Future Challenges in the Development of Mechatronic Products in the Automotive Industry: Analysis of Safety-Related Use Cases

Master Thesis Nr. 357

Scientific Thesis for aquiring the degree
Master of Science
at the TUM Department of Mechanical Engineering
of the Technical University of Munich.

Supervisor: Chair of Product Development
Hugo d’ Albert

Submitted from: Maria Belinda del Carmen Saura Pablo
Matriculation number: 03681334
ga83boz@mytum.de

Submitted on: Munich, 18.07.2018

Future Challenges in the Development of Mechatronic Products in the Automotive Industry: Analysis of Safety-Related Use Cases

Future Challenges in the Development of Mechatronic Products in the Automotive Industry: Analysis of Safety-Related Use Cases

1 Introduction

1.1 Description of the current situation

> *"Transportation is the center of the world! It is the glue of our daily lives. When it goes well, we don't see it. When it goes wrong, it negatively colors our day, makes us feel angry and impotent, curtails our possibilities."*
>
> *Robin Chase*

Mobility and transportation have been present in our society since a long time ago. Although there are different means of transportation, without any doubt the car is the most popular[1] due to the flexibility that traveling by road provides. Due to this reason, its inversion and grow in technology and design have been, are, and will be more than noteworthy, especially in the upcoming years (Liikanen, 2002, p.2).

As there are different criteria when classifying an automobile – type of engine power (steam, electric, gasoline), style... –, it is difficult to determine when the first car was invented and therefore how the technology has evolved since then, but what it is clear is that innovation in the automotive sector will continue in the coming years

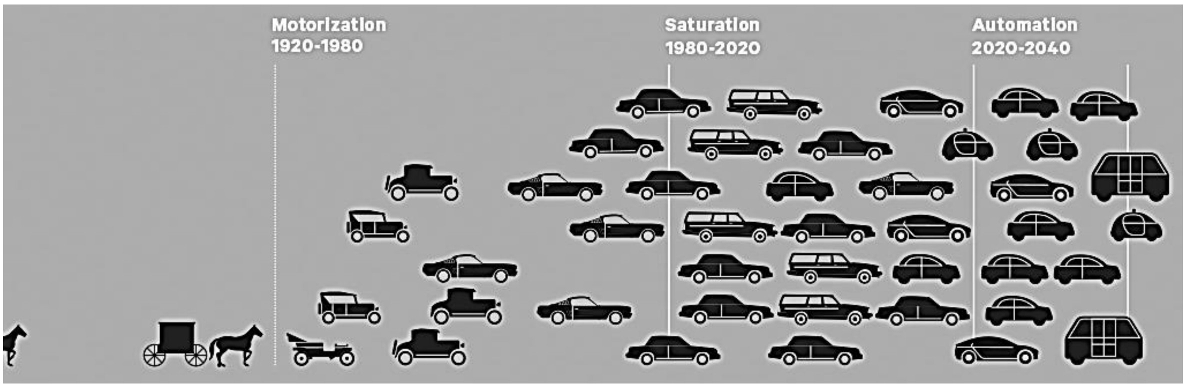


Figure 1-1: The Automobile's accelerating evolution (Boyer, 2017, pp.22-23)

It can be said that the action of driving is based on three key points: mobility, safety, and legality (Federal Automated Vehicles Policy, 2016, p.26). For a proper driving, all three should be accomplished. However, as it will be discussed in this work, sometimes one of them is missing to guarantee the other two. It is all about finding equilibrium between the three of them in order to accomplish the needs of the driver without disturbing the rest of the population. At the same time, mobility has a price, regarding the environment, sustainability and safety.

[1] Just in 2017 73.46 million cars (Statista, 2018) were produced and approximately 1.2 billion vehicles are on world's roads now (Voelcker, 2014).

Although these three aims of driving are important, this master thesis will focus on safety. According to a Eurobarometer’s survey performed by the European Commission, the drivers find safety one of the most important factors before buying a car (apart of the price) and as important as fuel consumption when choosing amongst different brands (Jarašūniene & Jakubauskas, 2007, pp.285-287).

Safety, described as the freedom of unacceptable risks, is an issue treated in different standards and norms like ISO 26262 and national and international organizations and associations (for instance Euro NCAP: The European New Car Assessment Programme). Those are concerned about how to improve people’s safety by developing new achievements not only in the cars but also on the road through safety programs).

But this matter is nothing new. Looking back through the automobile safety history[2], it can be seen how different safety systems have been incorporated in the cars and have helped to save millions of lives. Although today they can be taken for granted and assumed that all the cars will include for example seat belts, there was one point when they even did not exist, then they became an optative feature, and afterwards, they were mandatory for all the new cars. The same has happened with other safety systems such as airbags, anti-lock braking systems, head restraints…and a long et cetera.

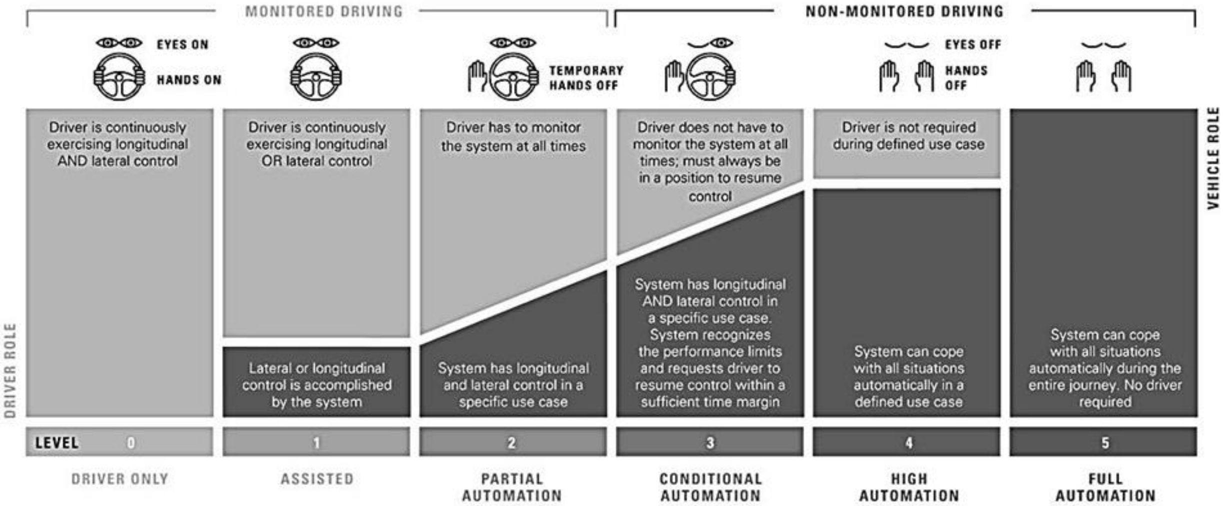
These days when it seems that all the mechanical safety-related features are already discovered, the efforts are directed to the electronic (or mechatronic) and software systems in order to improve or replace the current mechanical ones due to different reasons: some functions cannot be deployed without electronics (navigation), control for the achievement of lower fuel consumption, lower emissions, engine control, lower costs for the manufacturer, supplier and customer and last but not least, the increase of passive and especially active safety systems (Benz, 2004, pp.3-5).

Since passive safety systems (the ones that aim to mitigate the damages when a car accident has occurred) are already quite highly developed, the focus is the active safety systems, which aim to avoid the car accident per se (Vritika, 2015). And due to the new appearing innovative technologies and the decrease of cost of some of the already existing ones, it is practically obvious that the automotive industry will culminate at the end in autonomous driving: the driver will not take part in the drive under any circumstance and will be able to enjoy the ride as if he was one more passenger more. But what is more important, apart from this comfort, is that around 90% of car accidents can be avoided when eliminating the driver and thus the human factor (U.S DOT. NHTSA, 2008 cited in Smith, 2013, p.1).

According to Gerla et al. (2014, pp.241-246), the succeeding step in this evolution is just around the corner: the internet of autonomous vehicles. Like other important instantiations of the internet of things (IoT), autonomous vehicles will have communications, storage, intelligence, and learning capabilities to anticipate the customers’ intentions. The concept which will support this transition is called vehicular cloud (comparable to internet cloud for vehicles) providing all the services necessary for the autonomous cars.

[2] See Annex *A1 Safety car timeline*

However, this step to autonomous cars will not be absolute and direct but progressive. Depending on the automation level, the Society of Automotive Standard (SAE, 2016) distinguishes 6 levels:



Driver is continuously exercising longitudinal AND lateral control

Driver is continuously exercising longitudinal OR lateral control

Lateral or longitudinal control is accomplished by the system

Driver has to monitor the system at all times

System has longitudinal and lateral control in a specific use case

Driver does not have to monitor the system at all times; must always be in a position to resume control

System has longitudinal AND lateral control in a specific use case. System recognizes the performance limits and requests driver to resume control within a sufficient time margin

Driver is not required during defined use case

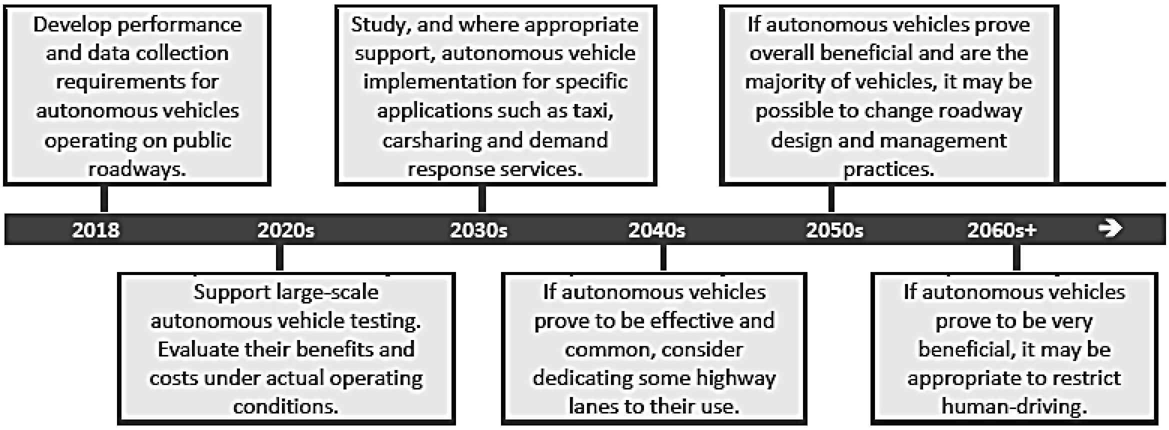
System can cope with all situations automatically in a defined use case

System can cope with all situations automatically during the entire journey. No driver required

Figure 1-2: Levels of automation (Lemanski 2016 cited in Hawes, 2016, p.1).

Autonomous driving will be treated with more detail in next chapters. However, even though it can be assumed that in the long-term future autonomous driving will be fully achieved and thus bring mobility safety to new heights, until that point there will be other, transitional forms of transport, as it will be described in *2.2Future trends and challenges*.

It will be precisely this coexistence and interaction between the different transitional technologies that will hamper the task of transportation professionals like planners, engineers and policy analysts or make it more difficult. According to authors such as Litman (2018, p.29), these stakeholders play important roles in the development and deployment of driverless cars. They will be affecting the transport planning until and beyond the full automation stage will be reached for the monopoly of cars on the roads.



2018: Develop performance and data collection requirements for autonomous vehicles operating on public roadways.

2020s: Support large-scale autonomous vehicle testing. Evaluate their benefits and costs under actual operating conditions.

2030s: Study, and where appropriate support, autonomous vehicle implementation for specific applications such as taxi, carsharing and demand response services.

2040s: If autonomous vehicles prove to be effective and common, consider dedicating some highway lanes to their use.

2050s: If autonomous vehicles prove overall beneficial and are the majority of vehicles, it may be possible to change roadway design and management practices.

2060s+: If autonomous vehicles prove to be very beneficial, it may be appropriate to restrict human-driving.

Figure 1-3: Autonomous vehicle planning requirement time-line (Litman, 2018, p.27)

As figures show, the increase in safety is more than enough reason to develop and make use of autonomous cars. In the next paragraphs those reasons will be justified and supported by other ones and also the disadvantages that are delaying its adoption will be presented.

Thus, this problem statement through the advantages and drawbacks of reaching further stages of automation will reveal the need of support that engineers have in the development process, as in *1.2.Problem statement. Motivation* will be justified.

This concept of safe system approach and the vision of zero accidents have become increasingly adopted by researchers, road safety practitioners, and stakeholders internationally (Yannis & Cohen. 2016, pp.14-15).

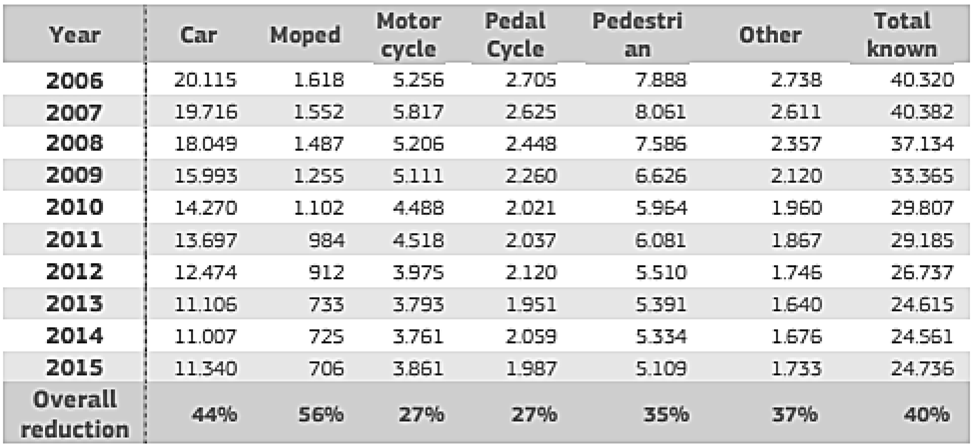
> "*Every year, 1.2 million people are killed in traffic accidents. Many more are maimed and injured. Artificial intelligence holds a promise to save millions of lives by making our cars smart enough to avoid accidents. At the same time, it promises to offer mobility to people unable to operate a vehicle".*

(Pratt, 2016, p.1)

This means, according to Gill Pratt, CEO of Toyota Research Institute at the GPU Technology Conference (Pratt, 2016, p.1) that driverless cars will be able to save more than a million lives every year.

Moreover, as the Road safety statistics that the CARE[3] (CARE, 2017) shows, the number of road fatalities by car has declined around 44% since 2005 (data available in May 2016).

Table 1-1: Number and reduction of road fatalities by mode of transport, EU, 2005-2015 (CARE, 2017, p.12, Table 3).



Year	Car	Moped	Motor cycle	Pedal Cycle	Pedestri an	Other	Total known
2006	20.115	1.618	5.256	2.705	7.888	2.738	40.320
2007	19.716	1.552	5.817	2.625	8.061	2.611	40.382
2008	18.049	1.487	5.206	2.448	7.586	2.357	37.134
2009	15.993	1.255	5.111	2.260	6.626	2.120	33.365
2010	14.270	1.102	4.488	2.021	5.964	1.960	29.807
2011	13.697	984	4.518	2.037	6.081	1.867	29.185
2012	12.474	912	3.975	2.120	5.510	1.746	26.737
2013	11.106	733	3.793	1.951	5.391	1.640	24.615
2014	11.007	725	3.761	2.059	5.334	1.676	24.561
2015	11.340	706	3.861	1.987	5.109	1.733	24.736
Overall reduction	44%	56%	27%	27%	35%	37%	40%

Nonetheless, with around 25600 deaths in 2017 and a vast number of serious injuries for every loss every year in European traffic (CARE, 2018), the road remains as the mode of transport less safe. Apart from this data, what is also worrying is that around 94% of crashes can be tied back to either human error or bad decisions, according to a report recently released by the NHTSA (Welch, 2016, p.1).

Due to this fact, although the numbers of fatalities have decreased in the past years, the need for safety systems that makes it possible to increase the level of safety (not only for the

[3] Community Road Accident Database that European Commission provides every year.

passengers but also for the pedestrians and other drivers) and reliability (without forgetting the affordability) is still evident. As Gill Pratt in the GPU Technology Conference pointed out:

"How about saving lives? Do we have to wait until the system is perfect? Well, the answer is no. In fact, anti-lock brakes have saved many lives now. Stability control has saved lives. There's something called automatic emergency braking, which is when the car stops if it's about to hit something in front. So, these systems can save lives now. You don't have to wait until you're perfect and can drive on the road 100 percent of the time."

(Pratt, 2016, p.6)

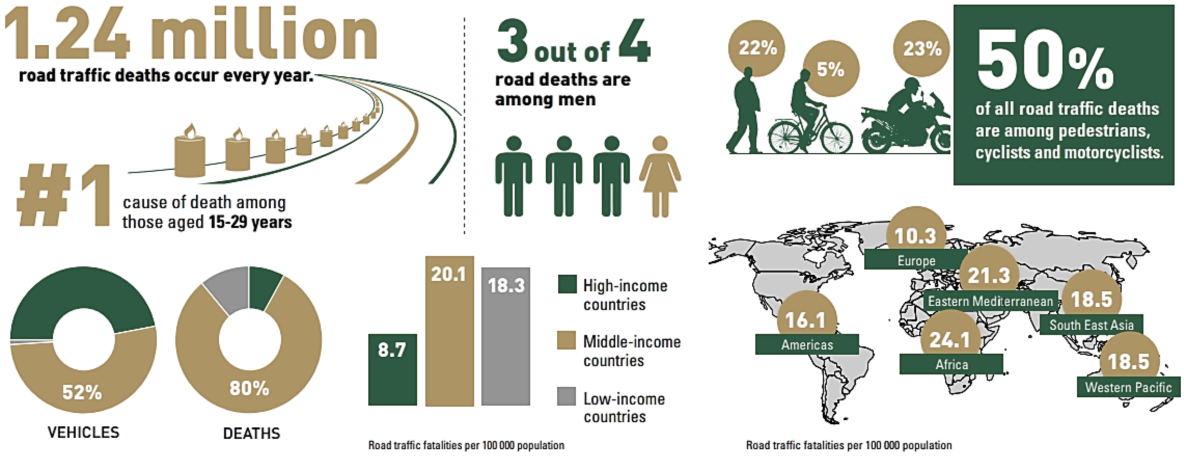


Figure 1-4: Road traffic injuries: the facts (World Health Organization, 2014)

Apart from the unquestionable safety aspect, there are also other advantages such as the comfort and relief of vehicle occupants from driving and navigations chores; possible mobility also for old people and those with disabilities; reduction of fuel consumption and pollution thanks to more foresighted driving decrease in the need for traffic police and vehicle; reduction of space required for vehicle parking; improvement of the traffic and fuel efficiency; increase of free time.... To sum up, autonomous cars will be environmental-friendly machines, that make streets safer and save time and space. (Litman, 2018, pp 5-12)

Nonetheless, the adoption of driverless cars cannot be possible as easy and quick as it would seem for the following reasons.

Firstly, a recent survey performed by AAA (Monticello, 2016, p.1) shows that 84% of respondents who do not want semi-autonomous features on their next vehicle (about 40%) trust their own driving skills more than the technology.

According to Olsen (2017, p.3), when they were asked "How much would you consider paying for a car that completely drives itself," the 48 % said, "*I would never purchase a car that drives itself*." The reasons are mainly the following ones: "*loss of control*" (37%), "*I don´t trust it*" (29%), "*It will never work perfectly*" (25%), "*It´s not safe*" (21%).

William Wallace, the policy analyst for Consumers Union, also points out in Olsen (2017, p.3): "*Companies developing autonomous cars have a lot of work to do before consumers* *will be ready to turn over the driving and to build trust, they should share test data with the public that demonstrates safety benefits".*

Other impediments summarized in the work of Goodman (2016, p.4) are the high price due to its advanced technology and sophisticated components, out of the price range of most ordinary people; the loss of jobs such as truck and taxi drivers and car insurances (Simpson, 2017, p.1); the fact that a computer malfunction might cause worse crashes than the ones caused by human factor, the uncertainty about who's fault is in case of accident (software designer, owner of the car…); privacy concerns about the data collection; security issues due to hackers; possible problems under certain types of weather (heavy rain might interfere with roof-mounted laser sensors, wind could cause sensors misaligning, snow can confuse the cameras…); the challenges for a robot to read, interpret and react to human road signs (Brooks, 2017, pp.1-3); the relaxation, over-trust, and decrease of experience and careless of drivers with respect to the usual driving; possible modification need of new road systems and infrastructures; possible use for terrorists, using them as moving bombs (Harris, 2014, pp.1-3); ethical problems derived from the decision making when the car is programmed to react to a conflictive situation (Lin, 2015, pp.69-82); driving down of organ donation (Houser, 2018, p.1). etc…

As previously seen, there are lot of advantages that encourage the society to adopt autonomous cars in the nearly future as the safest mobility option, but there are also a lot of problems, or better called, challenges (especially in the mechatronics systems) that still need to be discovered, analysed, solved, tested and improved. Autonomous cars will be the culmination of this drive to the future (Litman, 2018, p.27) and also the core part of this work. However, other trends are going to be analysed as well, since they also take part on these future challenges and autonomous cars are one just one of many factors that affect future transport demands, as Litman (2018, p.24) affirms.

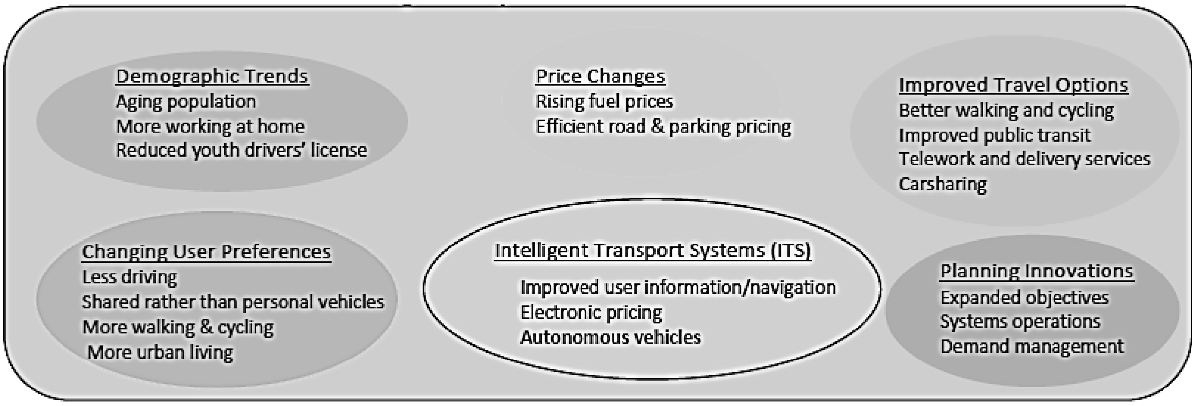


Figure 1-5: Factors affecting transport demands (Litman, 2018, p.24)

1.2 Problem statement. Motivation

Until now it was seen what could be considered as an overall vision of the current or initial situation with regard to transportation, safety and the expectations gradually shifted towards autonomy and its benefits for the society.

Since this is a scientific work framed within the field of product development in the industrial engineering, it can be said that the motivation of this work is to help engineers to find an approach to identify, analyze and model the future challenges that will be found in the complex development process of these new forms of transportation. Concretely, this approach will take place in earlier phases of the product development process such as the Concept phase and concretely along the Item definition suggested by ISO 26262

As explained in the Expose at the beginning of this work, in the same way it happened from the 90's till nowadays, in the upcoming decades the automotive industry (and any other technology industry) will experiment the development and adoption of new mechanical, electrical and electronic components. These new mechatronic products, along with new software, will come hand in hand with an indisputable increase in complexity, especially as regards product development process. As Abdulkhaleq et al. (2017, p.3) suggest, this unceasingly growing complexity and amount of functions and networked ECUs will result in new requirements design for the new technologies and modules as well as major redesign of E/E architecture and their design criteria. This fact motivates indeed the elaboration of this master thesis, since it aims to accomplish a process or engineers' work less complex, more optimized, transparent and safer.

It is true that with the release and the obligatory compliance of ISO 26262 in 2011, automotive development process experienced impressive progress. As it can be seen along this document, this standard titled "Road Vehicles – Functional Safety" (ISO, 2011) discusses at some length the different requirements that electric and electronic systems must follow to guarantee their functional safety. Before its publication, there were no directives on functional safety in the automotive industry and the car manufacturing companies were able to decide to adhere or not to the requirements of IEC 61508- Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (International Electrotechnical Commission, 2010), according to Cherfi (2015, p.19).

However, as the work of Abdulkhaleq et al. (2017, pp.3-4) points out, the scope of ISO 26262 becomes too small regarding future trends with no driver's presence: the existent approaches will turn to be less effective (they focus on component failures) and there will be new causes of accidents that nowadays are not envisaged (they will happen not only because of component failures but also not due to them. i.e. component interaction accidents). Apart of these, these authors identify some challenges of ISO 26262 for future trends, especially for full-autonomous drivers: it does not recommend any method for system definition; it suggests diverse hazard analysis but focused only on functional safety (non-functional safety is not covered); it is not established for fully automated driving, assuming that the role of the driver is always present and not considering other hazardous events.

With the uncertainty and no availability of any further standard than ISO 26262 for the future trends, the motivation of this work is to face this problem, to find, based on the framework of ISO 26262, a new approach for the future challenges.

Moreover, research lacks a standard that provides practical guidelines for practitioners who want to develop safety cases[4] for cars. There is no standard that describes how the safety arguments should be evaluated in the functional safety assessment process (Birch, 2013, p.154; Baumgart, 2016, p.i). Thus, the aim of this thesis is giving engineers procedures for the development process of new mechatronic products that guarantee safety and reliability, or maybe further properties that in the future will become more relevant.

By making use of a modelling language, this work will suggest some safety-related use cases trying to model the risk situations that there are in mobility in order to give an approach for how to construct a safety case that guarantees the different safety requirements. While doing that, it will be tried to broad the scope of ISO 26262 regarding models for product development[5] and quality methods[6] among others.

Besides of that, this problem is also strengthened with the fact that although drivers and operators are blamed for accidents most of the time (since they are the direct result of the operator’s loss of control of the system), further investigations have revealed that the 75% of them are caused by system malfunctions that preceded the operator’s actions. In its turn, along with reports at the 2003 Informatics Conference in Germany, 55% of these failures or malfunctions are caused by software and electronics (Schoitsch, 2005, p.7). Hence these imperfections in the system leave the most difficult situation to a human operator, after every attempt carried out by the system is unsuccessful and cannot correct the situation, as Kim (2016, p.1) points out.

To sum up, the motivation of this work is underpinned by the fact that current systems are getting more and more complex with the goal of giving users more functionality by integrating diverse components with different technologies. These multi-disciplinary systems (normally mechatronic systems) need new appropriate processes, tools, and methodologies for their design, analysis, verification, and validation processes. Mhenni (2014, p.i) points out that these new approaches must make systems and their development processes to remain competitive also in terms of cost and time-to-market, but what is more important for our work, they have to ensure safety.

[4] Or argument in which the safety requests are exposed to be complete and fulfilled by the evidence generated from ISO 26262 work products.

[5] See chapter *2.4Procedural models for system development of mechatronic systems.*

[6] See chapter *2.3Quality methods*

1.3 Aims

As the title of this document enunciates, this master thesis aims to evaluate the safety-related challenges related to new ADAS (Advanced driver-assistance systems) and their impact on the possible failures. In this context, the related current methods or standards will be assessed how far they will be able to overcome the challenges of the future.

This analysis will be carried out through the description of different uses cases and the succeeding modelling through an appropriated modelling language.

While doing this study, this thesis also aims to acquire new knowledge about the type of failures in development process of safety-related components and their impact on the whole item (car), and the causality of them, as well as different process development methods and standards that help when developing new, safer and more reliable systems.

Furthermore, this master thesis intends to support automotive developers with the creation of new mobility trends by identifying possible safety problems and translating them into uses cases for subsequently modeling them.

As already seen in the introduction, the number of traffic fatalities underlines the urgency of developing safer automotive functions. Partly due to this reason, new forms of mobility are starting to irrupt in our roads and lives (and they will do even stronger in the not too distant future). These new trends, in turn, will imply new challenges for engineers due to the high level of complexity of their functionalities and features. Hence, it is the goal of this thesis to derivate the threats or challenges that will arise during the development process of future transportation technologies. In summary, this work aims at supporting engineers to ensure a safe and secure development process, by generating scenarios where hazards or risks can be identified with the help of use cases approach and their modelling.

As already stated in the Motivation of this work, different standards such as ISO 26262 require the elaboration of safety cases in order to argument and guarantee the compliance with the safety requirements. However, they do not specify how to demonstrate it. For that reason, it is intended to assist the developers in the automotive industry in providing an approach based on the elaboration of use cases that addresses the threats and challenges of the forthcoming mobility forms.

To sum up, this thesis has the following aims:

- Identify the challenges of the future related to reliability and safety of the technical systems.
- Identify the methods or approaches in use today to meet the challenges of tomorrow.
- Identify the gap that can be closed by the current methods and give recommendations for new approaches.

1.4 Research methodology

The methodology used for writing this master thesis is the one detailed explained in the book *DRM, a Design Research Methodology* by Blessing & Chakrabarti, 2009. In their book, an overall framework and a stepwise, hands-on approach to design research is described. It is intended to support them by proposing methods and guidelines to perform the stages of design research, providing pointers to already existing useful approaches, and helping to document and disseminate research results effectively (Blessing & Chakrabarti, 2014, pp.10-11, 14).

DRM consists of four stages, which are: Research Clarification (RC), Descriptive Study I (DS I), Prescriptive Study (PS) and Descriptive Study II (DS II) (Blessing & Chakrabarti 1992; Blessing & Chakrabarti, 1995). The correlation between these steps is shown in the figure below:

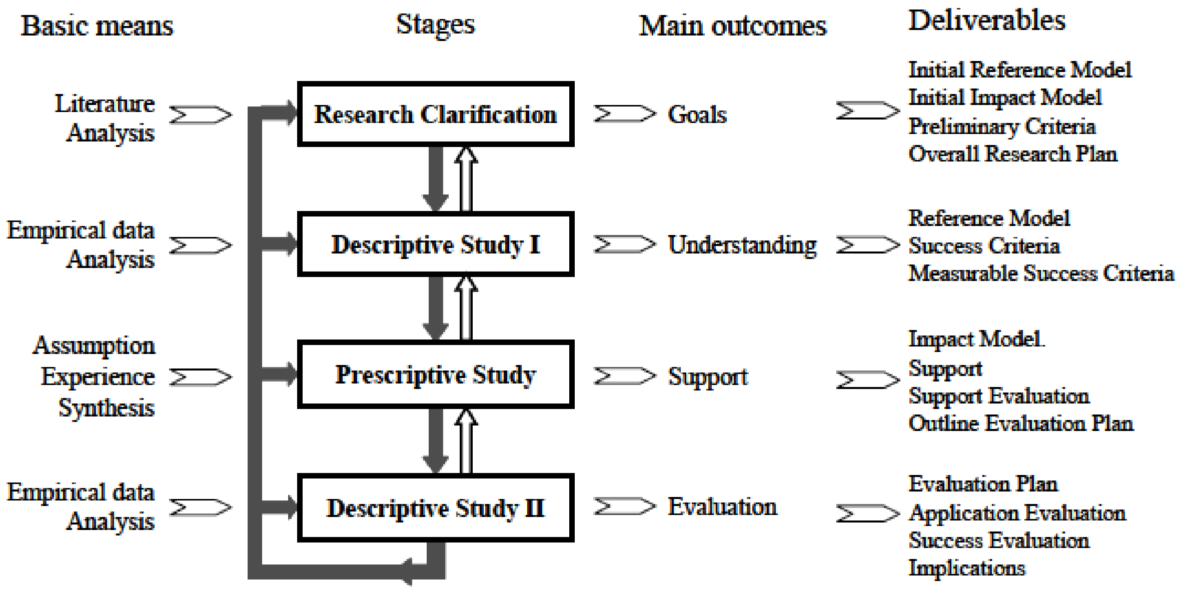


Figure 1-6: DRM framework: stages, basic means, and deliverables (Blessing & Chakrabarti, 2009, pp.15,39).

As it can be seen, this methodology is a four-stage iterative process where through different means diverse goals are achieved and diverse deliverables are generated.

In the following paragraphs, a brief explanation of each stage according to the authors of the book is given, according to Blessing & Chakrabarti (2009, pp 14-16):

In the first stage, *Research Clarification*, the researchers aim at finding evidence or indications that support their assumptions with the purpose of formulating a realistic and worthwhile research goal. This is achieved by reviewing the literature for factors that influence task clarification and product success. Based on the findings, an initial description of the existing, current or initial situation is developed, as well as a description of the desired situation (Blessing & Chakrabarti, 2009, pp. 15, 29-31, 43)

In the *Descriptive Study I* (DS-I) design science researchers review the literature for more influencing factors to elaborate the initial description of the existing situation. In order to determine which factors should be addressed to improve, task clarification should be carried out as effectively and efficiently as possible. Therefore, the second stage aims at increasing the understanding of not only the existing situation but also the design and its success factors thorough reviewing the literature about empirical research, undertaking empirical research and reasoning (Blessing & Chakrabarti, 2009, pp. 15-16, 31-33, 75)

For the *Prescriptive Study* (PS), Blessing & Chakrabarti state that in this stage

> *"Researchers use their increased understanding of the existing situation to correct and elaborate on their initial description of the desired situation. This description represents their vision of how addressing one or more factors in the existing situation would lead to the realisation of the desired, improved situation. They develop various possible scenarios by varying the targeted factor(s)."*
>
> (Blessing & Chakrabarti, 2009, p.16)

The main objective of this stage is the determination of the factors that improve the existing situation, using the understanding from DS-I and DS-II.

Afterwards, researchers proceed to the *Descriptive Study II* (DS-II) stage to examine the application and impact of the design support and its capability to realise the desired situation thorough empirical studies. Therefore, while the aim of DS-I is to increase the understanding of design, the goal of DS-II is to understand the usability and applicability of what they call Actual Support (Application Evaluation) and its usefulness (Success Evaluation) Blessing & Chakrabarti, 2009, p. 16, 35-36, 41, 181).

1.4.1 Structure of the thesis

The structure that this thesis follows adheres to the DRM design research process described above. Although the DRM design is the core of this thesis' structure, the division and the title of each section do not follow the DRM stages but also include recommendations sections. Nonetheless, between the stages and the different sections of this work exists a correlation. In the following this connection is explained.

The first stage, *Research Clarification*, would clearly correspond with the first chapter, the 1. *Introduction*. As already mentioned, the goal of this stage is to find evidence through a literature analysis, that supports the goal of the master thesis and describe not only the current situation but also the desired one. That was exactly what in *1.1 Description of the current situation* is done, where general facts about the act of driving were presented as well as how safety, legality, and mobility must go hand in hand to guarantee it. Also the automobile evolution was briefly mentioned, i.e., in which point we are nowadays and in which direction we will drive in the upcoming years. Figures and facts that call for an increase in safety were searched and exposed. In *1.2 .Problem statement. Motivation* the situation in the roads is put aside in order to give way to the product development process situation. In this way, due to different issues that ISO 26262 leaves open and will be even more uncertain, complex and challenging in the future, the elaboration of this thesis is justified and supported in *1.3Aims*. In it, clear goals and focus are attained (the aim of the stage I) and described Therefore, through secondary data from scientific papers, journals, conferences, manuals, articles, slides, videos and safety programs, not only qualitative data can be gathered but also some quantitative regarding the number of deaths and crashes.

The stage II (Descriptive Study I) corresponds with chapter *2.State of the art.* In this chapter, different influencing factors of the problem will be reviewed in the literature to have a good understanding of the existing situation. A few examples of factors that not only might influence the initial description but also will improve task clarification will be named. E.g. quality methods and procedural models used in system development; standards related with automobiles and safety; system modeling languages; and also a deep overview of principles or fundamentals linked with automotive industry.

The next stage, Prescriptive Study, would be embodied in chapter *3. Analysis and modelling of Use Cases* since as the authors suggest, through developing possible scenarios an initial description of the desired situation can be elaborated as well as determining which factors improve (or not) that situation.

This master thesis will be concluded in chapter *4. Conclusions, limitations and future work*, which will extract the findings and limitations. Moreover, recommendations for future will be given. This outlook to the future will reflect the idea of Blessing & Chakrabarti (2009, pp. 38,181) about identifying necessary improvements for the desired situation.

2 State of the art

The concept *state of the art* refers to the most recent, sophisticated or advanced stage in the development of a product, process or technology. In other words, it shows the level of development reached at any particular time generally as a result of modern methods.

This chapter will be based on a literature review and will be divided into different sections: the first one, *2.1 Dependability*, will introduce this key concept as an umbrella term for other properties that future products should ensure. One of these included attributes is safety, which will be addressed with greater detail.

In the chapter *2.2Future trends and challenges,* the future forms of mobility that will emerge until reaching the total autonomy are presented. The principal components as well as their advantages and disadvantages are described in order to clarify the possible threats or challenges.

Later on, in *2.3 Quality methods,* different approaches, both inductive (such as FMEA) and deductive (like FTA) will be briefly defined. These well-known methods are essential for performing safety analyses of systems and their components, which in turn are assessed by different risk classification schemes suggested by ISO 26262 such as HARA or ASIL. Those are used to determine the safety aims for the item in order to avoid an unreasonable risk. In order to be efficiently exploited by systems designers, those safety analyses have to be carried out since the early design stages. The benefit of influencing design requirements in an early phase is that the later those changes are made the more expensive they become (Mhenni et al. 2014, p.34).

The named design stages are envisaged in the different system engineering models contemplated by ISO 26262 and outlined in section *2.4 Procedural models for system development of mechatronic systems.*

This ISO26262, as well as other norms related to safety and process design, will be covered in *2.5Safety-related standards.*

Finally, in *2.6 System modeling languages,* different tools for graphically modeling complex systems will be presented. Thanks to the literature, it will be possible to choose the most appropriated one for modelling the future challenges that the upcoming mobility trends will have to face.

2.1 Dependability

According to Ross (2016, p.26), ISO does not use this term, but mainly safety, reliability and the relation between them. However, this fact does not mean any contradiction since dependability is a concept that encompasses diverse characteristics, including safety and reliability among them, as it will be seen in the following sections. The adoption of this broader feature can be attributed to its wider scope, which as soon as new products for including new functions start to emerge, the challenges and hazardous situations to face will also appear, which will be more complex and therefore demanding. For this reason, dependability, and thus safety, will be the term utilized in order to reach and address the greater number and types of challenges in the future.

Dependability is the ability of a system to deliver its intended level of service to its users (Laprie, 1992 cited in Dubrova, 2013, p.5). For Avizienis et al. (2005, p5), dependability of a system is the aptitude to deliver service which can be justifiably trusted or the ability to avoid service failures that occur more often and are more severe than is acceptable.

It is related to the terms dependence and trust and has three fundamental characteristics (attributes, impairment, and means) that are going to be explained hereafter:

2.1.1 Attributes of dependability

They describe the required/expected properties of a system. The three primary are reliability, availability, and safety, while maintainability, testability, performability, and security would be labelled as secondary, which might vary depending on the authors. Dubrova (2013, pp.6-9), defined them as:

- Reliability: Probability of success and that a system offers a continuous delivery of correct service in an interval of time.
- Availability: Probability that a (discontinuous) system operates correctly at a certain instant of time.
- Safety: Probability that the system either performs its functions correctly or stops in a fail-safe manner. This attribute as well as other aspects related with it will be explained at the end of this subsection due to the importance ISO 26262 gives to them and the relevance for this work.

- Maintainability: Measure of the restoration time from the last experienced failure, or equivalently, of the continuous delivery of incorrect service. In other words, it measures the ability to undergo modifications and repairs.
- Testability: Measure of the easiness in which a system can be tested in order to also measure its correctness.
- Performability: Measure of how well a system performs over a period of time.
- Security: Measure of the prevention of unauthorized access and/or handling of information. For other authors is considered as a property independent of

dependability which brings in concerns for confidentiality (absence of unauthorized disclosure of information), availability (readiness for correct service) and integrity (absence of improper alterations) (Avizienis et al. 2004, pp.1, 5).

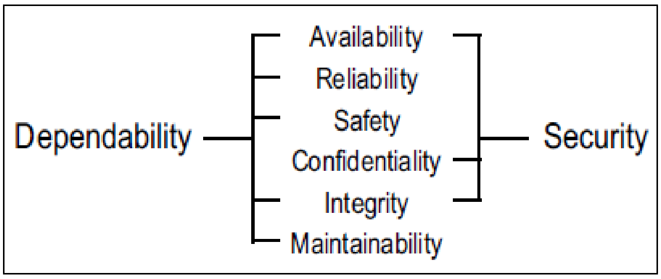


Figure 2-1: Dependability and security attributes (Avizienis et al. 2004, p.5).

As pointed out above, some of the secondary attributes such testability and performability are sometimes not included and substituted by confidentiality and integrity. There are also other attributes particularly relevant for security, which depending on the authors, they might vary. Examples of them, according to Cachin et al. (2000) cited in Avizienis et al. (2004, p.21) are accountability, authenticity and non-repudiability, which are a combination of availability and integrity with respect to the identity of the person, the origin and content of the message and its sender or receiver, respectively.

Not all these attributes may be required for a given system since every class of faults and environment have their own requirements in terms of acceptable frequency and severity of failures (Avizienis et al. 2004, p.5).

Returning to safety attribute, according to ISO 26262 (ISO, 2011 cited in Ross, 2016, p.8), in relation to technical systems or products, safety is described as the freedom of unacceptable risks.

It is divided into non-functional safety and functional safety, which is addressed in the mentioned standard. These two types of safety, as well as other safety-relevant subjects, will be in the next paragraphs defined.

Functional safety

ISO 26262 defines it as the absence of unacceptable risk due to hazards, which are caused by malfunctioning behaviour of E/E systems. It is the correct technical reaction of a technical system in a defined environment, with a given stimulation as an input of the technical system (Ross, 2016, p.8).

According to IEC 61508 (IEC-International Electrotechnical Commission, 2010), functional safety involve the detection of a potentially dangerous condition and the activation of a protective or corrective device or mechanism in order to prevent hazardous events arising or providing mitigation to diminish its consequences respectively. For Birch (2013, p.156) the concept of functional safety specifies safety measures in the vehicle architecture, (together with fault detection and failure mitigation mechanisms) in order to satisfy the safety goals, as well as technical, software and hardware safety requirements. These claims follow this hierarchy:

- Safety Goals (hierarchy 1) – the vehicle in its environment.
- Functional Safety Requirements (hierarchy 2) – the vehicle and its systems.
- Technical Safety Requirements (hierarchy 3) – the E/E system.
- Hardware and software requirements (hierarchy 4) – component and part level.

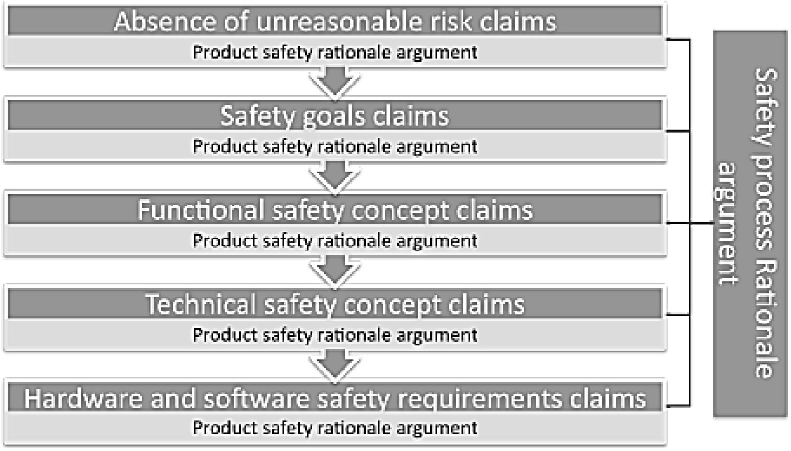

Absence of unreasonable risk claims
Product safety rationale argument
Safety goals claims
Product safety rationale argument
Functional safety concept claims
Product safety rationale argument
Technical safety concept claims
Product safety rationale argument
Hardware and software safety requirements claims
Product safety rationale argument
Safety process Rationale argument

Figure 2-2: Implicit ISO 26262 Safety Argument Structure.(Birch, 2013, p.157).

On the other hand, the Functional safety *assessment* is concerned with making a judgement on the functional safety achieved by the item and therefore with the characteristics of the product.

Non-functional safety

According to Cherfi (2015, p.19), "u*ndesired events such as electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy, are considered as non-functional unless directly caused by malfunctioning behaviour of E/E safety related systems".*

Operational safety

According to Abdulkhaleq et al. (2017, p.7), operational safety or roadworthiness is the ability of a vehicle to be in an appropriate operation condition or meeting adequate standards for safe driving.

Safety Case

Argument that the safety requirements for an item are complete and satisfied by evidence compiled from work products of the safety activities during development (ISO 26262 cited in Birch, 2013, p.155). According to Kelly (1998, p.22), a safety case should communicate a clear, comprehensive and defensible argument that a system is reasonably safe to operate in a particular situation.

Safety goals

According to ISO 26262 cited in Ross (2016, p.90) they are the result of hazard and risk analysis and seen as safety requirements of the highest level.

Safety-Lifecycle

It condenses the most important safety activities in the conceptual phase, the series production and the series production release.

A central management task is the planning, coordination, and proof of these activities throughout all phases of the lifecycle. It is divided into 3 phases: Concept-, Product development and After production release/approval (Ross, 2016, p.36).

Safety-in-use

It is the absence of hazards due to human error (Abdulkhaleq et al., 2017, p.7). It considers that the intended function, since it operates or behaves correct, does not lead to any harm. The classical failure analyses cannot be considered for this analysis (Ross, 2016, p.171).

Safety of the intended functionality

According to Abdulkhaleq et al. (2017, p.7), it is the lack of unreasonably hazardous functionality.

Safety validation

In ISO 26262, Part 4, Clause 9 the objectives of this stage are stated:

> "*The first objective is to provide evidence of compliance with the safety goals and that the functional safety concepts are appropriate for the functional safety of the item.*
>
> *The second objective is to provide evidence that the safety goals are correct, complete and fully achieved at the vehicle level. "*

(Ross, 2016, p.238)

2.1.2 Impairments of dependability

They express the reasons for a system to cease to perform its functions. These also called threats to dependability are frequently defined, depending on where the problem occurred, in terms of faults (physical level), errors (computational level) or failures (system level).

Dubrova (2013, pp.9-10) defines them as:

- Fault: Physical defect, imperfection, or flaw that occurs in some hardware or software component (for example a short circuit in the batteries of an electric vehicle).
- Error: Deviation from correctness or accuracy in computation, which occurs as a result of fault (for example incorrect information was received in a connected car).
- Failure: Non-performance of some due or expected action. The system fails or has a failure if the service it delivers to the user deviates from compliance with the system specification for a specified period of time as a result of a fault (Laprie, 1992 cited in Dubrova, 2013, p.9).

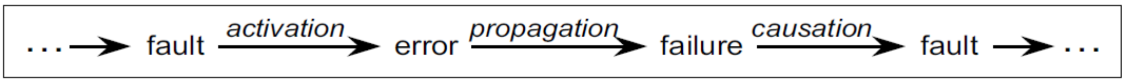


Figure 2-3: The fundamental chain of dependability and security threats (Avizienis et al. 2004, p17).

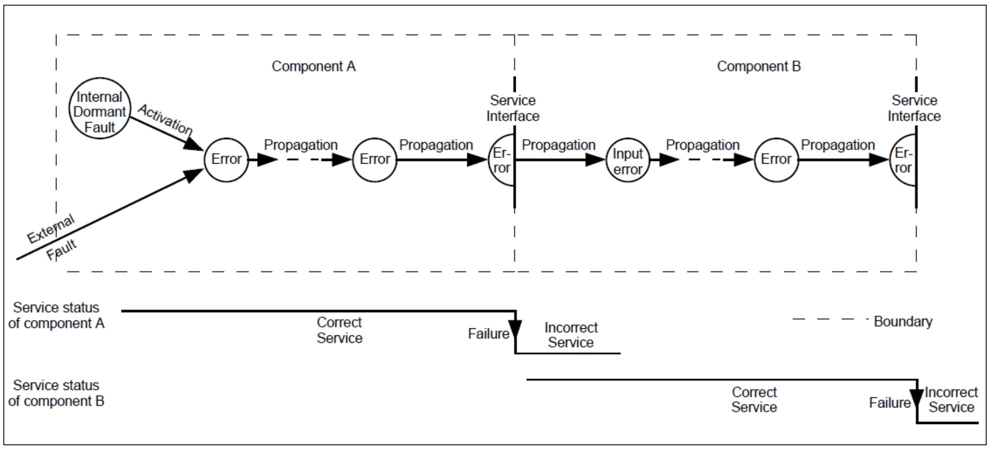


Figure 2-4: Error propagation (Avizienis et al. 2004, p17).

Neither this author nor ISO 26262 give an explicit definition of accident and hazard, but according to STPA (Systems Theoretic Process Analysis) cited in Thomas (2013, p.11):

- Hazard: A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss) (Thomas, 2013, p.11).
- Accident: An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.[7] (Thomas, 2013, p.11).
- Risk: Probability of damage or loss as a result of a distinct behaviour or events; this

[7] See annex *A.2Type of car accidents*

> refers to hazardous/dangerous situations in which unfavourable consequences may occur but do not necessarily have to. (Ross, 2016, p.7)

According to ISO 26262, part 3, appendix B1:

> *"A risk (R) can be described as a function (F), with the frequency of occurrence (f) of a hazardous event, the ability of the avoidance of specific harm or damage through timely reactions of the persons involved (controllability: C), and the potential severity (S) of the resulting harm or damage: R = F(f ; C; S")*[8]

(Ross, 2016, p.11)

All these concepts are interconnected as the figure below shows: Faults are reasons for errors, errors are reasons for failures and failures are reasons for hazards, and hazards, depending on the level of risk, can be reasons for accidents. But not every one of them causes the other. A fault is active when it causes an error, and if not, it is dormant (Avizienis et al, 2004, p.4).

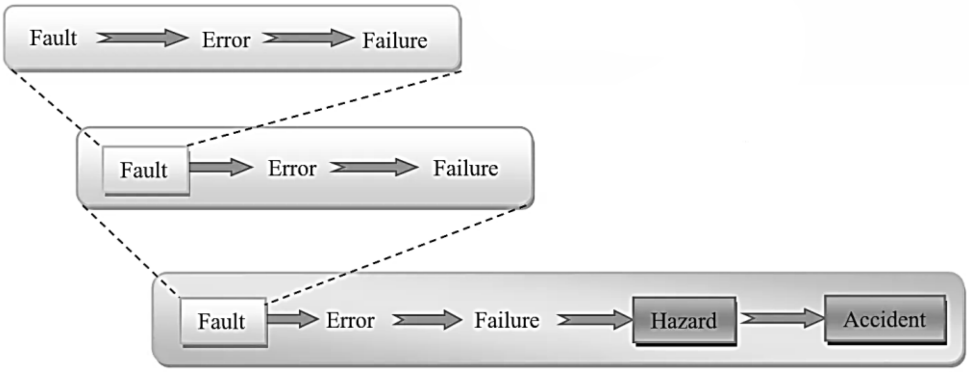


Figure 2-5: Fault-error-failure cascade can lead to life-threatening hazards. (Kalinsky, 2005)

As for the origins of failures, Dubrova (2013, pp. 10-11) enounces that they can be occasioned due to different causes, ranging from diverse problems occurring at the specification, implementation or fabrication stages of the design process to external factors like human actions (accidental or deliberate), environmental disturbances…[9]. According to their origin and this author, faults can be classified in:

- Specification faults: They result from incorrect specifications, i.e. incorrect algorithms, architectures or requirements.
- Design faults: They are due to incorrect implementation, i.e. when it does not adequately implement the specification. They can be both in hardware (poor component selection, logical mistakes, poor timing or poor synchronization) and in software (bugs in the program code).

[8] See section *2.3.2.1 HARA*
[9] See annex *A.3Causes of car accidents*

- Component defects: They comprise manufacturing imperfections, arbitrary device defects, and components wear-outs.
- External factors: They come from outside the system boundary, the environment (weather, temperature, vibration, electrostatic discharge), the user or the operator (software viruses, hacker intrusions).

Dubrova (2013, pp. 12-15) also classifies the faults under other criteria:

- Common-Mode faults: A fault that occurs at the same time in two or more redundant components, which due to the dependency created can fail simultaneously. Examples of systems that are vulnerable to this type of faults are the ones that trust on a single source of power, cooling or Input/output bus.
- Hardware faults: They are classified regarding their duration into permanent (remain active until a corrective action is taken), transient (soft-error, remain active for a short period of time), and intermittent faults (a transient fault that becomes active periodically).
- Software faults: their main sources are design faults, associated with fuzzy human factors, hardware problems.

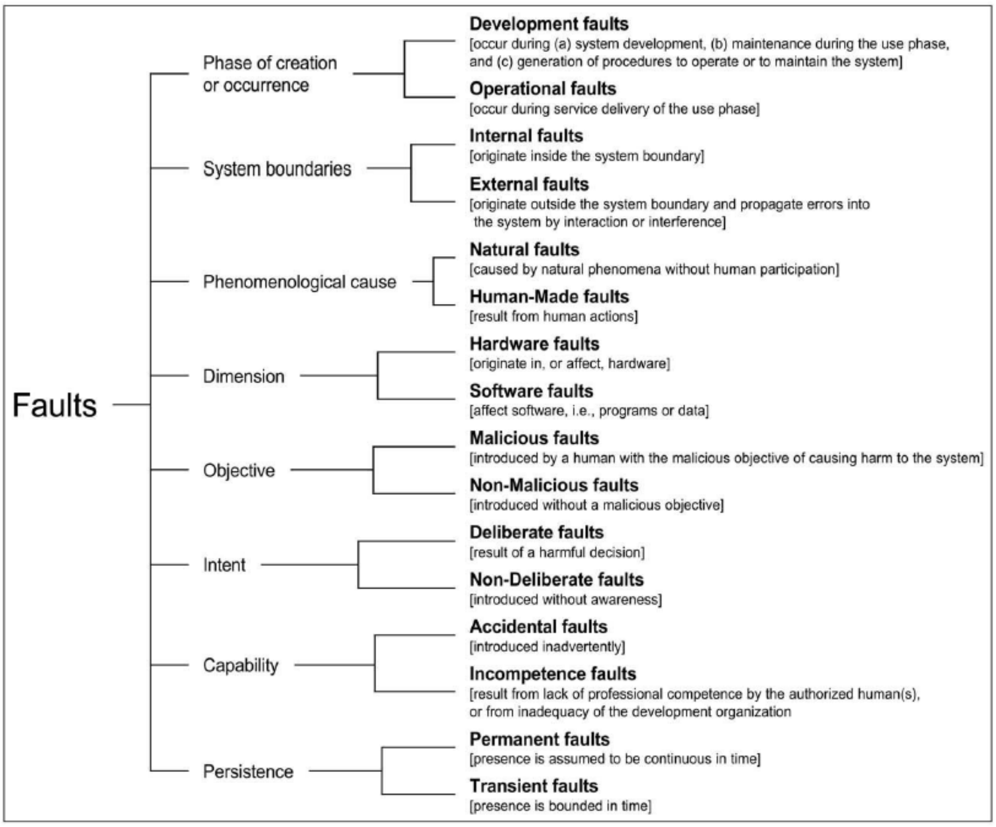

Faults
Phase of creation or occurrence
Development faults
[occur during (a) system development, (b) maintenance during the use phase, and (c) generation of procedures to operate or to maintain the system]
Operational faults
[occur during service delivery of the use phase]
System boundaries
Internal faults
[originate inside the system boundary]
External faults
[originate outside the system boundary and propagate errors into the system by interaction or interference]
Phenomenological cause
Natural faults
[caused by natural phenomena without human participation]
Human-Made faults
[result from human actions]
Dimension
Hardware faults
[originate in, or affect, hardware]
Software faults
[affect software, i.e., programs or data]
Objective
Malicious faults
[introduced by a human with the malicious objective of causing harm to the system]
Non-Malicious faults
[introduced without a malicious objective]
Intent
Deliberate faults
[result of a harmful decision]
Non-Deliberate faults
[introduced without awareness]
Capability
Accidental faults
[introduced inadvertently]
Incompetence faults
[result from lack of professional competence by the authorized human(s), or from inadequacy of the development organization
Persistence
Permanent faults
[presence is assumed to be continuous in time]
Transient faults
[presence is bounded in time]

Figure 2-6: The elementary fault classes (Avizienis et al. 2004, p.8).

As seen in the previous figure, depending on the authors, this classification might vary.
This fact also happens with failures, which are generally classified into minor or catastrophic failures, depending on the magnitude of their harmful consequences, but can also be grouped under other criteria, as the figure below shows. Regarding to errors, these

can be detected or latent, depending on if their presence is indicated by an error message or signal or if not.

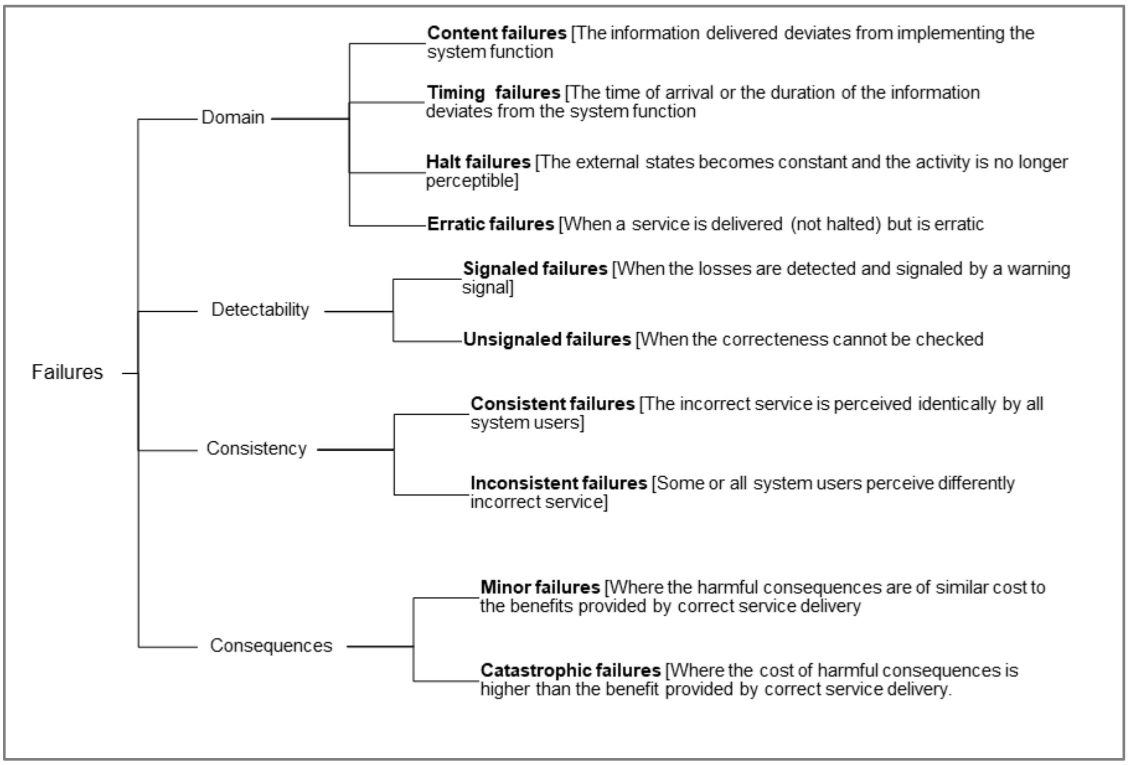

Failures
Domain
Content failures [The information delivered deviates from implementing the system function
Timing failures [The time of arrival or the duration of the information deviates from the system function
Halt failures [The external states becomes constant and the activity is no longer perceptible]
Erratic failures [When a service is delivered (not halted) but is erratic
Detectability
Signaled failures [When the losses are detected and signaled by a warning signal]
Unsignaled failures [When the correcteness cannot be checked
Consistency
Consistent failures [The incorrect service is perceived identically by all system users]
Inconsistent failures [Some or all system users perceive differently incorrect service]
Consequences
Minor failures [Where the harmful consequences are of similar cost to the benefits provided by correct service delivery
Catastrophic failures [Where the cost of harmful consequences is higher than the benefit provided by correct service delivery.

Figure 2-7: Service failure modes (Own elaboration according to Avizienis et al. 2004, p.14).

The types of threats to dependability that a system may experiment in its life cycle have been covered. Those faults, errors, and failures can occur in the development and/or operational phase and depending on which one(s), the cause or element that trigger off the fault can be different:

In the development phase, the development faults are caused due to its environment elements, which are the physical world and its phenomena, the human developers (who might have lack of competence or a malicious objective), the development tools (software and hardware) and the production and test facilities (Avizienis et al. 2004, p.6).

The use phase consists of service period, service outage and service shutdown, plus the maintenance actions during each of them. The elements that can origin faults in this phase are: the physical world, administrators (maintainers or anybody that has authority to manage, modify and repair the system), users (any person or system that get service from the system at their user interfaces), providers (entities that provide services to the system), infrastructure (entities that deliver specialized services such as information, communication, power sources to the system) and intruders (malicious and unauthorized entities that aim to alter or halt the service: hackers, vandals, malicious software, hostile organizations…) (Avizienis et al. 2004, p.7).

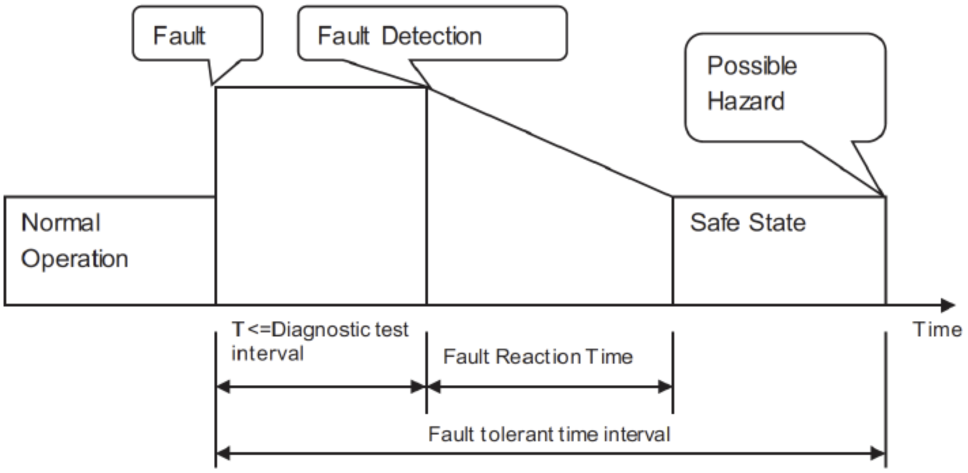


Figure 2-8: Fault tolerance (ISO, 2011).

2.1.3 Means of dependability

They are the methods and techniques that enable the development of a dependable system. Dubrova (2013, pp. 15-17) classifies them in:

- Fault tolerance: It aims to develop systems that work correctly in the presence of faults. It also contains fault masking, fault detection, and fault containment.
- Fault prevention: It aims to prevent the occurrences or introduction of faults. It is accomplished by quality control techniques during the specification, implementation and fabrication stages of the design stage process.
- Fault removal: It aims to reduce the number of faults present in a system. It is carried out not only the development phase (which contains three steps: verification, diagnosis, and correction) but also the operational life (corrective and preventive).
- Fault forecasting: It aims to estimate the number of present faults, possible future occurrences and the impact or consequences of the faults on the system. It is performed through a qualitative or quantitative evaluation. The first ones identify, classify and rank the failure modes or event combinations that cause system failures, whereas the second ones evaluate in terms of probabilities the extent to which some attributes are satisfied (becoming after that *measures*) (Avizienis et al. 2004, p.28).

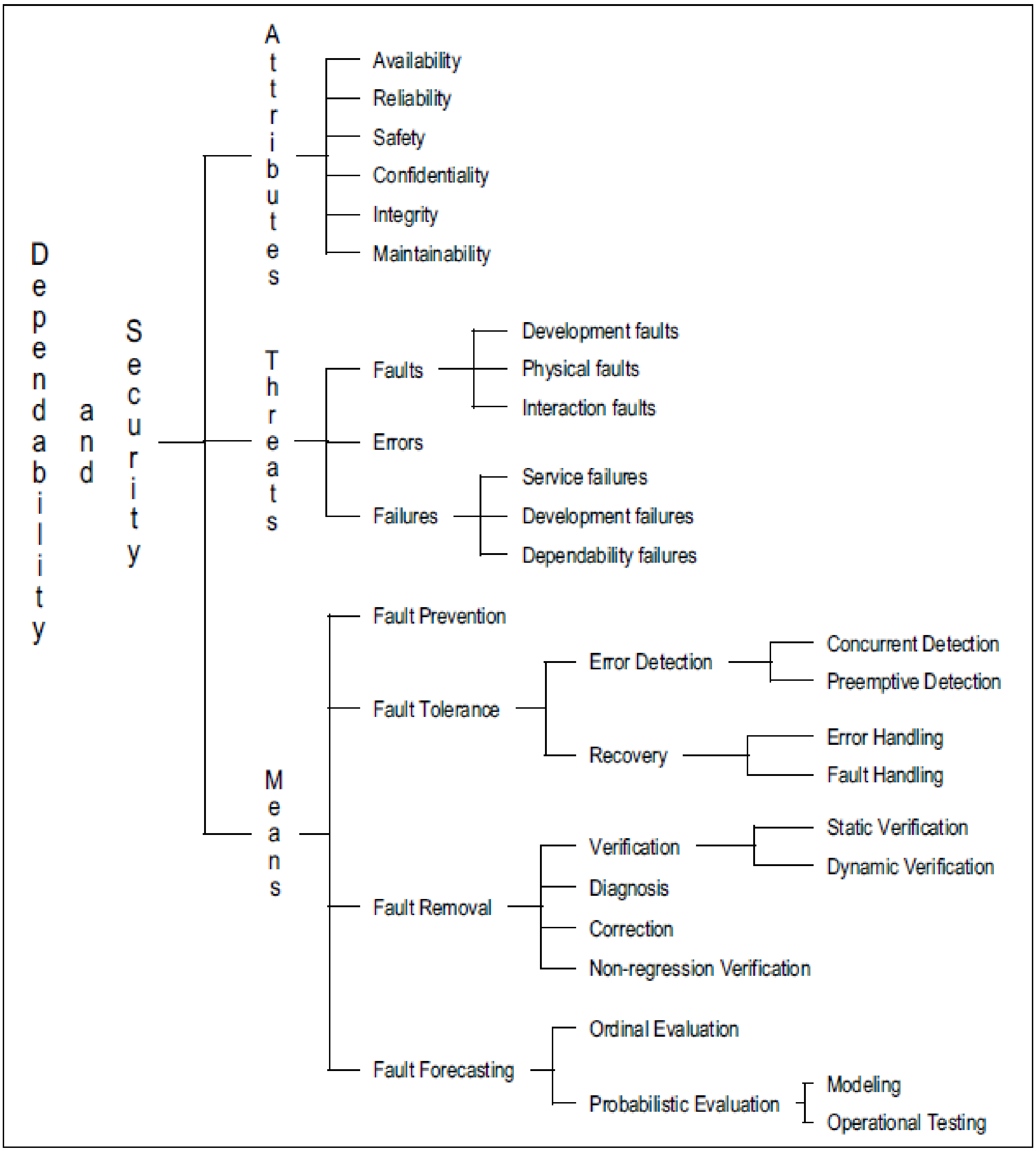
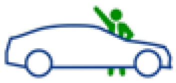
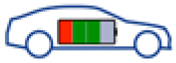
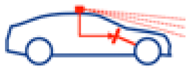


Figure 2-9: A refined dependability and security tree (Avizienis et al. 2004, p.32)

2.2 Future trends and challenges

According to the European New Car Assessment Programme (2020 Roadmap, 2015), the new urban mobility solutions that are emerging and will co-exist in the nearly future in order to reduce deaths, emissions and money are the following ones:

Table 2-1: Future mobility trends. (Own elaboration based with pictures from siliconvalleymobility.com).

COMMODITIZATION	Shared vehicles		Car-and ride-sharing offer new mobility solutions, change ownership model.
ELECTRIFICATION	Electric vehicles (EV)		Fossil fuel based powertrain gets replaced by electric components.
COMMUNICATION	Connected vehicles (ITS)		Vehicles exchange data with infrastructure and with one another.
AUTOMATION	Autonomous vehicles		Driving task is taken over by vehicle; the driver becomes an observer and then passenger.

The adoption of each one will not happen overnight, but in a relatively slow and transitory process. In the following sections these future trends will be described regarding to their components, classification, advantages, disadvantages and especially their challenges and threats, in order to create from them possible safety-related uses cases in further chapters.

2.2.1 Commoditization

Millard- Ball (2005, p.11) define car-sharing as a service that provides different members with access to a fleet of vehicles on an hourly basis throughout the day.

Car sharing includes both B2C (Business-to-costumer) offerings and largely informal peer-to-peer (P2P) arrangements. It is distinct from ride sharing, which involves being driven rather than driving.

Although it has existed on an informal basis for as long as there have been cars, ultimately they are evolving into organized taxi services and more recently into new models. These modalities of sharing offer different potential advantages that Barth & Shaheen (2002, p.105) identified as:

- They can improve transportation efficiency by reducing the number of (private) vehicles required to meet total travel demand. As a result, vehicles spend a lot less idle time in parking lots and are used more often by several users.
- Individual transportation costs saving since vehicle expenses (e.g., payments, insurance, maintenance) are shared among all system users.

- Achievement of energy and emissions benefit when low-polluting cars (e.g., electric, hybrid-electric, natural gas) make up the shared-use vehicle fleet.
- The increase of transit ridership when individuals use shared vehicles either through a direct transit linkage or indirectly because users are now more conscious in their trip making and modal choices.

Barth & Shaheen (2002, p.106) also propose a classification framework for shared-use vehicle systems:

Neighborhood carsharing model.

In this modality, the user typically books a shared-use vehicle in advance, gets access to the car, does the trip and returns the auto back to the same lot (two-way rental).

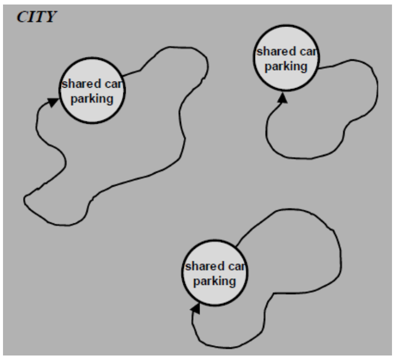


Figure 2-10: Neighbourhood carsharing model (Barth & Shaheen 2002, p.106).

Multimodal Shared-Use Vehicles.

The user does not have to return the car to the initial lot or station. He can commute his trips by using different vehicles taken at different stations. This one-way rental increases flexibility for users but also management complexity due to vehicle relocation.

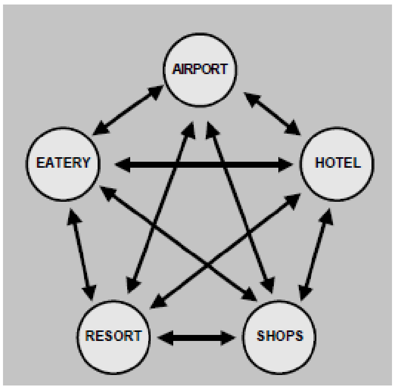


Figure 2-11: Multimodal shared-use vehicle model (Barth & Shaheen 2002, p.107).

According to the work of Cohen & Kietzmann (2014, pp. 283-288), the business models that exist in this mobility trend are: summarized in the following paragraphs

Business-to-Consumer (B2C) carsharing

The company purchases vehicles and supplies them at key points throughout a city. Users generally use their smartphones to geolocate the nearest available vehicle, open the vehicle up with their membership card, and drive it only for the time needed. This guarantees that the idle time of a car is kept to a minimum and that the economic cost and benefits of carsharing are distributed appropriately.

They can also be further categorized by roundtrip models (require members to return the vehicle to the same location) and point-to-point models (allow members to leave the vehicle parked on the street near their destination).

Nonprofit/Cooperative carsharing

Members cooperatively contribute resources and manage the carsharing organization without the expectation of financial gain.

P2P (peer-to-peer) carsharing

This model trusts on some form of intermediation using the web and/or mobile technology to connect owners (i.e., private individuals, not companies) of sub-optimized products with potential drivers.

Other authors such as Le Vine et al. (2014, pp.5-6), differentiate the several forms of carsharing between round-trip, peer-to-peer, point-to-point free-floating (flexible carsharing) or point-to-point station-based carsharing.

2.2.1.1 Threats of shared cars

Faster deterioration

Since the users of the cars are not the owners of the vehicle, they are not as much carefull, without taking the piece of advice to increase the lifespan. Moreover, the cars are always on the street and the weather conditions, street vandalism or neglect by other drivers are some factors that foster this fast deterioration.

Operational difficulties

Sharing economy services still need to be more developed, regarding the contact, book and paying methods.

Security

Since shared vehicles are being continuously used for different members, it is not possible to know if the car has been manipulated previously. That means that the driver/users cannot have a direct control of the car and therefore his security can be damaged in somehow, in case somebody has placed in the car some device, ranging from a recorder to a bomb.

Crash propensity

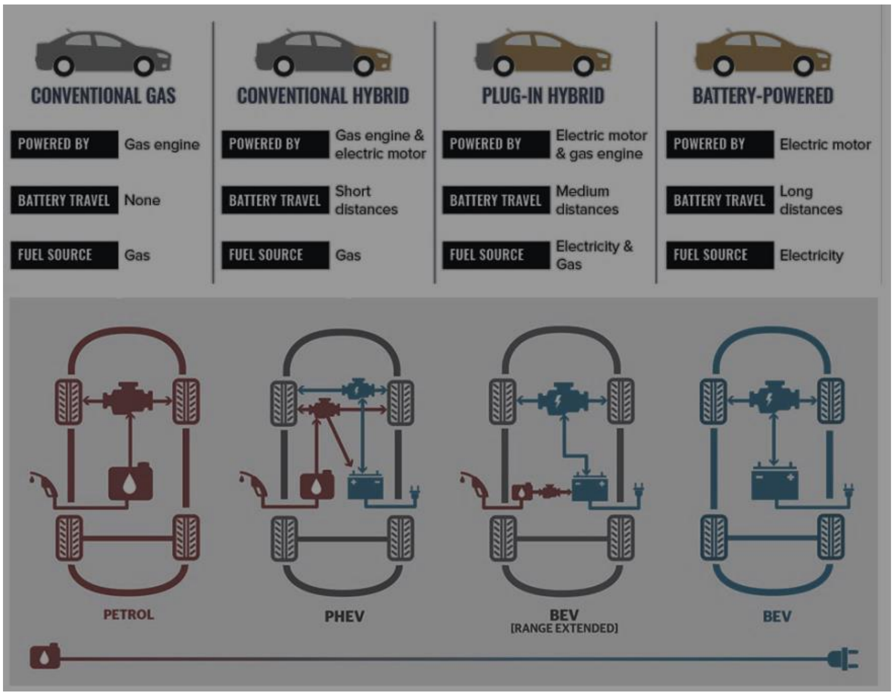
Very dependable of the car-sharing users. For example, according to one study carried out with data of carsharing users in Sydney, it is known that users of carshare who drive less frequently, have at least one car, have less number of accidents in the past ten years, have chosen a higher insurance excess and have had a license for a longer period of time are less likely to be involved in a crash (Dixit, 2014, p. 140).

2.2.2 Electrification

Leaving safety as the major reason to develop new ways of transportation to one side, due to not only new eco-friendly trends in our society but also facts such as the climate change, ozone layer depletion, etc., it seems that the energy future will be less tolerant with the continual production of greenhouse gas emissions. Since cars and transportation in general play an important role in greenhouse gas emissions and oil consumption, it is more than probable that in the nearly future electric cars will take our roads. Also the improvement in air quality (especially in urban areas), the no requirement of too large investment in infrastructure and other significant advantages relating energy security are some of the reasons that could foster its implementation. However, it is still necessary to take care of some aspects firstly in order to make sure that the occupants' safety is maintained and that the transport networks and infrastructures are suitable.

Electric vehicles (EV) use electric motors instead of internal combustion engines (ICE) to propel the vehicle. According to the way to get the propulsion power, King (2015, pp.22-24), distinguishes three types of electric vehicles:

- Hybrid vehicles: They involve a conventional internal combustion engine supplemented by smaller electrical engines at low speed or when additional power is needed.
- Plug-in hybrid vehicles: They operate like a conventional hybrid but they have an electric engine supplementing the internal combustion engine, so the electric motor can be literally "plugged in" to a wall socket to recharge the battery and the vehicle can operate independently on electric power at low speeds until the charge is expended.
- Battery electric vehicles: They are the next logical evolution from plug-in hybrids and are sufficiently developed to not require a supplementary internal combustion engine, thanks to advancements in battery technology.



	CONVENTIONAL GAS	CONVENTIONAL HYBRID	PLUG-IN HYBRID	BATTERY-POWERED
POWERED BY	Gas engine	Gas engine & electric motor	Electric motor & gas engine	Electric motor
BATTERY TRAVEL	None	Short distances	Medium distances	Long distances
FUEL SOURCE	Gas	Gas	Electricity & Gas	Electricity

Figure 2-12: Types of electric cars (NYSERDA, nd.)

Battery power and capacity limitations will initially limit the availability of plug-in and battery electric vehicles. Advancement in battery capacity is required before these vehicles can be mass produced to provide the same mobility benefits of an internal combustion engine, as well as a reduction in their prices. Precisely due to these low capabilities, most of the current electric car models are small, lightweight, low range, low speed, cheaper and designed just for urban environments. These are the so-called "quadricycles".

Although these last ones are suitable to reduce the pollution in the cities, they present some inconvenient regarding safety: light structure, no provisions for frontal impact (they do not have to pass frontal impact tests) or seatbelts anchorages. To sum up, they are made to lesser standards (King, 2007, p.15).

Apart of these light city cars, the new improvements in battery systems are allowing the manufacture of heavy electric vehicles, since battery systems have always been the Achilles heel in the electric automotive industry. This affirmation is supported by Affanni et al. (2005, pp.1343) who affirm that the battery system choice is the most crucial item. Consequently, the necessity of an accurate detection of battery state of charge (SoC) plus battery expected life (battery state of health) are among the major drawbacks that prevent the introduction of electric vehicles in the consumer market. Other battery characteristics suggested by Miller (2002, pp.113-118) required for EV: high energy density, high output power (density), long life, high charge-discharge efficiency, wide range of use from low temperature to high temperatures, minimal self-discharge, good load characteristics, good temperature storage characteristics, low internal resistance, no memory effects, fast charging, high degree of safety, high reliability, low cost, and good recyclability.

Although Li-ion batteries pose a higher safety risk from thermal incidences than NIMH batteries (Taylor et al. 2012, p.1), thanks to an increasing emphasis on vehicle range and performance they are becoming the most viable candidate. According to the same author, they can hold twice as much energy as NIMH batteries due to its suitable number of cells series-connected. However they present also different safety-related challenges regarding the design of a practical battery protection circuit (since it has to be small and economical enough for the manufacturer to include it inside the battery back) and regarding the battery management system (that also have to include a SoC monitoring in order to optimize autonomy instead of performance or vice-versa) (Affani et al.2005, p. 1343).

Overcharging and overdischarging (which reduce cycle life), repeated charge/discharge cycles, overload and short-circuits are just some examples of safety issues that EV may have, apart from the ones that a common vehicle (ICEVs) already present. In the worst case, they could even cause electrocution or explosion. Nevertheless, as Taylor et al. (2012, p.1) explain, ISO 26262 does not report hazards like electric shocks, smoke, corrosion, fire, toxicity among others if they are not triggered by the malfunctioning behaviour of E/E (electric/electronic) safety-related systems.

In the work of Taylor, Krithivasan, and Nelson (2012, p.1) it is exemplified how all the elements are interconnected in a way that the fault of one of them might create malfunctions and hazardous situations in others:

> *"Failure of the hardware electronics controlling the battery contactors may lead the contactors to fail closed, thereby disabling a fail-safe thermal protection mechanism.*

> *This could result in potentially dangerous temperatures and conditions for the Li-ion cells. Such a failure may also be the result of a systematic software failure, either in the battery management system (BMS) or a related control system such as an onboard charger or powertrain inverter".*

(Taylor et al., 2012, p.1)

Other non-safety related challenges suggested by Käbisch et al. (2010, p.161) that electric vehicle will have to face are the ones regarding the infrastructure: setup and deployment of a future-proof common standard for smart grids; smooth communication between electrical vehicles; power supply equipment and smart grid during the charging process; consideration of different kind of charging locations; charging characteristics as well as some vehicle to grid stakeholders.

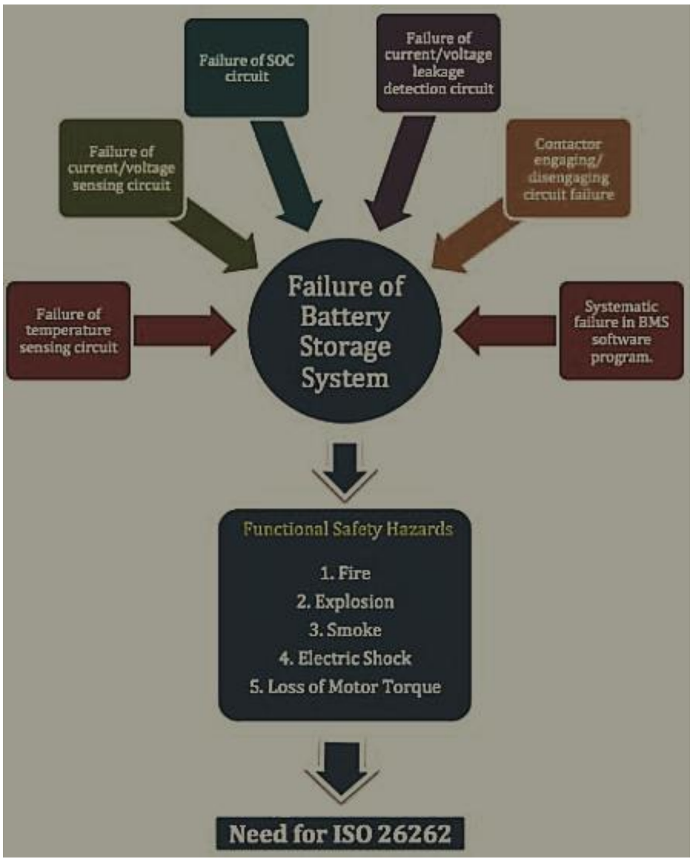

Failure of SOC circuit
Failure of current/voltage leakage detection circuit
Failure of current/voltage sensing circuit
Contactor engaging/ disengaging circuit failure
Failure of temperature sensing circuit
Failure of Battery Storage System
Systematic failure in BMS software program.
Functional Safety Hazards
1. Fire
2. Explosion
3. Smoke
4. Electric Shock
5. Loss of Motor Torque
Need for ISO 26262

Figure 2-13: Overview of the need for ISO 26262 in a battery storage system (Taylor, 2012, p.2).

2.2.2.1 Threats of electric cars

Returning to the core aspect of this work, safety, Kjosevski et al. (2017, pp.169-170) distinguish four main characteristics of the hybrid and electric vehicles regarding electrical safety. These are summed up in the following paragraphs:

Safety of the electrical system

Voltages used in electric vehicles are potentially dangerous and therefore care should be taken to prevent electric shock in direct or indirect contact. As for the direct contact, parts under voltage should be protected through insulation or inaccessibility while for the indirect contact; this is closely connected with errors in the car body and can lead to dangers such as short circuit, electric shock, or uncontrolled operations. Batteries should be sufficiently sheltered from adverse weather conditions and sharp objects.

Safety in the system function

The drive system of the electric vehicle must ensure reliable and safe operation of the vehicle. IT is mandatory to have the presence of a device in case of emergencies, a warning device to prevent inadvertent movement, auxiliary power supplies (lighting, wipers of the windscreen…), regenerative braking…

Safety while charging batteries

As already stated by other authors, the battery is the most critical part for the electric vehicle since it holds diverse potential risks: electrical, mechanical, chemical and danger of explosion. Therefore, protection elements against electric shock and short circuit are needed (fuse), as well as special caretaking when charging the batteries to avoid the risk of electric shock.

Maintenance and operation of the vehicle

In the first line, the user has to take care of the maintenance of the car and be protected against all risks of direct contact. After that first line of maintenance come at the workshops, which have to be thoroughly trained in the safe maintenance actions (battery disconnected before any task). The third row of maintenance belongs to workshops manufacturer, which do the main electrical repairs, test resistance of insulation and earth leakage, battery status…

These safety aspects could be extracted from accidents that have already happened and which Kjosevski et al. (2017, pp.171-172) collected in their work:

- Batteries ignition after a side impact at low speed due to the entering of a small amount of coolant into the housing of the battery at high voltage collision. This causes a short circuit followed by an uncontrolled heat state.
- In situations of hurricanes or heavy rains, flooding can cause a short circuit in the batteries leading to a disruption in the thermal condition and ignition.
- Hitting against a heavy or/and pointed object can damage batteries and lead to thermal instability.
- Crash with another vehicle or element at high speed where the battery afterwards might fly out of the vehicle and catch fire.
- Risks for the people who first assist a car accident such as potential electric shock from damaged systems turned off during or after the crash. For this reason, associations recommend that manufacturers of EVs install switches that stop energy from the battery case in accidents.
- Lack of information, training and good preparation to users, personal in workshops, drivers of towing services.
- Low noise at low speeds can be dangerous to pedestrians and cyclists since they use traffic sounds to reveal the presence of vehicles and predict their movements. To palliate this effect, electric vehicles should be equipped with a warning that allows pedestrians to reveal their presence and direction of movement.

2.2.3 Communication

Another trend in our way to the future driving/mobility is connected cars. In this context, they are considered as the key enabling technology to improve road safety, traffic efficiency and driving experience, as well as to foster the emergence of next-generation cooperative intelligent transport systems (ITS) and a bit later the emergence of future autonomous vehicles (Hamida et al. 2015, p.380).

According to Jenkins & Mahmud (2006, p.3), the need for active safety, highway guidance, telematics, traffic management, cooperative driving, driver convenience and automatic toll payment will require future intelligent vehicles to communicate with other vehicles as well as with the roadside infrastructure. However, inter-vehicle and vehicle to roadside infrastructure communications will impose some security threats against vehicles' safety and their proprietary information.

In order to get a better understanding, this new technology will allow the vehicles to communicate with other nearby elements through vehicular communications (VC) and telematics services and concretely through direct short-range communications (DSRC), such as:

- V2V-Vehicle to vehicle.
- V2I-Vehicle to infrastructure.
- V2P-Vehicle to pedestrian.
- V2X-Vehicle to anything.

According to Hamida et al. (2015, p.382), ITS will have a great potential in the near future since their aim and advantages are clear: reducing the number of accidents. Nevertheless, there are many open challenges and issues that need to be tackled as they will impose some security threats against vehicles’ safety and security (those will be described later on).

As far as ITS Architecture concerns, it comprises three main communication domains, as shown in the next figure:

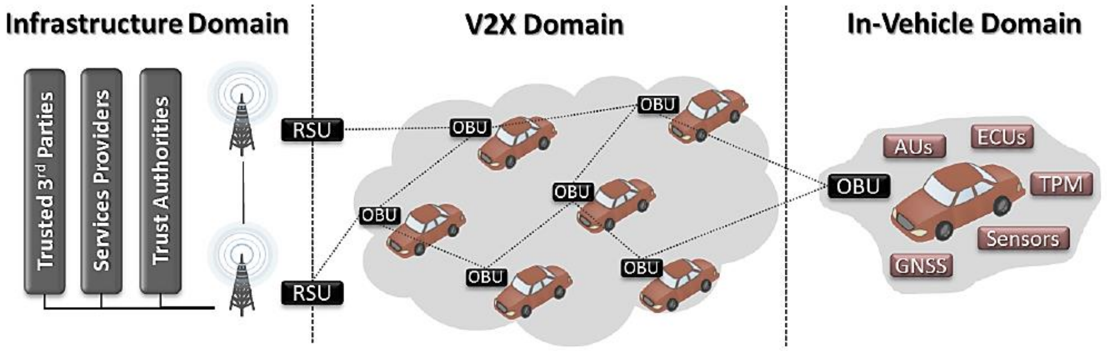


Figure 2-14: ITS high-level architecture (Hamida et. al.2015, p.383).

To give a brief understanding that summarizes the work of Hamida et al. (2015, pp.383-384), the In-vehicle domain comprises a connected vehicle equipped with electronic control units (ECUs), wireless-enabled onboard units (OBUs), a trusted platform module (TPM) and an application unit (AU). ECUs gather data about the dynamics of the car (such as location, speed, heading, vehicle size, etc.), and also the context (number of neighbouring vehicles, traffic conditions…) and will control its functionality by exchanging messages with the OBU (owns the communication capabilities) and AU (responsible for running one or multiple applications), forming an in-vehicle network (onboard network) as it is shown in the picture above. The TPM enables secure and efficient communications and manages different keys and certifies. A Global Navigation Satellite System (GNSS) unit obtains accurate location information.

The V2X domain comprises vehicle OBUs and road-side units (RSUs) positioned along the roads. These OBUs exchange in real time the information collected from nearby ITS entities using various vehicular communication technologies (V2X) seen above (Hamida et al. 2015, pp.383-384).

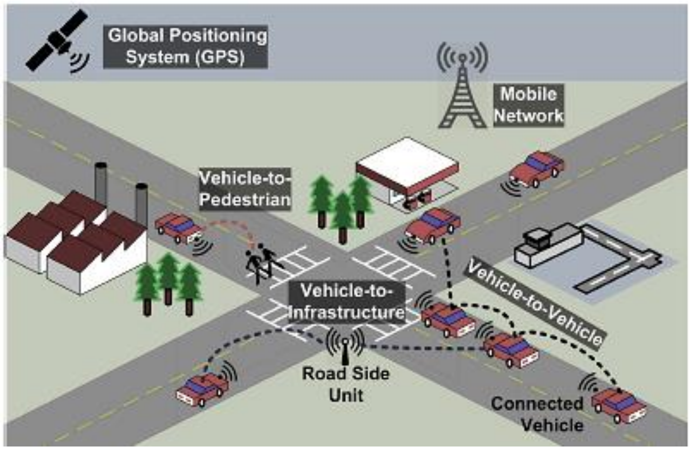


Figure 2-15: ITS V2X communications (Hamida et al.2015, p.384).

As for the infrastructure domain, this one includes the trusted third parties (TTP), such as vehicles manufacturers, service providers (SPs, they provide applications to the vehicles AUs and are responsible for software updates, billing and deliver added-value services) and the trust authorities (TA, they register and authenticate the RSUs and OBUs) according to Hamida et al. (2015, pp.383-384).

In the work of Hamida et al. (2015, pp. 386-389) summarized in the next paragraphs, among the ITS' applications can be found intersection collision warning, wrong way driving warning, remote diagnostic of vehicles… which can be classified as the figure below shown and which are characterized by the following main features: powerful capacity, high mobility, dynamic network topology, time sensitivity, sufficient energy, good physical protection, unbounded network size, wireless communications, heterogeneous V2X communication technologies, heterogeneous environment, security, and privacy.

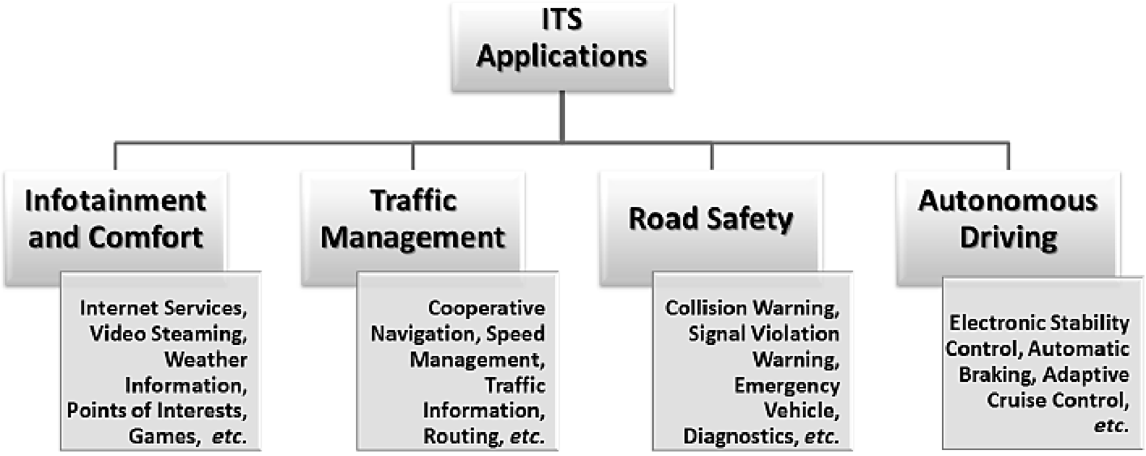

ITS Applications
Infotainment and Comfort
Internet Services, Video Steaming, Weather Information, Points of Interests, Games, etc.
Traffic Management
Cooperative Navigation, Speed Management, Traffic Information, Routing, etc.
Road Safety
Collision Warning, Signal Violation Warning, Emergency Vehicle, Diagnostics, etc.
Autonomous Driving
Electronic Stability Control, Automatic Braking, Adaptive Cruise Control, etc.

Figure 2-16: Classification of ITS applications (Hamida et al.2015, p.386)

Infotainment and Comfort

They aim at enhancing the driving experience through giving different added-value services (offered by trusted service providers). Examples of this application could be the remote vehicle diagnostic and maintenance application where information from the in-vehicle sensors is gathered and communicated to drivers, provide Internet access to the passengers…

Traffic Management

They aim to improve the management and coordination of traffic flows and to deliver different cooperative navigation services to drivers, by collecting, analysing and exchanging ITS messages to create and maintain global traffic map databases.

Road safety

Road safety applications use wireless V2X communications to decrease traffic accidents and to protect passengers and pedestrians from diverse road hazards. Examples of this application are emergency electronic brake lights warning, stationary vehicle indication, roadwork warning, intersection collision avoidance, lane change warning and others like the shown ones in the following figure:

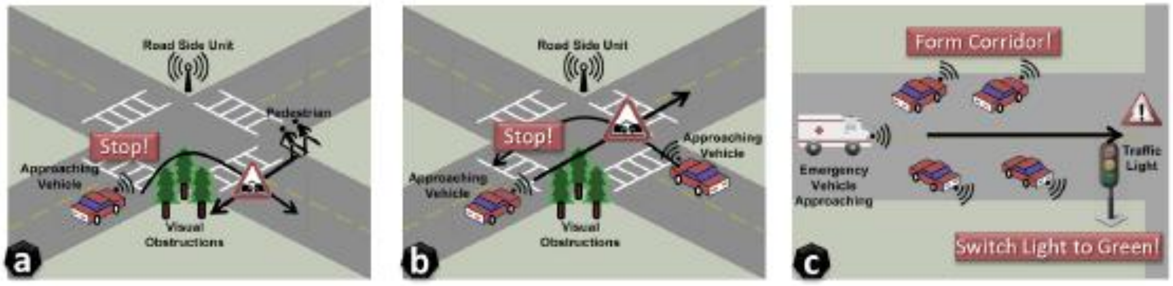


Figure 2-17: Examples of road safety applications: a)pedestrian crossing warning; b)left turn driver assistance; c)approaching emergency vehicle warning (Hamida et al.2015, p.388).

Autonomous Driving

Automated driving has between its technologies V2X communication, in order to enable the car to communicate with the external elements already seen. This application will be seen more detailed in succeeding sections.

2.2.3.1 Threats of connected cars

According to Hamida et al. (2015, p.394), the main ITS threats and attacks and possible solutions are summed up in the next figure:

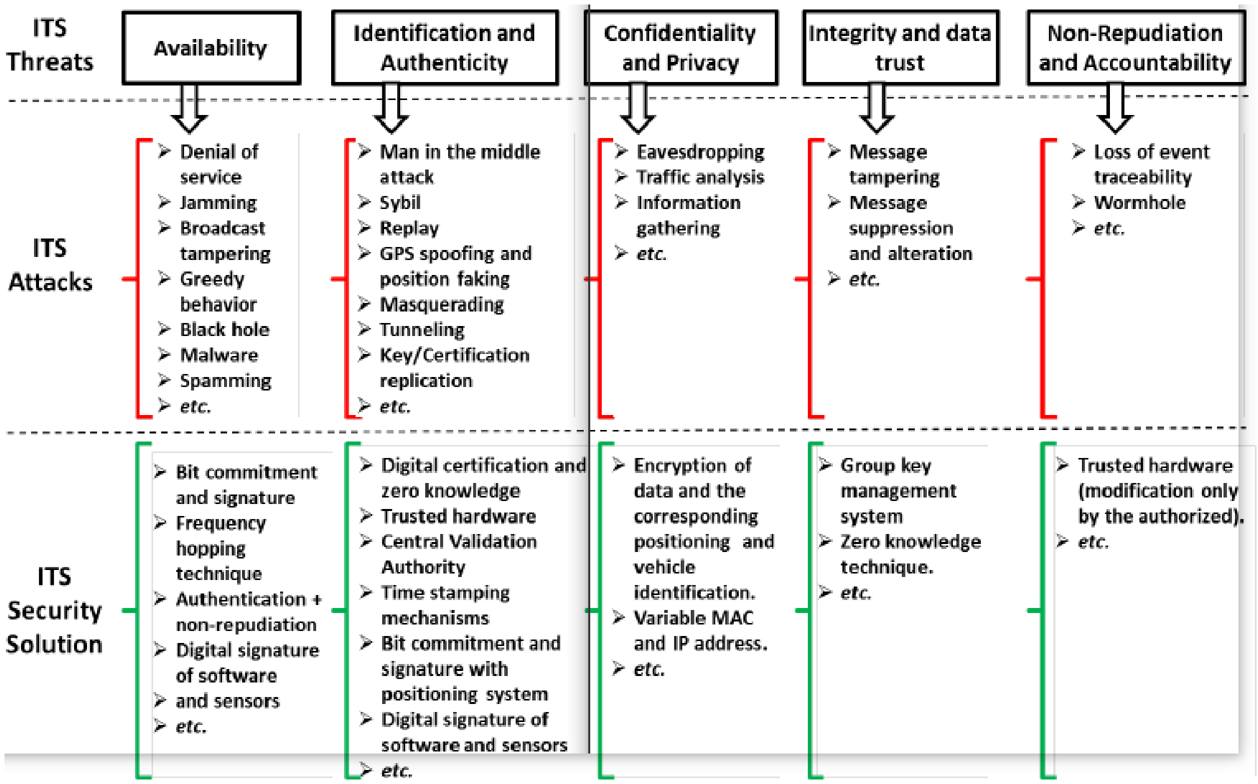

ITS Threats
Availability
Identification and Authenticity
Confidentiality and Privacy
Integrity and data trust
Non-Repudiation and Accountability
ITS Attacks
Denial of service
Jamming
Broadcast tampering
Greedy behavior
Black hole
Malware
Spamming
etc.
Man in the middle attack
Sybil
Replay
GPS spoofing and position faking
Masquerading
Tunneling
Key/Certification replication
etc.
Eavesdropping
Traffic analysis
Information gathering
etc.
Message tampering
Message suppression and alteration
etc.
Loss of event traceability
Wormhole
etc.
ITS Security Solution
Bit commitment and signature
Frequency hopping technique
Authentication + non-repudiation
Digital signature of software
and sensors
etc.
Digital certification and zero knowledge
Trusted hardware
Central Validation Authority
Time stamping mechanisms
Bit commitment and signature with positioning system
Digital signature of software and sensors
etc.
Encryption of data and the corresponding positioning and vehicle identification.
Variable MAC and IP address.
etc.
Group key management system
Zero knowledge technique.
etc.
Trusted hardware (modification only by the authorized).
etc.

Figure 2-18: Examples of ITS threats, attacks, and countermeasures (Hamida et al.2015, p.394).

The entities involved are the drivers, the onboard unit (OBU), the roadside unit (RSU), third party entities and the attackers. All these entities have seen before except attackers, which try to violate the security of ITS systems using diverse techniques. They can be active (transmit malicious packets to harm other nodes and normally have permission to operate in the network) or passive (they spy the communications in the network to extract useful information; external (not authenticates and authorized to operate within the ITS network) or internal(they belong to the ITS network and can perform any type of attack); malicious (no specific target, just destroying network) or rational (have specific target and can be very dangerous because they are unpredictable).

The challenges that connected cars have to front are summed up in the following paragraphs, according to Hamida et al. (2015, 398-404):

Availability

The information that is exchanged should be processed and available in real time. Denial of service (DoS) attacks is the most dangerous threat to the availability of ITS systems, due to their big effect on the network resources. Other typical attacks are jamming attacks, flooding attacks, Sybil attacks, malware attacks, spamming attacks, blackhole attacks, gray hole attacks, sinkhole attacks, wormhole, tunneling attacks…

Authentication

The most important requirement, divided into three types: user authentication (to avoid Sybil attacks), source authentication (to ensure legitimate messages), location authentication (to ensure integrity and relevance of received information). Several examples of these attacks on authenticity are falsified entities attacks, cryptographic replication attacks, GNSS spoofing and injection attacks, timing attacks…

Data confidentiality

Exchanged messages should be properly encrypted and protected to avoid the disclosure of sensitive information to unauthorized parties. Examples of attacks that jeopardize data confidentiality are eavesdropping attacks, data interception attacks, and brute force attacks.

Privacy and anonymity

The data privacy of the vehicle/driver should be controlled and guaranteed.

Data integrity

ITS entities should verify and validate the integrity of the received information to avoid unauthorized or malicious modification or deletion during transmission. Examples of these attacks are masquerading attacks, data playback attacks, data alteration attacks, map database poisoning attacks, data tampering attacks, man-in-the-middle attacks….

Non-repudiation

Each ITS entity should be exclusively associated with its information and actions in order to get authentic and original data.

Traceability and revocation

The trust authority (TA) should be able to track and revoke timely malicious ITS identities.

Authorization

Access control and authorization for the different entities should be defined.

Robustness against external attacks

ITS entities should be robust enough to avoid external attacks and the software should be free of vulnerabilities and logic flaws.

2.2.4 Autonomy

Jo et al. (2014, p. 7131) define an autonomous car as "*a self-driving vehicle that has the capability to perceive the surrounding environment and navigate itself without human intervention*". Nevertheless, numerous definitions in the literature contemplate a vehicle as autonomous even if it is not 100% independent of the presence of a human being on the driver's seat. This classification according to the level of autonomy is provided by the Society of Automotive Engineers (SAE 2016) and is directly cited below:

- Level 0 – No Automation

"The full-time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems."

- Level 1 – Driver Assistance

"The driving mode-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver performs all remaining aspects of the dynamic driving task."

- Level 2 – Partial Automation

"The driving mode-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the human driver performs all remaining aspects of the dynamic driving task. It means that the "driver is disengaged from physically operating the vehicle by having his or her hands off the steering wheel AND foot off pedal at the same time," but he has always to be ready to take the control of the car back."

- Level 3 – Conditional Automation

"Driver is still necessary for this level, but under certain traffic or environmental conditions can change to "safety-critical functions". The driving mode-specific performance by an Automated Driving System of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene (not instantaneously)."

- Level 4 – High Automation

"The driving mode-specific performance by an Automated Driving System of all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene. It is limited since it cannot cover every driving scenario but it is "designed to perform all safety-critical driving functions and monitor roadway conditions for an entire trip"."

- Level 5 – Full Automation

“The full-time performance by an Automated Driving System of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver.”

Judging by the given definitions by SAE and the supported graphic showed below, it could be said that nowadays mobility founds itself between the levels one and two (L1-assisted and L2-partial automation).

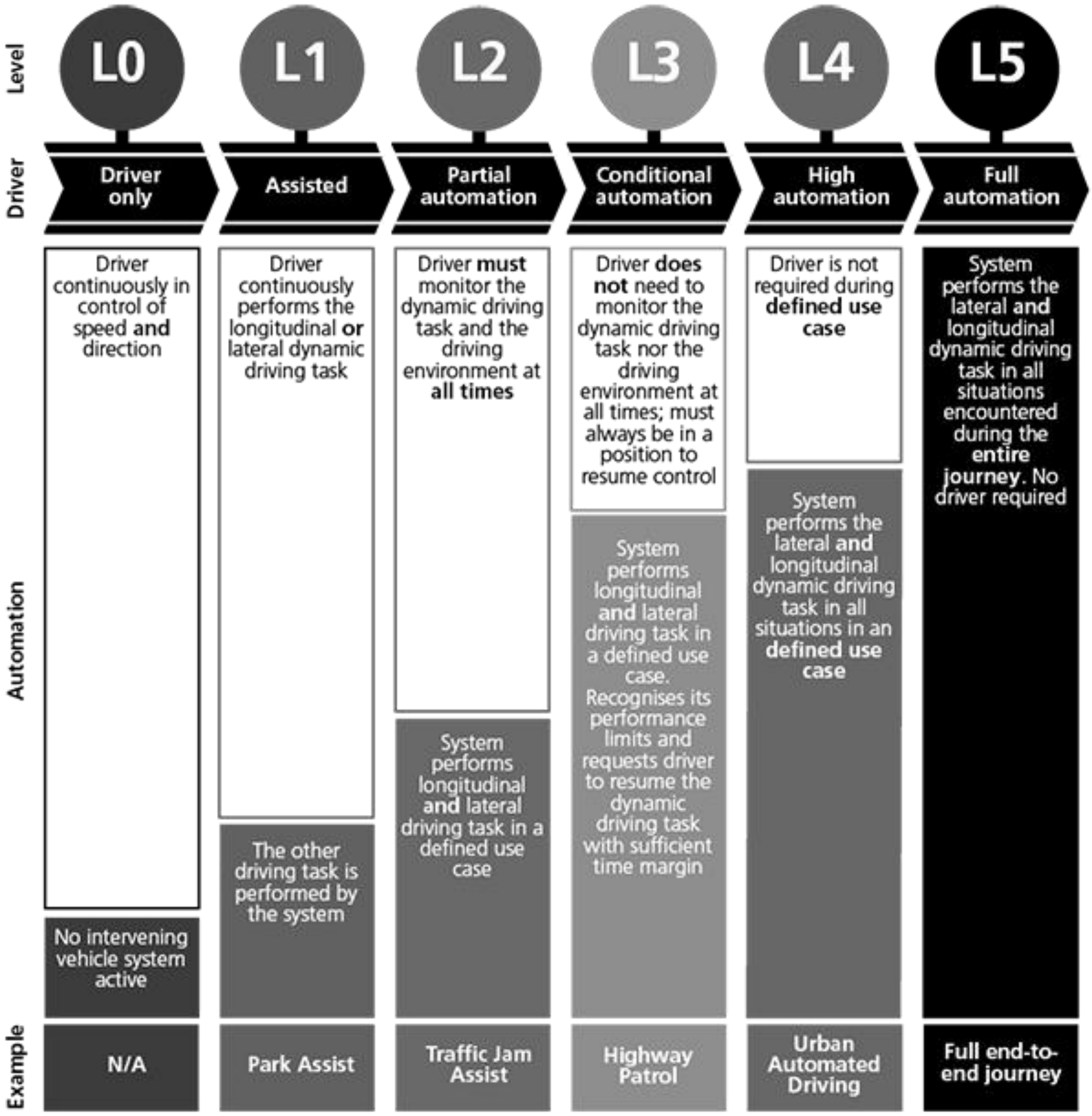

Level
Driver
Automation
Example
L0
L1
L2
L3
L4
L5
Driver only
Assisted
Partial automation
Conditional automation
High automation
Full automation
Driver continuously in control of speed and direction
No intervening vehicle system active
Driver continuously performs the longitudinal or lateral dynamic driving task
The other driving task is performed by the system
Driver must monitor the dynamic driving task and the driving environment at all times
System performs longitudinal and lateral driving task in a defined use case
Driver does not need to monitor the dynamic driving task nor the driving environment at all times; must always be in a position to resume control
System performs longitudinal and lateral driving task in a defined use case. Recognises its performance limits and requests driver to resume the dynamic driving task with sufficient time margin
Driver is not required during defined use case
System performs the lateral and longitudinal dynamic driving task in all situations in an defined use case
System performs the lateral and longitudinal dynamic driving task in all situations encountered during the entire journey. No driver required
N/A
Park Assist
Traffic Jam Assist
Highway Patrol
Urban Automated Driving
Full end-to-end journey

Figure 2-19: Defined levels of automation (Parliament UK, 2017).

Independently of the level of automation reached, five fundamental functionalities have to be provided, which are shown in the next figure:

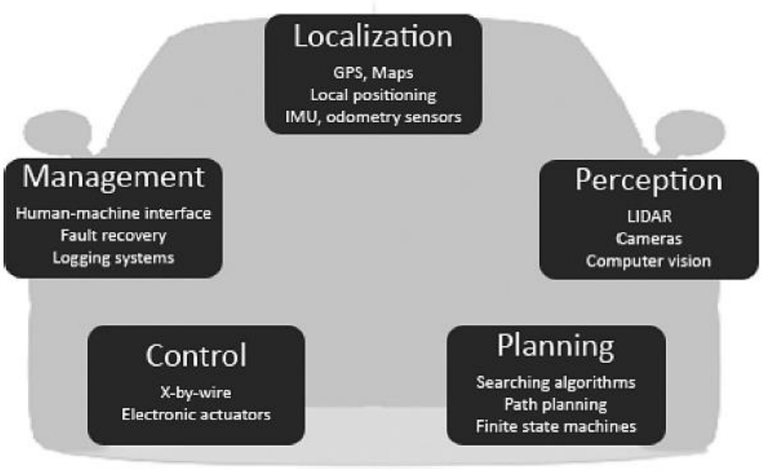


Figure 2-20: Functionalities of an autonomous vehicle (Coppola et al. 2016, p.23).

For accomplishing these features, vehicle autonomy relies on a mix of a balanced combination of the following technologies:

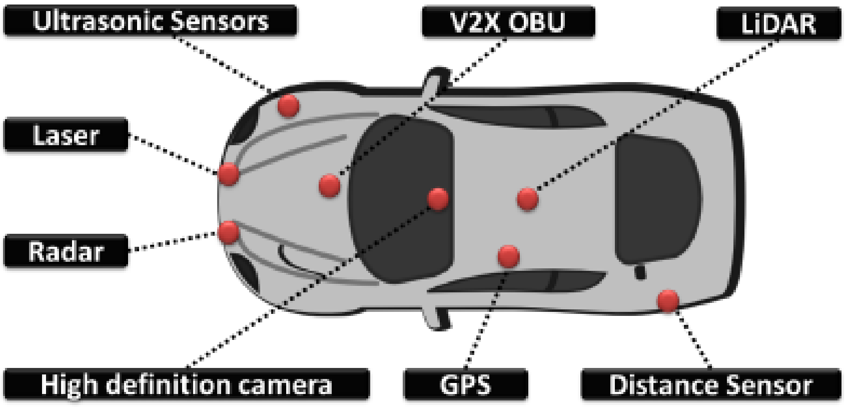


Figure 2-21: Key technologies enabling autonomous cars (Hamida et al. 2015, p.390).

Cameras

They are an effective substitute for driver’s eyes, letting the car ‘see’ what’s happening in the world around it (objects, weather conditions, variations in lighting) since they are the only sensor technology that can capture texture, color and contrast information.

They can process colours, and even though cameras could seem less impressive (and less expensive) than more modern tech, they play an important role in autonomous driving. However, the disadvantage is that high-definition cameras placed on all corners of the cars require powerful processors for making sense of millions of pixels for every frame, every second. Unlike LIDAR and RADAR, they are considered passive safety systems (Osman, 2017).

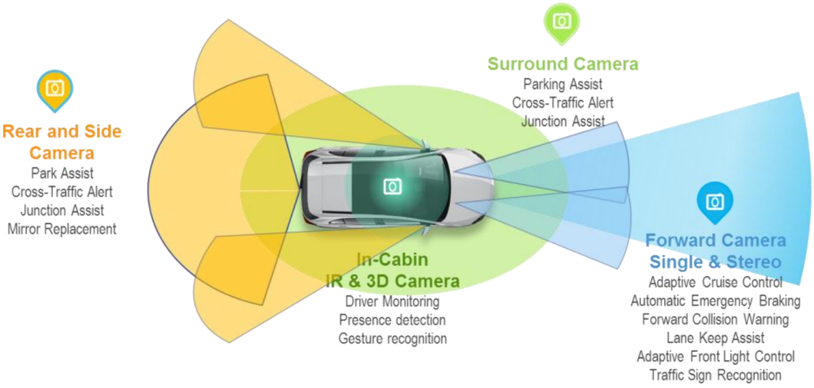


Figure 2-22: Different types of cameras in a car (Osman, 2017)

According to Osman (2017), some examples of ADAS application level evolutions enabled by cameras are:

- Adaptive Cruise Control (ACC): currently distinguish full-width vehicles such as cars and trucks but in the future need to be able to catalogue a motorcycle and keep distance.
- Automatic High Beam Control (AHBC): currently do high-low beam switching but have to progress to be able to detect oncoming vehicles and contour the ray of light accordingly.
- Traffic Sign Recognition (TSR): current systems identify speed limits and various limited subset of signs. Upcoming systems need to recognize supplemental signs and context, detect traffic signals to adapt ACC, stop, slow down etc.
- Lane Keep Systems (LKS): currently distinguish lane markings and upcoming systems need to detect drivable surface, adjust to construction signs and multiple lane markings.

LIDAR

According to the work of Osman (2017) summed up in the following paragraphs, Light Detection and Ranging sensors measure the distance to an object by calculating the time taken by a pulse of light to travel to an object and back to the sensor. It can scan more than 100 meters in all directions (360° 3D), and consequently can generate a complete and precise 3D map of the immediate world around it, in order to avoid obstacles.

It is the most technologically varied (and therefore expensive) of the three sensors used on autonomous cars nowadays. The vehicle can use this map to make informed decisions on how to react in diverse situations, and the sheer amount of information processed instantly makes driverless cars more advantageous over non-autonomous cars when it comes to awareness.

They also need even more powerful processors, since the amounts of data generated in less than a second are larger and the laser technology used has to be “eye-safe”.

The recent goal is to replace mechanical scanning LiDAR (that physically rotate the laser and receiver assembly to gather data over an area that widths up to 360°) with Solid State LiDAR (SSL) that have no moving parts and are consequently more reliable especially in an automotive atmosphere for long-term reliability. SSLs at present have lower field-of-view (FOV) coverage but their lower cost offers the possibility of using multiple sensors to reach a larger area (Osman, 2017).

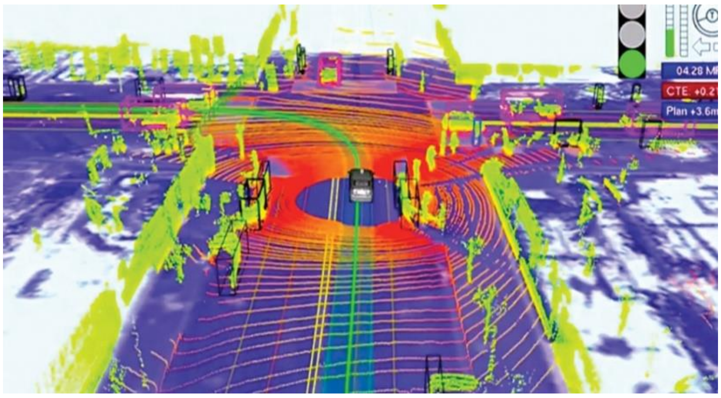


Figure 2-23: LIDAR vision (Higgins, 2017, p.1).

RADAR

Since cameras and LIDAR cannot know how far an object is, the use of radio waves becomes a necessity, also for determining the exact speed, they are moving and the also the range and angle. (Santo, 2017)

The advantage is that radio waves can be reflected (no need of sight line), it can work in almost all environmental conditions and the data output to process is much lower and therefore they do not need higher processing speeds.

Radio Detection and Ranging sensors can be classified per their operating distance ranges, according to Osman (2017):

- Short Range Radar (SRR):0.2 to 30 m range
- Medium Range Radar (MRR): 30-80 m range
- Long Range Radar (LRR): 80m to more than 200m range (used in Adaptive Cruise Control or ACC and highway Automatic Emergency Braking Systems or AEBS). They have to be combined with camera in order to deliver additional information in the detection, since used alone can react incorrectly in situations such as a car cutting in front of a vehicle, detecting thin profile vehicles such as motorcycles being staggered in a lane and setting distance based on the wrong vehicle due to the curvature of the road.

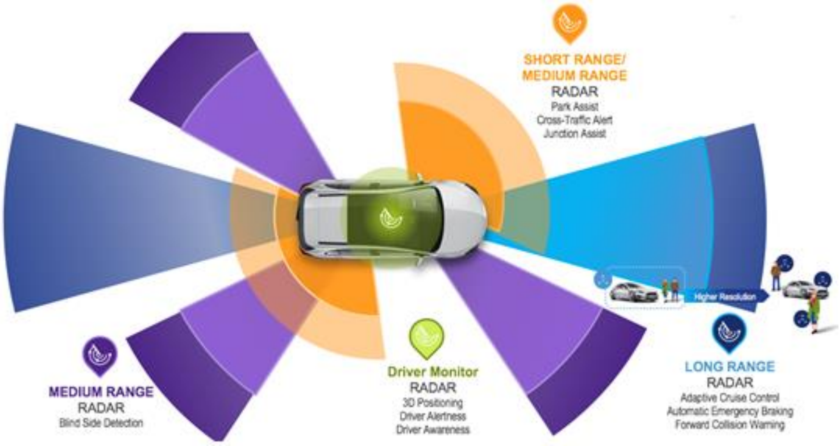


Figure 2-24: Radar for autonomous cars (NXP cited in Lapedus 2017).

Software

According to Musk (Musk, 2016 cited in McMahon, 2016), "*Software is the last obstacle to fully autonomous vehicles*". In other words, "Full autonomy is really a software limitation".

Autonomous cars promise remarkable capabilities for many different applications, but there is still too much work to do in developing intelligent systems software that guarantees safety and reliability in inexpensive autonomous vehicles. Good software engineering practices must be followed to guarantee them.

Long et al. (2007, p.1) state that future systems (despite their difficult use and the challenge of being able to learn) will probably rely on a mix of computational intelligence methods (traditional control), fuzzy logic, neural networks, genetic algorithms, rule-based methods and symbolic artificial intelligence.

These intelligent systems software should consider biological (human) systems, including abilities like sensing, reasoning, action, learning, cooperation, and conscientiousness.

Intel CEO, Brian Krzanich recently assumed that each driverless car will generate approximately 4,000 GB (4 terabytes) of data a day. In contrast, the normal person, by using PCs, phones, smart watches etc. currently generates 650 MB of data a day (Mendes, 2017, p.1).

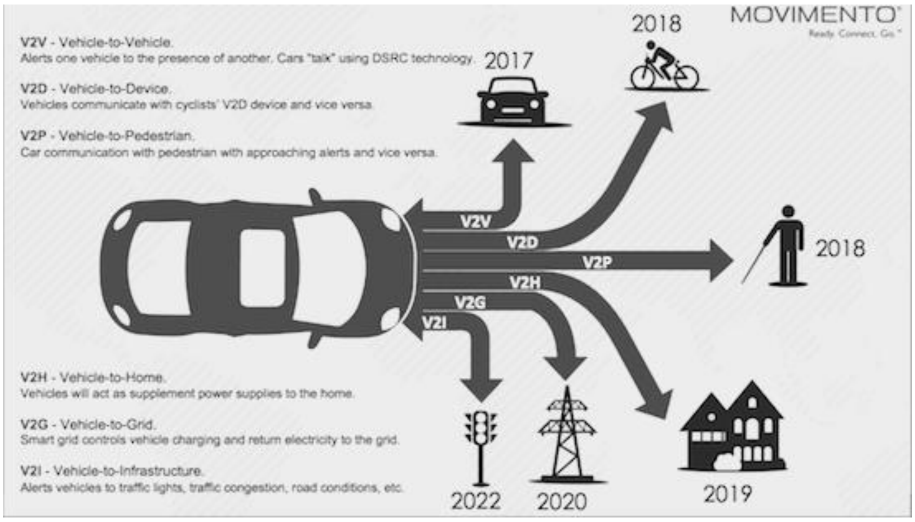
Due to the fact that autonomous cars have to react to road changes in less than a second, safety is a critical factor not only for software but also for hardware. Therefore, according to the functional safety standard ISO 26262, all the parts involved in the supply chain have to develop their products with the proper quality and safety. In the software case, this has to be integrated into a given hardware platform and system (like steering or braking) previously to be accepted.

To sum up, the three key pillars that Intel has identified for supporting the future of driverless cars are, according to Mendes (2017, p.5):

- the car (comprising in-vehicle computing and human-machine interfaces-HMI),
- the cloud and data center
- the communications that connect them (for example 5G mobile networks)

V2X

As already summarized in connected cars, Vehicle-to-X refers to an intelligent transport system where all vehicles and infrastructure systems are interconnected with each other. It is a vehicular communication system that incorporates other more specific types of communication as V2I (Vehicle-to-Infrastructure), V2V (Vehicle-to-vehicle), V2P (Vehicle-to-Pedestrian), V2D (Vehicle-to-device) and V2G (Vehicle-to-grid). The main push for V2X is safety, with energy savings also being important. However, there are still obstacles preventing the roll-out of this technology, mainly legal issues and the fact that, unless almost the totality of the existing vehicles adopts it, its effectiveness is rather limited (Wiseguy Reports, 2018).



V2V - Vehicle-to-Vehicle.
Alerts one vehicle to the presence of another. Cars "talk" using DSRC technology.

V2D - Vehicle-to-Device.
Vehicles communicate with cyclists' V2D device and vice versa.

V2P - Vehicle-to-Pedestrian.
Car communication with pedestrian with approaching alerts and vice versa.

V2H - Vehicle-to-Home.
Vehicles will act as supplement power supplies to the home.

V2G - Vehicle-to-Grid.
Smart grid controls vehicle charging and return electricity to the grid.

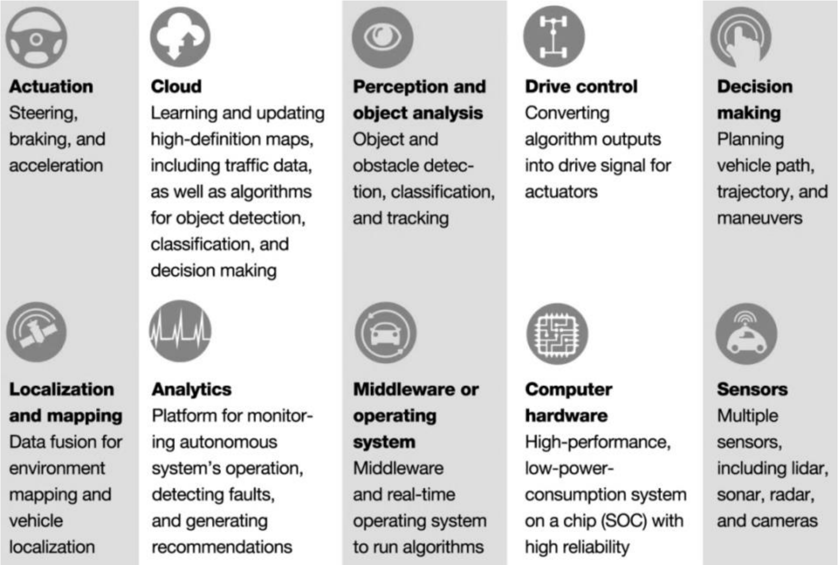
V2I - Vehicle-to-Infrastructure.
Alerts vehicles to traffic lights, traffic congestion, road conditions, etc.

Figure 2-25: V2X in autonomous vehicles (Alam, 2017)

This connectivity will provide more precise knowledge of the traffic situation across the entire road network which in turn will help (Siemens, 2015, p.1):

- Optimize traffic flows
- Reduce congestion
- Cut accident numbers
- Minimize emission

To sum up, the system and sensors that make possible the substitution of a human in autonomous cars, the following figures are presented:



Actuation
Steering, braking, and acceleration

Cloud
Learning and updating high-definition maps, including traffic data, as well as algorithms for object detection, classification, and decision making

Perception and object analysis
Object and obstacle detection, classification, and tracking

Drive control
Converting algorithm outputs into drive signal for actuators

Decision making
Planning vehicle path, trajectory, and maneuvers

Localization and mapping
Data fusion for environment mapping and vehicle localization

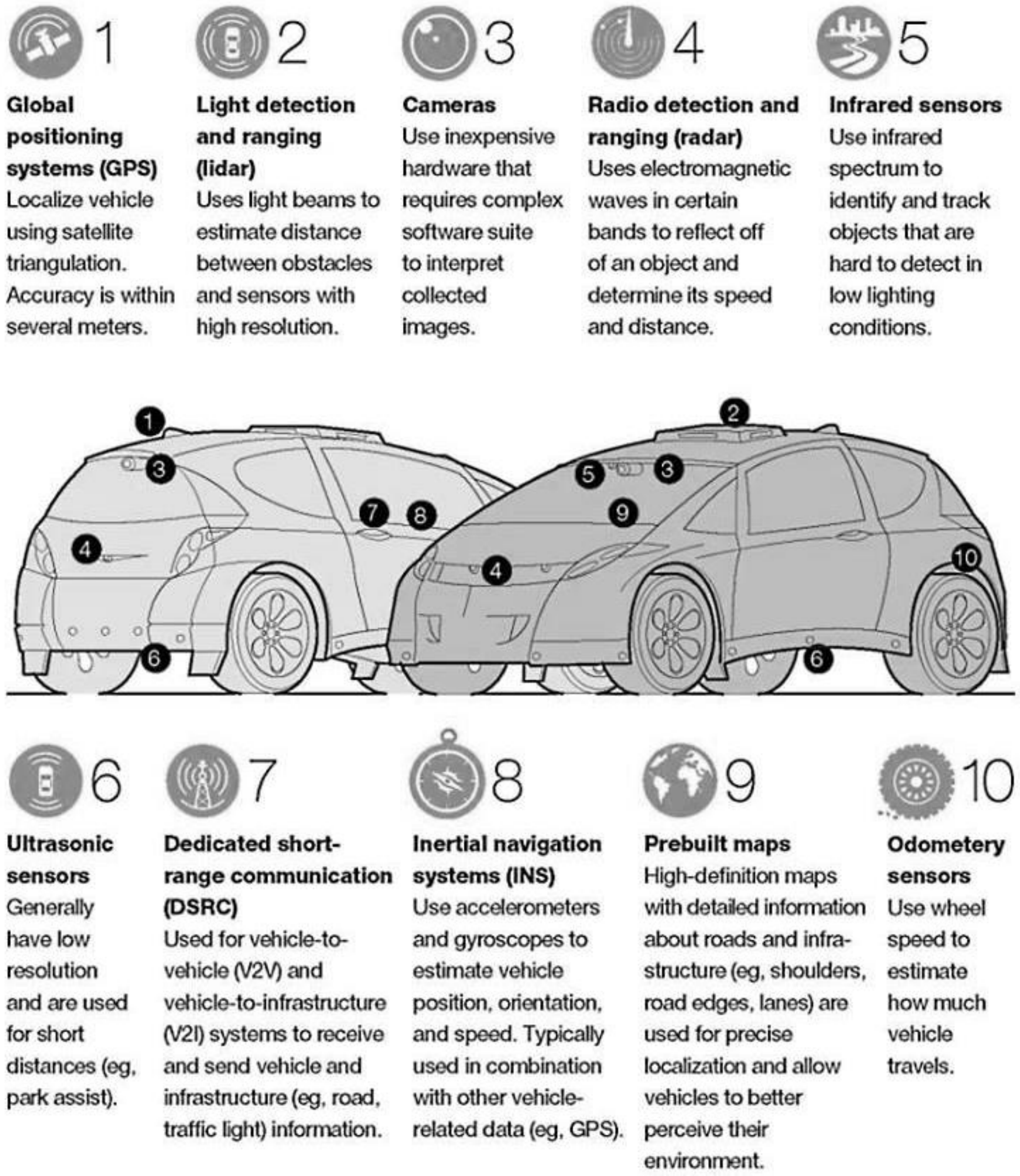
Analytics
Platform for monitoring autonomous system's operation, detecting faults, and generating recommendations

Middleware or operating system
Middleware and real-time operating system to run algorithms

Computer hardware
High-performance, low-power-consumption system on a chip (SOC) with high reliability

Sensors
Multiple sensors, including lidar, sonar, radar, and cameras

Figure 2-26: Elements of the autonomous driving system (Heineke et al. 2017).



1 **Global positioning systems (GPS)** Localize vehicle using satellite triangulation. Accuracy is within several meters.

2 **Light detection and ranging (lidar)** Uses light beams to estimate distance between obstacles and sensors with high resolution.

3 **Cameras** Use inexpensive hardware that requires complex software suite to interpret collected images.

4 **Radio detection and ranging (radar)** Uses electromagnetic waves in certain bands to reflect off of an object and determine its speed and distance.

5 **Infrared sensors** Use infrared spectrum to identify and track objects that are hard to detect in low lighting conditions.

6 **Ultrasonic sensors** Generally have low resolution and are used for short distances (eg, park assist).

7 **Dedicated short-range communication (DSRC)** Used for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) systems to receive and send vehicle and infrastructure (eg, road, traffic light) information.

8 **Inertial navigation systems (INS)** Use accelerometers and gyroscopes to estimate vehicle position, orientation, and speed. Typically used in combination with other vehicle-related data (eg, GPS).

9 **Prebuilt maps** High-definition maps with detailed information about roads and infrastructure (eg, shoulders, road edges, lanes) are used for precise localization and allow vehicles to better perceive their environment.

10 **Odometery sensors** Use wheel speed to estimate how much vehicle travels.

Figure 2-27: Sensors /subystems autonomous cars (Heineke et al. 2017).

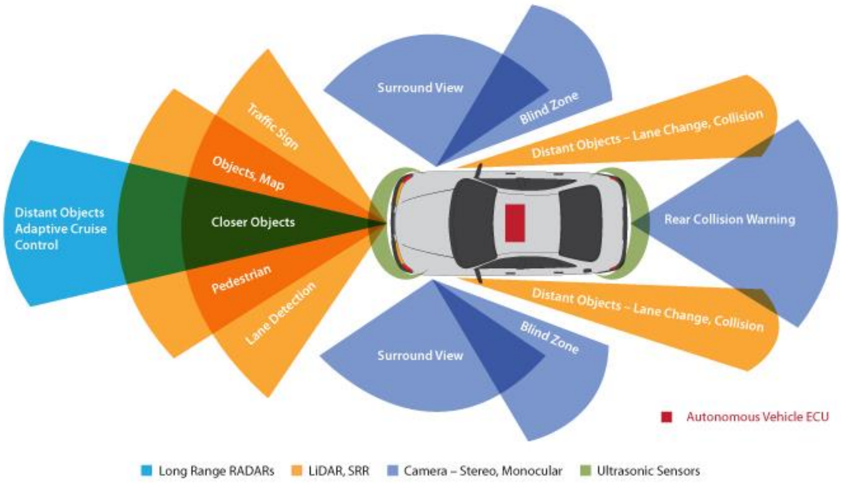


Figure 2-28: Autonomous vehicle systems. (Arya, 2017)

As it was already said in the introduction of this master thesis, since the human behavioural factor is the most fatal cause of car accidents, driverless cars are proclaimed as the solution of this problem, is this indisputably the most important advantage. Also facilitating mobility for people that are not able to drive and reducing time and costs are secondary reasons that support this implementation.

2.2.4.1 Threats of autonomous cars

Based on Federal Automated Vehicles Policy (U.S DOT-NHTSA, 2016, pp.15-35) the challenges that, depending on the automation level, driverless cars will have to face are described in the following pages:

Data recording and sharing

There are different types of data that can be recorded in the different levels of car automation. The higher the level, the larger amount of data recorded. This data can be very diverse, including the identity of the "driver" and the passengers, details of the journey (start and end points, route, time and date, speed…), payment method (in case it is a rental vehicle), video or audio recording inside of the car (like a black box in the airplanes)… This collected and generated data will be transferred continuously to the cloud and reside in the power of the manufacturers and/or car sharing problem.

But the information transferred is not restricted to the driverless vehicles and its own passengers; since other vehicles on the road, depending on their level of automation, will be also gathering data, at the end all of this information can be shared creating a big net of information. And this is going to play an important role in the safety of passengers, pedestrians, and bicyclists, i.e. all the elements that interact on the roads, in an active and passive way: this will prevent car accidents thanks to the data collected by sensors and cameras and also through the net, knowing the behaviour of the cars around yours, and also in case of accident, it will be able to alert the emergency systems plus know whose fault was and therefore who to blame.

It can also be known who exceed the speed limit, the real-time and place where the police and ambulances should go, the infractions of bad drivers (insurance companies), the movements of potential criminals and terrorists (security and law enforcement), which are the streets more used (maintenance and logistics) etc.

However, the problem is not the quality nor the quantity of data collected, but the use that car manufacturers or insurance could make of it. Problems that could appear might be that they provide this data to third companies for letting them know the costumes, routines and likes the car users might have (or order to target their sales, doing marketing and advertisement…) and also in spy companies. This data recording and sharing, depending on in whose hands is, might attempt to the confidentiality of the driver and therefore should exist some legislation that ensures security and discretion and/or commitment with data secrecy and security. (U.S DOT-NHTSA, 2016, pp.17-18)

Privacy

This safety aspect is much related to the previous one since car manufacturers should take steps to protect consumer privacy and ensure (U.S DOT-NHTSA, 2016, pp.19-20):

- Transparency, in order to force entities to do a proper collect, use, share, secure, audit, and destroy of the data generated.
- Choice, by offering car owners choices regarding the processing of their data, i.e. gathering, use, distribution, retention, and deconstruction of data, including geolocation, biometric, and driver behaviour data that could be reasonably linkable to them personally.
- Respect for context, which means using the data collected just in ways that are consistent with the purposes for the collection
- Minimization, de-identification, and retention, by gathering and keeping the minimum data just as long as necessary.
- Data security, by taking measures to protect the data thinking what would happen if a non-authorized member had access or if this data disappear.
- Integrity and access, through the implementation of methods to keep the accuracy of personal data and allow the owners of the review of the car and correct it.
- Accountability, through the evaluation and auditing of privacy, to make sure the entities comply with the purposes and the privacy of the data.

Vehicle cybersecurity

This threat or challenge could be considered as one of the most important and therefore one of the car manufacturers and/or software developers should worry more about. As William Sachiti pointed out:

> *"My nightmare scenario is that your autonomous car is driving along some small country road in the middle of nowhere, it all of a sudden pulls over, everything shuts down apart from the screen which now reads 'we've hacked your car. Pay 100 bitcoin to get it back'. We need to work hard to try to ensure this doesn't happen."*
>
> (Sachiti, 2017).

Although at lower levels is obvious that this peril does not exist, as long as the level of automation goes up, endless situations in which cybersecurity can be violated might appear: blackmailing forcing the car owner to pay to get it back (as seen before), remote control of the car, modifying the route to murder, attack, robber etc. As with safety data occurs, industries should also share cybersecurity, by reporting the vulnerabilities of the software that they have discovered when they have designed, tested, analysed and changed the systems in order to make them more robust, traceable and secure and not experience them again. (U.S DOT-NHTSA, 2016, pp.21-22)

Human machine interface

This scenario refers to the interaction between the car and the driver/passenger. Depending on the automation level, this interaction entails a certain dependency among them.

For example in cars of SAE Level 3, the driver is expected to return to the task of monitoring and be always available to take the control of the vehicle back. Although the car alerts the driver with quite enough anticipation through vibratory or audio signals, the risk of these being ignored by the driver still exist, due to reasons as overconfidence or over trusting with the car, sleepiness…and this can be a focus of serious car accidents, since in some Autopilot models, when the driver does not take the control of the car after repeated alerts, it stops. Level 5 cars, which will be able to pick up people and therefore drive without any passenger, will have to also accommodate old people and/or with disabilities via visual, auditory and haptic systems…and deal with it.

The HMI (Human Machine Interface) design, through a different type of sensors and facial recognition, should include also the environment of the vehicle: pedestrians, animals, bicyclists, conventional and automated vehicles…

The indicators should inform if the Human Machine Interface is working properly or has any malfunction in the HAV system if currently is engaged in automated driving mode if this one is available or not, requesting the control transition from HAV system to the operator. (U.S DOT-NHTSA, 2016, pp.22-23)

Crashworthiness

Although one of the main motives to introduce autonomous cars is to decrease the number of crashes (since with them the most fatal factor in car accidents will be avoided, the human factor), car manufacturers still have to consider these incidents. In other words, they have not only to keep the currently active and passive safety systems but also improve them.

The crashes can be of different types, as can be consulted in annexes. Whilst in lower levels the crashes can be due to factors such as human (~90%), weather, mechanical… in higher levels, the first one would be erased but there will still be unavoidable elements such as fog, snow, rains, animals crossing the roads, flat tyres…

The point here is: How autonomous cars will respond or try to evade these unavoidable elements? Regarding the weather conditions, these could cause a misaligning of the camera or sensors, and produce a false perception of the reality and a crash. The snow can also cover the objective of the camera, the lanes of the road or just create a fake surface, cheat the sensors, and make the car go in the wrong direction.

Also, vandalism is a huge problem, not only while the car is parked but also while it is driving. As an anonymous autonomous car user said: "*All it will take is a 12-year-old with a can of spray paint. They'll step out in front of the car, knowing that it will stop safely; then they'll paint over all the sensors*."

As for the animals, different sizes and different scenarios need to be analyzed. If in a city the car detects dog, probably behind him there is a person trying to catch him (it would be the same with a ball and a kid) and the car must stop. This will be its priority, even if the car sees a green light in the traffic lights. However, when the car is driving at 120 km/h in a high motorway and an animal of the same dimensions or smaller interrupts its way, maybe it is safer not to stop rather than brake and cause a chain accident.

Regarding the manufacturing errors, there is no device 100% perfect. There will always exist a little probability of failure in the mechatronic systems (U.S DOT-NHTSA, 2016, p.23-24).

Consumer education and training

It is assumed that in the levels where the driver has to take the control of the car full or partial time, the driving license will be mandatory. In SAE Level 5 this fact is not as obvious since if they are capable of driving without any person inside, they are able to carry a shortage person, old persons, people with some disabilities etc.

However, as far as the cars owners are concerned, a proper education and training should be obligatory in order to ensure a safe deployment of automated vehicles. Hence, car makers and entities are responsible for the development, documentation, and maintenance of programs directed to autonomous car owners and aimed to ensure the necessary level of understanding safely and efficiently these technologies (HMI, virtual reality, cameras, sensors…). These programs must be constantly evaluated and updated, thanks to continuous testing and the feedback from users.

This scenario could be a cause of the accident if, due to the car owner unawareness, he would ignore the alerts of the car to check or change any component. (U.S DOT-NHTSA, 2016, p.24).

Registration and certification

Since almost every software can be updated, the level of automation of a car can also scale. The more popular HAV (High automated vehicles) become, the more old cars will try to follow the tendencies and technologies, getting a more advanced SAE Level.

The problem here is, whilst the software is quite easy to update, the hardware or physical parts are not. It can be more difficult, costly and even dangerous. What would happen if the system allows the owner to update the software (or it is automatically done), but the hardware and other components required for the new features, are old-fashioned or inexistent?

The car manufacturers, when they produce a car with a certain level of automation, should offer an additional semi-permanent labeling. These may include the current characteristics and capabilities, as well as possible future ones and the limitations (U.S DOT-NHTSA, 2016, pp.24-25)

Post-crash behaviour

If a good maintenance is very necessary for the current cars, it could be said that this is even more important in autonomous cars. If the sensors or other critical safety systems have been damaged after a small crash, although apparently, the car is still in perfect conditions, the car should not operate in HAV mode and preserve until appropriately serviced. There could exist a misaligning of cameras or sensors that might cause another bigger accident. However, the car itself, when starting the car, should review and inform if all the systems are in a good state (U.S DOT-NHTSA, 2016, p.25).

Federal, state, and local laws

What would happen if a car has to pass a broken-down vehicle, a rock or a fallen tree in a double lines roadway? If someone is the drivers of the car, he or she will not doubt inviolate the law some seconds in order to avoid the peril as long as it does not suppose another hazard for others. But if the car is driving by itself, what would it do, taking into account, that it has been programmed for not crossing the double lanes? Here are just one of hundreds of examples, wherein certain safety-critical situations humans have the ability to temporarily infringe the rules but high automated vehicles have also to violate its own principle (lines of programming code).

The same happens if the car has to follow the indications of a policeman, and these are against the current traffic signals. How can the autonomous cars recognize these orders and obey them? The system should identify the policy and assume that his orders are preferable. It could scan the uniform and detect the presence of an authority (otherwise the car would follow the order of whoever that makes movements with his arms and/or use a whistle. As the police uniforms are different in each country and the recognition could not be possible through them, a special chip could be added in the clothes of the personnel, to make possible that the autonomous cars can detect them and follow their instructions above others.

Another aspect that might be considered is that the traffic rules sometimes are different from country to country. Maybe the STOP signal is the same in different countries, but if they have another alphabet or color systems, the car could be confused and act wrongly. Also in countries such as the UK, the driving is done in the left side and the system should detect this and be able to drive in all the countries independently of the traffic laws (or lack of them, in countries like India) (U.S DOT-NHTSA, 2016, pp.25-26).

Ethical considerations

This is, along with security, one of the most important and complex challenges that autonomous cars will have to face. In lower levels where is the human who drives the car, the responsibility of his actions corresponds to him and his decisions. Sometimes the period for taking those is so short or inexistent that it can say that the azar decides it.

As already stated, the aims of driving are basically three: safety, mobility, and legality. Most of the time those three can be reached without conflict, but as seen before, sometimes is necessary to infringe the law to guarantee safety (crossing the lane to avoid the disruption). For a person might be obvious to react in that way, but level 5 vehicles have to be programmed for knowing how to react in every situation, also in the ones that imply ethics.

And here it is not about programming the car to stop if there is red light, a stop signal or a policeman. It is more about programming the car for situations in which it is unavoidable to run over someone, crash into something (another vehicle, a wall, a ditch) or deal with situations such as (Lin, 2015, pp.69-82):

- The car must either swerve left and run over an 8-old year or swerve right and run over an 80 years old woman. Should the car be programmed to, in case of having to choose and via facial recognition, killing the person of larger age?
- The car finds itself with having to crash toward a light vehicle or a heavy one. Might the car be programmed to crash to the weakest vehicle or to the safest one? Will be more ethical to protect the own car and the own life or the weakest passenger?
- If the situation to choose is between a motorcyclist with helmet and another one without, should the autonomous car swerve towards the weakest one although he was not complying with the law? Maybe this reckless motorcyclist does not survey and the other one yes, thanks to the helmet. Is it more ethical to program the car to save the weakest or the one that does not infringe the law?
- The car has two options in a narrow curvy road: either slam on the brakes and crash into

a scholar bus risking everyone’s lives, or drives off the cliff, sparing the lives of everyone in the bus. Should the car aim to save the greatest number of people or to save the own passengers?

- Also, it is not the same as killing somebody than letting die. In a critical situation, if the car does nothing, it would continue straight and would run over 5 people. However, if he turns left, he would just kill one person. What should the car do? (Trolley problem)
- Should the car makers program vehicles according to various degrees of morality depending on what customers want? (i.e. Should a driverless car hit a pedestrian to save its passengers’ life?).
- Should the government order that all autonomous vehicles share the same value of protecting the maximum good, although it is not good for its passengers?

Thus, in front of these dilemmas HAVs need to be properly programmed to apply particular and difficult decision rules when safety, mobility, and legality come to a conflict, without forgetting the ethical and moral aspects. The algorithms used for solve these conflict situations must be developed transparently taking into account the input from regulators, drivers, passengers, pedestrians…and the consequences that a highly automated vehicle has on them. (U.S DOT-NHTSA, 2016, pp.26-27).

Operational Design Domain (ODD)

The car manufacturers have the obligation to hang in a document in which, apart from the characteristics of the car, the operational design domain must also be included. This will contain the capabilities of the car, in other words, in which values/conditions it will work properly and safely, such as the roadway types, the geographic area, the environmental conditions (weather, day, night…), etc.

As for the speed, since there is no driver to press the pedal, there should not be any problem in maintaining the limits, but this has to be adapted to the state of the roadways and the weather conditions. There might be maintenance, works or bad weather conditions that make a road impassable. The sensors should be able to detect that, and when they do, in case that the car is not able to drive in that road, they should find an alternative in the safest way possible. The same happens with the environmental conditions: the car should find a safe state and not stop and abandon its passengers in the middle of nowhere in case of a heavy snow storm (U.S DOT-NHTSA, 2016, p.27).

Object, Person and Event Detection and Response

A research performed by California PATH has determined the following examples of behavioural competencies (which are the abilities of an automated vehicle to operate in the regular traffic situations):

- Detect and respond to: speed limit changes, encroaching oncoming vehicles, stopped vehicles, lane changes, static obstacles in the path of the vehicle, traffic signals and stop/yield signs, access restrictions (one-way, no turn, ramps, etc.), work zones, people directing traffic in unplanned or planned events, temporary traffic control devices, emergency vehicles, detours and other temporary changes in traffic patterns.
- Perform: high/low speed merges, car following (stop and go).
- Move out of the travel lane and park.

- Detect: passing and no passing zones and perform passing maneuvers.
- Navigate intersections (and perform turns), roundabouts, parking lot and locate spaces.
- Make appropriate right-of-way decisions.
- Follow local and state driving laws, police/first responder controlling traffic, construction zone workers controlling traffic patterns, citizens directing traffic after a crash.
- Yield to pedestrians and bicyclists at intersections and crosswalks.
- Provide safe distance from vehicles, pedestrians, bicyclists and side of the road, emergency vehicles, temporary work zones, and other unusual conditions.

In this scenario, the person or pedestrian detection can be contemplated, but the problem is not to detect them but how to react to them. Reading body language or understanding non-verbal communication is a pure problem that nowadays cars could not deal with it since it is very difficult interpreting the way a person moves or hold himself as the case below shows:

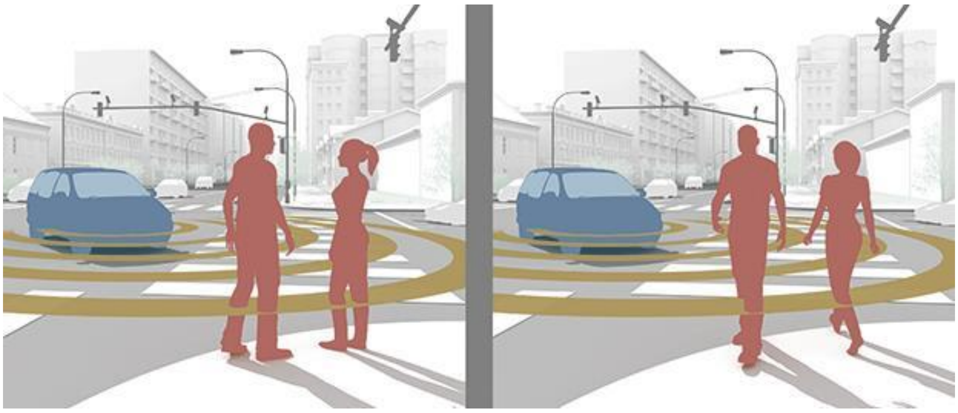


Figure 2-29: Reading Body language (Brooks, 2017).

In the left picture, the couple is talking and it does not seem that they are going to wander into the traffic, therefore, the driverless car should not stop. However, in the picture of the right side, if one person turns away in the direction of the traffic, which means that he wants to cross and the car must stop (U.S DOT-NHTSA, 2016, pp.28-30).

Fall Back (Minimal Risk Condition)

Fall back actions to bring the car to a minimal risk condition will variate according to the level of automation and of course also to the type of problem or risk.

The highly automated cars systems should give information, as the cars nowadays do with the state of the battery or the oil, about the malfunction or the risky situation, out of the operational design domains (ODD).

In lower levels, when this happens, it probably will ask the car driver to take the control of the car back. At the same time, the car should check if the driver is not under influence of alcohol or drugs, or physically handicapped (drowsy for example).

In the highest level where no driver is needed, the car should find a safe state by itself, if possible outside of an active lane of traffic (U.S DOT-NHTSA, 2016, p.30).

2.3 Quality methods

According to Mhenni (2014, p. 2), since the development of new mechatronic products in an industry like the automotive require a rigorous validation and verification of their performance for guaranteeing quality and safety, the possible risks or hazards of those mechatronic systems have to be carefully identified and guarded against. In this way, for bringing them to an acceptable level, it is required not only suitable systems engineering approaches but also rigorous safety analysis techniques in order to manage the complexity and satisfy performance and safety requirements.

An overview of this development process suggested by ISO 26262 and summed up in a V-model process under the name Functional Safety Management, is in detail recorded in the annexes and is made up of different stages that can be appreciated in the next figure. Some of the most important steps in the Concept phase and in the Product development at the system level are enounced below, regarding ISO 26262 and cited in the work of Taylor et al. (2012, pp.3-5):

- *Item Definition (ISO 26262 Part 3, Clause 5)*
- *HARA- Hazard Analysis and Risk Assessment (ISO 26262 Part 3 Clause 7)*
- *Functional Safety Concept (ISO 26262, Part 3, Clause 8)*
- *Allocation of Requirements to Elements (ISO 26262, Part 3, Clause 8.4.3)*
- *Technical Safety Requirements (ISO 26262, Chapter 4, clause 6)*

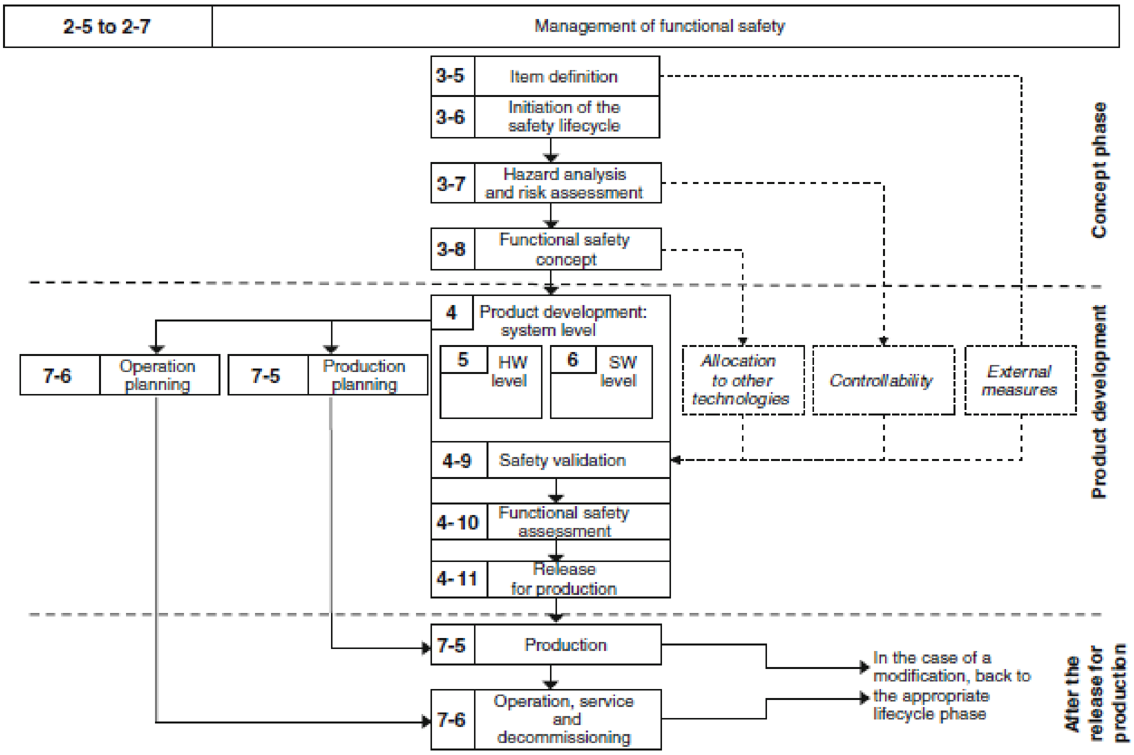

2-5 to 2-7
Management of functional safety
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
Concept phase
4 Product development: system level
5 HW level
6 SW level
7-6 Operation planning
7-5 Production planning
Allocation to other technologies
Controllability
External measures
4-9 Safety validation
4-10 Functional safety assessment
4-11 Release for production
Product development
7-5 Production
7-6 Operation, service and decommissioning
In the case of a modification, back to the appropriate lifecycle phase
After the release for production

Figure 2-30: Safety-lifecycle according to ISO 26262 (ISO 26262 cited in Ross, 2016, p.36).

In order to address the underlying steps, Schoitsch, (2005, pp.12,13), and more specifically

IEC 61508 (IEC, 2010), suggest some questions to be answered by engineers through Hazard identification, Hazard analysis and Risk analysis in order to define and allocate Safety Requirements and establish a Safety Design (Unified Approach). These questions are:

- *What hazards does the system pose?*
- *What are their possible causes and consequences?*
- *What is the likelihood of their occurrence?*
- *What are the risks associated with each of the hazards?*
- *By how much do we need to reduce the risks*

Those questions, as well as the methods that will be in the following described, do not follow a consecutive order since the different approaches (for Safety analysis and Functional safety assessment can report more than one question, or need an iterative process to be answered). For example, the first question is carried out by HARA, for which inductive and/or deductive safety analysis such as FMEA or FTA might be needed respectively in order to answer the second question. HARA also enables to determine the third and fourth question, thus obtaining an ASIL. Depending on the ASIL acquired, the last question can be determined and also which type of inductive or maybe also deductive analysis need to be carried out.

2.3.1 Safety Analysis

As already stated, diverse methods for safety analysis exist in order to assess the system safety during the design phase and to ensure that it has got a satisfactory level (Mhenni, 2014, p. 17). They are also used on the verification stage of the development process (Ross, 2016, p.228).

These methods can be classified according to different criteria such as the type of models they are constructed upon, type of elements they are interested in, a life-cycle phase they are performed in…For this work, they have been classified in inductive or deductive methods, and although there are lots of them[10], the following ones have been selected, guided by ISO 26262.

2.3.1.1 Inductive methods

Bottom-up approach. They investigate unknown failures effects from known failure causes.

2.3.1.1.1 FMEA

According to Ross (2016, pp.115-117), Failure Mode and Effect Analysis is an inductive method for the safety analysis based on the sequence of failure cause, failure and failure effect. The evaluation factors of failures are: Severity of damages (S), the probability of the

[10] Since each hazard analysis technique is a unique analysis methodology that use specific guidelines and rules aiming at identifying hazards, mitigating them and assessing system residual risk (Mhenni, 2014, p. 17).

error occurring (O) and the probability of the error detection (D) and the severity-class is determined by the failure effect and referred to the vehicle itself.

It consists of 5 steps, which were already developed by VDA (Verband der Deutschen Automobilindustrie) and are shown in the picture below:

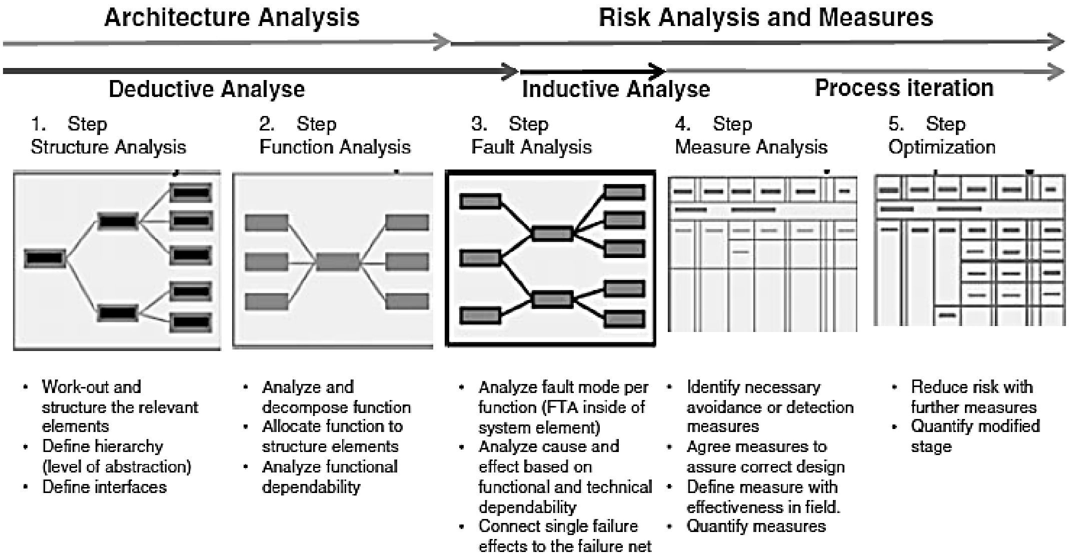

Architecture Analysis
Risk Analysis and Measures
Deductive Analyse
Inductive Analyse
Process iteration
1. Step Structure Analysis
2. Step Function Analysis
3. Step Fault Analysis
4. Step Measure Analysis
5. Step Optimization
• Work-out and structure the relevant elements
• Define hierarchy (level of abstraction)
• Define interfaces
• Analyze and decompose function
• Allocate function to structure elements
• Analyze functional dependability
• Analyze fault mode per function (FTA inside of system element)
• Analyze cause and effect based on functional and technical dependability
• Connect single failure effects to the failure net
• Identify necessary avoidance or detection measures
• Agree measures to assure correct design
• Define measure with effectiveness in field.
• Quantify measures
• Reduce risk with further measures
• Quantify modified stage

Figure 2-31: FMEA in 5 steps (Ross, 2016, p.117).

As it can be seen in the figure above, steps 1 and 2 are analyses and information, necessary for the step 3, the fault analysis. These three steps can be seen as the illustration of a deductive analysis since functions and structures are broken down or decomposed. They are followed by a fourth step (Measure Analysis) and a fifth for the Optimization, which makes up the process iteration.

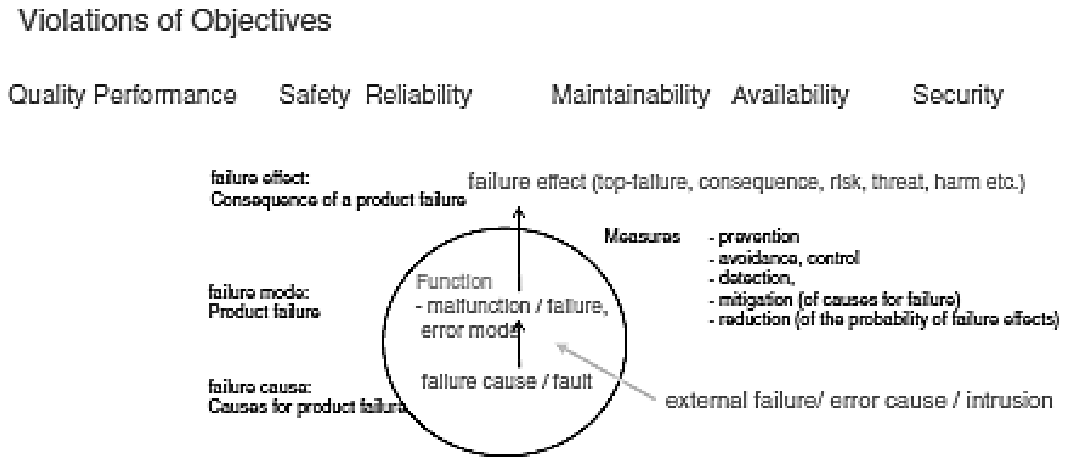

Violations of Objectives
Quality Performance
Safety Reliability
Maintainability Availability
Security
failure effect: Consequence of a product failure
failure effect (top-failure, consequence, risk, threat, harm etc.)
Measures
- prevention
- avoidance, control
- detection,
- mitigation (of causes for failure)
- reduction (of the probability of failure effects)
failure mode: Product failure
Function
- malfunction / failure, error mode
failure cause / fault
failure cause: Causes for product failure
external failure/ error cause / intrusion

Figure 2-32: Basic principle of (inductive) failure analysis (Ross, 2016, p.116).

To conclude, this traditional technique has the objective of evaluating the effects of potential failure modes of components/functions and eliminating them in the system design

2.3.1.1.2 ETA

Event Tree Analysis aims to complement driving situations in the system FMEAwhen they become too complex. According to Goldberg et al. (1994, pp.3(51-54)), this inductive method is very useful when an accident has wide spectrum of results and the consequences are determined by subsequent failure or operation of other components or subsystems (safety or protection devices) and by human errors made in response to the initiating event.

It can be used in a qualitative or quantitative way and the process consists on:

- Asking “what if” the initiating event occurs
- Analyse every possible sequence of event that results from assuming failure/success of the components/humans affected.
- Attach probabilities if needed

Among its advantages are the assessment of probabilities of coexisting faults or failures and the no need of end events to be anticipated. However, it addresses only one initiating challenge and it has to be foreseen by the analyst. Also, discrete levels of success and failure cannot be distinguishable according to Goldberg et al. (1994, p.3-3)

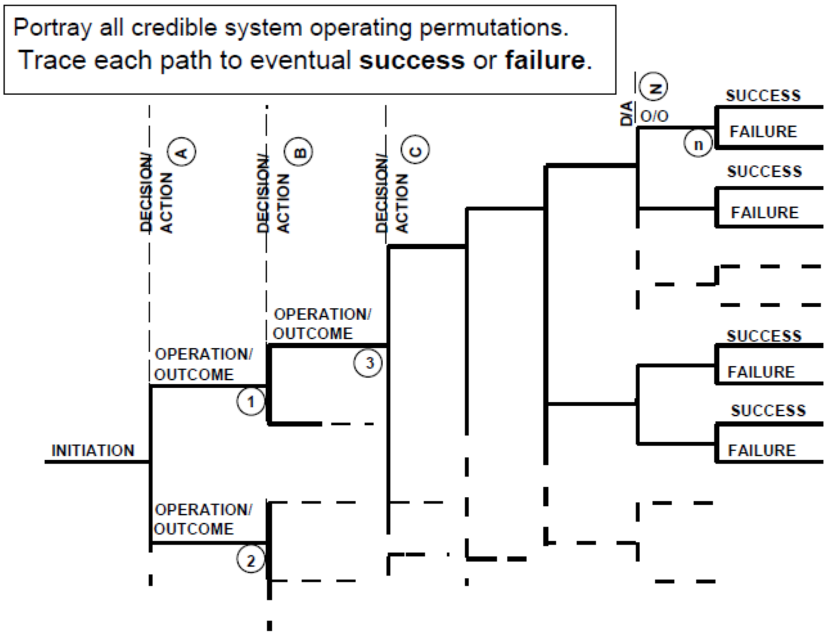


Figure 2-33: Event tree (generic case) (Goldberg et al. 1994, p.3-52).

2.3.1.1.3 Markov analysis

It assesses the transition from one condition to another. For (Gagniuc 2017, p.16) it is a stochastic model used for modeling randomly changing systems. The future states are dependent just of the present position or state and not on the previous events.

2.3.1.1.4 HAZOP

British Standard Institution (2002) defines this hazard and operability studies or analysis as a structured and systematic qualitative risk assessment tool. It examines complex planned or existing process or operation in order to identify and evaluate problems that could cause risks. The qualitative approach aims to stimulate the imagination of participants in order to recognize potential hazards, failure conditions or malfunctions of individual technical elements.

According to Mhenni et al. (2014, p.21), this hazard identification process consists on identifying potential deviations by comparing system parameters to a list of key guide words (more, less, no, reverse, late and so forth) which are combined with process/system conditions or parameters (speed, flow, pressure…). Later on, a team of multidisciplinary experts will decide if the designed safeguards are satisfactory or it is needed additional actions for reaching an acceptable level of risk.

The main disadvantage of HAZOP approach is that its success is extremely dependable of the team and its ability in predicting deviations based on experiences in the past and general matter expertise (Mhenni et al. 2014, p.21).

2.3.1.2 Deductive methods

Top-down approach. They examine the unknown causes of failure from known failure effects.

2.3.1.2.1 FTA

According to Clemens (1993) cited in Goldberg et al. (1994, 3-56), Fault Tree Analysis is a top-down symbolic logic model generated in the failure domain. It traces the failure pathways from a predetermined, undesirable condition or event (TOP event) of a system to the failures or faults (fault tree initiators) that could act as causal agents.

Goldberg et al. (1994, 3-56) explain that FTA includes generating a fault tree (symbolic logic model), introducing failure probabilities for each fault tree initiator, propagating failure probabilities to determining the TOP event failure probability, and determining cut sets (if all occur, cause TOP event) and path sets (if none of them occurs, TOP event cannot occur).

Fault Tree Analysis permits qualitative and quantitative analysis: the first one identifies the necessary and sufficient combinations of basic events that result in the manifestation of the undesired TOP event (minimal cut sets), while the second one, quantitative analysis is carried out in order to calculate the probability of the TOP event (Mhenni et al. 2014, p.20).

FTA is, therefore, a key method for the development and analysis of safety-relevant systems in almost all industries and has its origins in the military sector. Thanks to the fault tree analysis and Boolean logics, relevant elements that could fail and cause undesired states or events like failures can be determined.

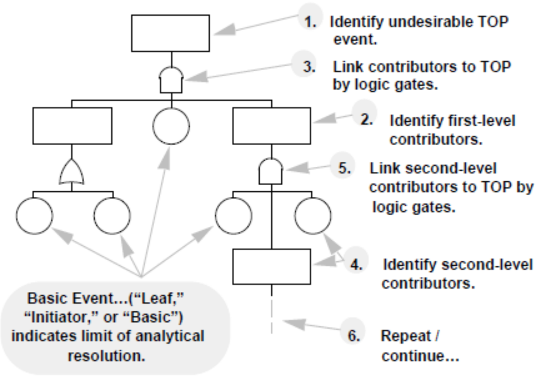

1. Identify undesirable TOP event.
3. Link contributors to TOP by logic gates.
2. Identify first-level contributors.
5. Link second-level contributors to TOP by logic gates.
4. Identify second-level contributors.
Basic Event...("Leaf," "Initiator," or "Basic") indicates limit of analytical resolution.
6. Repeat / continue...

Figure 2-34: Fault tree construction process (Goldberg et al. 1994, p.3-37).

2.3.1.2.2 Reliability Block Diagrams (RBD)

According to Gough et al. (1990) cited in Goldberg et al. (1994, 3-30), Reliability Block Diagram is a backwards symbolic logic model generated in the success domain. It is constructed of series, parallel or combined elements (which represent an event or system function) between an input and an output point and illustrates system reliability, which is the probability of successful operation during a defined time interval. When a component fails, the block is removed from the diagram. Therefore, the system is operational if there is at least one path between the input and output points

They are similar to FTA since are also an example of deductive analysis and the blocks can be logically related thanks to Boolean algebra. According to Mhenni (2014, p.21), the main advantage of this approach is its simplicity (it can be understood not only by engineers from different disciplines but also non-technical stakeholders) but the main drawback is its non-ability to capture the dynamic behaviors of large and complex systems. For this reason, new reliability models such as Dynamic Reliability Block Diagrams (RBD) are getting introduced.

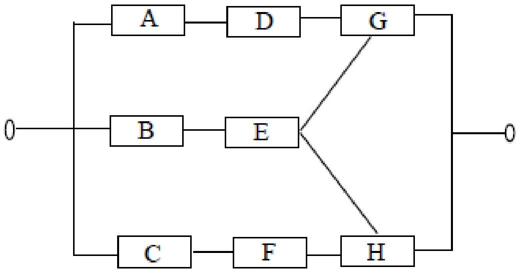


Figure 2-35: Typical complex RBD (Goldberg et al. 1994, p.3-31)

2.3.2 Functional safety assessment

Until now quality or analysis methods that help engineers to identify causes or effects of faults or failures were covered. Once they are recognized, ISO 26262 suggests different methods for Functional Safety Assessment

According to ISO 26262 (ISO, 2011), Part 3, Clause 7,

> "*Hazard analysis, risk assessment, and Automotive Safety Integrity Level (ASIL) determination are used to determine the safety goals for the item such that an unreasonable risk is avoided. For this, the item is evaluated with regard to its functional safety. Safety goals and their assigned ASIL are determined by a systematic evaluation of hazardous events. The ASIL is determined by considering the estimate of the impact factors, that is, severity, the probability of exposure and controllability. It is based on the item's functional behaviour; therefore, the detailed design of the item does not necessarily need to be known.*"
>
> (Ross, 2016, p.81)

2.3.2.1 HARA

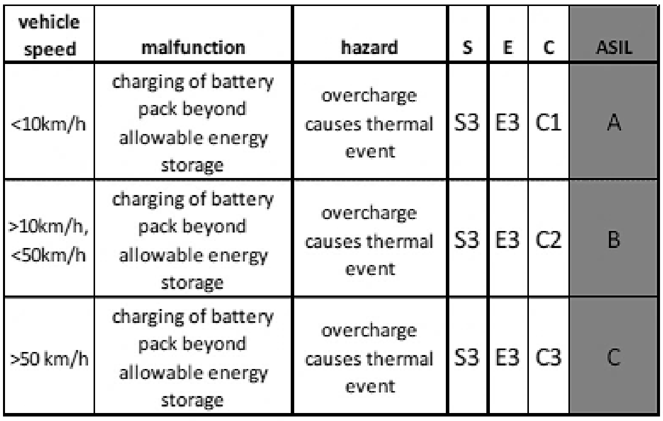
The objective of Hazard analysis and risk assessment is to "*identify and categorize the hazards that malfunctions in the item can trigger and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk". (ISO, 2011)*

It is a critical feature described in ISO 26262 Part 3, Clause 7 and this process consist of 4 key stages, according to ISO (2011) cited in Taylor et al. (2012, pp. 3-4):

- Identifying potential hazards associated with E/E system malfunction. Defined not at item level but vehicle level.
- Determining the Severity Rating (S) related with the hazard. From S0 to S3, where 0 would not cause injury or harm and 3 severe injuries or death.
- Determining the Exposure Rating (E) linked with the hazard. From E0 to E4, where 0 reflects conditions never seen or only in extreme cases and 4 conditions seen by the major part of drivers.
- Determining the Controllability(C) associated with the hazard. From C0 to C3, where 0 reflects a situation where the majority of the drivers could deal with and 3 where the drivers very improbable might bring the situation under control.

With these three ratings and the safety analysis methods seen in the previous section, the Automotive Safety Integrity Level or ASIL described below can be determined.

Table 2-2: Excerpt from a simplified Hazard Analysis and Risk Assessment (HARA) (Taylor, 2012, p.4, Fig.5)



vehicle speed	malfunction	hazard	S	E	C	ASIL
<10km/h	charging of battery pack beyond allowable energy storage	overcharge causes thermal event	S3	E3	C1	A
>10km/h, <50km/h	charging of battery pack beyond allowable energy storage	overcharge causes thermal event	S3	E3	C2	B
>50 km/h	charging of battery pack beyond allowable energy storage	overcharge causes thermal event	S3	E3	C3	C

2.3.2.2 ASIL

In ISO 26262, Part 1, Clause 1.6, ASIL is defined as” *one of four levels to specify the item’s or element’s necessary requirements of ISO 26262 and safety measures to apply for avoiding an unreasonable residual risk, with D representing the most stringent and A the least stringent level”.*

An adequate and acceptable level of safety of an E/E system is reached through demonstrating the absence of unreasonable risk associated with each hazardous event caused by the malfunctioning behaviour of the item. This can be accomplished by defining safety goals to avoid unreasonable risk through the prevention or mitigation of the identified hazardous events (occurrence of a hazard in a particular operational situation). Each one of them is assigned an Automotive Safety Integrity Level (ASIL), based on the mixture of three factors (Birch, 2013, p.3) already seen in the Hazard Analysis and Risk Assessment:

- severity (extent of human harm)
- the probability of exposure (to operational situations)
- controllability (ability for persons at risk to take action to avoid harm)

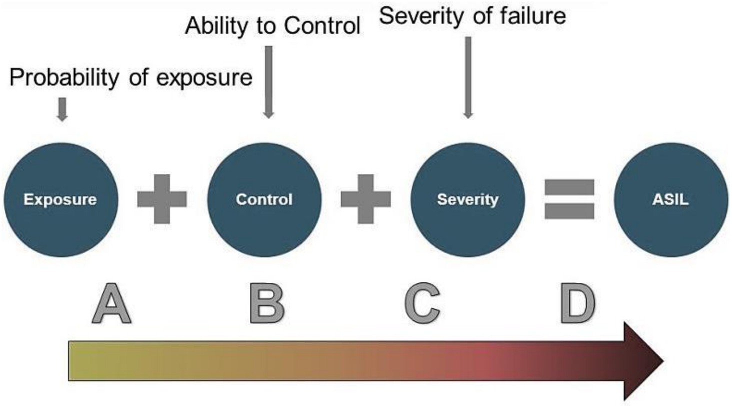


Figure 2-36: ASIL risk levels (National Instruments, 2016)

ASIL assessment, therefore, measures the obligatory risk for a specific system component and gives assistance in choosing ways to reach a certain level of integrity. As risk rises, more strict and rigorous approaches and tests must be employed to guarantee safety.

The ASIL label is made at the commencement of the development process and helps to determine how thorough the testing must be for each component. To fulfill ISO 26262, software organizations need to prove a functional safety management plan, a quality management plan, along with evidence of a safety culture and people who are skilled and responsible for enforcing that culture in the development and production phases.

As Ross (2016, p.123) states according to ISO 26262, the inductive analysis seen are normally demanded all ASIL requests and the deductive analysis only for ASIL C and D.

2.4 Procedural models for system development of mechatronic systems

A process model describes a set of functions or a progression at the type level in a descriptive, prescriptive and explanatory way. It is used frequently for the development of many applications, in our case, in software and mechatronic products in the automotive industry. They are utilized to identify the behaviour of the system under consideration and to derive technical decisions in its development process by mapping the reality of certain relevant aspects depending on the abstraction rate, the quality of knowledge and the validity of the assumptions made (Spanfelner, 2012, p.8).

These system development models specify how activities must be organized in the total system development effort. Examples of them are summed up in the next paragraphs. Moreover, after them, an explanation of what mechatronic systems are and examples of them applied to active and passive safety are given in a specific section.

2.4.1 Process models suggested by ISO 26262

2.4.1.1 V-Model

The V-model is a graphical way to represent rigorous development lifecycle systems. It includes the main steps to take into account through an iterative process of verification and validation not only in the project definition (left side) but also in the project test and integration (right side). According to Mathur & Malik (2010, p.30), the V-model demonstrates the relationships between each phase of the development lifecycle and its associated phase of testing. Instead of moving down linearly, the process steps are determined upwards after the coding phase, forming the V shape.

The IEEE Guide Adoption of PMI Standard a Guide to the Project Management Body of Knowledge (2004) defines the verification and validation as follows:

- Validation: "*The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders. It often involves acceptance and suitability with external customers".*
- Verification: "*The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. It is often an internal process."*

This model aims to improve efficiency and effectiveness of software development, to reflect the relationship between test and development activities in order to minimize the risks of the project, to improve and guarantee quality, to reduce the total cost of the project and its system lifecycle and to improve the communications between stakeholders.

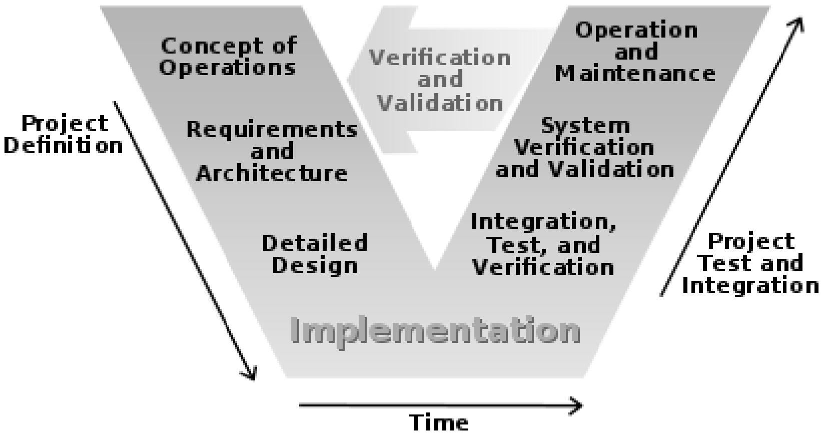

Project Definition
Concept of Operations
Requirements and Architecture
Detailed Design
Implementation
Verification and Validation
Operation and Maintenance
System Verification and Validation
Integration, Test, and Verification
Project Test and Integration
Time

Figure 2-37: V-model (Federal Highway Administration (FHWA), 2005)

In the standard ISO 26262 this model can be found in its XT variety as the figure below shows:

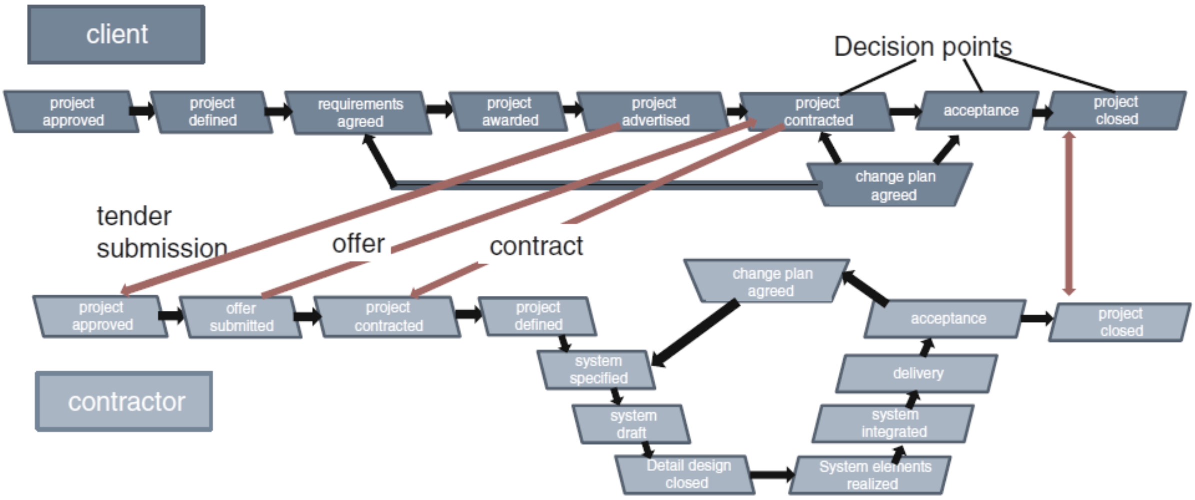


Figure 2-38: V-model customer-supplier according to V-model XT (Ross, 2016, p. 22)

The V-model XT describes the V only for individual products. The customer-supplier relationship is firstly described. This phase determines the product scope and the fundamental requirements (Ross, 2016, p.23).

In software development, the process steps are set upwards after the coding phase (instead of going down linearly) forming a V shape. The V-Model establishes the relations among each stage of the development lifecycle and its linked phase of testing. The horizontal and vertical axes denote time or project completeness (left-to-right) and level of abstraction, respectively.

This can be considered as an extension of the waterfall model.

2.4.1.2 Waterfall Model

According to Ross (2016, p.30), the waterfall model is a linear sequential approach for product (often tools and software) development that differs from the V-model because it is non-iterative, does not have a specific source of origin and his level of abstraction is even higher. Also, V-based process models describe vaster parts of lifecycles.

It progresses downwards (simulating a waterfall) including phases like conception, initialization, analysis, design, construction, testing, deployment and maintenance. In this way, the output of one phase becomes the input for the next one but sometimes is not possible to know the specified requirements before the beginning of the next phase.

Verma et al. (2014, p.1067) suggest that the waterfall model is most appropriate when:

- The end product is stable.
- Requirements are well documented, clear and fixed from the starting stage.
- Technology is understood and static.
- The project is short.
- Not good methodology for the complex and object-oriented project.
- Difficulty in accommodating changes after project development.

A derivation of the waterfall model for the automobile industry would surely bear a resemblance to parts of the safety lifecycle of ISO 26262 or the various APQP standards

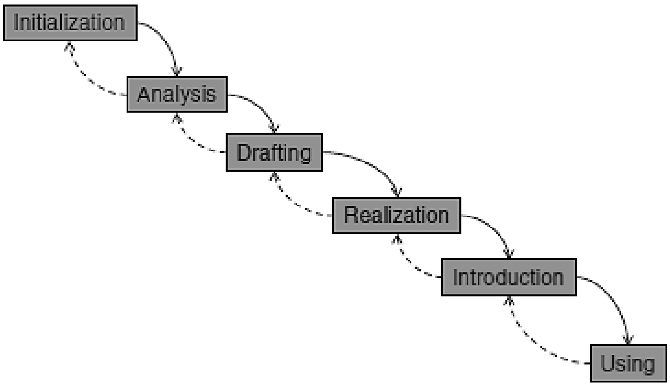


Figure 2-39: Waterfall model (Ross, 2016, p.30).

2.4.1.3 Spiral Model

The spiral model is a risk-driven process model creator. It leads a team to the adoption of elements of one or more process models. In the automotive industry is considered as the traditional model, in contradistinction to V-model (Ross, 2016, p.31).

In the picture below it is shown the sequential process and the respective iterations in a spiral shape:

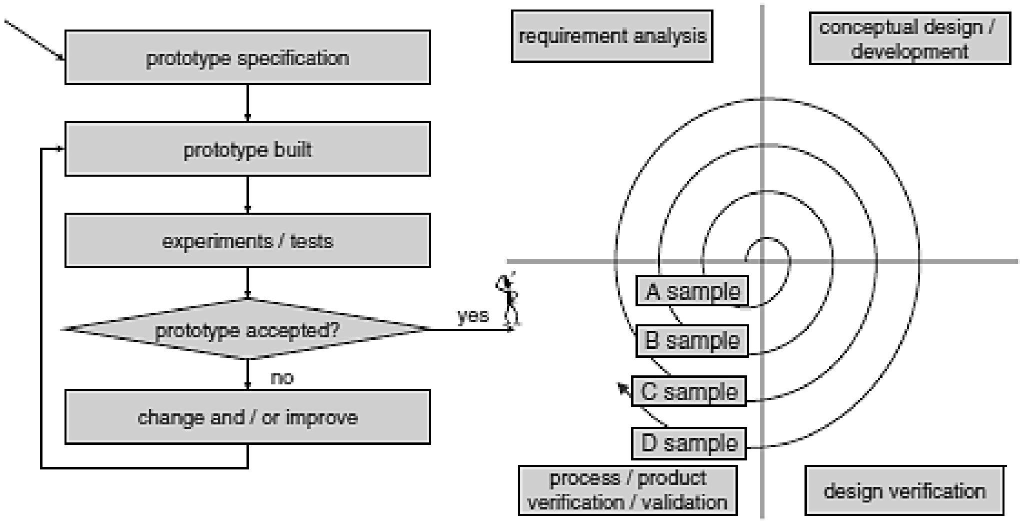


Figure 2-40: Spiral model for a prototype or sample-cycle approach as a basis for many automotive maturity models (Ross, 2016, p.31).

The phases of the spiral would be the focus on prototypes and Verma et al. (2014, p.1067) recommend this methodology when:

- Risk evaluation is important.
- The customer is not sure of their requirements.
- Requirements are complex and need clarity.
- It can work well with the changing user requirements.
- This methodology is mainly used for large projects.
- Budget is high.
- Little documentation is required as compared to waterfall methodology.

2.4.2 Other process models

2.4.2.1 Prototyping model

In this system development method (SDM), instead of freezing the requirements before a design, a prototype is made, proved and rebuilt as many times as necessary until it is acceptably successful. This iterative and trial-and-error process works well in environments where not all the projects requests must be known.

Prototyping is a smart idea for complicated and large systems for which there is no manual process or existing system to help to determine the requirements.

The advantages of this model are that errors can be detected earlier and so better solutions and users are involved in the development process giving a quicker feedback.

From the study of Verma et al. (2014, p.1067) it can be affirmed that prototyping is a basic idea for complicated and large systems for which there is no manual process or existing system to help to determine the requirements.

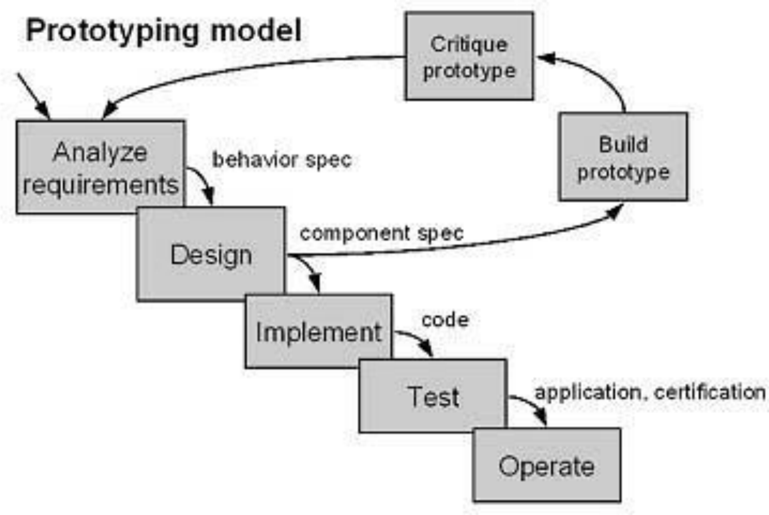


Figure 2-41: Prototyping model (unknown)

2.4.2.2 Agile Model

Agile modeling is an iterative and incremental method used in model and documentation of software based on best practices. It has more flexibility than the traditional modeling methods seen above and it is recommended for dynamic environments that change fast. It is based on repetitive work cycles and functional merchandise and here groups have more than one chance to get the aspects of the project right (Watts-Roy, 2017).

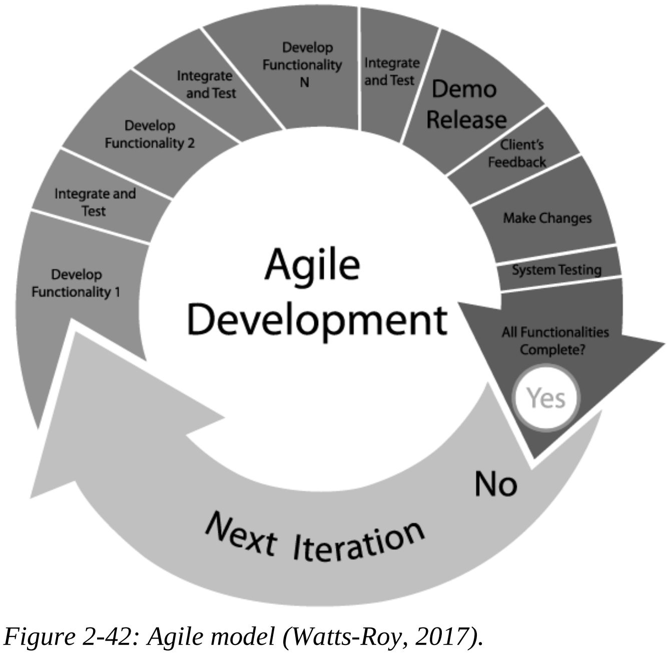


Figure 2-42: Agile model (Watts-Roy, 2017).

2.4.2.3 Incremental model

This model is a process of software development where the design, implementation, and test are done incrementally until the final product and its requirements are reached. Therefore, incremental model is a combination of waterfall and prototyping (Ghahrai, 2017).

The main disadvantage of this model might be the exceeded costs and future problems that are not obvious in the early prototypes.

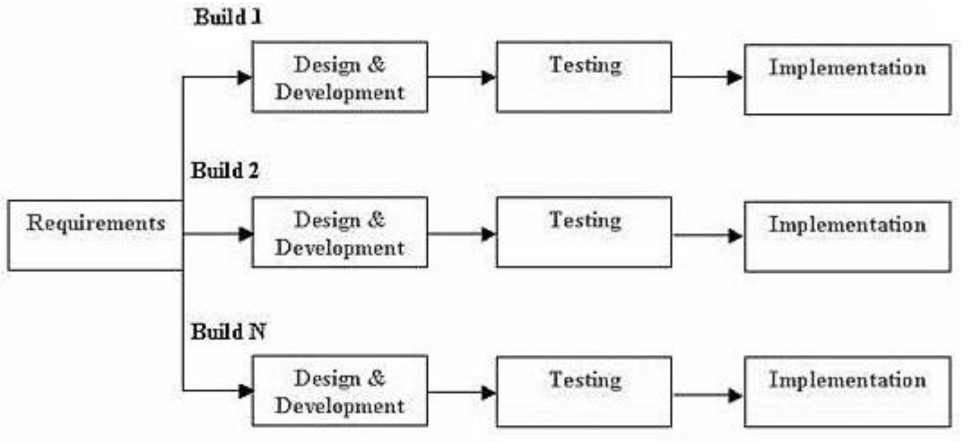


Figure 2-43: Incremental life cycle mode. (Son & Adam, 2017).

2.4.2.4 Iterative model

The iterative model starts with a simple implementation that progressively becomes more complex adding functional capabilities until the system is complete. Additions and modifications are done in every step. The limitations of this model are that it does not give complete information and some details might not be merged in the development system and at the end, it results time-consuming and not too much cost effective. However, it still offers an inherent versioning, rapid turnaround, and easy adaptability, especially in agile organizations, according to Powell-Morse (2017).

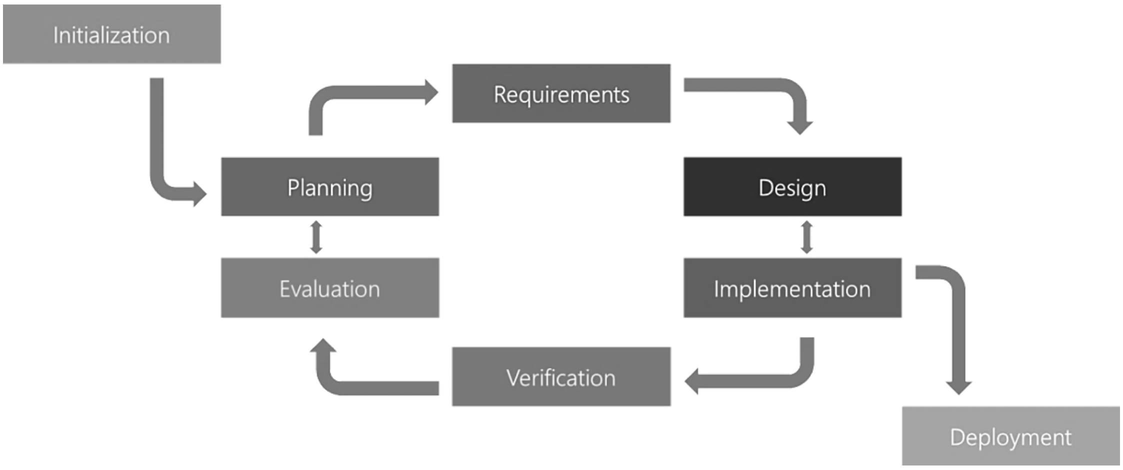


Figure 2-44: Iterative model. (Powell-Morse, 2017)

2.4.2.5 RAD model

Rapid Application Development model is an incremental model where the components or functions are developed in parallel like if they were subprojects. The developments are time-boxed, provided and gathered into a working prototype. This allows the user to use the previous product and to give feedback (Micro & Donnely, 2017).

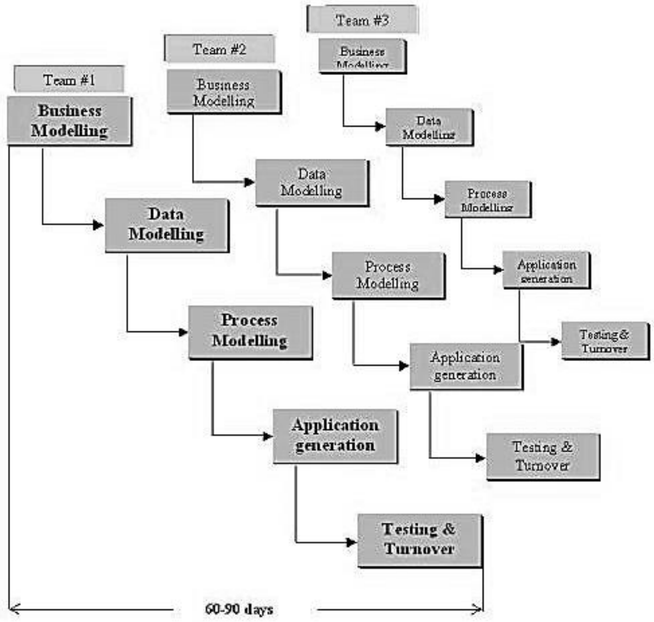
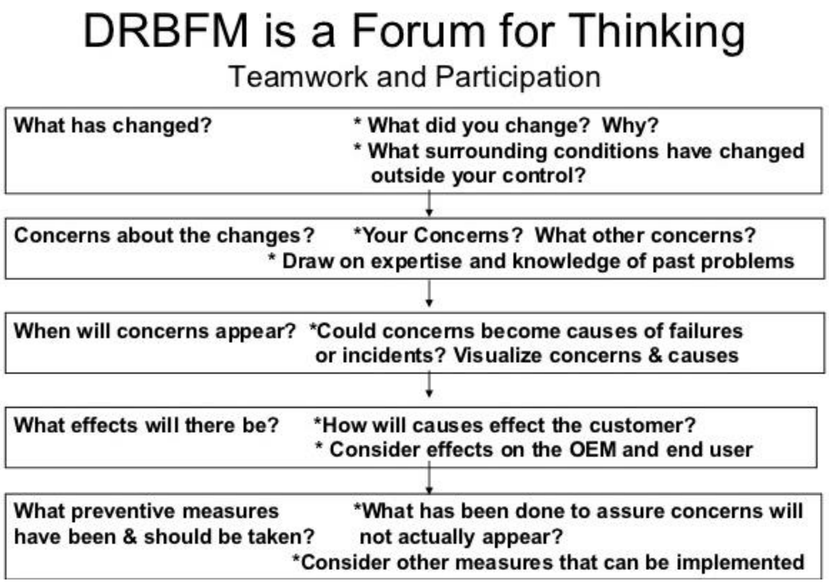


Figure 2-45: RAD model (Micro & Donnely, 2017)

2.4.2.6 DRBFM

This Design Review Based on Failure Model is a stable method, often used in modern architectural developments, that was developed by Toyota. It assumes that designs problems happen when modifications are made to already existing engineering designs which have succeeded and introduces new iterations and describes a comparison based on features. The results of DRBFM are only adopted for the specifications after the effects analysis and are then accepted as a modification for the product (Haughey, 2007).



DRBFM is a Forum for Thinking

Teamwork and Participation

What has changed? * What did you change? Why? * What surrounding conditions have changed outside your control?

Concerns about the changes? *Your Concerns? What other concerns? * Draw on expertise and knowledge of past problems

When will concerns appear? *Could concerns become causes of failures or incidents? Visualize concerns & causes

What effects will there be? *How will causes effect the customer? * Consider effects on the OEM and end user

What preventive measures have been & should be taken? *What has been done to assure concerns will not actually appear? *Consider other measures that can be implemented

Figure 2-46: Design Revier Based on Failure Model (Haughey, 2007).

2.4.3 Mechatronic systems

The VDI guideline 2206 –Development methodology for mechatronic systems points out that:

> *“Mechatronics refers to the synergetic interaction of the disciplines of mechanical engineering, electrical engineering and information technology in the design and manufacture of industrial products as well as in process design."*

(VDI, 2004 cited in Gausemeier, 2002, p.787)

Mechatronic systems consist of the simplest form of sensors, actuators, information processing and basic system. These four components interact with each other in a control loop, which is shown in the next figure:

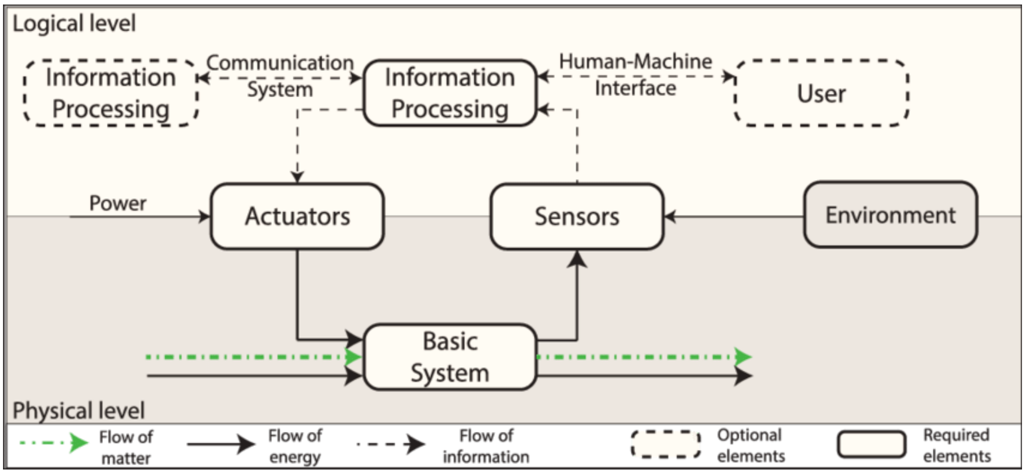


Figure 2-47: Basic structure of a mechatronic system (VDI 2206, 2004 cited in Casner, 2017, p.4))

In other words:

> *"Mechatronic systems result from the simultaneous design and integration of following disciplines:*
>
> - *mechanical and coupled systems*
> - *electronic systems*
> - *control and information technology.*
>
> *The integration is between the components (hardware) and the information-driven functions (software), oriented towards finding an optimal balance between the basic mechanical structure, sensor and actuator implementation, automatic digital information processing, and overall control. In addition, synergetic effects are created, resulting in enhanced functionality and innovative solutions.".*
>
> (Isermann 2005, p.11)

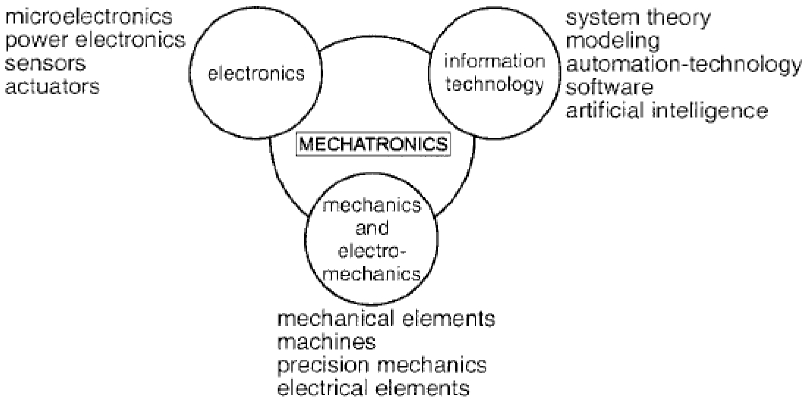


Figure 2-48: Mechatronics: synergetic integration of different disciplines. (Isermann, 2005, p.5)

The framework within which our master thesis is confined is the automotive industry. As briefly viewed in the introduction, the origins of car safety and its systems to guarantee it dates back to the invention of the car in itself. Therefore, in the next section as well as in annexes *A4. Active safety systems* and *A.5Passive safety systems* the actual safety-related mechatronic can be seen. Also in Annex *A.1.Car Safety timeline* the lector can have a general overview of how the actual state of the art has been reached. A great part of these safety devices that we have nowadays and in the modern automobile can be taken for granted, they are no more than the result of a great deal of trial and error and unfortunately lives.

2.4.3.1 Active and passive safety systems

As just stated, over the years different safety systems have been introduced as soon as once invented, it was proved that they had the potential to save lots of lives and/or reduce the injuries (and they were affordable). They can be classified into active or passive.

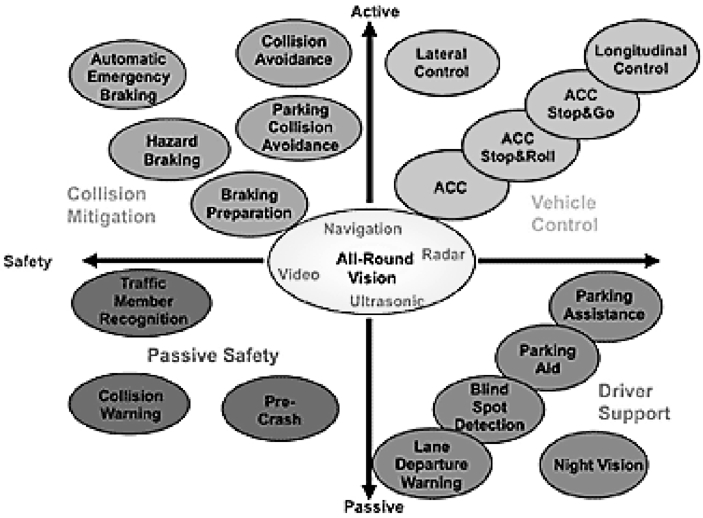
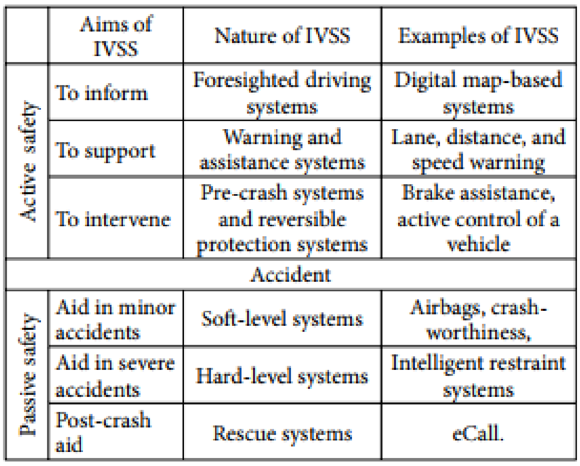


Figure 2-49: Safety systems. (Troppmann, 2006)

Table 2-3: Active and passive safety systems. (Jarašūniene & Gražvydas Jakubauskas, 2007, p.286, Table 1)



	Aims of IVSS	Nature of IVSS	Examples of IVSS
Active safety	To inform	Foresighted driving systems	Digital map-based systems
	To support	Warning and assistance systems	Lane, distance, and speed warning
	To intervene	Pre-crash systems and reversible protection systems	Brake assistance, active control of a vehicle
Accident			
Passive safety	Aid in minor accidents	Soft-level systems	Airbags, crash-worthiness,
	Aid in severe accidents	Hard-level systems	Intelligent restraint systems
	Post-crash aid	Rescue systems	eCall.

In the following paragraphs, a brief description and examples of these systems are shown, according to Jarašūniene (2007, pp.284-287).

Active safety systems

The active safety systems are the features that aim to prevent the risk of a collision or an accident.

The main elements that influence the active safety improvement are an optimal usage of the traction, an acceleration of the time in which the driver-vehicle last in react when changes on the road are concerned, an increase of the number or size of data for the driver about the car’s motion state and its surroundings etc. These features interpret signals from various sensors in order to help the driver to control the car and they may be activated by a human operator, automatically by a computer driver system, or even mechanically.

Table 2-4: Active safety systems

Type of active safety system	System
Dynamic bases systems	Anti-lock brake system (ABS)
	Autonomous Emergency Braking System (AEB)
	Brake Assist System (BAS)
	Electronic Brake-force Distribution (EBD)
	Electronic stability control (ESC)
	System steering the braking force (EBV or AFU)
	Traction control systems (ASR or TCS)
Driver information and assistance systems	Active Vision Enhancement (VE)
	Blind Spot Support
	Curve Adaptive Lighting (CAL)
	Drowsiness Detection Systems (DDS)
	Intelligent speed assistant (ISA)
	Lane departure warning systems (LDW)
	Lane Keeping Assistance (LKA)
	Tyre pressure monitoring systems(TPMS)
	Traffic jam assistance (TJA)
Integrated (or Advanced Driver Assistance) safety systems	Adaptive Cruise Control (ACC)
	Collision Mitigation systems (CMS)
	Brake override engages
	Collision Mitigation and Avoidance Systems (CMAS)
	Computerized Active Brake
	Front crash prevention
	Hazard/warning indicator lights

As for the Intelligent Vehicles Safety Systems, there might be the following ones among others:

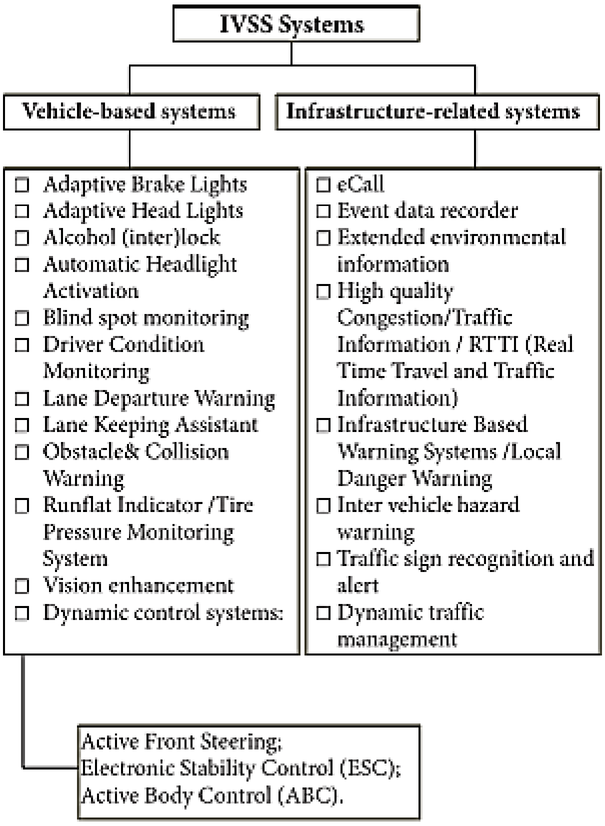

IVSS Systems
Vehicle-based systems
Infrastructure-related systems
□ Adaptive Brake Lights
□ Adaptive Head Lights
□ Alcohol (inter)lock
□ Automatic Headlight Activation
□ Blind spot monitoring
□ Driver Condition Monitoring
□ Lane Departure Warning
□ Lane Keeping Assistant
□ Obstacle& Collision Warning
□ Runflat Indicator /Tire Pressure Monitoring System
□ Vision enhancement
□ Dynamic control systems:
□ eCall
□ Event data recorder
□ Extended environmental information
□ High quality Congestion/Traffic Information / RTTI (Real Time Travel and Traffic Information)
□ Infrastructure Based Warning Systems /Local Danger Warning
□ Inter vehicle hazard warning
□ Traffic sign recognition and alert
□ Dynamic traffic management
Active Front Steering;
Electronic Stability Control (ESC);
Active Body Control (ABC).

Figure 2-50: IVSS systems (Jarašūniene & Gražvydas Jakubauskas, 2007, p.287).

Passive safety systems

The passive safety features are the systems that, as its name indicates, are passive until called into action. They become active when there is an accident and helps to minimize the damage from the collision and the risk of injury or death.

Table 2-5: Passive safety systems

System
Airbags
Crumple zones
eCall
Frontal Protection System (FPS)
Fuel pump kill switch
Head restraint
Laminated windshields
Rollover bars
Safety cell
Seatbelts
Strong body structures

2.5 Safety-related standards

In this chapter it is going to be briefly analysed different standards relevant for the work. Some of them have been already mentioned along this document because they were either safety-related and/or they included some important points related with the state of the art of this master thesis.

One of those is ISO 26262, which serves as a basis or starting point for the author's approach. Therefore, this will be analysed in a little more detail and a sum up of it can be found in annexes *A6 Overview of ISO 26262*.

Apart from this one published by the International Organization for Standardization(ISO), there are others from the International Electrotechnical Commission (IEC), Society of Automotive Engineers (SAE) and European Telecommunications Standards Institute (ETSI).

2.5.1 ISO 26262: Road vehicles − Functional safety

The safety standard ISO 26262 has been developed to provide guidance, in the form of requirements and processes, for avoiding unreasonable residual risk caused by the malfunctioning behaviour of E/E systems, leaving them to the developers to interpret these requirements in the context of their products(ISO 26262 cited in Birch, 2013, pp.1-2).

The goals of ISO 26262 are summarized in the following statements from Kucharski et al. (2012):

- Provide an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and support tailoring the necessary activities during these lifecycle phases.
- Cover functional safety aspects of the entire development process (including activities like requirements specification, design, implementation, integration, verification, validation, and configuration).
- Provide an automotive-specific risk-based approach for determining risk classes (Automotive Safety Integrity Levels or ASILs).
- Use ASILs for specifying the item's necessary safety requirements for achieving an acceptable residual risk.
- Provide requirements for validation and confirmation measures to ensure that a sufficient and acceptable level of safety is being achieved.

According to the International Standard Organization (2011) this standard is an extension of IEC 61508 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 passenger cars with a maximum gross vehicle mass up to 3500 kg. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities (ISO, 2011).

Since it only addresses to possible hazards caused by malfunctioning behaviour of E/E safety-related systems, it does not contemplate hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behaviour of E/E safety-related systems(ISO, 2011).

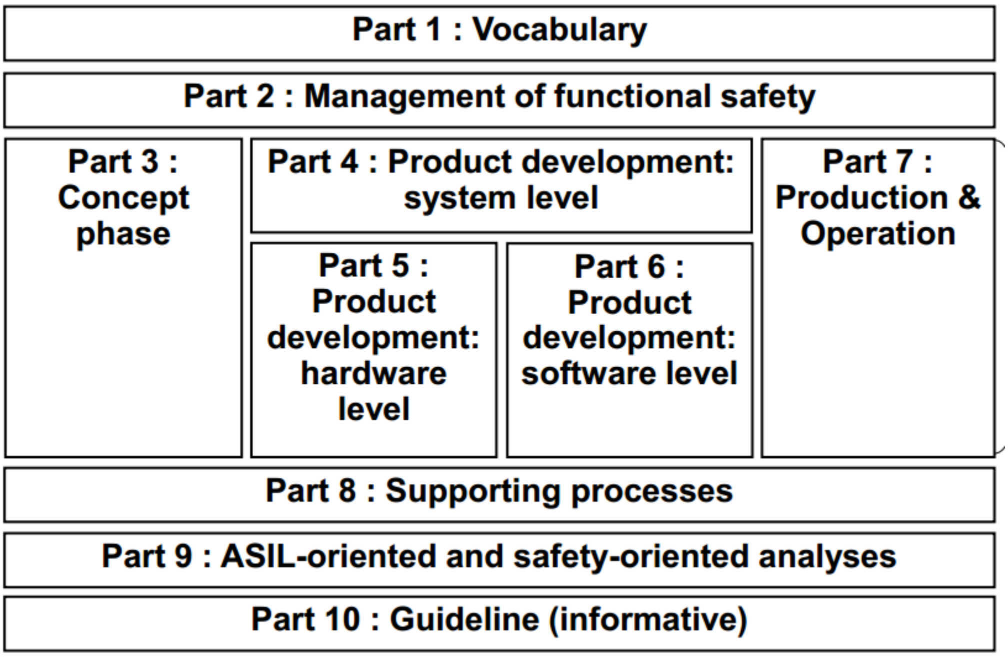

Part 1 : Vocabulary
Part 2 : Management of functional safety
Part 3 : Concept phase
Part 4 : Product development: system level
Part 5 : Product development: hardware level
Part 6 : Product development: software level
Part 7 : Production & Operation
Part 8 : Supporting processes
Part 9 : ASIL-oriented and safety-oriented analyses
Part 10 : Guideline (informative)

Figure 2-51: The Ten Parts of the ISO 26262 (ISO 26262, 2011cited in Cherfi, 2015,p.20)

2.5.2 Other relevant standards

IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES).

IEC 61508 is intended to be a basic functional safety standard applicable to totally types of industry. Functional safety is here defined as: “part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.”

This standard covers the complete safety lifecycle and might request interpretation to develop sector-specific standards. Its origins remain in the process control industry.

It was developed to remedy the fact that software introduced new sources of errors and it is difficult to prove if it is correct and if it faithfully responds to its specifications (Mhenni, 2014, p. 23)

IEC 61850: Communication networks and systems for power utility automation.

This one is an international standard that defines communication protocols for intelligent electronic devices at electrical substations. Between its features, there are Data modeling, reporting schemes, fast transfer of events, setting groups, sampled data transfer, commands, and data storage (IEC, 2018).

IEC 61058: Switches for appliances

According to the International Electrotechnical Commission (IEC, 2016), this standard applies to switches (mechanical or electronic) for appliances actuated by hand, by foot or by other human activity, to operate or control electrical appliances and other equipment for household or similar purposes with a rated voltage not exceeding 480 V and a rated current not exceeding 63 A.

IEC 62502: Analysis techniques for dependability - Event tree analysis (ETA)

It aims to consolidate basic principles of Event Tree Analysis applied in any branch of industry, in which reliability and risk-related measures for the consequences of an initial event need to be considered (IEC, 2010).

SAE J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles

SAE (2016) through this Recommended Practice describes the full range of levels of driving automation in –road motor vehicles, including functional definitions and related terms for further levels of automation but not specifications and requirements.

SAE J2980: Considerations for ISO 26262 ASIL Hazard Classification

This SAE Recommended Practice (SAE, 2018) published firstly in 2015 presents a method and example results for determining the Automotive Safety Integrity Level (ASIL) for automotive electrical and electronic (E/E) systems, i.e. identifying and classifying hazardous events. This activity is required by ISO 26262 (which has a wider scope) and consistent with it. Additionally, the scope of this suggested practice is limited to collision-related hazards and motion control (while in ISO 26262 other accidents and functions are covered).

ETSI TS 103 097: Intelligent Transport Systems (ITS); Security; Security header and certificate formats.

According to the European Telecommunications Standards Institute (ETSI, 2017), this technical specification identifies security header and certificate formats for Intelligent Transport Systems, in order to secure G5 communications.

2.6 System modeling languages

According to Kaiser (2013 p.4), the three components used for describing system models are modeling languages, methods, and software tools.

The first ones are suitable for the representation of a system structure and are the ones that concern the subject of this master thesis. These graphical modeling languages aim to enable a holistic view of Model-Based System Engineering. The most common ones are defined in the next paragraphs. Afterwards, the most suitable for our approach will be described.

2.6.1 Examples and suitability of some modelling languages

2.6.1.1 CONSENT

CONSENT language (CONceptual design Specification technique for The Engineering of Complex Systems) contains model concepts to describe in a structured, easy and intuitive way the system structure, which takes place in two partial models (environment and active structure). Despite its suitability for the design of complex mechatronic systems and cyber-physical systems (CPS) the distinction of relationships is focused on mechatronic systems so that interactions can be presented. This includes. also the condition that only elements which have the same interfaces can be interconnected. Nevertheless, the formalization of the active structure is not sufficient to achieve comparability, completeness or correctness (Kaiser, 2013 pp. 46-47). Their natural language is very intuitive and easy to understand, but this fact can also produce ambiguity, misunderstandings and flaws in the system design, according to Balzert (2010) cited in Bernijazov (2015, p.8).

2.6.1.2 METUS Language

METUS allow the representation of the elements and the linking of these to modules. The effect of the elements is not shown but can be seen implicitly by the connection of the elements with the functions. The integration of the system into its environment, and thus their interaction is not addressed (Kaiser, 2013 p.45).

2.6.1.3 OPM

OPM (Object-Process Methodology) is a simple and intuitive modelling language for describing complex systems. The ability to describe different levels of constructs contributes to clarity. Mechatronic systems, as part of complex systems, can also be mapped with this language. However, OPM contains too few concepts to describe the interactions between the elements (Kaiser, 2013, pp. 46-47).

2.6.1.4 UML

According to Rumbaugh et al. (2017, p.3), UML (Unified Modelling Language) is a general-purpose visual modelling language utilized to specify, visualize, construct and document the artifacts of a software system. Abled to be used with all development methods, lifecycle stages, application domains and media, UML captures information about not only the static structure but also the dynamic behavior of a system. It is addressed for discrete systems and therefore it is not suitable for continuous systems in engineering and physics.

2.6.1.5 SysML

According to the Object Management Group (OMG, n.d), SysML(System modelling language), which is derived from UML, is also a general-purpose graphical modeling language utilized for specifying, analyzing, designing, and verifying complex systems. These include not only software like in UML but also hardware, information, personnel, procedures, and facilities.

In particular, the language provides graphical representations with a semantic foundation for modelling system requirements, behavior, structure, and parametric, which is used to integrate with other engineering analysis models. As it is shown in the figure below, SysML reuses a subset of the UML language and adds extensions to meet the requirements in the UML for SE RFP (System Engineering Request for Proposal), according to Friedenthal, Moore & Steiner, 2011, p.87).

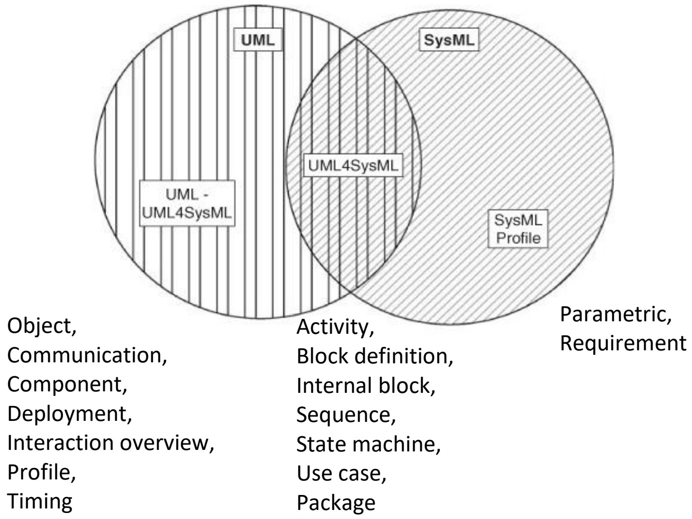

UML
SysML
UML4SysML
UML - UML4SysML
SysML Profile
Object, Communication, Component, Deployment, Interaction overview, Profile, Timing
Activity, Block definition, Internal block, Sequence, State machine, Use case, Package
Parametric, Requirement

Figure 2-52: Relationship between SysML and UML. (Friedenthal, 2011, p.88)

According to Sabetzade et al (2011, p. 2), SysML is very suitable for safety-critical software embedded in other greater technical systems with electronic and mechanical parts (i.e. mechatronic systems), the reason why considering software with non-software elements is crucial. To sum up, with respect to UML, SysML has the following advantages, according to this author:

- It encompasses not only software systems but others like hardware, information, personnel, procedures, and facilities.
- SysML expresses systems engineering better than UML, thus reducing the prejudices UML has towards software. The classes of UML are replaced in SysML for blocks, which are a modular unit of system description (a structural concept in a system and its environment).

- SysML has integrated cross-cutting links for interdepending requirement and design elements. This fact help engineers to associate requirements and design elements/models described at different levels of abstraction.

All these reasons make SysML more suitable than the others when having to choose a modelling language to represent the use cases with the future scenarios. The rest of the chapter will be exclusively addressed to SysML and its Use Case Diagrams.

As already stated, SysML is not specifically designed for mechatronic systems since it claims to be universally valid (Kaiser, 2013, pp. 49-51). However, it helps to identify and construct systems and specify its components that can then be designed using other domain-specific languages such as UML for software design and VHDL for hardware design.

SysML provides a structural description of the system in the IBD (internal block diagram) and BDD (Block Definition Diagram) diagram types. Other authors such as Mhenni (2014, p.47) add to these two, the Parametric Diagram (Par) and the Package Diagram (Pkg). The model concepts are not specifically

As showed in the following figure and later summarized, according to the job of Friedenthal et al. (2011, pp.30, 88) the nine diagrams included in SysML are:

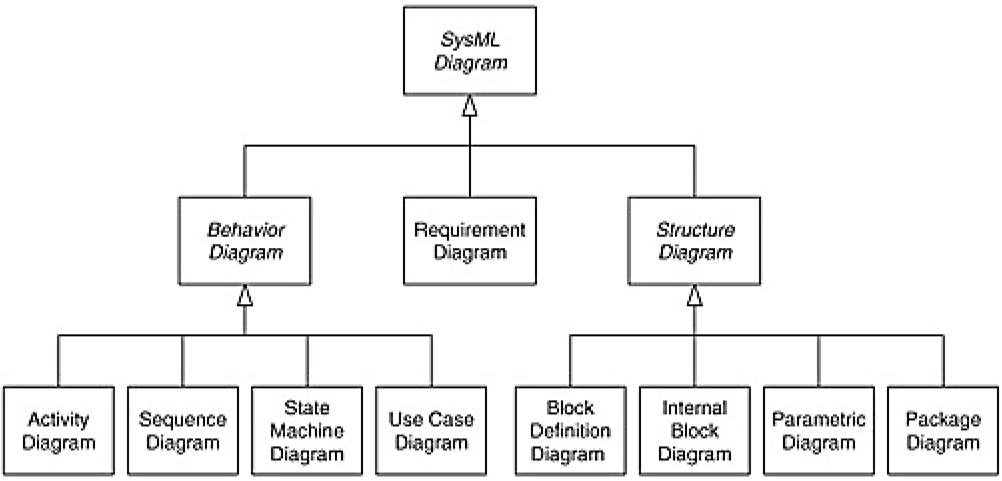


Figure 2-53: SysML diagram taxonomy (Friedenthal, 2011, p.30).

- Requirement diagram***:*** It represents text-based requirements and their relationship with other requirements, design elements, and test cases to support requirements traceability (not in UML).
- Activity diagram***:*** It represents behaviour in terms of the ordering of actions based on the availability of inputs, outputs, and control, and how the actions transform the inputs to outputs (modification of UML activity diagram).

- Sequence diagram**:** It represents behaviour in terms of a sequence of messages exchanged between parts (same as UML sequence diagram).
- State machine diagram**:** represents the behaviour of an entity in terms of its transitions between states triggered by events (same as UML state machine diagram).
- Use case diagram: It represents functionality in terms of how a system or other entity is used by external entities (i.e., actors) to accomplish a set of goals (same as UML use case diagram).
- Block definition diagram: It represents structural elements called blocks, and their composition and classification (modification of UML class diagram).
- Internal block diagram: It represents interconnection and interfaces between the parts of a block (modification of UML composite structure diagram).
- Parametric diagram: It represents constraints on property values, used to support engineering analysis (not in UML).
- Package diagram: It represents the organization of a model in terms of packages that contain model elements (same as UML package diagram).

The SysML profile is organized into the following discrete language units that extend the language, which means that Uses cases will also have to include them (Friedenthal et al. 2011, p. 88):

- Requirements. Textual requirements and their relationships to each other and to models.
- Blocks. System structure and properties.
- Activities. Extensions to UML activities to support continuous behaviour.
- Constraint blocks. Parametric models.
- Ports and flows. Extensions to the UML structural model to support the flow of information, matter, and energy between system elements.

2.6.1.5.1 Use Case diagram

As already seen in the last section, use case is one of the most popular diagrams used in both UML and SysML.

According to Friedenthal et al. (2011, p.303), they describe the functionality of a system in terms of how its users use that system to achieve their goals. In other words, they sequence the interactions of outside entities (actors) with the system and at the same time system actions that yields an observable result of value to the actors.

The users and other interested participants of a system are described by the actors, which may represent external systems or humans who use the system (Friedenthal et al. 2011, p.303).

Use case technique has a textual and graphical description that may be further elaborated with detailed descriptions of their behaviour, using activities, interactions, or state machines. The graphical part, the use case diagram, is composed therefore of its actors, the scenarios that describe the interactions between the actors and the system, and these relationships or communication paths between them ("communication", "include", "extend" and "generalization") (Friedenthal et al. 2011, pp.306-307).

In order to create use case diagrams, according to the approach of Jegadeesan (2008, pp. 43-44), the steps to follow are:

Step 1 – Choosing system boundary
 -Clarified by defining what is outside
 -Once external Actors are identified the boundary becomes clear

Step 2 & 3 – Finding primary actors & goals
 -Identify Primary Actors by asking questions e.g. Who start/stops the system?
 -Actors have goals that must be satisfied by the system.

Step 4 – Define use-cases
 -Start use-cases with a verb
 -Create, read, update and delete goals.

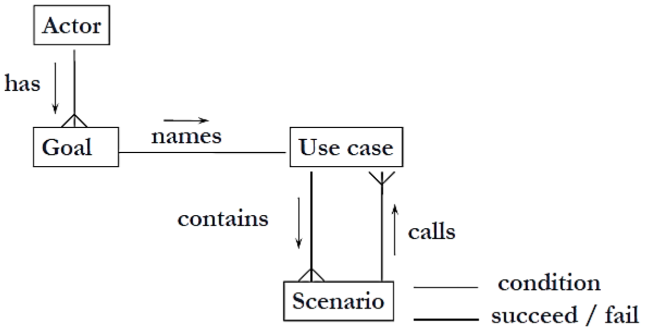


Figure 2-54: Use case. (Jegadeesan, 2008, p.23)

Friedenthal et al. (2011, p. 309), suggests that a typical use case description should include the following:

- Preconditions: a necessary condition for the use case to begin.
- Postconditions: a condition that must hold on once the use case has completed).
- Primary flow: most frequent scenario of the use case.
- Alternate and/or exception flows: less frequent scenarios or scenarios that are not directly in support of the goals of the primary flow.

Other authors such as Cockburn (2012) or Fowler also add:

- Title: the goal of the use case is trying to satisfy.
- Primary actor: Stakeholders that have direct interaction with the system.
- Main success scenario: steps or statements of the interaction between the actor and the system
- Extensions: a condition that results in different interactions from the main success scenario.

Hence, a Use Case Template with different relevant fields for describing the scenarios will be used. This template by De Francisci (2016) can be found in annexes and consists of two sections. The first part is for the *Use Case Identification* (with the *Use Case ID* and *Use Case Name*, which will be a concise, results-oriented name, with a verb and a noun, that reflect the tasks the user needs to complete using the system.

The second part of this template is for the *Use Case Definition*, which includes the following fields:

- *Description*: a brief explanation of the reason for the use case and its outcome. In other words, this would be a more extended version of the Use Case Name section.
- *Actors*: here the author distinguishes between primary actors and optionally, supporting actors and stakeholders and interests.
  - Primary Actors are the ones that perform the use case. They can be a person, an element, or a parameter that interact directly with the system or scenario.
  - Supporting actors would be the ones that support Primary Actors to achieve his goal.
  - Stakeholders and their Interests might not interact with the system but they have an interest in the use case outcome.
- *Preconditions*: as already stated, they are the activities or conditions that must take place for the use case to start
- *Postconditions*: success and/or failure states of the system when the use case concludes.
- *The frequency of use*: estimation on how oft the use case can take place.
- *Scenario*: as in the Actors field, here it can be distinguished between the Main Scenario (normal course), and if desired, Alternative Courses or Extensions, and Exceptions.
  - Main Scenario: the main flow of events, stated as a numbered list of actions carried out by the actor, from preconditions to postconditions.
  - Alternative Courses/Extensions: branches from the main flow of events.
  - Exceptions: anticipated error conditions that could take place during the execution of the use case, and how the system reacts to them.
- *Special requirements*: performance, security, user interface, functional or non-functional requests before, during or after the execution of the use case.
- *Issues*: further comments about the use case or remaining open or to be determined issues that need to be solved by somebody until some due date.

For the use case diagram, also known as modelling or graphical part, a simplified version of the guidelines for notation given in Friedenthal et al. (2011, p. 588) will be used[11]

[11] See Annex *A8.Use Diagram Notation*

3 Analysis and modelling of use cases

In this chapter the different challenges analysed in section *2.2 Future trends and challenges* will be grouped in different scenarios in order to reduce complexity and see what kind of risks or hazards might exist. The issues that arise from different situations will correspond with use cases.

For facilitating not only this creation process but also the understanding of the lector, this practical part will be divided into three parts. Firstly, the definition of a system followed by the composition of user stories for each upcoming mobility form. Lastly, the user stories lead to mobility-specific use cases.

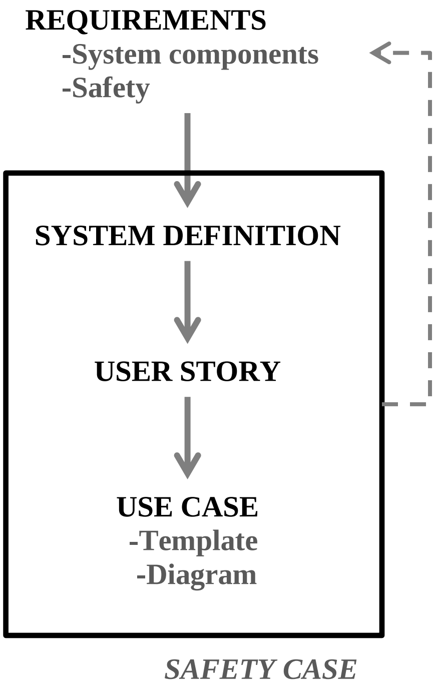


Figure 3-1: Safety case approach (own elaboration).

When engineers have to develop new automotive systems, different requirements must be defined from early on, in the Concept phase for the item definition. Those requirements may appear in the system and/or in its components, for example: reducing the weight of a piece, increasing the duration of a battery, or changing the precision of a sensor. The specifications usually go hand-in-hand with safety requests, which are no more than measures aiming to overcome the described challenges. Since it is mandatory to check if those requirements are fulfilled before a new car model is released to the streets, the idea of a safety case presented in standards and in this work needs to materialize itself. Therefore, in this chapter and through the approach raised, this unspecified concept is going to take shape.

3.1 System definition

Recapitulating some points of the theoretical part, the focus was on *dependability* since this is a broad and fundamental concept for mechatronic (and embedded[12]) systems. Moreover, it is also an umbrella term for diverse system attributes such as safety and others summarized in the figure below:

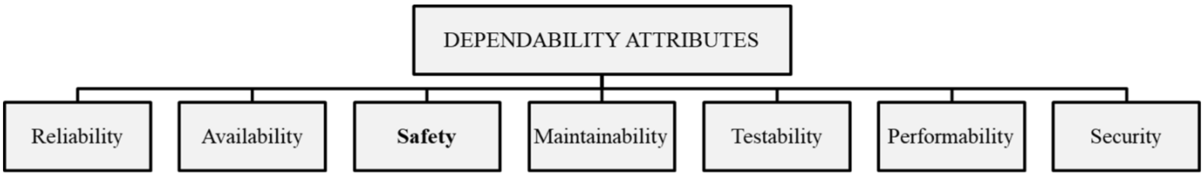


Figure 3-2: Dependability attributes (own elaboration)

These features may be affected by one (or normally more than one) succession of impairments or malfunctions that result in scenarios or sources (i.e. hazards) that may cause harm or adverse health effect on the actors, depending on the level of likelihood or risk. In the worst case, when the level of risk is very high, this initial fault will end up in an accident, as the figure 3-3 on the next page shows.

Figure 3-4 illustrates an integrated safety approach and could be considered as a detail view of what happens between hazard and accident in the figure 3-2. The different active safety systems (mostly mechatronic) will try to manage to elude the accident. They do so, by detecting and avoiding the hazard or in case this hazard prevention is not possible, mitigating it/them. If all of this does not work and the accident takes place, the passive safety systems will aim to reduce the damage.

Depending on the hazard and risk dimension, one or more attributes (in most cases more than one) will be hampered. Dependability and its attributes are directly related to the system and its components. However, it is not the system alone that might be affected by this fault-error-failure chain, but also the environment. It is in this environment where the already mentioned traffic actors come into play, from pedestrians up to infrastructure stakeholders and elements. In the following paragraphs, the potential hazards and actors of use cases will be examined. These actors or traffic elements that play a role in the upcoming scenarios will be compared with the classical ones that already exist nowadays.

[12] See chapter *8.Glossary and abbreviations*

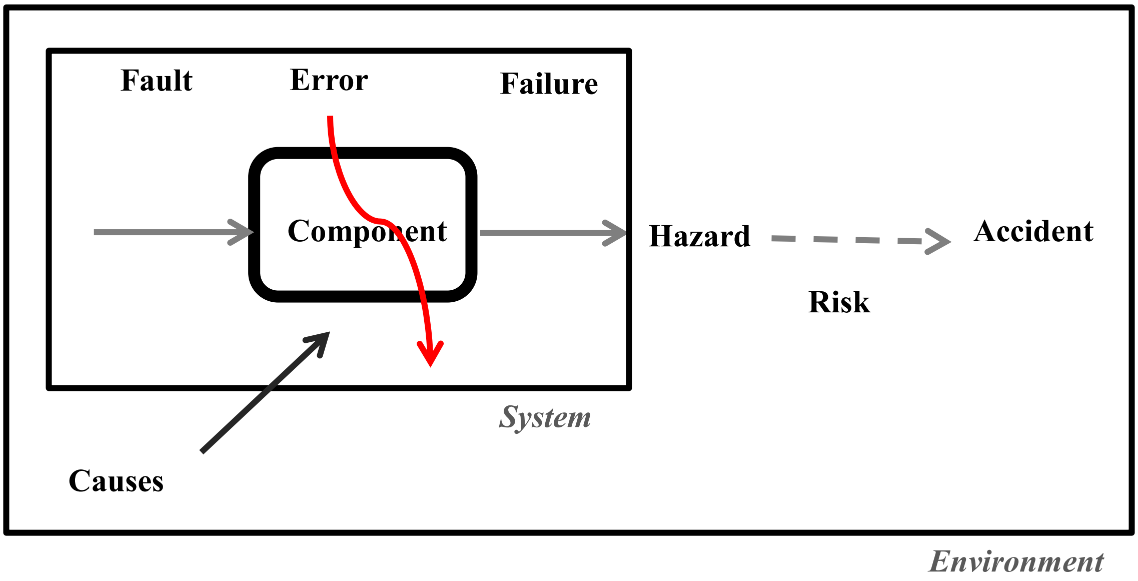


Figure 3-3: Accident parameters diagram (own elaboration)

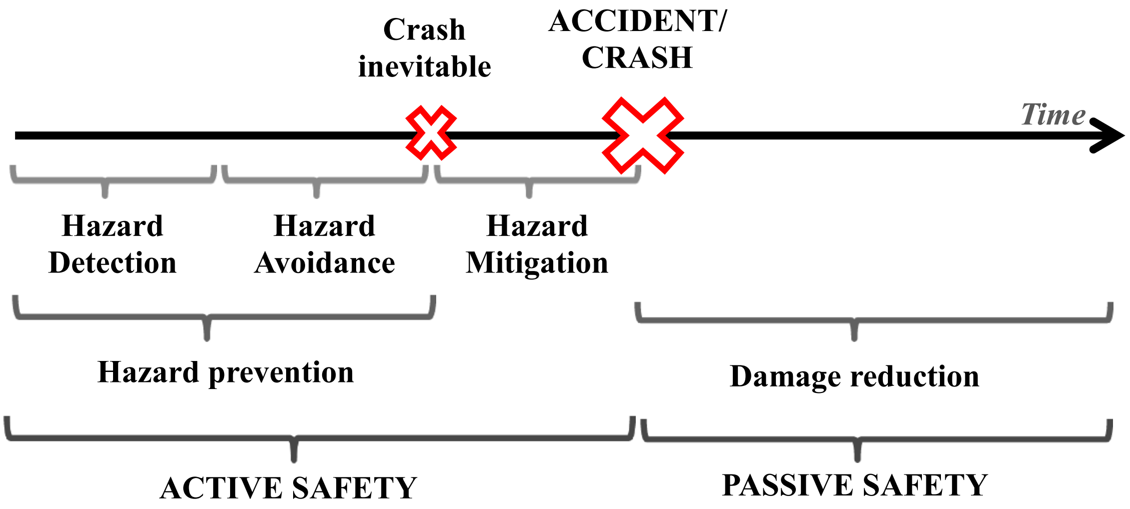


Figure 3-4: Integrated safety approach (own elaboration based on Bońkowski et al. 2017).

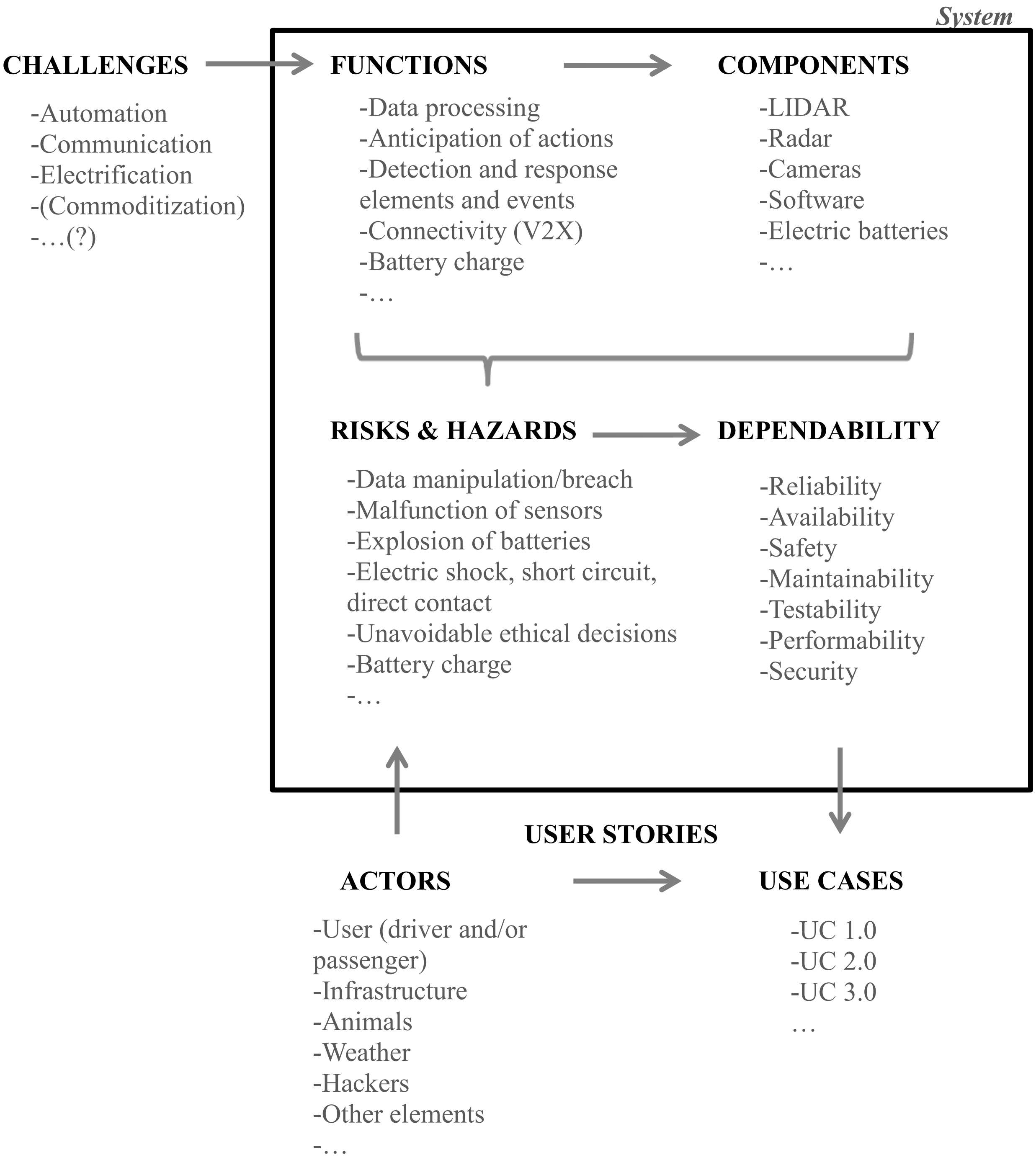


Figure 3-5: System definition scheme (own elaboration).

For a better understanding of the approach or basis, as it is shown in the system definition diagram (Figure 3-5) different terms are bound together and play their own role in the system framework:

Nowadays, most of the cars utilized and manufactured are conventional ones (ICEV). Nevertheless, engineers are developing and improving the mobility of the future, in order to make them as safe as possible and also affordable in order to produce revenues.

The ***challenges*** identified in previous chapters were the following: automation or self-driven cars, communication or connected cars, electrification or battery-powered vehicles, and - with less impact - commoditization or shared cars. It can be assumed that in a long-term future there will only be autonomous cars in our roads. However, until that point, engineers and practitioners are still pondering how the transition and gradual process will look like since the interaction of all of them will be without any doubt the most challenging issue. Thanks to their work, the challenges of today will become guarantees tomorrow.

These innovative forms of mobility are considered challenges due to the new ***functions*** they carry implicitly. Depending on the level of abstraction, and/or if the extra functions added to the new trends are considered, different functionalities can be identified. This means that any vehicle, today or in the future, will have the classic basic car functions such as braking, accelerating, comfort and ergonomics, cooling, passenger and pedestrian protection, climate, etc. Although in the future this will be in a much more improved version, they can be taken for granted. Nonetheless, due to the scope and aims stated at the beginning, the functions that are relevant for our hazard and risk analysis adhere to the non-conventional ones. Examples of these further functionalities are data processing (recording, use, storage, erasure, alteration, and transfer); software updates; cyber-attacks protection; capacity to anticipate to actions carried out by other traffic participants; detection and response to elements and events in verbal and non-verbal situations; connectivity or communication with other traffic participants, the battery charge; protection for direct contact; short circuit, among others.

For carrying out those functions, autonomous, connected and electric cars will rely on the performance of different ***components***, mainly of the sensors and actuators that will replace the human action or in other words, his eyes for detecting elements, his foot for braking, his brain for taking decisions, his hands and arms for holding the steering wheel etc.

Off these components, whose nature can be non-physical (software) or physical (the vast majority) the fault-error-failure can be triggered. Apart from the typical components with whom cars are and will be endowed (brake system, passive safety systems, cooling system, air conditioning system etc.), there will be new components that substitute the driver activation of the classical systems. As already described at the time, these physical components will be LIDARs (Light Detection and Ranging), Radars (Radio Detection and Ranging), Cameras, GPS (Global Positioning Systems), infrared sensors (for the object detection in bad light conditions), DSRC (dedicated short-range communication, in order to gather and send vehicle and infrastructure data), INS (Inertial navigation systems composed of accelerometers and gyroscopes that along with GPS, estimate the car position, orientation and speed), prebuilt or precomputed maps (high-definition and high-detailed maps that give information about roads and infrastructure for a better perception of the reality), odometry sensors (estimation of the distance travelled thanks to the wheel speed), electric batteries (substitution of fuels in the vehicle empower), sensors, actuators and protection elements for the electrical circuit and a long etcetera of other mechatronic components.

If a malfunction or a fault takes place on these components or systems, they are not able to carry out the functions they are related with and therefore this can end up in a hazardous event.

Since ***hazards*** are undesired events that will be normally caused by the malfunctioning behaviour of mechanic, electrical, electronic, or programmable items, they and their correspondent ***risks*** can be classified into diverse categories: there might be mechanical risks, as well as electrical, chemical, acoustic or cyber-attacks among others. Those can occur at the same time as a result of the same fault-error-failure chain directly or indirectly due to the breakdown of other components.

In the worst cases, depending on the risk, they can end up in accidents (crashes or run-overs) if the driver/car (depending on the level of automation) is not able to detect and respond to the hazard or if it is simply unavoidable.

Normally these crashes are caused by a mechanical failure, which means that due to different reasons, the sensors have not done “their job”. Although the probability of a manufacturing defect is little but existent, these hazards normally come from the external action of an actor, which will be treated in next paragraphs. When crash situations are unavoidable, another factor to take into account is the ethics under it was programmed to crash.

Since the future mobility forms are expected to offer more features or functionality, they will have to include more sensors and other mechatronic components, too. This fact will increase the complexity and dependence among them, whilst dependability should be maintained or even increased. For this reason, a little misalignment in a single sensor may have a terrible impact on the whole car as a system. Since a false perception of the reality might deliver a false signal or data, a false interpretation and actuation of sensors might start a cascading failure or error chain. Those faults or wrong perceptions are closely related with the external conditions of the car. For example, bad weather conditions (heavy snow, rain, glare or dust storms); poor road and visibility conditions, often related with the previous ones (snow fake areas, iced or wet slick surfaces, low lighting levels…); vandalism (manipulation of sensors and cameras…) etc.

Apart from those mechanical risks above mentioned, electrical cars might have to face other hazards that could end up in accident. In other words, thermal instability or loss of motor torque due to a fault in the batteries can induce electric hazards with high level risk such as short circuit, electric shock, direct contact or electrocution. Moreover, chemical risks, which can start with corrosion or smoke, can culminate in the ignition/explosion of the batteries and the whole car. The acoustic problem in electric cars normally at low speeds is also a fact, due to the too low noise they emit.

Cyber-attack hazards, although they might not affect directly any physical component but the software, can become high-risk scenarios by providing wrong data for the system. This may lead eventually to the same effect as mechanical failure. Examples of those attacks can be found in the chapter *2.2.3 Communication.* Those IT attacks might affect availability, authentication, data confidentiality, privacy, anonymity, data integrity, non-repudiation, traceability and revocation, authorization, robustness etc. Also, the system updates can turn out to be hazards if the already-existent components are not suitable for the update.

Another factor to take into account for the system definition is the ***actors*** that interact directly or indirectly with it. For future electric car use cases the actors are mainly the same like the traditional actors. For example, drivers, pedestrians, cyclists, motorcyclists, other vehicles, animals, infrastructure elements, traffic lights and traffic signals, weather, other elements or objects, among others.. It is in connected cars and along the different automation levels of autonomous cars where new actors come into play. Example of these actors are hackers, delinquents, and instead of drivers and passengers, simply users. The latter, with their capabilities or wants, are contemplated in depth in ***User Stories.***

Once the potential hazards and actors that play a role are clear they can be correlated with ***dependability*** by asking which attributes (reliability, availability, safety, maintainability, testability, performability, and security) are linked with every risk.

Starting with safety, all the situations described have an effect on the safety of passengers or other actors if they take place. According to the safety definition stated in the chapter *2.1.2 Dependability*, the system will always try to perform the functions already mentioned above (as well as the classical ones), and when this is not possible, it will stop in a fail-safe manner. Nevertheless, this is not always possible since accidents are very time sensitive and sometimes there is no option and time to regain the control of the system to recover it.

Reliability, performability, and availability are about to offer a constant and correct service over a continuous and discontinuous period, respectively. This means that not only the batteries need to constantly work along with a journey but they also must be ready for usage when needed with a proper performance. The problem comes with time when batteries do not last very long or they self-discharge if the car has not been used in a while. Other hazards related to these attributes are about proving that the shared and received data are reliable and available. Although the system is constantly gathering, spreading and updating data, this one can be intentionally damaged without the system being able to detect this fact, and the same can happen with the precomputed maps: if they are not trustworthy and accessible, the risk of a fatality is imminent.

Security is another key attribute that will grow in importance as soon as the different levels of automation and connected cars become more widespread and affordable and gain strength within the population. Security, understood as a mixture of availability, integrity, and confidentiality, might be threatened in every system update. Every of the thousands of lines of code of the software that allow the connection of the car with everything in connected cars, and the partial or total driver abolition along the different automation levels, is vulnerable when a cyber-attack takes place.

Testability might be disturbed if after a minor crash, while the car is driving or parked, the car is not able to detect, check and inform about the car status. Also, it should be able to test if the components are appropriated for a new software update.

In case this measure of correctness can be done in an effective, easy and quick way, the system will have the benefit of a good maintainability if after detecting those anomalies, it can restore itself and continue providing a good service. This characteristic affects all components, from sensors and cameras right through batteries and software.

After having defined all the elements that make up the system framework, in the last step what still remains is grouping the different risky scenarios in order to encompass the greatest number of hazards possible in the same use case. For doing that, this thesis will rely on the elaboration of user stories as already said.

3.2 Creation of User Stories

Since in the state of the art there was no mention to user stories, this chapter is going to be divided into two. In the first one, it will be explained what a user story is as well as which properties they must have in order to be considered as good user stories. Also not only the main similarities and differences with use cases but also the approach or methodology to create them will be pointed out

In the second part, using that approach, the different user stories will be created and clustered in a logic way, in order to make sure that the different scenarios are covered and ready for being modelled in SysML.

3.2.1 User story approach

User stories, utilized mainly in the Agile methodologies for system development, are a very recurrent natural language description of one or diverse software systems. They describe functionality that will be valuable to a user or purchaser of a system or software and should be independent, negotiable, valuable to users or customers, estimable, small and testable. (Cohn, 2004, pp.4, 17),

Its key feature is the user since unlike use cases, user stories aim to capture the voice and perspective of the user of the application/system using informal language(Alexander et al. 2004, p.267). Therefore, the main difference between them is that user stories are descriptive and expressive of human desires and contain “what” and “why”, whereas use cases or scenarios cover the specifications of object interactions and contain “how”. According to Cohn (2004, p.253), the main differences between both are that user stories cover a smaller scope with fewer details than uses cases, and they are not projected to have any use after the iteration in which they are developed, whereas use cases are permanent through a project.

Despite all these differences and even it might seem that they are not compatible, different surveys such as the one presented in Madanayake et al. (2017, pp. 1-3) verifies the hypothesis that they both can be used together. It is so because they retain certain similarities: the role or user in a user story (which can be extended to other stakeholders) is similar to the actor of a use case model and the goal or desire in a user story is similar to a use case (Madanayake et al. 2017, p.2).

Thus, user stories or epics (its larger variant) will help to identify the actors and the scenarios of the use cases, by following several formats or templates suggested by different authors, such as the one proposed by Connextra (Cohn, 2004, p.81)

As a <role> I can <capability>, so that <receive benefit>

I as a <role> I want <function> so that <business value>

In order to follow a logic path for at least trying to cover the greater number of scenarios possible, and taking into account that user stories have to be small and independent among other characteristics, the different user stories will be clustered as follows:

- Firstly, according to the future trend, i.e., autonomous, connected and/or electrical car.
- Secondly under certain common processes or situations, in which different stakeholders can come into play

3.2.2 User story statement

Following the approach described above, the different user stories are in the following stated:

Autonomous vehicles

In fully automated vehicles, there are no drivers but passengers or users (HAV users). In lower levels, the driver and/or passengers will be named as AV users. If it is not further specified, it means that is for both types of users.

General

- *As a user, I want a trustable car so that I can feel safe and it is socially and legally accepted.*
- *As an HAV user, I want to know the code of conduct or behavior of my car so that I can be aware of the safety prioritization in normal operation and in case of an accident.*
- *As a user, I want that my data (and the one from the other users and infrastructure) is correctly processed so that my security and safety (and also the one from the others) are not jeopardized.*
- *As a user I want my data to be treated only for noble goals. So that traffic can be better controlled, car accidents can be prevented, accident causalities can be clarified, and emergency units can be alerted if necessary.*

Interruptions while driving

- *As an AV I want to be properly warned to take the control of the car so that I have a suitable margin of decision/ maneuver.*

- *As a user I want my car to know how to respond if the attack cannot be eliminated. So that, I can feel secure while it makes an eCall; halt the car in a safe mode; reset the system or tele-operate it.*
- *As a user, I want an effective IT protection system so that the attacks from intruders (hackers, vandals, malicious software…) can be detected and eliminated and if not, at least be informed.*
- *As a user I want the software of my car to update regularly so that I can take advantage of the latest information and features.*
- *As a user I want my car to check the suitability of my hardware when there is a new software update so that a failure or a crash due to unappropriated hardware can be avoided.*
- *As an AV user, I want a skilled human-machine interface that interacts with me on time so that misunderstandings and/or crashes are avoided.*
- *As a user I want my car to detect manufacturing or intended faults, errors or failures so that there is no false perception of reality, interpretation of signals, emergency instructions and non-verbal communication.*
- *As I user I want my car to recognize and follow the instructions given by permanent or temporal authorities so that it helps to facilitate the traffic flow and it is not bulled by whoever that makes gestures to the car.*
- *As a user I want my car to review itself before retaking the operation so that when faced with even the minimal impairment all the components perform correctly and there is no room for a car accident.*
- *As a user I want my car to be able to infringe the law temporarily when necessary so that it can avoid a peril.*

Critical situations while driving

- *As a user, I want a system that is well and ethically programmed so that it takes moral and legal action in unavoidable crash situations with more than one actor involved.*
- *As an HAV user I want to know who will take responsibility in case of accident, so that I am covered by the law, assurance company or car manufacturer.*
- *As a pedestrian, cyclist, passenger, user of another car, animal or other traffic actor, I want autonomous vehicles to be properly coded according to Ethics and Conduct Codes so that we feel safe.*
- *As a user, I want dependable ITS so that the car can predict, detect and respond to persons, traffic elements, and events and also rely on the precomputed maps.*
- *As a user, I will allow (just to the authorized entities) to gather the information of my vehicle, the journey detail, payment method and even video recording inside and outside the auto (if applicable) so that safety and security are given priority.*
- *As an intruder I want to affect or spread IT attacks so that data protection, privacy, integrity, and other security aspects are breached. Not only car accidents can remotely be caused, but also other safety violations such as terrorist attacks, murders, robberies…*
- *As I user I want my car to be able to adapt and recognize the traffic laws of every country so that I do not have to change settings when crossing a border.*

- *As a delinquent, I want to cause system malfunctions so that the car affected has a false perception and interpretation of the reality that ends up in an accident.*

Bad weather while driving

- *As the weather (condition) I can unintentionally create damage in the system components or infrastructure so the car has to cope with risky situations such as no visibility or false perception of reality.*
- *As a user I want my car to make a right decision in an extreme weather condition so that users' lives are not in any danger by halting the car, infringing temporarily the traffic law, claiming for teleoperation etc.*

Connected vehicles

Many of the user stories created for autonomous vehicles, especially the ones related to security, can also be applied to connected cars. Nonetheless, the main user story for users of that form of mobility is summed up as:

- *As a user, I want to trust the exchanged data between V2X (vehicles, infrastructure, pedestrian, and anything) so that ITS threats cannot put my life and the lives of other people in danger.*

Electric vehicles

The user stories of users of battery-powered cars are shown below, taking into account only the electrical part, independently if they are driven by a person or driverless cars.

General

- *As a user I want to feel safe when driving, charging the electric batteries or doing other maintenance actions so that any electrical, mechanical or chemical hazards can take place.*
- *As a workshop employee, user or external individual (pedestrian, assistant after a crash) I want to be well informed and the car to be equipped with the pertinent protective equipment so that electric hazards cannot take place when having direct or indirect contact with the car.*
- *As a workshop employee, I want to be well trained and equipped with the pertinent personal (and collective) protective equipment so that electric hazards have no room while performing any type of service.*

Charge of batteries

- *As a user, I want safe and lasting batteries so that I can drive safely without having to interrupt my journey to charge them so often.*
- *As a user I want the batteries of my car to be well protected, so that when hitting at high speeds with another vehicle or sharp-edged object the batteries do not explode causing the ignition of the car.*
- *As a user, I want to be informed about the status of the batteries; the presence of smoke; the performing of the electric protection measures; so that electric hazards due to over-charging, over-discharging, over temperature or intrusion of metallic dust*

cannot happen.

Driving

- *As the weather (condition) I can unintentionally cause damage to the batteries when heavy rains and flooding so electric hazards to users such as electrocution can take place.*
- *As a user I want my car to emit a right noise level between the acoustic spectrometer so that the other pedestrians, cyclists and traffic elements can notice the presence of my car.*

Shared vehicles

As mentioned before, although shared cars are considered as a new mobility form that is already emerging and will become more and more popular in the coming years, it presents innovation only in the management of the car but not in any mechatronic components. There will be autonomous, connected and electric cars that will be used in that car-sharing modality (or vice versa, shared cars that will be autonomous, connected or electric). Due to that, although they were covered in the state of the art, they are not going to be analyzed separately for the use cases. The consideration of security and safety in aspects like payment methods and video recording of the car were already done in the user stories for autonomous cars.

3.3 Use Case elaboration

In this section, different scenarios, challenges and user stories grouped into 4 different use cases are presented, following the approach presented in *2.6.1 Use Case Diagram* according to the template placed in *A7 Use Case Template.* For a better understanding, this use case technique consist of a textual part through a table or template form with the Use Case Identification and Definition, followed by its corresponding graphical part or diagram.

u.c 1.0: Cope with ethical, moral and legal problems and responsibilities in autonomous cars

Use Case Identification	
Use Case ID	1.0
Use Case Name	Cope with ethical, moral and legal problems and responsibilities in autonomous cars.
Use Case Definition	
Description	Until the reach of the mobility peak – full autonomy – the drivers of the vehicles are responsible for their actions since they are the ones that decide the behavior of the car, at least theoretically. That is why when self-driving cars will take our roads carrying all kinds of passengers (e.g. with disabilities) or even without them, is very important to have previously defined responsibilities in case of an accident (car manufacturer, insurance company, car owner). Moreover, driverless cars will be faced with critical situations where they will have to respond in the best way, which will be determined through prioritization rules when programming the code. The car, therefore, will have to discriminate between different types of elements (pedestrians, animals, motorbikes, other vehicles…) and also sort between actors of the same species, according to also to a different ordering scale (number of people damaged, protection of the weakest individuals, own passengers safeguarding…) This may lead to ethical and moral dilemmas. Moreover, legal issues may appear, since before the accident occurs the lines of code have to be written according to different moral rules beyond of car owner scope and accorded by policy makers through Ethics and Conduct Codes.
Actors	Primary Actors: Autonomous car user. Supporting Actors: All the different elements the autonomous car can crash into pedestrians, cyclists, motorcyclists, other vehicles, animals, urban infrastructure...

	Stakeholders and Interests: Policymakers, car makers, programmers, car insurance companies and other parties that play a role when defining responsibilities and ethical and legal behaviors of the car.
Preconditions	The full autonomous car (or an autonomous car in autopilot mode) is driving and a situation where it has to take a decision/prioritize is to be faced, either avoiding a crash or deciding into which element is “better” (more ethically correct, safer, less harmful, more legal…) to crash.
Postconditions	The priority objective towards a critical situation will be always avoiding the crash trying not to damage any secondary/ supporting actors. If the involvement of others is unavoidable, the final state will be crashing into the element with "less" priority.
Frequency of Use	Difficult to calculate, but every time a car is on the road, the possibility of an accident is always present, even if its likelihood is minimal in the extreme.
Scenario	1. The full-autonomous car is driving (with or without passengers). 2. Some unexpected actor interrupts its travel. 3. The car tries to avoid the unpredicted new actor (A) that has appeared in the scene. 4.a. If there is no option to change its route to avoid it, and whenever possible, the car will stop in a safe mode in order to avoid the crash. 4.b. If the crash into some element is unavoidable, the car will have to decide which element to crash into is safer and more ethical. 4.c. If the two new elements in the scene (A and B) belong to a different type (humans, animals, light vehicle, heavy vehicles, urban furniture), the car should avoid crashing into the weakest, without forgetting the safety of their own passengers. 4.d. If the two elements are of the same type, the car should try to save the greater number of lives possible, including itself. 5. The insurance company, owner of the car, car manufacturer or another party takes responsibility. 4.b.1 To avoid crashing with A, the crash with traffic element B is the only option possible.
Special Requirements	Responsibilities have to be defined before those scenarios take place.
Issues	Since infinite situations or scenarios can be given, it is technically

	impossible to contemplate all of them when the programmers code the lines of the autonomous cars. Prioritization rules are very questionable under certain circumstances and there will always exist a certain error percentage. For example, a person can be dressed up as an animal; difficulty to choose which life is more precious; the fact that not always is better to crash into urban furniture in order to save the life of an animal or a person if that supposes a vital risk for the lives' passengers, etc. Apart from that, there is a lot of bias around how ethical autonomous cars are. An incorrect decision made might lead to social and legal unacceptance, which is the reason why it needs to be treated so carefully.

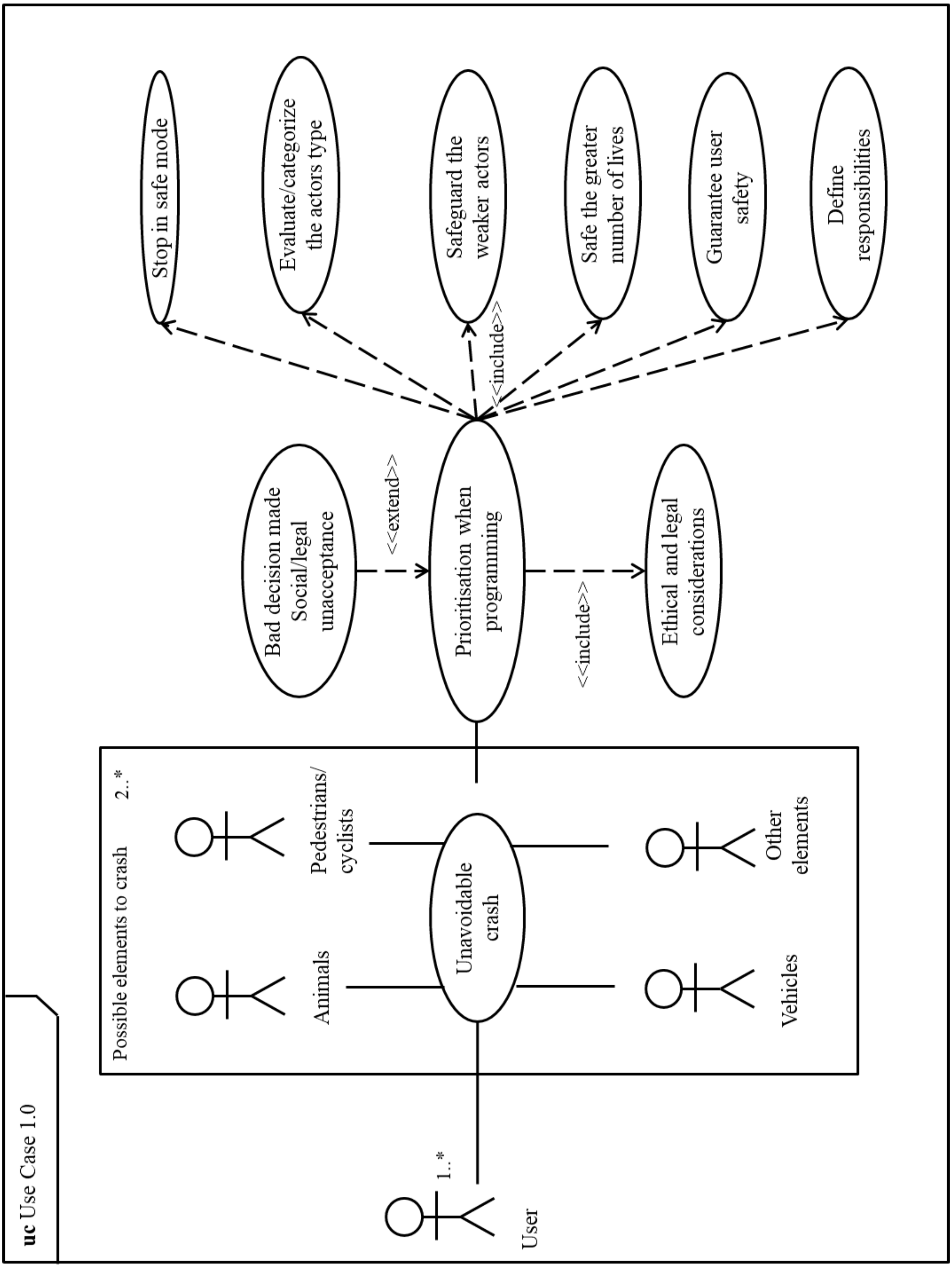

uc Use Case 1.0
User
1..*
Possible elements to crash
2..*
Animals
Pedestrians/ cyclists
Unavoidable crash
Vehicles
Other elements
Prioritisation when programming
Bad decision made Social/legal unacceptance
<<extend>>
<<include>>
Ethical and legal considerations
<<include>>
Stop in safe mode
Evaluate/categorize the actors type
Safeguard the weaker actors
Safe the greater number of lives
Guarantee user safety
Define responsibilities

Figure 3-6: u.c 1.0: Cope with ethical, moral and legal problems and responsibilities in autonomous cars (own elaboration)

u.c 2.0: Preserve security and privacy of autonomous and connected cars

Use Case Identification	
Use Case ID	2.0
Use Case Name	Preserve security and privacy of autonomous and connected cars.
Use Case Definition	
Description	In Intelligent Transport Systems (ITS), the amount of data recorded and shared is vast. This traffic of information released and received from different elements in the scene (own car system, other vehicles, infrastructure, car maker, software updates…) is very helpful for anticipating others' actions. Thus, car accidents can be prevented; accident causalities and culprits can be clarified; emergency units can be alerted in case of an accident; the maintenance and logistics can be facilitated thanks to a better traffic control. At the same time, this data must ensure privacy, confidentiality, authentication, integrity, anonymity, robustness, availability, choice, non-repudiation, traceability, revocation, robustness against attacks, among others. Although the data-managing entities assure to guarantee these properties to their users, the virtual disk will always run the risk of being attacked by hackers or other intruders that are always defying all the security measures. This violation of security, manifested in different forms, (or better said, attacks) such as denial of service, malware, timing, cryptographic replication, black hole, falsified entities…can be used to sell data to other companies and what is worse, for taking control of the car in terrorist attacks, murders or robberies. This supposes a severe handicap not only for the user that might be affected but also for the other related parties that must preserve the security and therefore being always overcoming the continuous and improved attacks of all manners of criminals. Another issue that may affect the security is the one related to the infrastructure adequacy: connected cars trust on the information received from other cars and urban elements (which may not exist, work properly or even been manipulated) and autonomous cars rely on precomputed maps and intelligent transport systems that permit the detection and response of different objects, person and event (and even the prevention) as well as recognizing traffic barrels, lines, signals and lights. Again, the proper functioning of them can be interfered or damaged by different causes, attempting the (cyber) security and safety of passengers and other users.

Actors	Primary Actors: Users of autonomous and connected cars. Infrastructure (precomputed maps, traffic lights and other elements that send data). Intruders (hackers, vandals, malicious software, hostile organizations…), delinquents, criminals, and terrorists that interfere in the users' security. Other stakeholders like: Software programmers, policy, maps and infrastructure developers.
Preconditions	There are no preconditions. It is not necessary that the car is turned on and driving for being hacked. The different attacks can take place at any moment.
Postconditions	The success post-condition would be that the car itself reviews, analyses and updates constantly the system in order to detect, inform the user and eliminate possible attacks. The failure post-condition would be not being able to detect and/or eliminate the cyber attack and being stolen, blackmailed, or what is worse, murdered.
Frequency of Use	If there is a good antivirus, security system or attack prevention, the failure post-condition should occur rarely.
Scenario	1. The autonomous or connected car is turned on or off, and it is continuously doing updates and reviewing the system and its security. 2. The system detects some malicious attack when the data processing 3. If the car can eliminate or reject the attack, it continues its normal journey. 4. If the car is not able to distinguish which type of attack it is, it should inform the user, car manufacturer service hotline and/or policy. 5. After a first and fast examination, there should exist an emergency protocol to take the corresponding measures, if possible: reset the system, stop the car in a safe mode, making an eCall, taking remote control of the car, send police units to the car location, reset the system… 6. If after trying all these measures is too late or impossible to regain the control of the car, this can end up in not only security violations that affect privacy, confidentiality and other types of data protection but also safety ones such as car accidents, robbery, blackmailing etc. 1.a In case the car would stop sending and receiving data, it would be likely that the car has been taken, in that case, go to 5.

	2.a This data can come from ant ITS (autonomous vehicles, connected cars, precomputed maps…) 3.a The user should be able to choose if he wants to be warned every time there is a threat (even if the ITS is able to destroyed) or just in severe cases where the system has any available measure to face the attack. 1. Other parties such as connected infrastructure, other connected vehicles, precomputed maps etc. are hijacked. 2. If possible, those systems should inform the surrounding connected elements. 3. If the attack is more severe and malicious, there is no option to distinguish that the information received has been manipulated and it is therefore not trustable.
Special Requirements	The system should be constantly updating and reviewing possible anomalies. Also, the car manufacturer should offer a 24h emergency hotline to guarantee security to their users. The precomputed maps should also continuously being updated.
Issues	Since hackers and their cyber attacks are constantly reinventing themselves and although the protection systems have numerous updates and improvements (they recognize and adopt them at the first attempt), as a matter of principle it is impossible to guarantee users security and safety to a hundred percent. Another important issue related with the anticipation, detection, and response of certain situations related with pedestrians, surrounding elements or events, is the excessive conservative way in which autonomous cars will drive (they will be more likely to get hit than to be the hitters). Although it can seem that it is a positive feature, this ultra-cautious drive style can produce serious traffic problems.

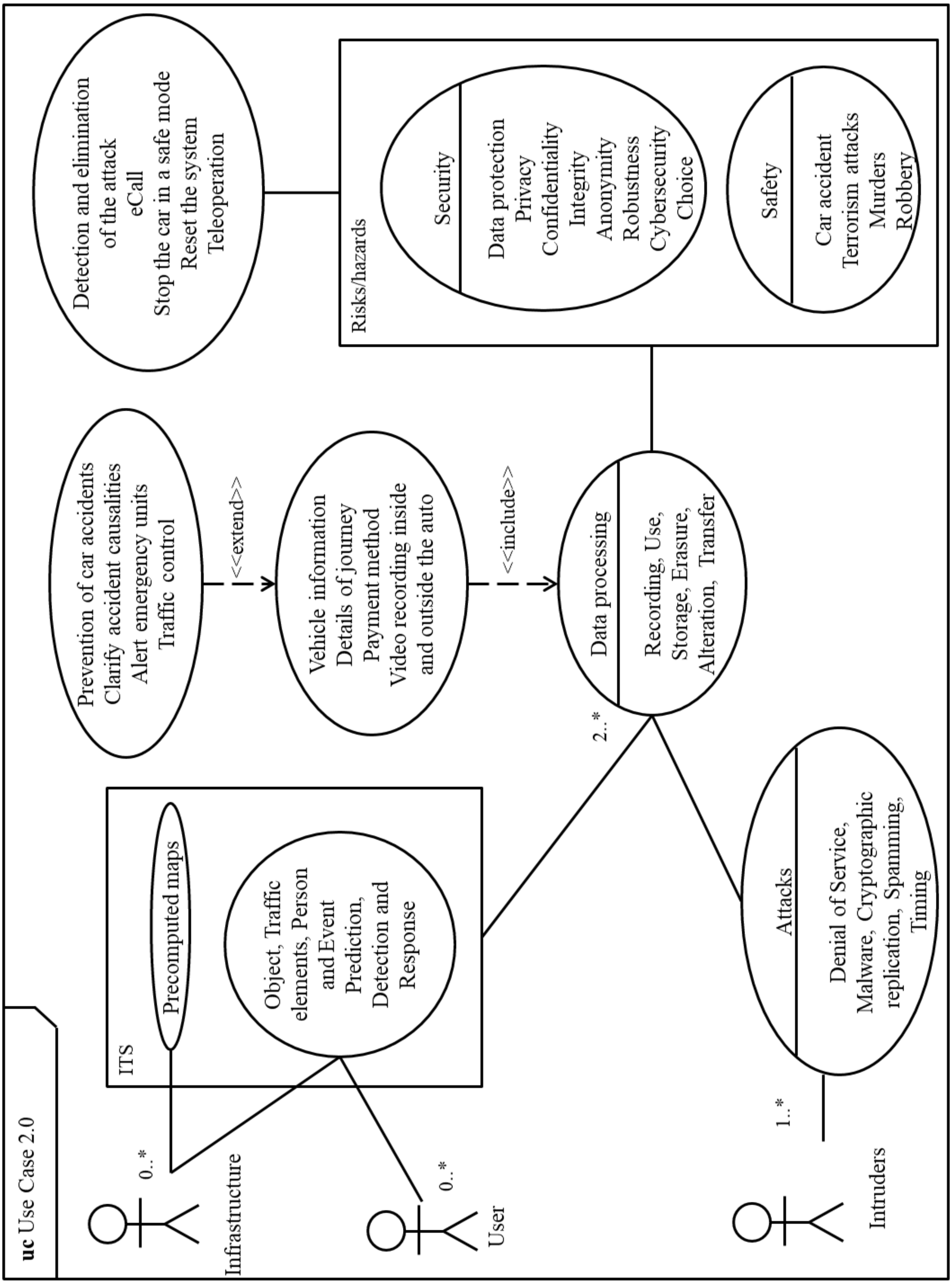


Figure 3-7: u.c 2.0: Preserve security and privacy of autonomous and connected cars (own elaboration)

u.c 3.0: Deal with hazardous driving conditions

Use Case Identification	
Use Case ID	3.0
Use Case Name	Deal with hazardous driving conditions.
Use Case Definition	
Description	In the not too distant future, the emerging mobility trends such as connectivity or full autonomy are mean to reduce or even eliminate car accidents. However, since there is no perfect machine, there are circumstances beyond our control or better said, beyond the developers, engineers and car manufacturers' one. Different driving conditions originated by different factors can become hazardous and end up in an accident. Examples of these are not ensuring the proper hardware after a software update or a (slight or severe) accident. Also, other elements of the car may suffer damage or loss of their properties or functionalities due to the human or weather activity: delinquents and bad weather conditions can cover or misalign cameras and sensors, causing either lack of visibility or a false perception of the reality. Moreover, and although with a smaller probability, manufacturing defects in mechatronic systems could also exist and notice them when is already too late. Apart of these dangerous situations related to the car itself, sometimes the vehicle is the one that must face and avoid the risky situations caused by others. In cars driven by humans, it is the driver the one responsible to manage the situation at his best and if necessary, infringe the traffic law temporarily. And here comes the problem again, when developers program autonomous cars to follow the laws, but there are infinite case studies where skipping the law it is the safest option for all the parties.
Actors	Primary Actors: Users of autonomous cars, weather, delinquents, and others Stakeholders and Interests: Software developers, car manufacturers, tele-operators.
Preconditions	The car must be running to experiment the hazardous driving situations.
Postconditions	The success post-condition would be that the car is able to successfully

	overcome the dangerous situations described. The failure post-condition would be not being able to cope with the situation and end up in an accident.
Frequency of Use	Dependent on the region: its weather, its crime rate…among others.
Scenario	1. The autonomous car is operating. 2. The system detects that a new software update is available. 3. The update is carried out but the current hardware does not meet the requirements for the new functionalities offered with the new update. 3.a The car should be able to detect itself which updates can afford with the hardware that the model of the car includes. 1. The autonomous car (whatever its level of automation) is operating. 2. The human-machine interface requires the driver to take the control of the car. 3. The driver ignores intentionally or unintentionally the vibratory and acoustic signals the car emit requiring his performance. 4. There is a misunderstanding between driver and car that can end in an accident. 1. The autonomous car is running. 2. Exceptionally adverse weather conditions come onto the scene (severe snow storm, heavy flood, hurricane, tornado, severe dust storm...) 3. Camera, sensors and other systems result affected in different ways: misaligned, covered, blocked, unable to distinguish, generate and compute the surroundings… 4. The car stops completely as soon as possible or whenever it is safe. 5. The vehicle picks up the drive when the peril is gone and thus it is safe to drive again. The car should be able to distinguish when it is secure enough to return to the journey and when not. 5.a If the car gets stuck or stumped, it might use a remote human operator to guide AV to a safe position (teleoperations) 1. The car is parked and it is manipulated/damaged by a delinquent. 2. The car turns on and should be able to detect if all the functions of its systems work properly and inform the user, in order to recover it.

	1.aThis intended system fault, error or failure can also be a manufacturing defect 2.a The car should also perform this step after a system update, a severe or slight accident, and moreover whenever the user desires (carrying out this revision every time the car is turned on could take too long and it would not be practical and efficient). 2.bThe car is not able to detect the failure and a collision occurs.
Special Requirements	Constant system functionality revision.
Issues	Each case is very specific, and again, it is very difficult for the developers to group, generalize and put them under the same behaviour or lines of code. Every situation has its own action protocoll.

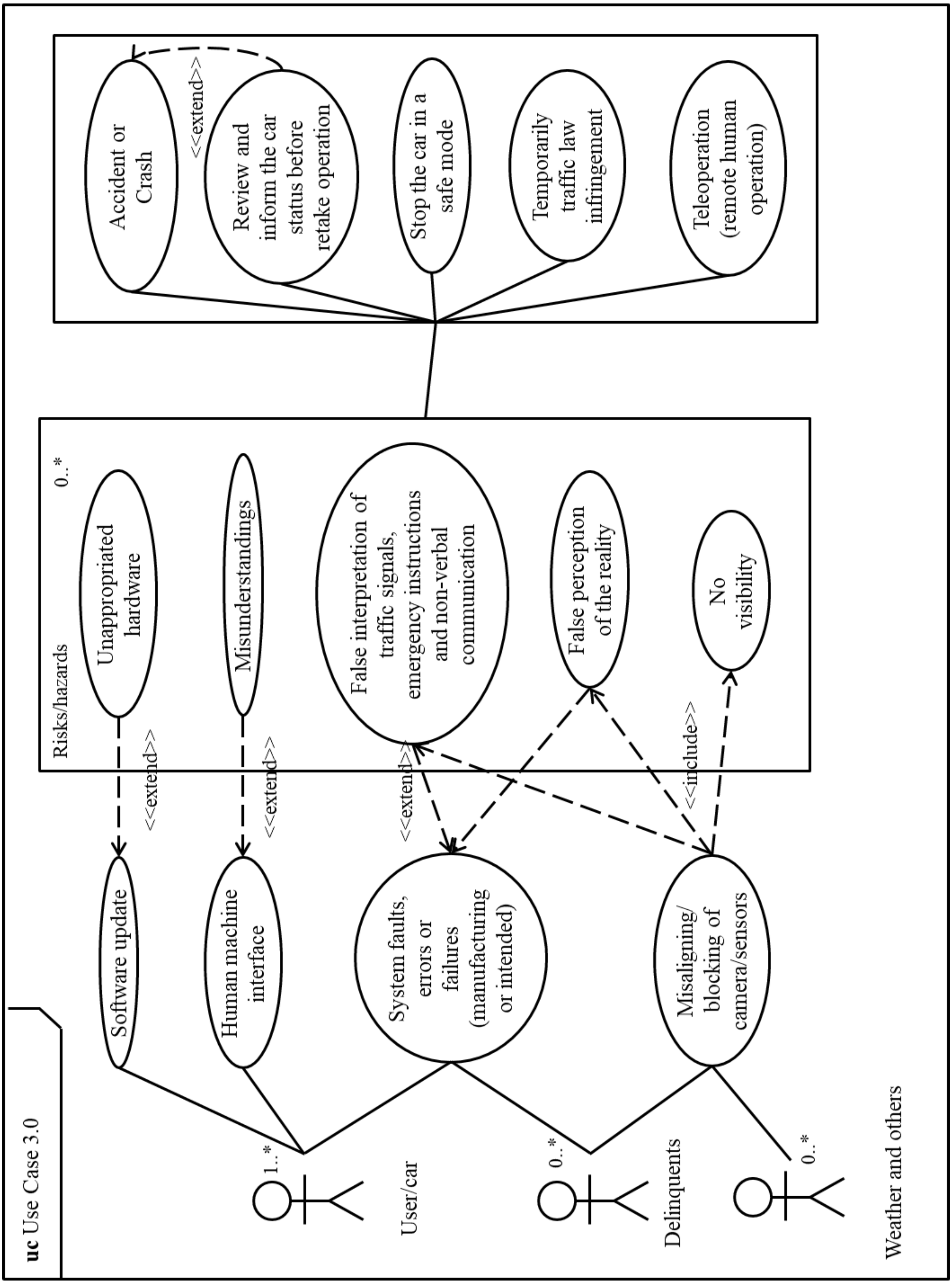

uc Use Case 3.0
User/car
1..*
Delinquents
0..*
Weather and others
0..*
Software update
Human machine interface
System faults, errors or failures (manufacturing or intended)
Misaligning/ blocking of camera/sensors
Risks/hazards
0..*
Unappropriated hardware
Misunderstandings
False interpretation of traffic signals, emergency instructions and non-verbal communication
False perception of the reality
No visibility
<<extend>>
<<extend>>
<<extend>>
<<include>>
Accident or Crash
Review and inform the car status before retake operation
<<extend>>
Stop the car in a safe mode
Temporarily traffic law infringement
Teleoperation (remote human operation)

Figure 3-8: u.c 3.0: Deal with hazardous driving conditions (own elaboration).

u.c 4.0: Handle electricity concerns in electric cars

Use Case Identification	
Use Case ID	4.0
Use Case Name	Handle electricity concerns in electric cars.
Use Case Definition	
Description	It is true that in conventional cars since they use the flammable substance (petrol or diesel) for the combustion and the working of the engine, the peril of an uncontrolled ignition in case of accident does exist. However, it is barely probable. This statement cannot be said as certainly for electric cars. Instead of fuel they use the power of electric energy stored in batteries. Moreover, these need to have a considerable size and voltage in order to guarantee reliability during a certain period of time. Therefore, not only during the operation of the car but also during the maintenance and the charge of batteries, potential dangers/accidents of various kinds (electrical, mechanical, chemical…) can be triggered. They can occur due to different reasons ranging from bad weather conditions such as heavy storms and floods to hitting with objects occasioning the damage of the batteries, short circuits, electric shocks, direct contact, thermal instability and ignition or explosion in the worst cases.
Actors	Primary Actors: Users of electric cars, weather, (sharpened and pointed) objects, other vehicles... Stakeholders and Interests: Maintenance personnel at workshops, pedestrians.
Preconditions	Depending on the case, the preconditions needed are bad weather with flooding, car on battery charging modus, a car driving at high speeds…
Postconditions	The success post-condition would be that the protection measures for direct and indirect contact are effective and efficient, the car revises regularly the state of batteries and does not allow the driver to make use of the car if they are not in a good state. The failure post-condition would be a direct contact and burns, short circuits without protection, batteries damaged when crashing into a sharpened or pointed object or another car at high speeds, ignition of electric system and explosion of the car

Frequency of Use	More or less frequent depending on the scenario.
Scenario	1. The electric car user and/or workshop employees, either because of ignorance, recklessness or lack of information and preparation, have direct contact with high-voltage power during maintenance of the car or charge of batteries. 2. If the correspondent protection measures (personal and collective protection equipment) are available and work properly, major consequences should not arise 3. If the negligence is too serious or the protection methods are not enough or they are not in suitable conditions, fatal consequences may occur. 1. The electric car is running at high speed. 2. The car crashes into another vehicle or an object especially heavy, sharpened or pointed. 3. The battery is seriously damaged. 4. Electrical shock, ignition, the explosion may happen. 1. The electric car is operating. 1.b Especially at low speeds, the emission of noise, is very low. 2. Pedestrians, cyclists, and other traffic elements might not notice the presence of the car. 3. Collision risk. 1. Risks can originate from accidents, but accidents can originate other risks 1. Actions such as over-charging. Over-discharging, the intrusion of metallic dust. 2. Thermal instability or loss of motor torque.
Special Requirements	The maintenance personnel, workshop employees and last but not least, the owners of electric cars should be well informed and trained in the safe maintenance actions

Issues	Batteries are the most critical and challenging element in electric cars and therefore the ones that need special care, revision, and maintenance.

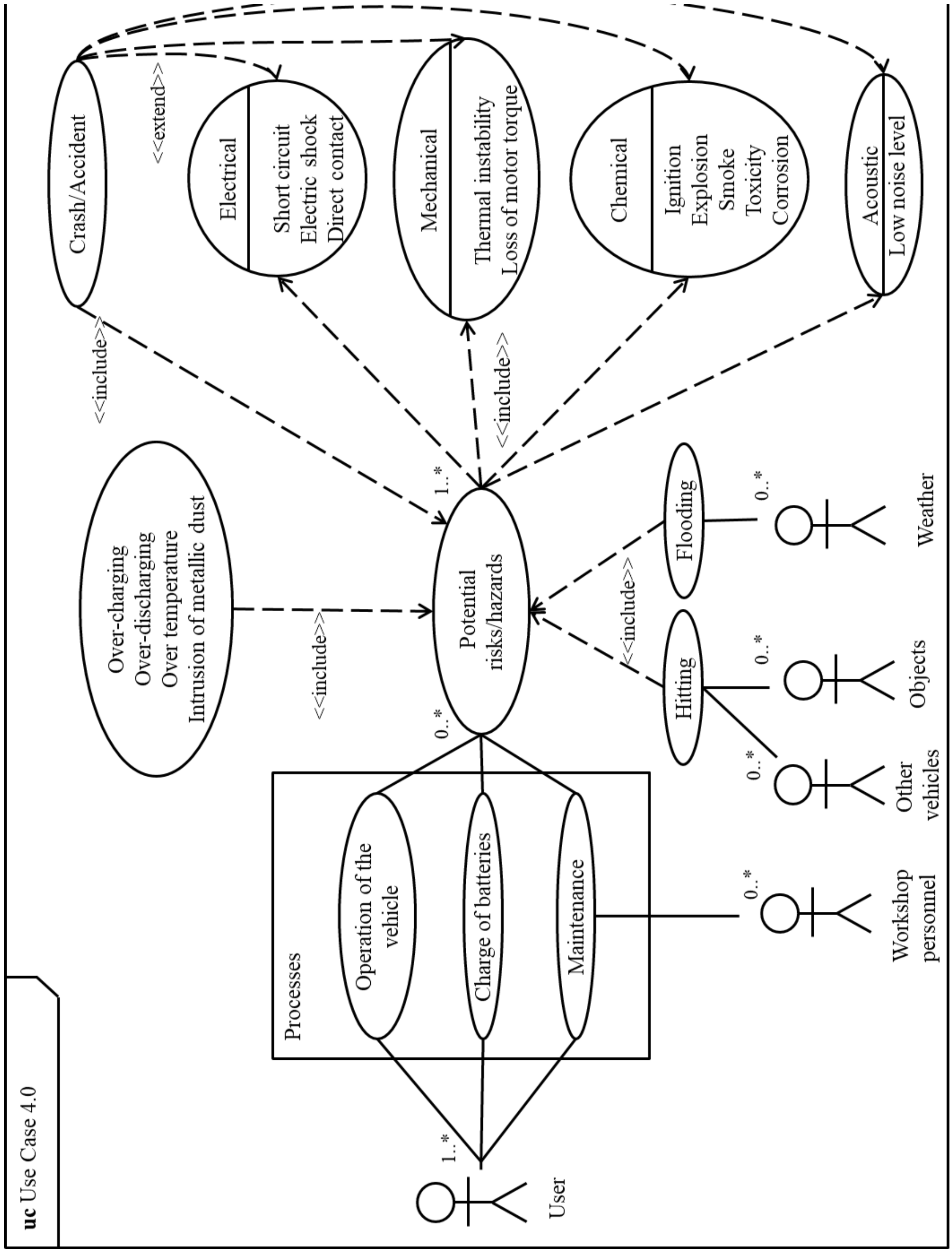


Figure 3-9: u.c 4.0: Handle electricity concerns in electric cars (own elaboration).

4 Summary, conclusions, limitations and future work

Summary

This work is framed under the product development discipline, in particular in the development of mechatronic systems in the automotive industry.

As it is described in the first chapter, the large number of vehicle crashes, injuries, and fatalities on the roads motivates automotive engineers to re-consider new forms of mobility with new modern mechatronic functionalities with the expectation of increasing safety and reliability. Since the major cause of car accidents is the human factor, these future trends will culminate in what it is known as full-autonomous cars, but not without first (or at the same time) going through other transport modalities such as shared, electric and/or connected cars. From the point of view of the framework of this thesis, product development process, the truly problem for engineers and developers will be having to cope with these new challenges and the increase in complexity. This fact motivates the main goal of this master thesis: helping engineers in the development process of new mechatronic products by offering them a new approach based on use case technique. Through a suitable modelling language, this approach will help to derivate future risks and hazardous situations as well as to argument the fulfilment of safety requirements.

In the second chapter, an extended literature review will allow knowing the state of the art when it comes to dependability and its different characteristics; quality methods necessary for performing safety analysis and assessing functional safety, which, in turn, will be used in some stages of procedural models for system development; safety-related standards as well as different system modelling language such as Sys ML and particularly use cases diagrams.

In the third chapter or practical part, an approach for supporting automotive developers and engineers to ensure a safe and secure development process will be presented. It will be based upon the challenges and threats of those future trends. Through a system definition, the statement of user stories and the descriptive and graphical conception of safety-related use cases, the idea of safety case or how to argument that a mechatronic product has satisfied its safety requirements will be materialized, helping thus to define the item.

To finish with this work, in the fourth chapter, the conclusions to which the author has come will be given by discussing the approach and the results. Besides that reflexion, some limitations of the approach will be pointed out, as well as an outlook for future work to carry out.

Keywords: safety, safety case, use case, user story, SysML, ISO 26262, concept phase, product development, dependability, autonomous cars, mechatronic products, security.

Conclusions

The conclusions of this work are nothing else than the answer to the question *have we reached the goals proposed at the beginning of this master thesis?*

This question is going to be answered through the reflexion or discussion of the results, which will be preceded by the discussion of the approach suggested by the author.

Discussion of the approach

Due to the lack of previous knowledge, the literature review carried out along the first and especially second chapter, allowed the author to have an overview of the existing situation or state of the art with respect to product development in the automotive industry (based since a few years on the standard ISO 26262). Although future is uncertain, it was possible to identify the threats that the upcoming mobility trends will bring with, as well as a suitable modelling language that could consider those challenges. As explained at the beginning of chapter 3, this approach is to be used in the concept phase, in order to help with the item definition and the setting of safety requirements. The proposed methodology consists of a system definition where all the factors and their interactions can be overviewed followed by the elaboration of user stories. Since the statement of these user stories is short, independent, easy to understand and can be extended to other stakeholders apart from the final users of autos, this fact made a lot easier to carry out the elaboration of use cases, culmination of the approach. The combination and supplementation between the analysis (through a template) and the modelling (through SysML) allowed the author to cluster and cover different type of scenarios with different actors and type of risks, thus making the approach satisfactory.

As for the research methodology, it is true that there was large amount of literature, i.e. journals, books, dissertations etc. very helpful for the state of the art, but since this work is future-oriented, the author found herself with not too many scientific forward-looking literature.

Discussion of the results

Summarizing chapter *1.3Aims*, the foreseen goals of this master thesis were:

- Identify the challenges of the future related to reliability and safety of the technical systems.
- Identify the methods or approaches in use today to meet the challenges of tomorrow.
- Identify the gap that can be closed by the current methods and give recommendations for new approaches.

The first aim was reached in the chapter *2.2Future trends and challenges*, where not only the future mobility trends (commoditization, electrification, communication and automation) could be identified, but also the threats, challenges or limitations they will carry with. Since these challenges will have higher complexity and scope, those reliability and safety will be encompassed by another broader term that includes other relevant characteristics: dependability.

Other boundaries that these challenges will find in the future, which are not directly related with the product development process though, are explained in the annexe *A9 Boundaries for the future.*

The second aim has been covered through different subchapters under *2.State of the art*, where different approaches used in the product development process suggested by ISO 26262 were presented. Examples of these methods that therefore justify the meeting of the objective are: quality methods for safety analysis that help to identify causes or effects of failures like FMEA or FTA and help to ensure a satisfactory level of safety; approaches for functional safety assessment, such as HARA and ASIL, which help to determine the safety goals in order to avoid risks; different procedural models for system development that support the task's organization of the lifecycle of the product to develop, such as V-model or Waterfall-model; and different approaches or languages to model systems making easier the understanding of their structure, elements and behaviour, such as UML or SysML.

The third aim has been accomplished through the approach presented. It combines an existing modelling language for representing safety-related use cases, with the description of user stories and a system definition based on different parameters. This idea of safety case based on dependability, user stories and SysML is expected to optimize and make the future development of a mechatronic product a process less complex and safer.

Limitations

Although the author of this thesis has followed a systematic approach during the research and development of the thesis this study has some limitations due to different reasons.

One of these is the time window and the previous experience of the author on the topic

Another limitation is, as it has been briefly mentioned in the discussion of the approach, the fact that there are not too many current scientific papers, journals, books or magazines focused on the future of mobility and its evolution with respect to the development process.

The lack of availability and access to different standards when needed, even when being able to consult handbooks or internet, resulted to be sometimes a drawback.

The uncertainty of the future and the suppositions made is another factor that plays against the approach presented. Maybe other mobility forms come into play, or maybe developers never reach the demanding safety level for autonomous, connected or electric cars, and they are not able to take the roads.

Among the uncertainty limitations, there is the no possibility to test the approach presented. The author found a suitable modelling language for for specifying, analyzing, designing, and verifying complex systems in the nearly future, but we cannot be certain today at 100% that the method presented will indeed help engineers and less still, ensure that the number of accidents will be reduced with the improved development process.

The amount of different possible scenarios hampered the elaboration of both user stories and use cases. The coexistence and interaction of so many parameters, elements or stakeholders make this eagerness to cover all the likely hazardous situations an arduous task.

Another limitation was the no familiarity with any system modelling languages, in this case with SysML. Even though the follow of different guidelines and the literature review, this lack of acquaintance did not allow the author to take full advantage of this modelling language and maximize its benefit.

Future work

As to the outlook for the future and the work that should be done in further steps, in this section a couple of recommendations will be given.

Firstly it would be recommendable to say the least, interviewing practitioners, developers, engineers and other experts in the automotive industry in order to get a feedback of the raised approach. Their opinion would help to check the suitability and efficiency of the work performed and also to carry out modifications and improvements in the suggested methodology. Moreover, they may be able to contribute fresh ideas about other challenges or topics that are not in the literature and might enrich this work.

Secondly, if possible, it would be advisable to test the approach in a little application example or in a pilot project. Thus, although a risk is inherent in the nature of these experimental projects, the author would be able to evaluate the appropriateness of the approach and the feasibility, and adverse events among others, in order to improve it before it might be adopted in full-scale projects.

.

Acknowledgements

I would like firstly to thanks my thesis direct supervisor Hugo d'Albert from the Product Development Chair at the Mechanical Engineering School at Technische Universitát München. He consistently allowed this master thesis to be my own work but steered me in the right direction whenever he considered I needed it or whenever I asked him for.

I also want to express my very deep gratitude to my parents for giving me the opportunity to be whom and where I am. Thanks to my whole family, friends, and colleges for providing me with your unfailing support and incessant encouragement not only during these last six months while researching and writing this thesis, but also during my whole studies and since I have use of reason.

Last but not least, I would like to say big thanks to Julian for his unconditional support, patience, encouragement, and love day after day.

This accomplishment would not have been possible without all of you and therefore this work is also yours. Thank you

Belinda

5 Literature

Abdulkhaleq, A., Wagner, S., Lammering, D., Boehmert, H., & Blueher, P. (2017). Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles. *arXiv preprint arXiv:1703.03657*. 1-7.

Affanni, A., Bellini, A., Franceschini, G., Guglielmi, P., & Tassoni, C. (2005). Battery Choice and Management for New-Generation Electric Vehicles. *IEEE Transactions on Industrial Electronics*,52(5), 1343-1344. doi:10.1109/tie.2005.855664

Alam, M. (2017, December 21). V2X Solutions for Autonomous Vehicle: 5G or IEEE 802.11p? [Web log post]. Retrieved from https://movimentogroup.com/blog/v2x-solutions-autonomous-vehicle-5g-ieee-802-11p/

Alexander, I. F., & Maiden, N. (Eds.). (2005). *Scenarios, Â Stories, Use Cases: Through the Systems Development Life-Cycle*. John Wiley & Sons. 267

Alves, M. (2016, December 12). Automotive Systems course (Module 10) - Active and Passive Safety Systems. Retrieved January 29, 2018, from https://www.slideshare.net/MrioAlves18/10-safety-systems-in-cars

Anderson, J.M., Kalr, C. N. (2016). Autonomous Vehicle Technology. A Guide for Policymakers. RAND Corporation

Arya, A. (2017, June 05). World's leading OEMs pick Tata Elxsi's 'Autonomai' driverless car platform. Retrieved from http://www.india.com/auto/car-news/worlds-leading-oems-pick-tata-elxsis-autonomai-driverless-car-platform-30516/

Avizienis, A., Laprie, J., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing,1*(1), 1-36. doi:10.1109/tdsc.2004.2

Balzert, H. (2010). *Lehrbuch der softwaretechnik: Basiskonzepte und requirements engineering*. Springer-Verlag.

Barth, M., & Shaheen, S. (2002). Shared-Use Vehicle Systems: Framework for Classifying Carsharing, Station Cars, and Combined Approaches. *Transportation Research Record: Journal of the Transportation Research Board,1791*, 105-108. doi:10.3141/1791-16

Baumgart, S. (2016). *Incorporating Functional Safety in Model-Based Development of Product Lines* (Mälardalen University Sweden. School of Innovation, Design, and Engineering, 2016) (p. i). Västeras, Sweden: Arkitektkopia.

Benz, S. (2004). Dissertation Eine Entwicklungsmethodik für sicherheitsrelevante Elektroniksysteme im Automobil von Stefan Benz (Doctoral dissertation, Universität

Karlsruhe (TH), 3-5

Bernijazov, R. (2015). Systems and software requirements engineering for cyber-physical systems. *Bachelor's thesis, Paderborn University*. (8)

Birch, J., Rivett, R., Habli, I., Bradshaw, B., Botham, J., Higham, D., Palin, R. (2013). Safety Cases and Their Role in ISO 26262 Functional Safety Assessment. *Lecture Notes in Computer Science Computer Safety, Reliability, and Security*, 154-165. doi:10.1007/978-3-642-40793-2_15

Blessing, L. T., & Chakrabarti, A. (2009). *Drm, a design research methodology*. Heidelberg: Springer,10-16,29-39, 43,75,141,181

Bońkowski, T., Hyncik, L., & Šoltés, L. (2017). *MOTORIST D3.2: Accident Reconstruction* (Rep.). doi:10.13140/RG.2.2.32489.70247

Boyer, B. (2017). *Taming the Autonomous Vehicle: A Primer for Cities*. (Publication) (pp.22-23). Bloomberg-Aspen Initiative on Cities and Autonomous Vehicles. Retrieved https://www.bbhub.io/dotorg/sites/2/2017/05/TamingtheAutonomousVehicleSpreadsPDFreleaseMay3rev2.pdf

British Standard (2002). *Hazard and operability studies (HAZOP studies)- Application Guide* (IEC61882:2002) Brooks, R. (2017, July 27). The Big Problem With Self-Driving Cars Is People. Retrieved April 16, 2018, from https://spectrum.ieee.org/transportation/self-driving/the-big-problem-with-selfdriving-cars-is-people

Cachin, C., Camenisch, J., Dacier, M., Deswarte, Y., Dobson, J., Horne, D.,... & McCutcheon, T. (2000). *Malicious-and Accidental-Fault Tolerance in Internet Applications: reference model and use cases* (No. 00280, p. 113). LAAS report.

Campbell, T. (2015, July 31). Make your vehicles safer with active and passive technology systems. Retrieved January 29, 2018, from https://www.commercialfleet.org/fleet-management/safety/make-your-vehicles-safer-with-active-and-passive-technology-systems

CARE (2017). Traffic Safety Basic Facts 2017-Main figures. *Statistics – accidents data - Mobility and transport - European Commission*. Retrieved February 17, 2018, from https://ec.europa.eu/transport/road_safety/sites/roadsafety/files/pdf/statistics/dacota/bfs2017_main_figures.pdf

CARE (2018). Road fatalities in the EU since 2001. *Statistics – accidents data - Mobility and transport. European Commission*. Retrieved from https://ec.europa.eu/transport/road_safety/specialist/statistics_en

Casner, D., Houssin, R., Renaud, J., & Knittel, D. (2017). An Optimization-Based

Embodiment Design Approach for Mechatronic Product Development. *The Open Automation and Control Systems Journal*, *9*(1).4

Chase, R. (2012, June 22). How Robin Chase Reinvented the Transportation Industry [Interview]. *Forbes*.

Cherfi, A. (2015). *Toward an Efficient Generation of ISO 26262 Automotive Safety Analyses* (Doctoral dissertation, Ecole Doctorale Polytechnique). (19)

Clemens, P.L, (1993). *Fault Tree Analysis*. Sverdrup Technology.

Cockburn, A. (2012). *Writing effective use cases*. Boston: Addison-Wesley.

Cohen, B., & Kietzmann, J. (2014). Ride On! Mobility Business Models for the Sharing Economy. *Organization & Environment*, 27(3), 283-288. doi:10.1177/1086026614546199

Cohn, M. (2004). *User stories applied: For agile software development*. Addison-Wesley Professional. 4, 17, 81, 253

Coppola, R., & Morisio, M. (2016). Connected Car: Technologies, Issues, Future Trends. *ACM Computing Surveys*, 49(3), 21-30. doi:10.1145/2971482

Dardar, R. (2013). *Building a Safety Case in Compliance with ISO 26262 for Fuel Level Estimation and Display System* (Unpublished master's thesis). School of Innovation, Design and Engineering Mälardalen University Västeras, Sweden.

De Francisci, S. (2016, April 6). Use Case Template. Retrieved May 5, 2018, from https://webgate.ec.europa.eu/fpfis/mwikis/essnetbigdata/images/1/17/WP2_Use_Case_Template_WP2.xlsx

Dixit, V., & Rashidi, T. H. (2014). Modelling crash propensity of carshare members. *Accident Analysis & Prevention*,70, 140-147. doi:10.1016/j.aap.2014.03.005

Dubrova, E. (2013). Chapter 2: Fundamentals of Dependability. In *Fault-Tolerant Design*. New York, NY: Springer. 5-17. doi:10.1007/978-1-4614-2113-9_2,

European Telecommunications Standards Institute (2017) Intelligent Transport Systems (ITS); *Security; Security header and certificate formats* (ETSI TS 103 097) Retrieved from http://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf

Federal Highway Administration (FHWA). (2005). *Clarus Concept of Operations* (Publication No. FHWA-JPO-05-072).

Friedenthal, S., Moore, A., & Steiner, R. (2011). *Practical Guide to SysML*. Morgan Kaufmann. 29, 30, 88, 303-310

Funk, J., (2016, April 13). Autonomous Vehicles: Technologies, Economics, and Opportunities. Retrieved January 21, 2018, from https://www.slideshare.net/Funk98/autonomous-vehicles-60845449

Gagniuc, P. A. (2017). *Markov chains: from theory to implementation and experimentation.* Hoboken, NJ: John Wiley & Sons, Inc. 16-17.

Gausemeier, J., & Moehringer, S. (2002). VDI 2206- A New Guideline for the Design of Mechatronic Systems. *IFAC Proceedings Volumes,*35(2), 787. doi:10.1016/s1474-6670(17)34035-1

Gerla, M., Lee, E., Pau, G., & Lee, U. (2014). Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. *2014 IEEE World Forum on Internet of Things (WF-IoT),*241-246. doi:10.1109/wf-iot.2014.6803166

Ghahrai, A. (2017, July 2). Incremental Model. What is the Incremental Model. Retrieved May 20, 2018, from https://www.testingexcellence.com/incremental-model/

Goldberg, B. E., Everhart, K., Stevens, R., Babbitt, N., & Clemens, P. (1994). *System engineering "toolbox" for design-oriented engineers*. MSFC, Ala.: National Technical Information Service, distributor. 3(3, 4), 3(30-37), 3(5156)

Goodman, P. (2016, November 22). Advantages and Disadvantages of Driverless Cars [Web log post]. Retrieved April 16, 2018, from https://axleaddict.com/safety/Advantages-and-Disadvantages-of-Driverless-Cars

Gough, W.S., Riley, J., & Koren, James M. (1990). *A New Approach to the Analysis of Reliability Block Diagrams*. Proceedings from Annual Reliability and Maintainability Symposium, SAIC, Los Altos, NM.

Grave, R. (2015). Autonomous Driving – From Fail-Safe to Fail-Operational Systems. In (pp. 16-18). Much: Elektrobit.

Hamida, E., Noura, H., & Znaidi, W. (2015). Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures. *Electronics,*4(4), 380-415. doi:10.3390/electronics4030380

Harris, M. (2014, July 16). FBI warns driverless cars could be used as 'lethal weapons'. [Web log post]. Retrieved February 18, 2018, from https://www.theguardian.com/technology/2014/jul/16/google-fbi-driverless-cars-leathal-weapons-autonomous

Haughey, B. (2007). DRBFM. *Applied Reliability Symposium.*

Hawes, N. (2016, November 3). Driving the revolution [Web log post]. Retrieved May 20, 2018, from https://www.birmingham.ac.uk/news/thebirminghambrief/items/2016/11/driving-the-revolution.aspx

Heineke, K., Kampshoff, P., Mkrtchyan, A., & Shao, E. (2017, May). Self-driving car technology: When will the robots hit the road? Retrieved from https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/self-driving-car-technology-when-will-the-robots-hit-the-road

Higgins, S. (2017, March 7). Velodyne, Can the Lidar in Autonomous Vehicles Capture Survey Data? [Web log post]. Retrieved from https://www.spar3d.com/news/lidar/velodyne-can-lidar-autonomous-vehicles-capture-survey-data/

Houser, K. (2018, January 17). Self-Driving Cars Will Save Lives, But Will They Cause Organ Shortages?.[Web log post]. Retrieved February 18, 2018, from https://futurism.com/self-driving-cars-will-save-lives-on-roads-but-will-they-cause-donor-organ-shortages/

Institute of Electrical and Electronics Engineers (2004) *IEEE Guide Adoption of PMI Standard - A Guide to the Project Management Body of Knowledge* (ANSI/IEEE 1490-2003)

International Electrotechnical Commission (2010). *Analysis techniques for dependability - Event tree analysis (ETA).* (IEC 62502:2010). Retrieved from https://webstore.iec.ch/publication/7131

International Electrotechnical Commission (2010). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES).* (IEC 61508:2010). Retrieved from https://webstore.iec.ch/publication/22273

International Electrotechnical Commission (2016). *Switches for appliances - Part 1-2: Requirements for electronic switches).* (IEC 61058-1-2:2016). Retrieved from https://webstore.iec.ch/publication/24938

International Electrotechnical Commission (2018). *Communication networks and systems for power utility automation.* (IEC 61850:2018). Retrieved from https://webstore.iec.ch/publication/24938

International Electrotechnical Commission. (n.d.). Functional Safety. Retrieved from http://www.iec.ch/functionalsafety/explained/

International Organization for Standardization (1999). *Quality systems -- Automotive suppliers -- Particular requirements for the application of ISO 9001:1994* (ISO/TS 16949:1999)

International Organization for Standardization (2011). *Road vehicles – Functional safety* (ISO 26262-1:2011)

Isermann, R. (2005). *Mechatronic systems: fundamentals*. London: Springer. 5-11, 25-30

Jarašūniene, A., Jakubauskas, G. (2007) Improvement of road safety using passive and active intelligent vehicle safety systems. *Transport*, 22(4), 285-287

Jegadeesan, H. (2008, September 22). Writing Effective Use Cases. (pp.43-44) Retrieved May 3, 2018, from https://www.slideshare.net/harshjegadeesan/lecture-2-writing-effective-use-cases-presentation?qid=e0616466-105f-4f56-9215-03bb8bfcaa03&v=&b=&from_search=1

Jenkins, M., & Mahmud, S. M. (2006). Security Needs for the Future Intelligent Vehicles. *SAE Technical Paper Series*. 3,8. doi:10.4271/2006-01-1426

Jo, K., Kim, J., Kim, D., Jang, C., & Sunwoo, M. (2014). Development of Autonomous Car—Part I: Distributed System Architecture and Development Process. IEEE *Transactions on Industrial Electronics,*61(12), 7131-7140. doi:10.1109/tie.2014.2321342

Kaebisch, S., Schmitt, A., Winter, M., & Heuer, J. (2010). Interconnections and Communications of Electric Vehicles and Smart Grids. *2010 First IEEE International Conference on Smart Grid Communications*.161-164. doi:10.1109/smartgrid.2010.5622035

Kaiser, L. (2013). *Rahmenwerk zur Modellierung einer plausiblen Systemstruktur mechatronischer Systeme Framework to model a plausible system structure for mechatronic systems*. (pp. 4, 45-51) Heinz Nixdorf Institut, Universität Paderborn.

Kalinsky, D. (2005). Architecture of safety-critical systems. *Embedded Systems Programming*, 14-25.

Kelly, T. (1998). *Arguing Safety - A Systematic Approach to Managing Safety Cases* (Doctoral Dissertation, University of York) (22).

Kim, C. (2016, June). Safety Challenges for Connected Cars. *IEEE Transportation Electrification Community*. Retrieved March 30, 2018, from https://tec.ieee.org/newsletter/june-2016/safety-challenges-for-connected-cars

King, S. (2007). Electric Vehicles and New Zealand: Identifying Potential Barriers and Future Considerations. 6-7,15, 22-24. *Wellington. NZ Ministry of Transport*

Kjosevski, S., Kostikj, A., & Kochov, A. (2017). Risks and safety issues related to use of electric and hybrid vehicles. Scientific proceedings XIV International Congress *"Machines technologies materials",II*, 169-172.

Koopman, P., & Wagner, M. (2016). Challenges in Autonomous Vehicle Testing and Validation. *SAE International Journal of Transportation Safety,4*(1), 15-24. doi:10.4271/2016-01-0128

Kucharski, M., Trujillo, A., Dunlop, C., & Ahdab, B. (2012). *ISO 26262 Software Compliance: Achieving Functional Safety in the Automotive Industry*. Technical report.

Lanctot, R. (2017, June). *Accelerating the Future: The Economic Impact of the Emerging Passenger Economy* (Rep.). (p. 5) Retrieved https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/05/passenger-economy.pdf

Lapedus, M. (2017, November 20). Here Comes High-Res Car Radar. Retrieved from https://semiengineering.com/here-comes-high-res-car-radar/

Laprie J.C. (1992). Dependability: Basic Concepts and Terminology. Dependable Computing and Fault-Tolerant Systems, vol 5. Springer, Vienna. 3-37.

Le Vine, S., Zolfaghari, A., & Polak, J. (2014). *Carsharing: Evolution, Challenges and Opportunities*(Vol. 22 ACEA, pp. 5-6, Rep.). Centre for Transport Studies, Imperial College London. Association des Constructeurs Européens d'Automobiles.

Leitner, A. (2014*).* *Public Use Case AUTOMOTIVE. CRYSTAL*(Rep.). doi: D 307.011

Liikanen, E., (2002). Active and Passive Car Safety – An Integrated Approach to Reducing Accidents. *- 6th International Symposium on Sophisticated Car Occupant Safety Systems.2-8*

Lin, P. (2016). Why ethics matters for autonomous cars. In *Autonomous Driving* (pp. 69-85). Springer, Berlin, Heidelberg.

Lindemann, U., Maurer, M., & Braun, T. (2010). Chapter 10: Use Case-- Automotive safety development. In *Structural Complexity Management. An Approach for the Field of Product Design*(pp. 155-157). Berlin: Springer.

Litman, T. (2018, April 11). *Autonomous Vehicle Implementation Predictions Implications for Transport Planning*(Rep.). 5-12, 24, 27-29. Retrieved April 13, 2018, from Victoria Transport Policy Institute website: https://www.vtpi.org/avip.pdf

Long, L. N., Hanford, S. D., Janrathitikarn, O., Sinsley, G. L., & Miller, J. A. (2007). A Review of Intelligent Systems Software for Autonomous Vehicles. *2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications,*1-8. doi:10.1109/cisda.2007.368137

Luettel, T., Himmelsbach, M., & Wuensche, H. (2012). Autonomous Ground Vehicles—Concepts and a Path to the Future. Proceedings of the IEEE, 100(Special Centennial Issue), 1831-1833. doi:10.1109/jproc.2012.2189803

Madanayake, R., Dias, G. K. A., & Kodikara, N. D. (2017). User Stories vs UML Use Cases in Modular Transformation. *International Journal of Scientific Engineering* *and Applied Science (IJSEAS)–Volume-3, Issue-1.* 1-3

Markoff, J. (2016, June 23). Should Your Driverless Car Hit a Pedestrian to Save Your Life? Retrieved February 16, 2018, from https://www.nytimes.com/2016/06/24/technology/should-your-driverless-car-hit-a-pedestrian-to-save-your-life.html?action=click&contentCollection=Technology&module=RelatedCoverage&region=Marginalia&pgtype=article

Mathur, S., & Malik, S. (2010). Advancements in the V-Model. *International Journal of Computer Applications,*1(12), 30-35. doi:10.5120/266-425

McMahon, J. (2016, August 4). Software Is The Last Obstacle To Fully Autonomous Vehicles, Elon Musk Says. Forbes.

Mendes, N. (2017, May 17). What self-driving cars can teach us about software testing [Web log post]. Retrieved March 20, 2018, from https://www.atlassian.com/blog/software-teams/what-self-driving-cars-can-teach-us-about-software-testing

Mhenni, F., Rivière, A., Kadima, H., Rauzy, A., Demmou, H., Hammami, O. (2014). *Safety analysis integration in a systems engineering approach for mechatronic systems design.* Thèse de doctorat: Sciences pour lingénieur: Châtenay-Malabry, Ecole centrale de Paris. (pp.i, 2, 17, 20, 21, 23, 47,34)

Millard-Ball, A. (2005). *Car-sharing: Where and how it succeeds*. Washington: Transportation Research Board, ES-1, 11.

Miller, T. (2002). Lithium ion battery automotive applications and requirements. *Seventeenth Annual Battery Conference on Applications and Advances. Proceedings of Conference (Cat. No.02TH8576),*113-118. doi:10.1109/bcaa.2002.986381, 113-118

Mirco, O., & Donnely, T. (2017). What is RAD model- advantages, disadvantages and when to use it? Retrieved from http://istqbexamcertification.com/what-is-rad-model-advantages-disadvantages-and-when-to-use-it/

Monticello, M. (2016, March 6). Americans Have Big Concerns About Self-Driving Cars, [Web log post]. Retrieved February 2, 2018, from https://www.consumerreports.org/cars-americans-have-big-concerns-about-self-driving-cars--surveys-sho/

Monticello, M. (2016, March). Will Automotive Technology Allow My Car to Chauffeur Me?, [Web log post]. Retrieved February 16, 2018, from https://www.consumerreports.org/self-driving-cars/will-automotive-technology-allow-my-car-to-chauffeur-me/

Mraz, S. (2017, January 25). SAE's 6 Levels of Self-Driving Cars. Retrieved February 1, 2018, from http://www.machinedesign.com/blog/sae-s-6-levels-self-driving-cars

Musk, E. (2016). 2016 Shareholder Meeting. New York.

National Highway Traffic Safety Administration. (n.d.). NHTSA - A Drive Through Time. Retrieved from https://one.nhtsa.gov/nhtsa/timeline/index.html

National instruments. (2016, January 5). Best Practices for Embedded Software Testing of Safety Compliant Systems. 1.

Nkoro, A., & Vershinin, Y. (2014). Current and future trends in applications of Intelligent Transport Systems on cars and infrastructure. *17th International IEEE Conference on Intelligent Transportation Systems (ITSC).* 514-515. doi:10.1109/itsc.2014.6957741

NYSERDA. (n.d.). Drive Clean Rebate. What makes electric cars different. Retrieved from https://www.nyserda.ny.gov/All-Programs/Programs/Drive-Clean-Rebate/About-Electric-Cars/Types-of-Cars

Object Management Group. (n.d.). OMG Systems Modeling Language. Retrieved from http://www.omgsysml.org/

Olsen, P. (2017, May 25). Doubts Grow Over Fully Autonomous Car Tech, Study Finds [Web log post]. Retrieved February 4, 2018, from https://www.consumerreports.org/autonomous-driving/doubts-grow-over-fully-autonomous-car-tech/

Osman, A. (2017, May 24). RADAR, camera, LiDAR and V2X for autonomous cars [Web log post]. Retrieved from https://blog.nxp.com/automotive/radar-camera-and-lidar-for-autonomous-cars

Parliament UK. (2017). Connected and Autonomous Vehicles: The future? Retrieved from https://publications.parliament.uk/pa/ld201617/ldselect/ldsctech/115/11505.htm

Pfitzmann, A. (2004, September). Why safety and security should and will merge. In *International Conference on Computer Safety, Reliability, and Security* (pp. 1-2). Springer, Berlin, Heidelberg.

Pinnes, M. (n.d.). Top 25 Causes of Car Accidents. Retrieved from https://seriousaccidents.com/legal-advice/top-causes-of-car-accidents/

Plungis, J. (2016, October 19). Tesla Says It's Now Building All Cars with Fully Autonomous Capabilities. [Web log post]. Retrieved February 16, 2018, from https://www.consumerreports.org/tesla/tesla-now-building-all-cars-with-fully-autonomous-capabilities/

Powell-Morse, A. (2017, November 02). Iterative Model: What Is It And When Should You Use It? Retrieved from https://airbrake.io/blog/sdlc/iterative-model

Pratt, G. (2016, April 7). 2016 GPU Technology Conference (GTC16) - Dr. Gill Pratt. Retrieved February 18, 2018, from http://corporatenews.pressroom.toyota.com/releases/gtc16-keynote-toyota-gill-pratt.htm

Rumbaugh, J., Booch, G., & Jacobson, I. (2017). *The unified modeling language reference manual*. Addison Wesley.3

Ross, H.L. (2016). *Functional Safety for Road Vehicles. New Challenges and Solutions for E-mobility and Automated Driving*. Switzerland:Springer.7-45,81, 96, 115-127, 263

Sabetzadeh, M., Nejati, S., Briand, L., & Mills, A. E. (2011). Using SysML for Modeling of Safety-Critical Software-Hardware Interfaces: Guidelines and Industry Experience. *2011 IEEE 13th International Symposium on High-Assurance Systems Engineering*,1-9. doi:10.1109/hase.2011.23

Sachiti, S. (2017, September 7). Re: Computers on wheels: Who's going to keep track of driverless vehicles? - live chat [Web log comment]. Retrieved from https://www.theguardian.com/public-leaders-network/live/2017/sep/01/computers-on-wheels-driverless-vehicles-live-chat-data

Santo, D. (2016, July 7). Autonomous Cars' Pick: Camera, Radar, Lidar? Retrieved from https://www.eetimes.com/author.asp?section_id=36&doc_id=1330069

Schoitsch, E. (2005). Design for Safety and Security of Complex Embedded Systems: A Unified Approach. *Cyberspace Security and Defense: Research Issues NATO Science Series II: Mathematics, Physics and Chemistry*.5,7,12,13. doi:10.1007/1-4020-3381-8_9

Sheppard, E. (2017, September 13). Autonomous vehicles: 'We need to make sure we're not stuck behind a red flag'.. [Web log post]. Retrieved February 16, 2018, from https://www.theguardian.com/public-leaders-network/2017/sep/13/autonomous-vehicles-data-management-public-consultation

Siemens. (2015). *Vehicle-to-X (V2X) communication technology*[Brochure]. Author. Retrieved March 20, 2018, from http://www.middleeast.siemens.com/pool/news_press/siemens-vehicle-to-x-communication-technology-infographic.pdf

Simpson, A. (2017, March 27). 4 Million Driving Jobs at Risk from Autonomous Vehicles: Report. [Web log post].Retrieved February 18, 2018, from https://www.insurancejournal.com/news/national/2017/03/27/445638.htm

Smith, B. W. (2012). Automated Vehicles are Probably Legal in the United States. *SSRN*

Electronic Journal. doi:10.2139/ssrn.2303904

Smith, B. W. (2013, December 18). Human Error as a cause of vehicle crashes [Web log post]. Retrieved April 5, 2018, from http://cyberlaw.stanford.edu/blog/2013/12/human-error-cause-vehicle-crashes

Society of Automotive Engineers (2016). *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. (SAE J3016_201609). doi:10.4271/j3016_201609

Society of Automotive Engineers (2018). *Considerations for ISO 26262 ASIL Hazard Classification*. (SAE J2980_201804). Retrieved from https://www.sae.org/standards/content/j2980_201804/

Son, P. & Adam, M. (2017). What is Incremental model- advantages, disadvantages and when to use it?. Retrieved from http://istqbexamcertification.com/what-is-incremental-model-advantages-disadvantages-and-when-to-use-it/

Spanfelner, B., Richter, D., Ebel, S., Wilhelm, U., Branz, W., & Patz, C. (2012). Challenges in applying the ISO 26262 for driver assistance systems. *Tagung Fahrerassistenz, München,* 15(16), 2012.

Statista (2018) Car production: Number of cars produced worldwide 2017. Retrieved April 4, 2018, from https://www.statista.com/statistics/262747/worldwide-automobile-production-since-2000/

Taylor, W., Krithivasan, G., & Nelson, J. J. (2012, November). System safety and ISO 26262 compliance for automotive lithium-ion batteries. In *Product Compliance Engineering (ISPCE), 2012 IEEE Symposium on* (pp. 1-6). IEEE.

Thomas, J. (2013). Systems Theoretic Process Analysis (STPA) Tutorial. 11.Retrieved April 15, 2018, from http://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Systems-Theoretic-Process-Analysis-STPA-v9-v2-san.pdf

Thompson, C. (2016, November 16). Why driverless cars will be safer than human drivers [Web log post]. Retrieved from http://www.businessinsider.com/why-driverless-cars-will-be-safer-than-human-drivers-2016-11

Troppmann, R. (2006, June 22). Tech Tutorial: Driver Assistance Systems, an introduction to Adaptive Cruise Control: Part 1. Retrieved from https://www.edn.com/Home/PrintView?contentItemId=4011081

Types of Auto Accidents | McCamy, Phillips, Tuggle & Fordham, L.L.P. | Dalton. (n.d.). Retrieved February 16, 2018, from https://www.mccamylaw.com/Personal-Injury-Information-Center/Types-of-Auto-Accidents.shtml

U.S Department of Transportation. NHTSA-National Highway Traffic Safety

Administration. (2008). *National Motor Vehicle Causation Survey*. pp. 1-47, Publication. DOT HS 811 059

U.S Department of Transportation. Federal Aviation Administration (2000). Chapter 3: Principles of System Safety. In *FAA System Safety Handbook* (pp. 3-1 - 3-4).

U.S Department of Transportation Federal NHTSA- (September 2016). Automated Vehicles Policy. Accelerating the Next Revolution in Rodway. 5, (pp.15-35). Retrieved February 17, 2018, from http://www.safetyresearch.net/Library/Federal_Automated_Vehicles_Policy.pdf

Verein Deutscher Ingenieure (2004). *Entwicklungsmethodik für mechatronische Systeme. Design methodology for mechatronic system.* (VDI 2206). Düsseldorf: VDI.

Verma, J., Bansal, S., Pandey, H. (2014). Develop Framework for Selecting Best Software Development Methodology. *International Journal of Scientific & Engineering Research, Volume 5, Issue 4,* 1067

Voelcker, J. (2014, July). 1.2 Billion Vehicles On World's Roads Now, 2 Billion By 2035: Report. Retrieved February 05, 2018, from https://www.greencarreports.com/news/1093560_1-2-billion-vehicles-on-worlds-roads-now-2-billion-by-2035-report

Vritika. (2015, August 13). Difference between Active and Passive Safety Features on a Vehicle. Retrieved January 29, 2018, from http://www.differencebetween.info/difference-between-active-and-passive-safety-features-on-a-vehicle

Wachenfeld, W., Winner, H., Gerdes, J. C., Lenz, B., Maurer, M., Beiker, S., ... & Winkle, T. (2016). Use cases for autonomous driving. In *Autonomous driving* (pp. 9-37). Springer, Berlin, Heidelberg.

Waghe, R., & Gajjal, S. (2014). Study of Active and Passive Safety Systems and Rearview Mirror Impact Test. *SSRG International Journal of Mechanical Engineering* (SSRG-IJME),1(3), 10-14.

Walker &Walker Attorney Network. (2017, September 15). What Are the Different Types of Car Accidents? | 1-800-THE-LAW2. Retrieved from https://www.1800thelaw2.com/blog/types-of-car-accidents

Watts-Roy, J. (2017, March 15). Agile Method: Top Mistakes to Avoid When Using This Development Approach | Blog. Retrieved from https://number8.com/common-mistakes-using-agile-method/

Wei, J., Snider, J. M., Kim, J., Dolan, J. M., Rajkumar, R., & Litkouhi, B. (2013). Towards a viable autonomous driving research platform. *2013 IEEE Intelligent Vehicles Symposium (IV).* doi:10.1109/ivs.2013.6629559

Welch, S. (2016, July 21). New Data Shows 94 Percent of Car Accidents Caused by Human Error [Web log post]. Retrieved March 5, 2018, from http://southsideinjuryattorneys.com/lawyer/2016/07/21/Personal-Injury/New-Data-Shows-94-Percent-of-Car-Accidents-Caused-by-Human-Error_bl25860.htm

Wiseguy Reports. (2018, April 23). Automotive Vehicle to Everything (V2X) Communications Market 2018 Global Trend, Segmentation and Opportunities Forecast To 2023. Retrieved from http://www.crossroadstoday.com/story/38017972/automotive-vehicle-to-everything-v2x-communications-market-2018-global-trend-segmentation-and-opportunities-forecast-to-2023

World Health Organization. (2014, June 06). Organization Infographics on global road safety 2013. Retrieved from http://www.who.int/violence_injury_prevention/road_safety_status/2013/facts/en/

Woźniak, D., Kukiełka, L., Woźniak, J (2013). Modern active and passive safety systems in cars– chosen aspects. 272-276

Yannis, G., & Cohen, S. (2016). *Traffic safety* (Vol. 4). 14-15. London: ISTE.

2020 Roadmap. (March 2015). European New Car Assesment Programme, 2-18

6 List of figures

7 List of tables

8 Glossary and abbreviations

ADAS	Advanced driver-assistance systems
ASIL	Automotive Safety Integrity Level
AU	Application Unit
AV	Autonomous Vehicle
ECU	Electronic Control Unit
E/E	Electric/Electronic
ETSI	European Telecommunications Standards Institute
EV	Electric vehicles
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
GNSS	Global Navigation Satellite System
HARA	Hazard Analysis and Risk Assessment
HAV	High automated vehicles
HAZOP	HAZard and OPerability Analysis
HMI	Human Machine Interface
IBD	Internal Block Diagram
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ITS	Intelligent transport system
ICEV	Internal Combustion Engine Vehicle
IVSS	Intelligent Vehicle Safety System
NHTSA	National Highway Traffic Safety Administration
RSU	Road-Side Unit
OBU	On-Board Unit
RBD	Reliability Block Diagram
SAE	Society of Automotive Engineers
SDM	System Development Method
SysML	Systems Modeling Language
TPM	Trusted Platform Module

UML	Unified Modelling Language

Item

System or group of systems that implement one or more functions observed at the vehicle level (to which the ISO 26262 Safety Life Cycle is applied) (ISO 26262 cited in Birch 2013, p.2). The item is the maximum recognized object in the process and is thus the starting point for product-specific safety development under this standard.

Element

System or part of a system (components, hardware, software, hardware parts, and software units) that can be distinctly identified and manipulated (ISO, 2011).

Embedded systems

Combination of processors, sensors, actuators, "intelligence", "hidden computers" and massive deployment that interact intensively with uncertain environments (Schoitsch, 2005, p.5).

Quality

"The sum of characteristics of an entity regarding its suitability to fulfill defined and predetermined requirements". The term "entity" is here very vague. It is defined as follows: "Something that can be described and observed individually." Thus, quality refers to characteristics and features of a finished product. In general, it is assumed that these characteristics remain for a certain time after the production. Often this time period equals the warranty period. As long as it is stated in the specifications that the existing characteristics and features after the production should remain through the defined usage period, reliability is a part of quality". ISO TS 16949 (ISO, 1999) cited in Ross (2016,p.18)

Reliability

According to Robert Lusser's law (Ross, 2016, p.43), the total reliability occurs in the product of the individual reliabilities. Basically, this law says that: "The chain is as strong as its weakest link". Also, safety-related functions or safety mechanisms can only work as well as the individual parts of which they consist of. Reliability is technically seen as a quality factor normally described as a component characteristic as opposed to safety. (Ross, 2016, p.49).

System

The entity that interacts with other entities, i.e. other systems (hardware, software, humans, physical world…), which are considered the environment of the system, and which frontier is called system boundary (Avizienis et al, 2004, p.3).

Annexes

A1 Safety car timeline

The most significant events or major developments (milestones) are summed up in the following table (National Highway Traffic Safety Administration. (n.d.).:

Table 8-1 Milestones car safety. Source: own elaboration

Year	Milestone	Description
1889	Electric Headlight	Headlamp design (including the bulb, reflector, and lens) has evolved gradually, culminating in the introduction of the latest HID, LED and laser units
1895	Pneumatic tyres	Used on a car first by André Michelin, tyre development has been a significant contributor to road safety ever since.
1903	Four wheel brakes/drive	Fitted first to the Dutch Spyker 60/80 racer, which also boasted four-wheel-drive. Disc brakes are far more efficient than drum types, mainly due to their ability to shed their heat faster.
1903	Windscreen wipers	Early efforts to clear the front windscreen started and later progressions include rubber blades, powered wipers, manual and electric washers, self-parking, intermittent operation and rain-sensing abilities.
1912	Electric starter	As compression ratios rose, many drivers were breaking their wrists, starting their engines manually. Cadillac is credited with making the first mass-produced electric-start car, although starting handless survived in Europe, into the 1990s
1921	Hydraulic operated brakes	The Duesenberg Model A used a system that was based upon the principles, established by Malcolm Lockheed. Split circuits appeared from the 1960s so that if a leak occurred, some braking was still possible.
1931	Safety glass	UK legislation dictated that safety windscreens replaced plate glass, for all new cars from 1932. Even safer laminated glass, which appeared from the mid-1940s, took until1970s to become widespread.
1934	Unitary body	First chassis-less car. It paved the way for other carmakers to incorporate further proactive and impact absorbing qualities, such as a safety cage (the 1940s) and crumple zones (1950s).
1952	Disc brakes	Early disc brakes acted on the transmission, as per trams, lorries, aircraft and competition cars of the era.
1954	Self-leveling suspension	It helps a loaded car maintain its roar-holding and prevent its headlights from dazzling fellow road users.
1956	Safety steering column	Volvo’s 120 steering column broke away from the steering system in a major impact. Further developments in the motor industry saw collapsible columns and impact absorption qualities being introduced.
1958	Padded	Carmakers start to change interior designs so that protruding parts

	interiors	and bare metal surfaces could no longer cause injury when struck by an occupant.
1959	Three-point safety belt	Volvo introduces the seat belt, which is considered the most beneficial car safety device of all time. Other carmakers recognized the benefits, some of which were prompted by legislation.
1966	Anti-lock Brakes (ABS)	First mechanical anti-lock brakes based on aircraft technology. Bosch Automotive refined and popularized ABS for car use by the late 1970s.
1968	Automatic fuel cut off switch	To reduce the chance of a fuel leak and consequent fire, inertia switches cut off power to the fuel pump, in the event of an impact
1968	Heat restraints	Volvo offers head restraints at the front-seat, in order to protect the head and neck in rear-end crashes
1971	Traction control	Early electronic efforts attraction control appeared in North America, which went global from the mid-1980s. The system was refined later, often combined with stability control.
1973	Side impact protection	Door bars were fitted by Volvo in 1973. In 1991, the Swedes had developed a side impact protection system, which transferred impact forces around the car.
1978	Electronic ABS	Mercedes-Benz S-class is the first production car with electronic ABS.
1984	Airbag	Although cars featuring steering wheel airbags had been sold, prior to the mid-1980s, they had not become popular, until Mercedes Benz started offering a single driver's airbag. Today, a new car can have in excess of eight airbags fitted.
1986	Third brake light	The high-level third brake light is introduced by Volvo.
1987	Rear seat belts	They become a legal requirement for all cars sold in the UK. By 1991, all adults were required to belt up in the back.
1989	Advanced Brake Warning systems	Israel companies implemented these warning systems where the car driver would be alerted as to how hard the driver in front is pressing his brakes
1995	Stability control (+Traction control)	The system operates when it detects a lack of steering control, by applying the brakes of a skidding wheel (via the ABS) and cutting power, if needed. It has been described as one of the most vital safety aids of modern times.
1998	Brake assist	As 90% of drivers do not press the footbrake adequately in emergency situations, brake assist reduces the pressure needed at the pedal, depending on the rate at which it is depressed.
2004	Blind spot warnings	The Blind Spot Monitoring System (BLIS) warns the driver if an oncoming vehicle lingers in the vehicle's side blind spot.
2010	Automating braking	Although systems have been in place that pre-empts an impact, since the early 2000s, auto brake systems work in low-speed conditions, to warn the driver of an impending impact and apply

		the brakes fully, if there is no manual reaction.
2012	Pedestrian Airbag	Although methods to protect pedestrians have been in use for many years, including pop-up bonnets from the mid-2000s, a pedestrian airbag appeared first in 2012.
2012	Electronic Stability Control	ESC become mandatory in all cars sold in the USA.

A2 Types of car accidents

In the following lines, the different types of accidents are briefly described and illustrated (Walker &Walker Attorney Network, 2017)

- Head-on collisions

Head on collisions happen when the front of two vehicles that are facing each other collides. They are considered very fatal, especially when they are traveling at very high speed.

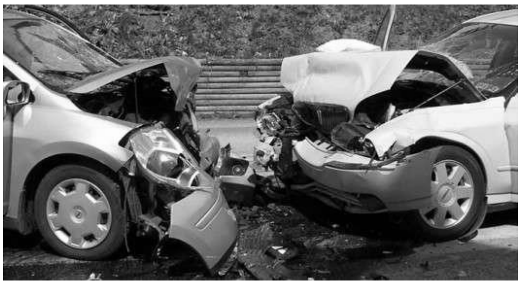


Figure 8—1: Head-on collisions. Source: daylybuzzsa in http://www.pulse.ng

- Hit-and-run accidents

Hit-and-run accidents occur when one driver leaves the scene of an accident. It might be difficult to find the vehicle and the author if there are no witnesses or video footage of the accident.

Figure 8—2: Hit-and-run accidents. Source: https://www.statefarm.com

- Multiple vehicle pile-up

They involve many vehicles and generally happen on freeways or highways. They are one of the deadliest traffic accident as some of the cars or other vehicles are not only hit once but multiple times and from different directions, and being trapped or trying to escape can also suppose a hazard.

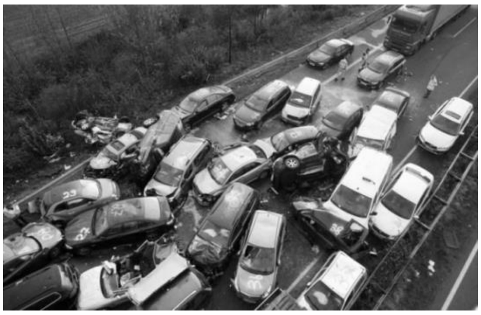


Figure 8—3: Multiple vehicle pile-up. Source: https://www.pinderplotkin.com

- Side-impact collision

Side impact collisions or T-bone collisions happen when the side of a vehicle is hit by the front or rear of another vehicle or object. Injuries and damage may be more or less severe depending on how reliable the safety features of the car are (airbags, crumple zones, vehicle construction, and materials) and also the speed of the cars involved in the accident.

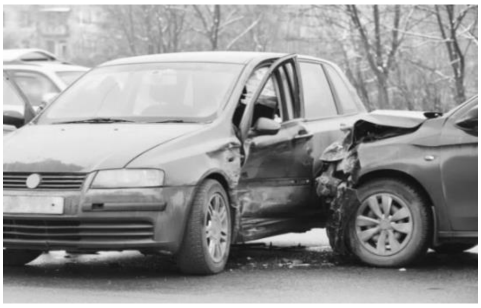


Figure 8—4: Side impact collision. Source: Queller, Fisher, Washor & Fuchs in http://www.quellerfisher.com

- Single car accident

At its name points out, it only involves one vehicle. Normally it happens because driver loses control due to drowsiness, sleepiness, brake malfunction etc.

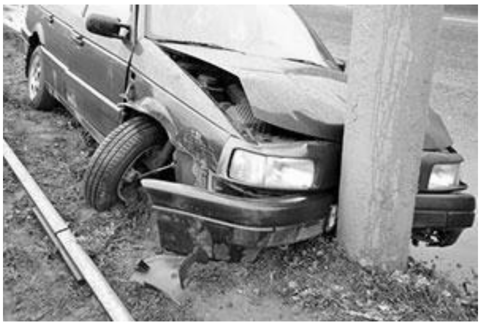


Figure 8—5: Single car accident. Source: https://www.jinkslaw.com

- Sideswipe collision

They involve the adjacent sides of two vehicles. If both vehicles are driving in the same direction and any driver loses control of the car, the damage may only be cosmetic, but if one driver loses control of the vehicle, there may be more serious injuries and damages.

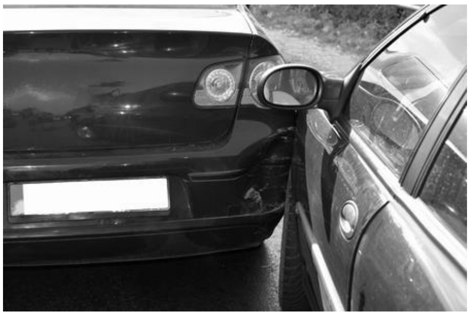


Figure 8—6: Sideswipe collision. Source: Tario & Associates, P.S

- Rear-end collision

It happens when one car hits the rear of the car in front of it. It typically occurs when the vehicle ahead suddenly decelerates or brakes or when the vehicle behind suddenly accelerates or simply not realize what is happening.

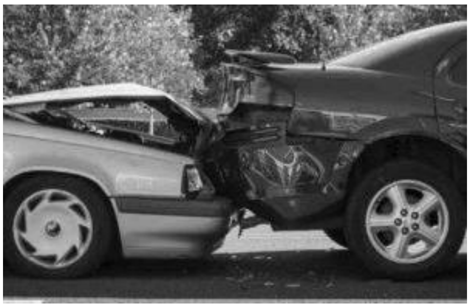


Figure 8—7: Rear-end collision. Source: The Pearce Law Firm in http://btsmithlaw.com/

- Rollover

It happens when vehicle flips over its side or roof and generally occurs when the car makes a high-speed sharp turn.

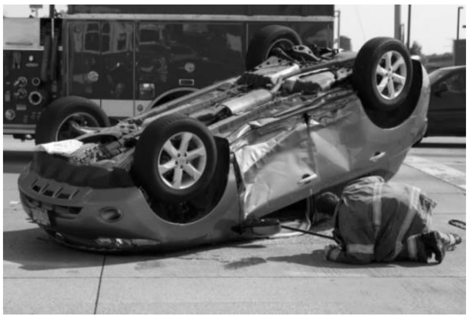


Figure 8—8: Rollover. Source: CBS Chicago in http://chicago.cbslocal.com

A3 Causes of car accidents

As it was stated been during the whole thesis, the main cause or reason of car crashes is the human factor, in all its different cases, and letting the mechatronic systems failures the smaller cause of accidents. Although autonomous cars could reduce human error in the future, it is yet to be seen how it will impact car accidents (Pinnes, n.d).

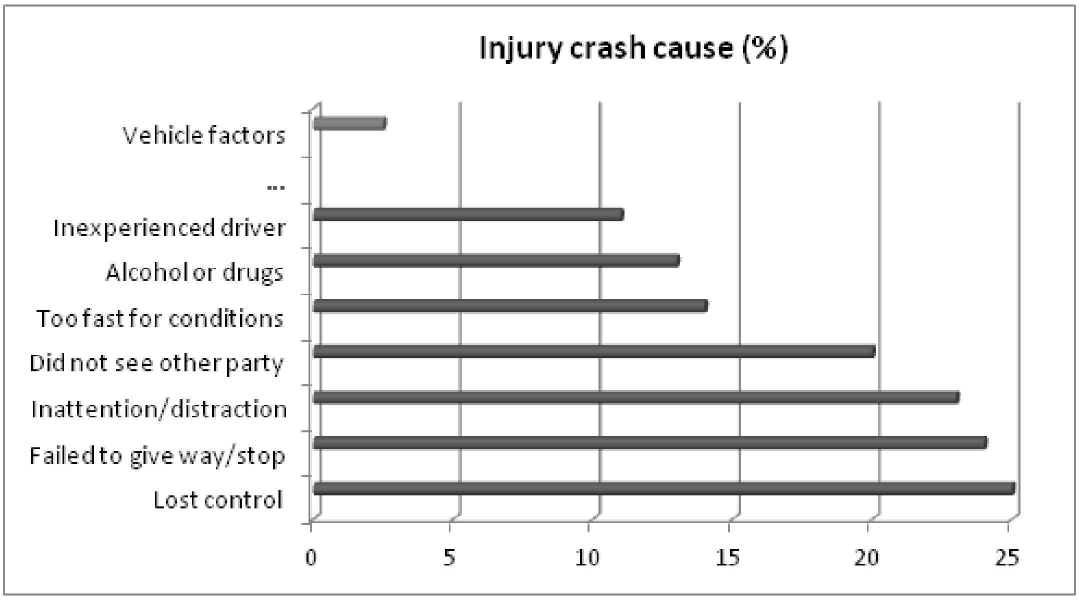


Figure 8—9: Injury crash cause. Source: Herniated Disc Car Accident Statistics in www.caraccidentherniateddisc.com

Therefore the causality of car accidents can be classified in three types according to the failure element:

Human Error Car Accidents

The human factor is the most common error among car crashes. It can be due to many different reasons: to us.

- Distracted Driving

Driving distracted has been the major cause of car accidents in the past decades, and it is still increasing due to the fact that every time there is more gizmos and technology gadgets such as mobile phones, DVD players, GPS that suppose a huge distraction for the drivers. And not only these devices but also others multi-tasking behind the wheel such as eating, drinking, talking…

- Drowsy Driving

Most of the car accidents caused by drowsy driving occur at night, but they also can happen if the driver has too much fatigue or is having trouble staying awake even in the day hours.

- Medical Conditions

Seizures, strokes, heart attacks, epilepsy attacks, schizophrenic or other mental illnesses attacks can be a very serious reason for car accidents. These medical conditions are often not controllable and therefore so risky.

- Night Driving

Lack of visibility makes hazards more difficult to see at night despite full lights. Driving in the hours of daylight can be hazardous, nonetheless driving at nightly closely doubles the risk of a car accident occurring.

- Old drivers

The elderly or biological aging presents a serious enough problem when driving.

- Reckless Driving

Reckless driving is a mix of different behaviors seen above: changing lanes too quickly and unsafely, doing road rages, speeding well over the limit, not using the signals properly, not following the traffic signals and acting aggressively on the roads can lead to horrible accidents caused by simple carelessness.

- Running Stop Signs/Red lights

When Stop signs are ignored, severe car accidents can frequently happen. Many rollover accidents and side-impact car accidents result from drivers that run stop signs without looking both ways.

- Speeding

It is the second most common origin of accidents. Traveling above the speed limit decreases the reaction time that could be needed to prevent a car accident.

- Tailgating

They occur when an impatient or reckless driver gets too close to the vehicle in front of him and does not keep the safe distance so when the first vehicle suddenly breaks, he cannot react in time and a fatal vehicle crash can happen, depending on the speed of both vehicles.

- Teenage Drivers

Teenagers are not frequently known for their carefulness and their lack of experience in unsafe conditions ends up causing accidents. When teen drivers hit the roads they do not always know what to do and that lack of experience ends up causing car accidents.

- Uncertainty

Being not familiar with an area (because the driver is lost, construction area, not aware of the laws, foreign country…) can be the cause of an accident too. It is not impossible to get turned around or drive faster than what is suggested in an area you are unaware of. Some people just flat out do not know how to drive. Not following the rules of the road, mistakes, and lapses while driving a car can cause horrible accidents.

- Under the Influence

Driving under the influence of drugs, alcohol, or cold medicine makes the driver not being of a clear mind and puts him at a high risk. Drunk driving is one of the most dangerous and deadly causes of accidents, even when they are on the top causes that can be avoided. And it is not only alcohol what is dangerous when mixed with drivers on the road, also legal and illegal drugs can damage the ability to drive properly.

System failure car Accidents

Mechatronic failure can occur for several different reasons. Sometimes it is out of control of the driver, and other time not.

- Deadly curves

Not taking too much account to traffic signs, speed limits, and caution when approaching to a dangerous curve can be one of the reasons of accidents, especially in motorists.

- Failure to maintain vehicle:

Not carrying out the correspondence maintenance regularly suppose thine borderline between mechanical and human failure (bald tyres, broken tie rod, bad brakes…).

- Faulty traffic lights

If a traffic light is out in the middle of the night, and especially when the driver is unfamiliar with the area and for example run through an intersection, can, without doubt, be the cause of an accident.

- Manufacturer Malfunction

Although it is not very common, sporadically accidents can occur because the vehicle was not built properly, since any product is ever made perfectly. Autos have hundreds of parts, and any of those imperfect parts can cause a grave car accident Automakers release recalls when a problem has been identified, but sometimes a recall only happens after several accidents have occurred.

- Tyre blowouts

Unexpected tyre blowouts can cause the lose control of the vehicle and therefore severe car accidents, especially in big automobiles like trucks.

Weather related car accidents

Dense fog, excessive rain, slick roads, and high winds can all origin major problems for drivers. Even extreme differences in temperature can create large potholes worthy of damaging a car.

- Fog

Although fog is not the most common weather occurrence, dense fog can makes driving a task extremely difficult when it exists.

- Ice

When hitting a black ice, the car can spin dangerously out of control and crash with another vehicle or object.

- Rain

Heavy and excessive rains can cause slippery and treacherous road conditions since the water creates slick, dangerous surfaces (making automobiles to spin out of control or skid while braking) and lack of visibility often origin car accidents

Others

- Animals

Since animals do not understand the risk of crossing a road and their behaviour is unpredictable, when a large animal such as a deer goes to cross the road at a high speed, they can run right into the side of the vehicle, and cause a fatal accident. Also, other animals like bees, or trying to avoid crashing into a dog can be the origin of an accident.

- Construction Sites

Sometimes the way a construction zone is set up can be confusing for the drivers and if it is not driven slowly and carefully, accidents can occur.

- Potholes:

They are very frustrating and sometimes, trying to avoid them, a crash can happen.

A4 Active safety systems.

The following paragraphs summarize the work or findings of different authors: (Liikanen, 2002; Woźniak et al. 2013; Waghe et al. 2014; Vritika, 2015; Alves, 2016; Campbell, 2015)

Dynamic based systems

- Anti-lock brake system (ABS)

They prevent the wheels from locking up when the driver brakes, enabling the driver to steer while braking and to adhere to the road surface. This distributes the braking force in such a way as to maximally use the traction by keeping the circumferential within the limit of maximal slipping with respect to the vehicle’s speed.

- Autonomous Emergency Braking System (AEB)

They automatically apply the brakes to decrease speed when sensors on the vehicle identify a likely collision and the driver has not applied sufficient braking force and is not attempting to steer away.

- Brake Assist System (BAS)

It assists in emergency braking by increasing the brake pressure, independently of how much the brake pedal is pressed, when the pedal is applied all of a sudden.

- Electronic Brake-force Distribution (EBD)

Electronic brake force distribution (EBD or EBFD) and electronic brake force limitation (EBL) change in an automatic way the amount of force applied to each brake, based on road conditions, speed, loading, etc.

- Electronic stability control (ESC)

It keeps the car under control and on the road in risky situations, improving the stability when driving through a turn by appropriately dosing (depending on the car’s angular speed, lateral acceleration, wheel skidding) drive forces and the braking forces.

- System steering the braking force (EBV or AFU)

It steers the braking force due to the increase of brake fluid case of rapid braking,

.

- Traction control system (ASR or TCS)

It regulates the driving force when sensors detect a loss of traction in some of the wheels, limiting the skidding in rapid acceleration by influencing the engine feeding and the braking system. It prevents the wheels from slipping while the car is accelerating.

Driver information and assistance systems

- Active Vision Enhancement (VE)

It illuminates the road, so a more detailed image is acquired, including lane markings and road boundaries, enabling the driver to differentiate between obstacles that are in their driving lane and those that are not.

- Blind Spot Support

It supports drivers by alerting them when a vehicle enters the car's blind spot. Visual or audio cues warn the driver not to change lanes or make a turn into the blind spot until they see the designated vehicle reappear.

- Curve Adaptive Lighting (CAL)

They direct the light beam partially in the direction in which the car is being steered. This system is appropriated on zigzagging roads with low light levels due to fog, rain, snow, darkness etc. since it gives a preview of road and traffic conditions during the turn.

- Drowsiness Detection Systems (DDS)

They, through the face examination and detection of fatigue in the driver, illuminate driver's face in a non-intrusive way in order to make him aware of his fatigue and lack of attention.

- Intelligent speed assistant (ISA)

It alerts drivers (through audio and visual warnings) when they exceed the speed limit.

- Lane departure warning systems (LDW)

They track road features (road marking, road edges) to determine if a car is deviating from a chosen lane or the road itself, due to driver fatigue, loss of concentration or poor driver lane discipline.

- Lane Keeping Assistance (LKA)

It intercedes in the steering impeding the lane change when an unplanned lane alteration is perceived by the system.

- Tyre pressure monitoring systems(TPMS)

They aware the driver if a tyre loses pressure or has other tyre defects.

Integrated (or Advanced Driver Assistance) safety systems

- Adaptive Cruise Control (ACC)

It maintains an automatically driver programmed speed and a safe distance, thanks to radar sensors used to calculate the distance from the vehicle in front and the relative speed. These systems also work on turns and use signals from the ESP (electronic stability program) system like longitudinal and angular speed and lateral acceleration.

- Collision Mitigation systems (CMS)

They use radar or LIDAR signals and sensors to perceive imminent crash and then arrange interventions to diminish the effects of the collision by deploying seatbelt tensioners, closing windows, adjusting head restraints and activating airbags before the collision occurs.

- Brake override engages

They deactivate the accelerator pedal in the event that both the gas and the brake pedal are pushed down simultaneously.

- Collision Mitigation and Avoidance Systems (CMAS)

Like CMS, CMAS will also be integrated with passive safety systems in order to minimize injuries to both vehicle occupants and pedestrians.

- Computerized Active Brake

It does not require the driver to have the intention of stopping and depressing the brake pedal. Thanks to infrared and radar signals, the car detects objects in front, back and sides of the car as well as lane position.

- Front crash prevention

It integrates a series of sensors into the front of the vehicle to monitor the closure speed between vehicles, alerting the driver when they are too close to the vehicle ahead. They include proactive measures to assist drivers such as precharging the breaks or activating them automatically.

- Hazard/warning indicator lights

They activate a warning system when a potentially dangerous situation is detected

A5 Passive safety systems.

This annex collect the work carried out by different authors (Liikanen, 2002; Woźniak et al. 2013; Waghe et al. 2014; Vritika, 2015; Alves, 2016; Campbell, 2015)

- Airbags (SRS)

They provide a cushion filled with compressed gasses to protect the driver and passengers during a crash, working just effectively if seatbelts are worn. In many new vehicles, airbags do not just inflate out of the steering column but also appear along the side-panels and even around the knees.

- Crumple Zones

They help to absorb and distribute crash forces before they reach the passenger and driver's seats.

Apart from the active and passive safety systems seen in the last paragraphs that nowadays most of the cars include, it could be added another type of systems, out of this active-passive classification.

- eCall

It is an electronic safety system that, in case of a serious accident, it automatically calls the nearest emergency center and transmits the exact geographic scene and other data, so the rescue workers can go to help within minutes. It can also be made manually at the push of a button, in case a third driver witnesses a car accident and any car occupant can give o receive information about the accident and how to react after it (Waghe &Gaijal, 2014).

- Frontal Protection System (FPS)

It is a device fitted to the front end of a car to protect both pedestrians and cyclists who are involved in a front end collision with a vehicle. Car design has been shown to have a large impact on the scope and severity of pedestrian injury in car crashes.

- Fuel pump kill switch

IT aims to decrease the chance of a fuel leak and consequent fire by cutting off the power to the fuel pump.

- Head restraints

They prevent the driver and passengers from getting whiplash during a rear-end collision. They keep the driver and passengers stationary within the living space of the vehicle.

- Laminated windshields

They remain in one piece when impacted, avoiding penetration of unbelted passengers' heads and keeping a minimal but adequate transparency for control of the car immediately following a collision. Tempered glass side and rear windows break into granules with minimally sharp edges, rather than splintering into jagged fragments as ordinary glass does.

- Rollover bars

They protect the car's occupants from injury if the vehicle rolls over during an accident.

- Safety Cell

The passenger compartment is reinforced with high strength materials, at places subject to high loads in a crash, in order to maintain a survival space for the vehicle occupants.

- Seatbelts

They hold passengers in place so that they are not thrown forward or ejected from the car. Advanced seatbelts can moderate the amount of tension across a person’s body, so as to reduce instances of seatbelt-related injuries.

A6 Overview of ISO 26262

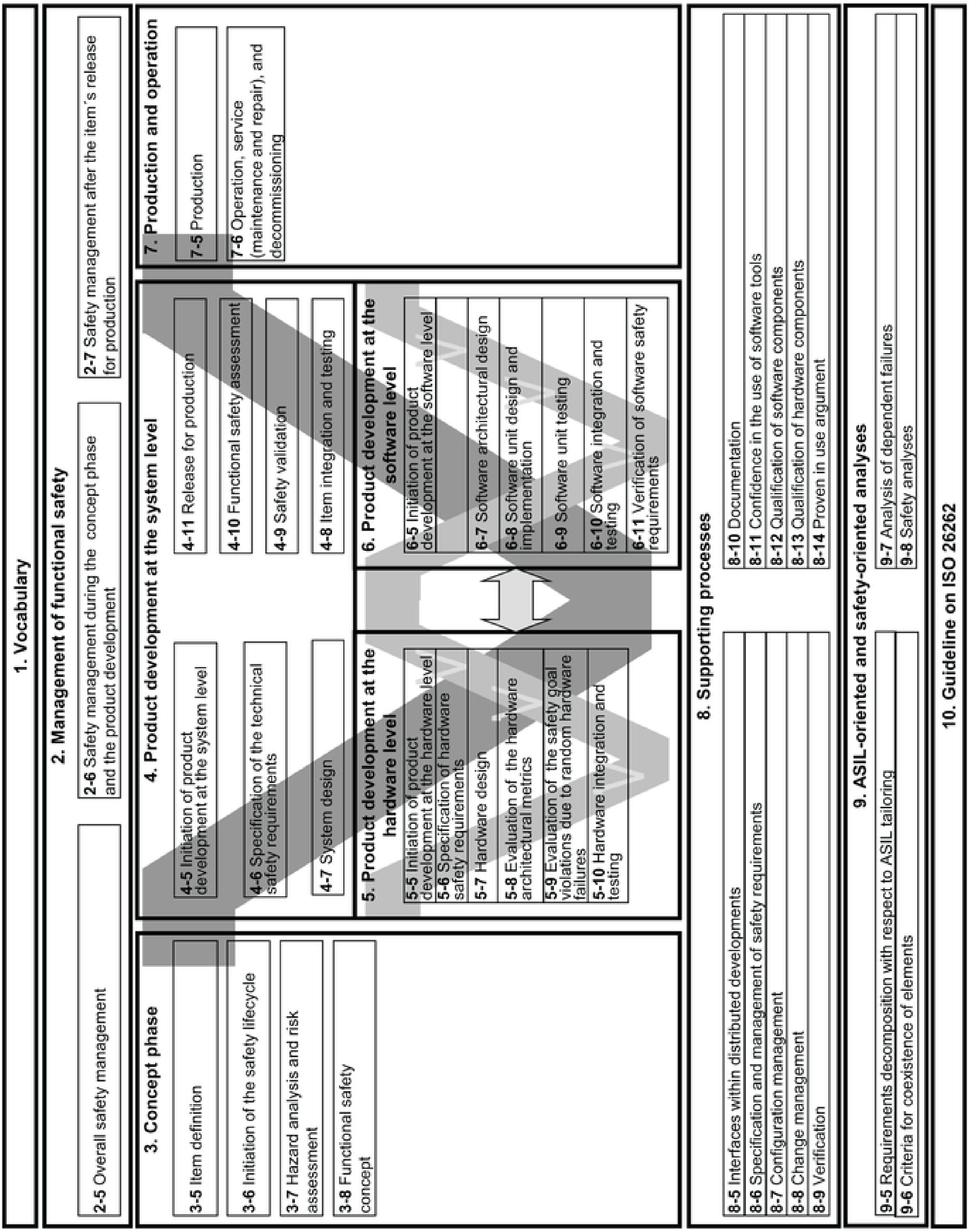

1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during the concept phase and the product development
2-7 Safety management after the item´s release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
4. Product development at the system level
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-8 Item integration and testing
4-9 Safety validation
4-10 Functional safety assessment
4-11 Release for production
5. Product development at the hardware level
5-5 Initiation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
5-9 Evaluation of the safety goal violations due to random hardware failures
5-10 Hardware integration and testing
6. Product development at the software level
6-5 Initiation of product development at the software level
6-6 Specification of software safety requirements
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements
7. Production and operation
7-5 Production
7-6 Operation, service (maintenance and repair), and decommissioning
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation
8-11 Confidence in the use of software tools
8-12 Qualification of software components
8-13 Qualification of hardware components
8-14 Proven in use argument
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
10. Guideline on ISO 26262

Figure 8—10: Overview of ISO 26262. (ISO, 2011)

A7 Use Case Template

Table 8-2: Use Case Template (De Francisci,2016)

Use Case Template

Use Case Identification	
Use Case ID	Give each use case a unique numeric identifier, in the hierarchical form: X.Y. Related use cases can be grouped in the hierarchy.
Use Case Name	State a concise, results-oriented name for the use case. These reflect the tasks the user needs to be able to accomplish using the system. Include an action verb and a noun.
Use Case Definition	
Description	Provide a brief description of the reason for and outcome of this use case, or a high-level description of the sequence of actions and the outcome of executing the use case. This is usually an expanded version of what you entered in the "Use Case Name" field.
Actors	**Primary Actors**: Name the actor(s) that will be performing this use case: a person, a user class, a role or a software/hardware system that interacts with your system to achieve the goal of this use case and has the primary interest in the outcome of this Use Case. *Optional:* (a) **Supporting Actors**: Name the actor(s) who have a supporting role in helping the Primary Actor achieve his or her goal. (b) **Stakeholders and Interests**: List Stakeholders and their interests. They may not directly interact with the system but they may have an interest in the outcome of the use case.
Preconditions	List any activities that must take place or any conditions that must be true, before the use case can be started. Number each precondition.
Postconditions	Describe the state of the system at the conclusion of the use case execution. Number each success and failure postcondition.
Frequency of Use	Estimate the number of times this use case will be performed by the actors per some appropriate unit of time.
Scenario	Main (Normal Course): Enter the Main flow of events. This is best done as a numbered list of actions performed by the actor, alternating with responses provided by the system. Describe the flow of events from preconditions to postconditions, when nothing goes wrong. *Optional:* (a) **Alternative Courses / Extensions**: Describe all the other legitimate usage scenarios for this use case. They are branches from the main flow to handle special conditions. For each alternative course/extension reference the branching step number of the Main flow and the condition which must be true in order for this extension to be executed. Number each alternative course/extension using

	the branching step number of the Main flow as a prefix, followed by a letter and a step number. (b) **Exceptions**: Describe any anticipated error conditions that could occur during execution of the use case, and define how the system is to respond to those conditions. Number each exceptions using the branching step number of the correct scenario.
Special Requirements	Enter any special requirements such as Performance requirements, Security requirements, User interface requirements and any other nonfunctional requirements.
Issues	List any additional comments about this use case or any remaining open issues or TBDs (To Be Determined) that must be resolved. Identify who will resolve each issue, the due date, and what the resolution ultimately is.

A8 Use Case Diagram Notation

Table 8-3: Use Case Diagram Notation (Friedenthal et al. 2011, p. 588).

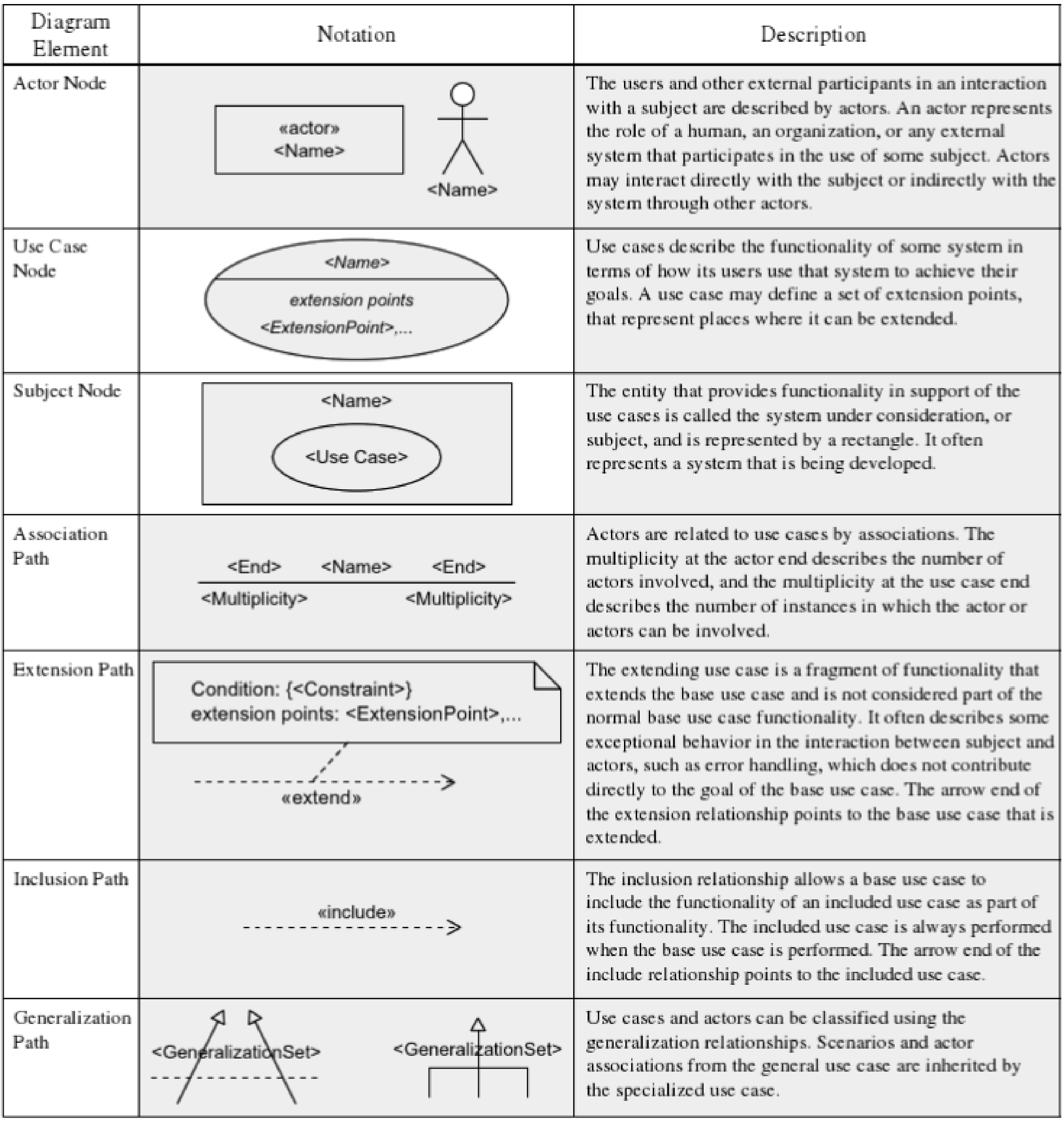


Diagram Element	Notation	Description
Actor Node	«actor» <Name> <Name>	The users and other external participants in an interaction with a subject are described by actors. An actor represents the role of a human, an organization, or any external system that participates in the use of some subject. Actors may interact directly with the subject or indirectly with the system through other actors.
Use Case Node	*<Name>* *extension points* *<ExtensionPoint>,...*	Use cases describe the functionality of some system in terms of how its users use that system to achieve their goals. A use case may define a set of extension points, that represent places where it can be extended.
Subject Node	<Name> <Use Case>	The entity that provides functionality in support of the use cases is called the system under consideration, or subject, and is represented by a rectangle. It often represents a system that is being developed.
Association Path	<End> <Name> <End> <Multiplicity> <Multiplicity>	Actors are related to use cases by associations. The multiplicity at the actor end describes the number of actors involved, and the multiplicity at the use case end describes the number of instances in which the actor or actors can be involved.
Extension Path	Condition: {<Constraint>} extension points: <ExtensionPoint>,... «extend»	The extending use case is a fragment of functionality that extends the base use case and is not considered part of the normal base use case functionality. It often describes some exceptional behavior in the interaction between subject and actors, such as error handling, which does not contribute directly to the goal of the base use case. The arrow end of the extension relationship points to the base use case that is extended.
Inclusion Path	«include»	The inclusion relationship allows a base use case to include the functionality of an included use case as part of its functionality. The included use case is always performed when the base use case is performed. The arrow end of the include relationship points to the included use case.
Generalization Path	<GeneralizationSet> <GeneralizationSet>	Use cases and actors can be classified using the generalization relationships. Scenarios and actor associations from the general use case are inherited by the specialized use case.

A9 Boundaries for the future

Although the focus of the project is the product development process, after the creation of use cases it was possible to make out different boundaries. Those uncertainties, although they should not have direct impact on the approaches used in the different development phases, will have to be takes into account by other stakeholders, implying big challenges for them.

The general limitations found are, among others:

Standards and methods.

As it could be appreciated, most of this works had the standard ISO 26262 Road vehicles-Functional safety as a basis, which is relatively new and updated since it even makes mention of autonomous cars. However, this one is too brief for the upcoming mobility trends to lean on it and hence a new standard more specific for autonomy should be developed in the nearly future, in order to address the issues seen in both theoretical and practical parts of this work. To sum up, the models described on it would be insufficient for the future due to the underlying reason exposed plus the excessive simplification and incomplete knowledge about the reality.

Another key point that would stress the need of new standards is the fact that the mentioned standard is only applicable to electrical and/or electronic, their functional safety and the hazards caused by the malfunctioning behaviour of these systems. This means that other mechanical or software components or hazards caused by/in other components would be outside its scope, fact that might restrict the usage of this standard in the future mobility (not only in connected and autonomous but also in electric cars, since hazards like fire, smoke, corrosion, toxicity, thermal unprotecting, cyber-attacks, too low noise, mechanical damages… would not be considered in this standard as long as they were not originated in an E/E component.

Moreover, after analysing all the challenges and threats related with security and therefore dedicating a use case just for this dependability attribute, it was noticed that as soon as the amount of data generated and processed becomes greater and greater, security problem will also increase in quantity and complexity, and it could be said that the already-existing standards are not prepared for that. Security issues are what safety issues were some time ago, and therefore there is a need to start considering them, also because they go hand in hand with the core aspect of this thesis: safety. It is true that safety is paired with all the other dependability attributes (reliability, availability, maintainability, performability, and testability) in a way that if at least one of them fails, safety is automatically affected, but with security, although nowadays is not the one most relevant, they will definitely be reciprocal: safety breaches might leave room for security attacks, and security problems will jeopardize safety. Therefore a standard or approach that contemplates both at the same time would be desirable.

Infrastructure.

Cities must adapt to new forms of mobility. Starting with shared cars, they need enough and well located key points throughout a city. Electric cars need points to charge the batteries, like conventional cars dispone of fuel stations. Connected vehicles need intelligent infrastructure in order to take advantage of its V2I and V2X features. Autonomous cars, depending on the level of automation, as well as their characteristics, may need some or all the requirements described in the lines above, as well as special precomputed maps. In the future a little further, where cars driven by humans will not exist, maybe it makes no sense to keep the infrastructure and rules subject to conventional traffic to prevent human fallibility or behaviour. In a TED Conference, Wanis Kabbaj suggested a new model of cities and transportation in a driverless world, where instead of 2 dimensions; a third dimension is introduced to increase the efficiency and effectivity of mobility, imitating the nervous system of the human body.

Related with infrastructure, another important key in autonomy are the precomputed maps. It needs to be defined if autonomous vehicles will have the necessity to have separate and special precomputed maps. Other aspects like who will provide them (external companies like Google with its Google maps, each car manufacturers independently, state authorities…) and depend on that, how much they will cost and who will bear the development, maintenance and updates costs have to be stipulated.

Since high levels of autonomous cars will not allow the driver the possibility to take the control of the car, the vehicle will rely completely on the infrastructure and on those precomputed maps, which need to be constantly updating, regarding to the new elements that take action, the state of the roads due to the action of the weather, traffic, topography, public works, the country in which it drives…Since the dependency of the infrastructure will be absolute, this needs to be adapted to the future trends.

Economy and costs.

During this work, the economic aspect has not been taken into account. On the one hand, in the large-scale autonomous cars will imply a huge impact on the global economy. Although the adaption of the already-existing structure and the creation of new one will also pose major costs, it is estimated that self-driving cars could add $7 trillion to the economy by 2050 (Lanctot, 2017,p.5).

On the other hand, on a smaller scale, the cost of the autonomous vehicles will represent an important boundary for consumers. As already seen, self-driving cars rely mainly on three systems: Radar (for detecting objects and their velocities at long distances), cameras (for colour and detail) and last but not least, Lidar (for seeing clearly in 3-D). The fact that these functions, especially Lidar, use high advanced (and therefore expensive) technology, make autonomous cars an expensive item not affordable for everyone.

Driving style.

Although autonomous vehicles are expected to eliminate the car accidents since they eliminate the driver role and therefore his errors, the moral scandal over a single death by a machine will be unavoidable. That means that the autonomous vehicles will be programmed to more probably get hit than to be the hitter ones, having this its advantages (less outrage and scepticism) but also its disadvantages: the extremely conservative driving style. This ultracautious behaviour can make taking wrong decisions such as decelerating, braking or stopping due to false interpretation of other elements approach (for example in overtaking manoeuvres from other vehicles, hampering the traffic flow). Since people will know that they are made for avoiding any type of crash, pedestrians or other drivers may dare, bullying or take advantage of them. In order to avoid that, it should exist some type of policy that penalizes those offenses, and regarding the conservative style, maybe it should not be that much restrained but more accurate in applicable situations. A balance to guarantee a moving traffic always under safe conditions will be needed, but if it these conditions are too extreme, the vehicles will not operate at all

Non-verbal communication.

Autonomous cars must be taught to predict the behavior of human drivers, cyclists, and pedestrians and be provided with subconscious communication ability in order to understand an eye contact, a honking, a turn, gestures from authority or further actors, or other human intentions. While other “human” functionalities can be carried out by sensors that substitute the 5 senses, non-verbal communication constitutes a huge handicap for developers since they have to teach cars the process of communication and its elements: sender/source, receiver/destination, message, channel…and this is very dependent on the age, culture, social status among other factors. Therefore a generalized algorithm that is able to adapt to those factors within different environments is needed.

Amount of scenarios.

When defining the Use Cases in the previous chapter, what all of them had in common was the section Issues, where it was noticed that the quantity of different possible scenarios hampered not only the definition of the use case but also the work of developers and engineers. It is expected that every new scenario will be recorded and added to the lines of code in order to be registered for further similar situations, but it will always be a first time for other new scenarios, whose biggest problem will not be the fact that it is the first time the car has to front that situation but the consequences of that fact.

Legislation.

Different legislation aspects at the state, national and international level need and must be treated not only before the cars take our roads but also before car manufacturers design them. As seen in the use cases, the ethical dilemmas and under which criteria they should make decisions requires a specific law that gives guidelines or models of actuation as well as protection if something happens.

Another legality aspect is related with the authorization for autonomous cars to drive or not in certain states, since nowadays under the current laws, in not every country or state driverless vehicles would be allowed. Also, it will have to be defined in which point, in a long-term future, human-driven cars will not be allowed to drive anymore, even if the most challenging scenario will be when all the different types of mobility interact on our roads.

Insurance companies (if existent) will also have to reconsider their policies in order to readapt to the new trends.

Traffic rules, signals, and regulations will need to be readapted to new forms of mobility/cities, as well as taught to cars in accordance to the country, culture or road conditions in which it is operating. Also, laws against autonomous cars trolling might be considered, as already stated.

As for the processing and protection of data, again the need of a specific law is patent, ranging from who will be the owner of the data (car manufactures, traffic institutions, assurance companies, authorities) to with who, when and with which finality this data can be shared.

Test and validations.

All the mobility forms seen require a lengthy and costly testing phase in order to ensure a total or at least high level of safety before the release. With this, car manufacturers make sure that they have reached an acceptable grade of all dependability attributes, that they record and incorporate different situations experienced to the algorithm, and that they are also accepted legally and socially. For doing that, car makers and other entities might develop test and validation approaches to show their performance or behavioural skills through not only simulations, tests environment and test tracks but also on-road tests. For those tests and validations, all the different parties need to be involved: car manufacturers, pedestrians and other traffic participants, insurance companies, suppliers, traffic entities, standards, and organizations etc.