem severity	Mitigation strategy*
❑Legal ❑Operat.								**2) Continuous employee education,** plus necessity to strengthen policy on PW protection. **3) Monitor network traffic for suspicious activity** – can you "see" in & outbound encrypted messages? **4) Upgrade and patch software immediately and promptly.** This must be done frequently as patches are released by the software vendor. **5) Implement robust Endpoint security** to protect your business from zero-day malware & user mistakes. **6) Upgrade Authentication inside and out** – including mobility & IoT policies. **7) Harden external facing web applications.** **8) Know where sensitive data resides,** then develop data protection strategy to include encryption monitoring. **9) Develop and implement** real-time monitoring strategy and analysis of log files and wire data. **10) Implement rigorous application development testing and code reviews.** **11) Perform annual penetration assessments** and vulnerability assessments. **12) Prepare for the worst-case scenario.** Develop emergency incident response (IR) plans.
✓Technical ❑Behavioural ❑Legal ❑Operat.	Too slow automated shuttles lead to low service use/ acceptance.	7	8	2	8	280	Severe	Some UCs (i.e. operation within a specific traffic environment, such as a hospital, clinic or university campus) may still be satisfied by lower speeds; expansion of service and UCs required however higher speeds**.**
✓Technical ❑Behavioural ❑Legal	Negative impact on the use of Public Transport (PT).	6	8	2	5	168	Moderate	UCs of complementarity ad co-existence need to be set-up and promoted.

Risk type* (select one)	Problem short description *	S*	O*	D*	R*	RN	Problem severity	Mitigation strategy*
❑Operat.								
✓Technical ❑Behavioural ❑Legal ❑Operat.	Risk of dealing with no-programmed situations.	8	8	5	5	320	Severe	Need for constant connection to a supervisory control centre, to decide and take over remotely the operation in such cases.
✓Technical ❑Behavioural ❑Legal ❑Operat.	More computing power required for higher speeds in shuttles (i.e. space and cooling issues).	6	7	2	8	210	Moderate	Will be possible for busses, trucks and even shuttles; but may delay private car applications.
✓Technical ❑Behavioural ❑Legal ❑Operat.	Issue of safety in automated shuttles due to the lack of safety belts and/or restraints for wheelchairs.	6	6	2	8	180	Moderate	They should be legislatively secured.
✓Technical ❑Behavioural ❑Legal ❑Operat.	User perception that the AV occupant protection is not high.	8	5	5	5			Need for awareness campaigns and user training.

4. Conclusions

The current Deliverable contains the risk analysis regarding the user acceptance of the autonomous vehicles in all transport modes. For this analysis, the extended Failure Mode and Effects Analysis (FMEA) approach has been used within the Drive2theFuture project, in order to identify risks and cluster them in categories, capturing all the dimensions of their probable impact. Using the extended FMEA methodology has allowed us to identify risks that are related to behavioural, legal, operational and technical issues related either directly to the project's outcomes, as well as indirectly to its stakeholders, and also prioritise them according to their probability, detectability, occurrence probability and severity.

Within this risk analysis, **50 risks** were identified in total for all categories, from which 14 were defined as behavioural, 8 legal, 18 as operational and 10 as technical. All identified risks have been ranked either as of moderate or as of severe significance. The risks that have arisen from this analysis are mostly related to the following issues:

- Overreliance on technology and/or wrong use of AVs technology by the users (i.e. mimicking of AV behaviour by non-equipped users, misuse of AVs autonomous braking, failure of HMI handover strategies, abuse of alcohol and drugs etc.).
- Impact on traffic density, pollution and safety, mainly in big cities.
- Need for the adaptation of legislation (i.e. relevant conventions, insurance schemes, etc.)
- Data protection and data ownership issues
- Employment and re/upskilling need and resources.
- Operational changes in TMC and logistics chains.
- Cost of relevant services.
- Issues of Integration with/ interaction to emergency services.
- Weather conditions.
- Communication failures and sensors malfunctions.
- Cybersecurity attacks.
- Impact on the use of Public Transport.

The Risk Assessment will continue until Month 30 of the project (October 2021) and will be fed also by other Activities, such as the analysis of social media in Activity 2.5 and mainly by the feedback that will be provided by the project's Pilots (WP5), which are expected to confirm or contradict the already identified risks but also identify new ones coming from social media activity and the realisation of the different pilot phases.

References

1. Bansal, P., Kockelman, K. M., & Singh, A. (2016). Assessing public opinions of and interest in new vehicle technologies: An Austin perspective. *Transportation Research Part C: Emerging Technologies*, *67*, 1-14.
2. European Commission, Autonomous Systems, Special Eurobarometer 427 / Wave EB82.4 – TNS Opinion & Social, 2015.
3. Becker, F., & Axhausen, K. W. (2017). Literature review on surveys investigating the acceptance of automated vehicles. *Transportation*, *44*(6), 1293-1306.
4. Bekiaris, E., Stevens, A. (2005), "Common risk assessment methodology for advanced driver assistance systems", Transport Reviews, Vol. 25, No. 3, p. 283-292, May 2005.
5. IEEE, 2014. You won't need a driver's license by 2040. Retrieved from http://sites.ieee.org/itss/2014/09/15/you-wont-need-a-drivers-license-by-2040/.
6. Liu, P., Yang, R., & Xu, Z. (2019). Public acceptance of fully automated driving: effects of social trust and risk/benefit perceptions. Risk Analysis, 39(2), 326-341.