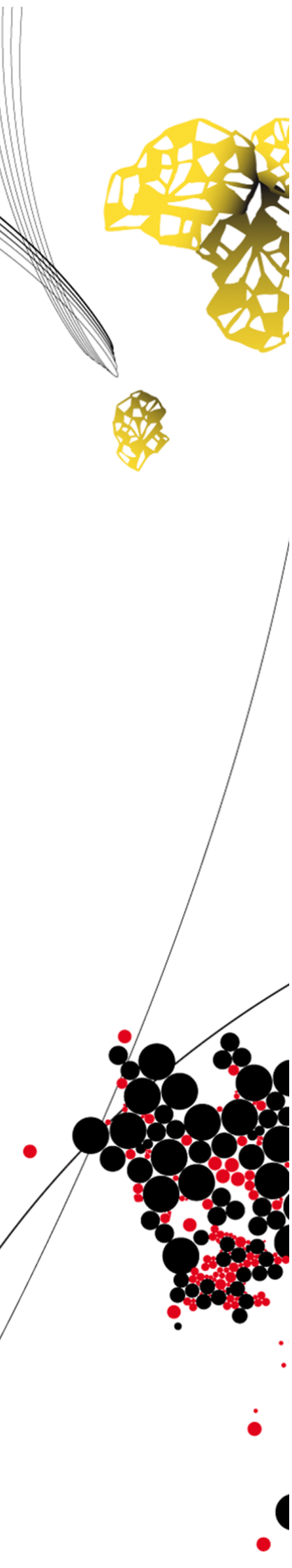

UNIVERSITY OF TWENTE.

Faculty of Engineering Technology,
Mechanical Engineering

Safety by Design

Autonomous Operation and Control:

Autonomous cars

Yusuf Bahar, s1795023
Cesar Nava Rosas, s2348004
Kasper Slagter, s1963252

Group Report - Safety by Design
December 6, 2020

Supervisors:
dr. M. Rajabali Nejad

Mechanical Engineering
Faculty of Engineering Technology,
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands

Contents

Chapter 1

Introduction

In the last decade, the automotive industry has reached improvements in matters of safety, manufacturing reliability, and affordability of vehicles. Due to serious advances in computation and communication technologies, the idea of autonomous cars is being materialized and some prototypes are already been tested covering millions of kilometres [1].

An autonomous car is a vehicle capable of being aware of its surroundings and operate without the assistance of a human being. Moreover, an autonomous car can go wherever a normal car goes and do what an experimented human driver does [2]. However, the jump from a normal car to a fully autonomous vehicle is huge, hence, 6 levels of driving automation were defined by the Society of Automotive Engineers (SAE) as presented in Appendix A [2]. Some of these levels of automation are already present in the automotive industry as driver assistant technologies like automatic braking systems to prevent accidents [3].

The benefits in terms of safety and comfortability are clear, but the highest benefit of autonomous cars is the capability of drastically lower the CO_2 emissions. According to a study of the Institute for Transportation and Development Policy (ITDP) the "Three Revolutions of Human Transportation" in 2050 could reduce traffic congestion (30% fewer vehicles on the road), cut transportation costs by 40%, reduce urban CO_2 emissions by 80% worldwide, among others benefits [4].

Certainly, the benefits of autonomous cars are enormous, but there are still some technical and non-technical issues remaining to solve to achieve a level 5 autonomous vehicle. Software complexity, real-time data analytics, testing and verification, among other technical challenges; but also, consumer stimulation, insurance management, ethical/moral concerns are serious non-technical issues [1]. However, ensuring the safety of autonomous cars must be the main focus and requires a multi-disciplinary approach across all levels of functional hierarchy [5]. The technology applied in autonomous cars must be safe, the different hazards must be addressed, and related control systems need to be developed.

1.1 Assignment organization

This assignment explains the system and safety challenges related to autonomous cars by the development of 5 steps.

The first step developed in chapter 2 defines the system by the application of the safety cube.

The second step developed in chapter 3 defines the safety objectives and the Safety Integrity Level.

Step 3 related to the Identification and mitigation of hazards, as well as step 4 Control of hazards are developed in chapter 4.

Step 5, related to the monitoring of the system is developed in chapter 5. In this chapter, some safety indicators are suggested for the SoI and a plan to influence the safety culture is given.

Finally, in chapter 6 the conclusions are provided.

Chapter 2

Scope definition

Using the Safety cube method, the scope of the system is researched. First a safety cube is set up to define the most important humans,the technical system, the environment and the interactions between these. Next a Design Structure Matrix is set up in which the interactions between different aspects are explored further.

2.1 Safety Cube

In the Safety cube, the six aspects of the system definition are explored. At the diagonal of this table, the stakeholders, technical system and environment is given. The remaining cells show the interactions between those aspects. .

	Human	Technical System	Environment
Human	Car drivers(private and service), passengers, other road users, regulators, insurance companies, service providers, manufacturers, energy suppliers	Steering, controlling, quality and condition control, driving behaviour	Non-verbal communication with other drivers
Technical System	Safety, comfortability, trust, economics	Autonomous car	Sensing equipment, lights, horn
Environment	Traffic regulations, driving signals	Traffic regulations, weather circumstances,	Road, signs and markings, other vehicles, parking, regulations

Figure 2.1: Safety Cube

2.2 Design Structure matrix

Using the information from the safety cube, a Design Structure Matrix was set up. The Humans and Environment are used in the DSM as discussed in the safety cube. The technical system was divided in some subsystems; car, engine, Lidar units (sensors), cameras, radar, global navigational satellite

system and computer. This subdivision would give a better view at how the different subsystems of the car are interacting. The six matrices containing the DSM can be found in Appendix E

By discussing the most important interactions, some assumptions were made. In Human/Human interaction the aspects with the biggest amount of interactions are drivers, either private or by profession. Because of the high amount of interactions, it can be concluded that drivers are the most important stakeholder for the analysis of the system. The interactions in the technical system make clear that most subsystems mentioned only interact with the computer. This is due to the way the matrix was set up with subsystems of the car that ,for most, are subsystems that work together to drive autonomously. Subsystems obvious for a car (e.g. seating, lighting) was taken out of the scope. Interactions between subsystems of the environment are scarce. The majority of the interactions focus on safety of the road. The subsystem weather is an important subsystem as change in weather conditions will interact with roads in such a way that different weather conditions provide different road conditions and thus different driving conditions.

In addition the interactions between different aspects are explained. For Human environment interaction again safety is an important interaction by providing regulations to the drivers. The Technical system/Human interaction the subsystem car has a lot of interaction, as the car provides transportation to drivers but also has to receive maintenance from repair shops. The only interaction the driver still has in the vehicle is that he/she will tell the car the destination and the car will drive here. The Technical system/Environment interactions mainly show interactions of subsystems of the car that are used to scan the environment to make the car knows what is happening around it and can react on that. The Lidar, cameras and radar are all important subsystems for this.

Chapter 3

Safety objectives

3.0.1 Regulations, standards, and level of protection/Safety Integrity Level (SIL)

Until the uprising of autonomous driving technology, vehicle drivers (and pilots, for an aircraft), have been certified with specific licenses that define the vehicles that are operated by drivers. The certification that relates to the automation of the vehicle is for its intended use; obviously, the ability to operate safely without human intervention needs to be rigorously designed, built, verified, and validated for safe operation.

For industrial automation in general, the International Electrotechnical Commission's (IEC) standard 61508 defines the safety integrity level (SIL) using requirements grouped into two broad categories: hardware safety integrity and systematic safety integrity [6]. In similar spirit, the vehicle autonomy uses an ASIL standard ISO 26262 [7], which is derived from the aforementioned ISO 61608 standard. The ASIL, or automotive safety integrity level, is established by performing a risk analysis of a potential hazard by looking at the severity, exposure, and controllability of the vehicle operating scenario [7]. The safety objective for that hazard carries the ASIL requirements. The standard identifies four levels: ASIL A, ASIL B, ASIL C, and ASIL D. ASIL D dictates the highest integrity requirements on the product; ASIL A the lowest.

The application of ISO 26262 is specific to applications for passenger vehicles, motorcycles and commercial motor vehicles, and more specifically to the practice of functional safety. ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E (Electrical/Electronic) safety-related systems, including interaction of these systems [8]. It does not address 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 [8]. Furthermore, ISO 26262 does not address the nominal performance of E/E systems, even if dedicated functional performance standards exist for these systems (e.g. active and passive safety systems, brake systems, Adaptive Cruise Control) [8].

Currently, there are no development standards or a state of the art for automated driving systems since such systems do not yet exist, and furthermore, the solutions that are available lack maturity and are not deployed. Existing standards do not present solutions to some of the most problematic topics of automated driving systems, such as the safety assurance of artificial intelligence (the most relevant algorithms derive from the fields of machine learning and neural networks, human factors and psychology), and the technological capability of the sensory devices used as inputs to the automated driving systems. In July 2019, a coalition of eleven companies, Aptiv, Audi, Baidu, BMW, Continental, Daimler, Fiat Chrysler Automobiles, Here, Infineon, Intel, and Volkswagen — published a whitepaper: "Safety First For Automated Driving" [9]. This document was produced to fill in the

gaps of ISO 26262 and help state, federal and other international agencies develop appropriate rules and regulations. It describes a framework for developing, testing, and validating “safe” autonomous vehicles. The automotive industry presently uses other resources in addition to ISO 26262 to define the safety design of an automated driving system, comprising of different revisions that are updated regularly. The second revision of ISO 26262 has matured to include more rigor and structure to support more complex automotive electronic systems [9]. The recently released ISO/PAS 21448 standard specifies a development process for the analysis, verification and validation of non-faulted scenarios and use cases of a system. However, ISO/PAS 21448 looks only at L1 and L2 automated systems [9]. It was developed to address the level of risk and hazards caused by the intended functionality, including foreseeable misuse [9]. As mentioned, danger stemming from E/E malfunctions of the system is addressed by functional safety using the globally established ISO 26262 standard, whereas danger as a result of deliberate manipulation is assessed from an ISO/SAE 21434 security point of view [9]. Implementing the safety standards ISO/PAS 21448, ISO 26262 and ISO/SAE 21434 would allow the combining of their procedures and methods. Hence, in summary, the safety standards comprising of safety for SAE automation level 1 and 2:

- ISO 26262:2018 Road Vehicles – Functional safety
- ISO/PAS 21448:2019 Road Vehicles – Safety of the intended functionality (SOTIF)
- ISO/SAE CD 21434 Road Vehicles – Cybersecurity engineering

A (preliminary) guideline for safety for SAE Automation Levels 3-5 is proposed by [10] in September 2017, set up by the Transportation Secretary Elaine Chao. It replaces the Federal Automated Vehicle Policy issued in September 2016. The new policy has two sections: Voluntary Guidance for Automated Driving Systems and Technical Assistance to States—Best Practices for Legislatures and State Highway Safety Officials Regarding Automated Driving Systems. The Voluntary Guidance focuses on vehicles with SAE Automation Levels 3-5. The Guidance recognizes that an ADS (Automated Driving System) may have no human driver. The Voluntary Guidance outlines 12 safety elements [10]:

- *System Safety*
  Design safety considerations should include design architecture, sensors, actuators, communication failure, potential software errors, reliability, potential inadequate control, undesirable control actions, potential collisions with environmental objects and other road users, potential collisions that could be caused by actions of an ADS, leaving the roadway, loss of traction or stability, and violation of traffic laws and deviations from normal (expected) driving practices.
- *Operational Design Domain (“ODD”)*
  The ODD defines where (such as roadway types and geographic areas and terrain) and when (under what conditions, such as speed, daylight, and weather limits) an ADS is designed to operate. The vehicle must also be able to move to a condition with minimal risk, such as stopping or returning control to the driver, when the ODD is exceeded.
- *Object and Event Detection and Response (“OEDR”)*
  OEDR is the detection and response by the driver or ADS of any circumstance relevant to the immediate driving task. Based on its ODD, an ADS should be able to deal with control loss; crossing-path crashes; lane change/merge; head-on and opposite-direction travel; and rear-end, road departure, and parking maneuvers.
- *Fallback (Minimal Risk Condition)*
  An ADS should detect that it has malfunctioned or is operating outside the ODD and then notify

the driver to regain control of the vehicle or to return the vehicle to a minimal risk condition independently.

- *Validation Methods*
  Testing may include simulation, test track, and on-road testing. It should demonstrate performance in normal operations, crash avoidance, and fallback strategies.

- *Human-Machine Interface*
  The vehicle must accurately convey information to the driver or operator regarding intentions and vehicle performance. For example, in a Level 3 vehicle, the driver must always be ready for a request to take back driving.

- *Vehicle Cybersecurity*
  Manufacturers and suppliers should minimize safety risks from hacking and should follow industry best practices, including response plans and reporting of incidents.

- *Crashworthiness*
  Occupant protection must continue to meet performance standards, including for new seating and interior designs.

- *Post-Crash ADS Behavior*
  An ADS should return the vehicle to a safe state and location after a crash.

- *Data Recording*
  To promote continual learning, entities engaging in HAV testing or deployment should collect crash data. Crash event data recorders are recommended to collect and store accident data, including ADS status and driver role

- *Consumer Education and Training*
  Education and training of manufacturer representatives, dealers, distributors, and consumers is imperative for safety. Education and training programs should address the anticipated differences in the use and operation of ADSs from conventional vehicles, and the need for drivers to be prepared to take back control in an instant

- *Federal, State, and Local Laws*
  Entities developing ADSs are encouraged, but not required, to publish Voluntary Safety Self-Assessments. In addition to complying with traffic laws, an ADS must also be able to violate a traffic law temporarily when safety demands, such as crossing a double line to avoid a disabled vehicle or a bicycle. An ADS must also be updated as traffic laws change.

To facilitate safety and development of fully autonomous vehicles, NHTSA (National Highway Traffic Safety Administration, USA) issued a Notice of Proposed Rulemaking in December 2016 requiring V2V technology in all cars and light trucks. The proposal contains V2V communication performance requirements for the use of on-board DSRC (Dedicated Short-Range Communications) devices, which will transmit Basic Safety Administration (“BSM”) messages about a vehicle’s speed, heading, brake status, and other information to nearby vehicles and receive the same information from them [10]. Other technologies are permitted if compatible with DSRC [10]. For security reasons, vehicles should contain “firewalls” [10] between the V2V modules and other vehicle modules connected to the data system. Finally, V2V devices should allow periodic software updates. Engineers have been working on specifications for DSRC devices for over a decade. Yet some automakers, wireless carriers, and chip makers believe that cellular systems will better handle V2V communications on future 5G networks [10]. Ultimately, some combination of DSRC and 5G may be used. 5G is not

expected until 2020. DSRC will likely come first [10].

In order to determine the ASIL standards for the additional components of a fully automated car, hence SAE level 4 and 5, some of the key technologies relevant to the development of HAVs (Highly Automated Vehicles) and connected cars include the following; noted should be that Individual systems in a car (airbags, power steering, sensors, etc.) are rated with the ASIL methodology; but overall functional safety of an autonomous vehicle must be rated on a systems basis. Considering the following components deemed for a safe fully autonomous functionality to the car, they are considered a severe hazard if the component fails, however, to define them in the ASIL methodology, the frequency of failure need to be determined, which will be done in Section 4.2.

- Automated automotive technologies, including automatic parking and braking systems and automotive engine control circuitry.
- Collision-avoidance technologies, including blind spot detection and lane control systems.
- Digital cameras, including the capture of analog images, conversion to digital signals, processing of those signals for display on a screen, and image processing algorithms for object detection.
- LiDAR and radar.
- Telecommunications, including DSRC technology for V2V communications and 5G.
- Artificial intelligence and machine learning, including cybersecurity for vehicles and object detection and characterization in digital images.
- Sensors and mesh networking technology, including distributed sensor networks and weight-sensing technologies.
- Diagnostic trouble code, data analytics, and telematics.

3.0.2 History of accidents

The recorderd safety data on SAE level 4 accidents is scarce. As of June 27, 2019, the California DMV has received 167 Autonomous Vehicle Collision Reports [11]. Google-Waymo has most mileage recorded and is thus of more interest than other company reports (DMV 2019). The data from Googles-Waymo cars is collected from the period 2009 to end of 2015. In the report [12], it is found that there were three police reportable accidents in California while driving 2,208,199 km, giving an accident rate of 1,36 police reportable incident pr. million km. This is 1/3 of reportable accidents of human-driven passenger vehicles in the same area. Tests with autonomous cars conducted in California by Google-Waymo have shown that 19 out of 21 accidents that the autonomous cars were involved in, were caused by expectation violations done by humans [12] [13]. These 19 rear-end accidents all occurred at signalized intersections, where the driver in the manually driven car behind expected the google vehicle to proceed on yellow light, but where the google car was programmed to stop. To solve this problem Google-Waymo has taken patent on the dilemma zone, estimating own speed, distance to stop line distance, length of the junction and time to pass, thus estimating if it is possible to pass the stop line on yellow light without violating rules of the road. 3.1 shows the reported accidents resulted in crashes for SAE level 2-4.

[14] [15]. There are few notable cases were accidents were caused by SAE level 4 and 5 situations.

Table 3.1: History of significant accidents for SAE level 3-5

Uber accidents *(SAE level 3)*

Date	Country	No. of fatalitites	System produce	Vehicle	Accident
18.03 2018	USA	1	Uber	Volvo (Refitted)	Pedestrian fatality

Tesla Autopilot accidents *(SAE level 2)*

Date	Country	No. of fatalities	System produce	Vehicle	Accident
20.01 2016	China	1	Tesla autopilot	Model S	Driver fatality
07.05 2016	USA	1	Tesla autopilot	Model S	Driver fatality
23.03 2018	USA	1	Tesla autopilot	Model X	Driver fatality

Google-Waymo *(SAE Level 4)*

Date	Country	No. of fatalities	System produce	Vehicle	Accident
29.02 2016	USA	1	Google Waymo	Lexus (Refitted)	Small collision with bus

Google did not claim responsible in all cases other than the February 2016 incident, stating that the vehicle itself was never at fault because the cars were either being manually driven or the driver of another vehicle was at fault [11]. Hence, although Google initially blamed other drivers for past collisions during testing, it accepted and claimed (partial) responsibility for one collision in 2016. On February 14, 2016, while creeping forward to a stoplight, a Google self-driving car Waymo attempted to avoid sandbags blocking its path, and during the maneuver, it struck the side of a bus [11]. The statement Google brought out was: ”In this case, we clearly bear some responsibility because if our car hadn’t moved there wouldn’t have been a collision”.

From media and public accident reports, there has been 4 (reported) fatal accidents worldwide (C1 Level). Three with semi-automated (SAE level 2) autopilot and one with a more fully automated vehicle on public roads (SAE level 3). This is the Uber accident in Arizona where a Volvo refitted with Uber self-driving technology killed a pedestrian in 2018 [11]. In all cases the autopilot was engaged, but without driver interaction or intervention with vehicle controls [11].

Tesla with their Autopilot has enabled automated driving at high speeds. Several serious accidents with Tesla autopilot have led Tesla to alter and limit their autopilot functionality. These partially automated vehicle systems on SAE Level 2, with temporary longitudinal and lateral assistance, are currently offered for series-production vehicles, but exclusively based on an attentive driver being able to control the vehicle [11]. The incidents that are known/reported, caused by vehicular component failure or infrastructure components are presented in Table 3.2.

3.0.3 Safety-critical functions of the ADS

Many topics of ADS concern with the functional level to replace single driver tasks with additional ADS functions. Next to that, there are issues that need to be covered are the basic actuation functions, such as accelerating, braking and steering, to implement the required autonomous vehicle movement. As of now, (non-autonomous) vehicles provide function-specific assistance for the human driver such as force support in braking systems by a hydraulic or an electro-mechanic brake [17]. However, systems for automated driving functions need to be improved to support the fully required brake force without a human driver. Furthermore, the safety concepts of existing systems must be updated because the ECU (Electronic Control Unit) (e.g. of the steering system) needs to detect any

Table 3.2: Amount and percentage of incidents with the responsible system failure [16]

System Failure	Description	No. of Incidents	Percentage of Incidents
Hardware system	Hardware discrepancy, issue with tuning and calibration, and unwanted maneuver	288	17.8439
Software system	Software discrepancy and unable to detect vehicle or obstacles	80	4.9566
Communication system	Planner data not received, drop off on received data, communication evaluation management failure	642	39.777
Nonautonomous vehicle crashes	Nonautonomous vehicle behaviors at low penetration level of autonomous vehicles	68	4.3131
Wrong command	Human uncomfortable to continue automation	487	30.1735
Construction zones	Signs, hand signals, lane closures, and sudden reduction of speed represent the construction zone scenarios	31	1.9207
Road conditions	Lane marking and adverse road surface conditions	111	6.4125
Weather	Rainy, sun glare, twilight, cloudy: poor sunlight conditions and nighttime are considered here.	18	1.1152

kind of malfunction and their effects have to be mitigated, because without a driver the system has to monitor, decide and react on its own [17]. Also, what needs to be taken account, is that different vehicle functions share the same sensors and actuators and all functional and technical condition has to be met. On a system level, the additional functions specific automated driving:

- Low speed automated driving
- High speed automated driving
- Collision avoidance
- Collision mitigation
- Co-operative manuevering

Another function that needs to be adressed is Eco-manuevering. However, the latter one does not influence safety standards and hence is not safety critical.

Chapter 4

Hazards

In this section, the hazards applying to the system of interest automated cars are identified, assessed, and evaluated according to the Safety by Design process [18]. According to the International Standard for the safety of machinery (ISO 12100) [19] a Hazard is a “Potential source of harm”, based on this definition the Safety by Design process was followed. Moreover, as previously mentioned, the only systems analyzed were the ones related to automated functions in the car, other common functions of regular cars were not considered.

4.1 Identification of hazards

The first step was to identify the potential functional, technical, and operational hazards in the environment, system, and subsystems levels within automated cars as presented in Appendix C. The functional hazards were related to the functions, expectations, and needs of the stakeholders previously identified. Furthermore, the technical hazards were associated with technical aspects of the different levels without the consideration of human interactions. In addition, past, present, and future hazards of automated vehicles were considered, however, no particular distinction in provided. Finally, the operational hazards were linked to the regular utilization of automated cars.

Moreover, the hazards identified were based on past events and scenarios previously discussed in addition to the present challenges the industry is facing.

In addition, all the hazards were identified with specific sequence characters (1,2,3...;a), b), c)...I, II, III...) according to their classification for further utilization.

4.2 Fault tree analysis (FTA) and probability

The fault tree analysis method was used to estimate risk based on the results presented in [16]. Two fault tree models based on the outcomes of the risk identification phase were developed. One is related to the autonomous vehicle failure related to vehicular components (Appendix B, Figure B.2), the other FTA is related to the failure of autonomous vehicles related to infrastructure (Appendix B, Figure B.1). It is interesting to seek and determine the minimal cuts for failure probabilities, which are indicated in Table 4.1.

The typical lifetime of a conventional vehicle is about 150,000 miles. This information can be integrated to calculate the autonomous vehicle failure probability per mile. Given that the overall probability of autonomous vehicle failure related to vehicular components is 14.22%, which means that autonomous vehicle operations could be stopped 14.22 times during the vehicle’s lifetime.

It was found that the failure of the communication system could be the most vulnerable event of all of the basic events; the failure probability is 9.513%. Hardware system failure, which is caused by sensitive sensor and actuator failures, was found in the second position with a failure probability of 4.249%. The failures due to infrastructure components, are presented as well. Noted should be

Table 4.1: Minimal cuts of FTA related to failure due to vehicular components and infrastructure.

Minimal cut-sets (vehicular components)	**Failure probability (%)**
Failure of communication system	9.513
Hardware system failure	4.249
Software system failure	1

Minimal cut sets (infrastructure)	**Failure probability (% per mile)**
Nonautonomous vehicles crashes	0.0134
Weather	0.0022
Passenger and vehicle interaction platform (wrong command)	7.4200 x 10^{-4}
Road condition	6.5600 x 10^{-5}
Construction zones	7.6264 x 10^{-6}
Cyclists	4.0897 x 10^{-6}
Pedestrians	2.9337 x 10^{-6}

the percentages in miles, converting these with estimated 150,000 miles in a lifecycle yields a high (frequent) probability of incidents due to non-autonomous vehicle crashes and weather.

4.3 Risk assessment

The next step was the assessment of the risks according to the military safety standard MIL-STD-882E [20]. For this, the severity and frequency of occurrence of the previously identified hazards were paired according to the categories presented in Figure D.1 and Figure D.2 contained in Appendix D.

Following this, the hazards were collocated in the risk assessment matrix as shown in Figure 4.1, where the color red indicates high risk, orange a serious risk, yellow medium, green low, and blue eliminated (no risk).

	Catastrophic (1)	**Critical (2)**	**Marginal (3)**	**Negligible (4)**
Frequent (A)		II, III		
Probable (B)		a)	d), e), j), k), o), s), t), VI, VII	
Occasional (C)		10, b)	3, 5, 7, 9, c), g), p), I,	2
Remote (D)		4, 12	6, 13, h), q), r), IV, V, VIII	u)
Improbable (E)	11		8, m), n)	f), i), l)
Eliminated (F)	1			

Figure 4.1: Risk assessment matrix of automated cars

4.4 Control of hazards

After assessing the risks, actions were considered to eliminate the hazards. However, in the cases that the hazard was not possible to be eliminated, the reduction of frequency of it was aimed. Moreover, if those two options were not possible, the isolation of the hazard was targeted by the use of other resources or inform the user about this.

4.4.1 High risks (red)

The priority of the hazards to be attended are the ones with the highest risks. In this category, probable (B) and frequent (A) critical (2) risks were identified and were addressed as follows.

- **Slippery roads compromising the response of system or subsystems** $\{a)\}$**:** This hazard cannot be eliminated, however, the risk can be reduced by communicating to the driver that the system or subsystems performance has been compromised so he/she can take control of the vehicle or execute automated protocols to return the vehicle to minimal risks conditions.
- **Inexperienced or uneducated drivers** $\{II\}$**:** Again, this hazard cannot be eliminated, nonetheless, it can be reduced by upgrading the current driving regulations to address the interaction with automated vehicles. Moreover, proper training can be provided to drivers by the automated car manufacturers on how to use these vehicles as well as providing guidelines for usage.
- **Interaction with other reckless vehicle drivers** $\{III\}$**:** This hazard can be reduced as well as the previous one by upgrading the current regulations and providing training to the current drivers. Also, implementations of V2V systems can help avoid incidents caused by human error.

4.4.2 Serious risks (orange)

In this section of risks, most of the hazards were concentrated in the category of probable (B) marginal (3) with the most hazards detected and one in the category of occasional (C) critical (2). These hazards were addressed as follows.

- **Poorly process yellow lights considering the distance, speed, and other factors to avoid collisions with other drivers behind** $\{d)\}$**:** This hazard can be eliminated by upgrading the software of the automated vehicle with improved algorithms to better mitigate the speed of the vehicle, distance to the stoplight, length of the junction, and time to pass resulting in a better decision of when to pass the stoplight in yellow without violating traffic rules and regulations.
- **Not able to interact with other vehicles and share information to avoid accidents** $\{e)\}$**:** This hazard can be eliminated by making regulations towards the share of data among automated cars regardless of the manufacturer for a common good.
- **Limitations of reacting to rear-end type of collisions** $\{j)\}$**:** This hazard can be eliminated as well by upgrading the software of the automated vehicles with improved algorithms to better address this situation and to implement more sensors and cameras in the rear part of the vehicle. Moreover, this hazard is influenced by the interaction with other drivers as well, therefore, more training and updating regulations must be considered to reduce this hazard.
- **No response of the system when a strange object or event is detected (e.g. emergency vehicles approaching and clear the road to allow their pass)** $\{k)\}$**:** This hazard also can be eliminated by upgrading the software and improving the algorithms to address this hazard.

However, this is expected that would not be done completely in one step but progressive since the complexity of this scenario is high.

- **Not violate traffic laws when required (e.g. avoid emergency vehicles when approaching)** $\{o)\}$**:** This hazard also can be eliminated by upgrading the software and improving the algorithms to address this hazard.
- **No detection of objects or events that are not common** $\{s)\}$**:** This hazard also can be eliminated by upgrading the software and improving the algorithms to address this hazard. Moreover, this hazard in some cases will require an upgrade in hardware systems to extend the range of the current sensors, cameras, among others.
- **Limitations of detecting to rear-end type of collisions** $\{t)\}$**:** This hazard also can be eliminated by upgrading the software and improving the algorithms to address this hazard. Moreover, this hazard may require an upgrade in hardware systems as well to extend the range of the current sensors, cameras, among others.
- **Lack of knowledge to operate the system and the scope of the system by the driver** $\{VI\}$**:** This hazard cannot be fully eliminated, therefore, it will be reduced by providing proper training to drivers by the automated car manufacturers on how to use these vehicles as well as providing guidelines of usage.
- **Lack of knowledge to operate the subsystems by the driver** $\{VII\}$**:** Hazard cannot be fully eliminated, hence, it will be reduced by providing proper training to drivers by the automated car manufacturers on how to use these vehicles as well as providing guidelines of usage.
- **Malfunctioning or failure of sensors, cameras, radars, GNSS** $\{10\}$**:** This hazard can be eliminated by applying the same logic as in the airplane industry with parallel or redundant systems which take control over when this hazard is present.
- **Road, signs, obstacles, other vehicles or pedestrians not detected due to low visibility in intense weather conditions** $\{b)\}$**:** Can be eliminated by communicating to the driver that the system or subsystems performance is not operating properly so he/she can take control of the vehicle or execute automated protocols to return the vehicle to minimal risk conditions.

4.4.3 Medium risks (yellow)

The medium risks have the most hazards paired with the functional ones as the most common type. In this category, occasional (C) marginal (3), remote (D) critical (2) and marginal (3), improbable (E) catastrophic (1) and marginal (3) hazards were related. The hazards $3, 4, 10, 6, 13$, and 11 can be eliminated by applying the same logic as in the airplane industry with parallel or redundant systems which take control over when these hazards are present. Moreover, hazards $5, 7, 9, g), p), 12, h), q), IV, 8, m)$, and $n)$ can be eliminated by upgrading the software and improving the algorithms to address this hazard. However, in the case of hazards $p)$ and $h)$ this is expected that would not be done completely in one step but progressive since the complexity of these scenarios is high. Furthermore, some of the hazards need extra actions. Hazards $5, 12$, and $n)$ will require an upgrade in hardware systems as well to improve their capacities or extend their range. Hazard $m)$ can also be eliminated with parallel or redundant systems that take control over when this hazard is present. Hazard 8 can be complemented by implementing an independent “master switch” to stop the automated assistances. In the case of Hazard IV, the upgrades in the software are considered to be able to execute automated protocols to return the vehicle to minimal risks conditions. Finally, the

upgrade for hazard 7 can be to communicate the driver that the system or subsystems performance has been compromised so he/she can take control of the vehicle or execute automated protocols to return the vehicle to minimal risk conditions.

Furthermore, hazards V and $VIII$ can be eliminated by communicating to the driver that the state of the systems or subsystems has changed when occurs. In addition, hazard $r)$ can be eliminated by only letting trained and certified personal deal with the placement of the hardware when repairs had been performed. In the case of hazard $c)$, this cannot be fully eliminated, therefore, it will be reduced by providing proper training and certifications to repair shops by the automated car manufacturers on how to address these vehicles' malfunctions or repairs. Moreover, the information on the certified repair shops that can address the problems in the vehicle must be provided to the driver or the owner responsible for the vehicle.

Finally, hazard I cannot be eliminated and requires different parties to reduce its frequency. First of all, the cities must be actively involved in the maintenance of the signs, roads, among others to ensure their integrity. This also can be improved by applying new regulations and education programs to avoid the vandalization and abduction of the signs. Moreover, the software can be upgraded and the algorithms can be improved to better detect these signs and road marks with a certain level of damage or alterations. Furthermore, the algorithm could save the location in the system's data records to remember the signs in case they are later compromised, this software must be capable of updating its data records in case of new signs or marks are changed in those areas by the cities or federal administrations.

4.4.4 Low (green) and eliminated risks (blue)

In the case of the low risks, these can be eliminated by the previous actions already described in the medium and severe risks. These actions include upgrading the software and hardware, communicate the issues to the driver, and utilize parallel systems as in the airplane industry. Finally, the only eliminated risk (no risk) detected was in the hazardous situation of the driver and passengers not protected by regular safety standards due to new settings or design. This since automated cars first need to meet regular car regulations which ensure those safety standards to be met.

4.5 Evaluation of solutions

In general, few solutions apply to most of the possible hazards identified. Since most of them are the upgrading of the software (sometimes hardware as well) and improving the algorithms, these can be achieved by the car manufacturer or developer with a relatively small effort applied. However, in some situations, the complexity of the hazards is considerably high that the efforts and resources applied for this solution are not enough or simply the technology available does not allow this. The good news about this is that the technology available is increasing exponentially each year and these solutions would be able to be addressed soon if they are not being or already addressed now.

Moreover, utilizing parallel or redundant systems is not a state-of-the-art solution, as previously mentioned, these are implemented in many systems and subsystems in the aviation industry. However, the difference between the aviation and automotive industries in matters of resources and price per unit is big. It would also be affordable/viable in a near future with technological advancements.

Finally, the solutions involving education to drivers and improvements in regulations are the hardest ones, and unfortunately, the ones with the highest risks. A big effort from third parties such as the government and the people is crucial to overcome these hazards. Fortunately, these solutions are being driven by the advancements in the technology related to automated cars.

Chapter 5

Monitor system

To measure the safety of a system, safety indicators can be applied. These indicators are tools used to measure the safety performance of a system by measuring the total end result of the safety, as well as the prevention of accidents and incidents. These indicators can be divided into lagging or leading indicators [21]. Lagging indicators define the safety by measuring accidents from the past. In the case of autonomous vehicles this would for example include the amount of collisions of the cars. These indicators give a total overview of how well the safety of the system actually is. Leading indicators on the other hand focus on future safety performance by measuring activities and events which prevent accidents. These leading indicators have the advantage that accidents do not have to happen to measure the safety.

For the case of an autonomous car, the amount of accidents and incidents are a measurement which can be used to define the safety of the car. The subsection 3.0.2 shows some important lagging indicators, namely the amount of collisions, the amount of accidents caused by human and the amount of accidents caused by the system. These indicators can be specified further to give an exact overview of the accidents. Ideas for this are the amount of accidents involving (fatal) injuring and the amount of (fatal) injured road users/cyclists/pedestrians. Another indicator that could be of importance are the amount of violations of the regulation (e.g. speeding, not stopping at crossings). These indicators give a total result overview of how safe the autonomous car actually is.

The high risks from subsection 4.4.1 show that slippery roads can cause hazardous situations. Some safety indicators could be provided to measure the actual safety when driving over these roads. A leading indicator would in this case be the friction between the road and the car wheels. By measuring this, the car can react to the change in friction, preventing accidents. A lagging indicator that could also be introduced for this case is the amount of accidents happening under specific weather circumstances, such as rain or snow.

The other two high risks mentioned in subsection 4.4.1 can be measured again by monitoring the amount of accidents caused by humans. A leading indicator that could be added specifically for these risks is measuring the amount of training a user is provided with before driving the vehicle. With this, possible accidents can be avoided and thus increase safety.

Safety indicators for usual cars nowadays have some specific fields: Alcohol and drugs, speed, protective systems and daytime running light [22]. Independent of the car being autonomous or not, these indicators will stay important. The driver should still not be allowed to drive while drunk, speed limits should be tolerated, seat belts should be applied and light should work. Next to these, already used indicators, for autonomous vehicles the earlier discussed indicators would add a better view of the safety and it therefore be suggested to add these to the already existing safety indicators.

Chapter 6

Conclusions

Despite the efforts already made to provide safety standards to autonomous vehicles, there is still room for improvement. Current standards such as ISO 26262 needs to mature and revised to keep up with the most problematic topics of automated driving systems, such as the safety assurance of artificial intelligence and the technological capability of the sensory devices used as inputs to the automated driving systems. Hence, it is crucial to keep developing safety regulations and standards for autonomous vehicles from level 3 to 5. Furthermore, the data of accidents and failure probabilities suggest there risks are mostly based on infrastructure rather than failure of vehicular components. The highest risk comprises of crashes resulting from reckless driving, tiredness and distractions of human operators in non-autonomous vehicles. By implementing upgraded V2V communications, incidents with non-autonomous vehicles (responsible for highest frequency of failure with 0.0134% per mile) can be reduced, hence failure due to human error can be prevented more. For this, the technological advancement of V2V modules is of essence, where it is expected that cellular systems will even better handle V2V communications on future 5G networks. By using this technology, visual, tactile, and audible alerts—or, a combination of these alerts— can be send to alert drivers. These alerts allow drivers the ability to take action to avoid crashes with the fully autonomous vehicle. Vehicular component failure of the ADS (telecommunication failure, hardware failure) can be reduced by addressing protocols and working together with the car manufacturing companies and third parties. Moreover, some guidelines are already proposed to help state, federal and other international agencies develop appropriate rules and regulations. The solution to the hazards still require new technological advances, however, this will not be a long period problem since the technological improvements are expected to grow fast.

Bibliography

[1] R. Hussain and S. Zeadally, "Autonomous cars: Research results, issues, and future challenges," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1275–1313, 2019.

[2] What is an autonomous car? [Online]. Available: https://www.synopsys.com/automotive/what-is-autonomous-car.html

[3] Automated vehicles for safety. [Online]. Available: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety

[4] (2017) Three revolutions in urban transportation. [Online]. Available: https://www.itdp.org/2017/05/03/3rs-in-urban-transport/

[5] P. Koopman and M. Wagner, "Autonomous vehicle safety: An interdisciplinary challenge," *IEEE Intelligent Transportation Systems Magazine*, vol. 9, no. 1, pp. 90–96, 2017.

[6] "IEC 61508 overview report," *exida*, January 2, 2006.

[7] (August 15, 2019) Vehicle autonomy is an automation challenge. [Online]. Available: https://www.arcweb.com/blog/vehicle-autonomy-automation-challenge

[8] (Jan 1, 2019) Nen-iso 26262-1:2019 en. [Online]. Available: https://www.nen.nl/en/nen-iso-26262-1-2019-en-254499

[9] Aptiv, Audi, Baidu, BMW, Continental, Daimler, Fiat Chrysler Automobiles, Here, Infineon, Intel, and Volkswagen, "Safety first for automated driving."

[10] J. Day, "Legal issues related to the development of automated, autonomous, and connected cars," November 2017.

[11] S. O. J. Gunnar Deinboll Jenssen, Terje Moen, "Accidents with automated vehicles - do self-driving cars need a better sense of self?" *26th ITS World Congress, Singapore*, October 2019.

[12] E. Teoh, "Rage against the machine? google's self-driving cars versus human drivers," *Journal of safety science 63 (2017) 57-60. Elsevier.*, 2017.

[13] F.M. Favarò, N. Nader, S.O. Eurich, and M. Tripp, "Examining accident reports involving autonomous vehicles in california," *Epub*, 2017.

[14] Wired. (February 2016) Google's self-driving car caused its first crash. [Online]. Available: https://www.wired.com/2016/02/googles-self-driving-car-may-caused-first-crash/

[15] L. A. Times. (February 29, 2016) Passenger bus teaches google robot car a lesson. [Online]. Available: https://www.latimes.com/local/lanow/la-me-ln-google-self-driving-car-bus-collision-20160229-story.html

[16] P. Bhavsar, P. Das, M. Paugh, K. Dey, and M. Chowdhury, "Risk analysis of autonomous vehicles in mixed traffic streams," *Journal of the Transportation Research Board*, 2017.

[17] D. W. H. Martin, K. Tschabuschnig, “Functional safety of automated driving systems: Does iso 26262 meet the challenges?” *Springer*.

[18] M. R. Nejad, *Safety by Design, Engineering Products and Systems*, 2020.

[19] E. C. F. STANDARDIZATION, *Safety of machinery — General principles for design — Risk assessment and risk reduction (ISO 12100:2010)*, January 2011.

[20] D. of Defence, *Military Standard Practice MIL-STD-882E*, May 2012. [Online]. Available: https://assist.dla.mil

[21] (April 24, 2020) A short guide to leading and lagging indicators of safety performance. [Online]. Available: https://ergo-plus.com/leading-lagging-indicators-safety-preformance/

[22] A. Hakkert, V. Gitelman, and M. Vis, “Road safety performance indicators: Theory. deliverable d3.6 of the eu fp6 project safetynet.” *European Commission*.

Appendix A

SAE automation levels of vehicles

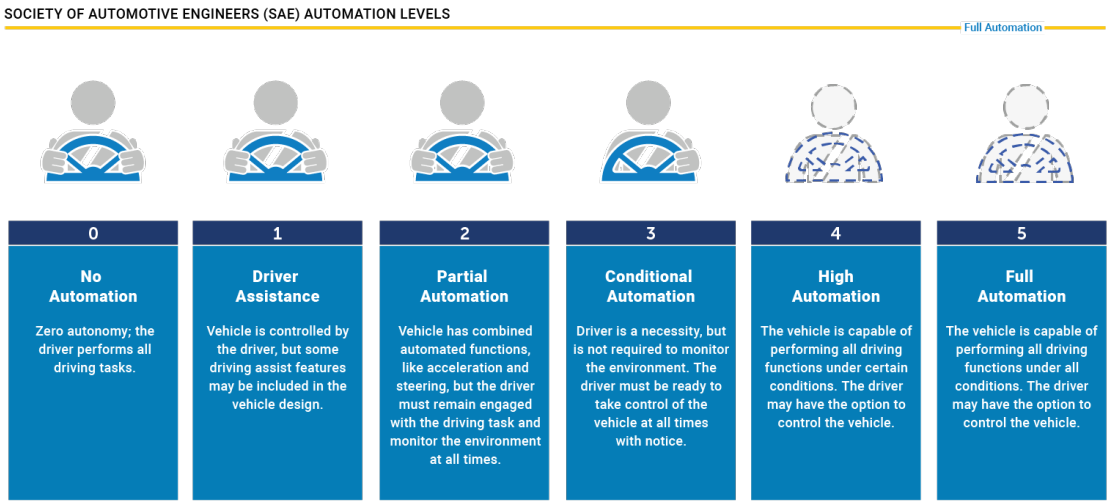

Figure A.1: SAE automation levels of vehicles

Appendix B

Fault tree analysis and probability analysis

Table B.1: Failure related to vehicular components

Event	Description	Failure probability (%)
Lidar failure	Laser malfunction, mirror motor malfunction, position encoder failure, overvoltage, short-circuit, optical receiver damages	10
Radar failure	Detection curves drawn with respect to signal and noise ratios	2
Camera failure	Foreign particles, shock wave, overvoltage, short-circuit, vibration from rough terrain, etc.	4.95
Software failure	System had to generate outputs from array definition language statements	1
Wheel encoder failure	Encoder feedback unable to be transferred, which can cause loss of synchronization of motor stator and rotor positions	4
GPS failure	Real-life tests performed with high-sensitivity GPS in different signal environments (static and dynamic) for more than 14 h	0.9259
Database service failure	Using new empirical approach, connectivity and operability data of a server system were collected.	3.86
Communication failure	Wi-Fi: Periodic transmission of 1,000-byte frames (average conditional probability of success after previous success considered)	5.125
Integrated platform failure	A two-state model with failure rates was developed to estimate the computer system availability	5.88
Human command error	Three data sets of over 115 months from NASA were analyzed and then validated by three methods (THERP, CREAM, and NARA) to facilitate NASA risk assessment.	2
System failed to detect human command	System unable to detect the accurate acoustic command; driver inputs the wrong command, and system unable to detect wrong commands	0.053

Table B.2: Failure probability relarted to infrastructure components

Event	Description	Number of Crashes (per 100 million miles)	Failure probability (% per mi)
Nonautonomous vehicles crashes	Crashes resulting from reckless driving, tiredness, hardware and distractions considered	133,901	0.0134
Cyclists	Daily 9 million bike trips made; crashes that cyclists were responsible for are included here	3,090	4.0897 x 10ˆ-6
Pedestrians	Crashes with pedestrians at fault for the annual 42 billion walking trips	8,625	2.9337 x 10ˆ-6
Construction zones	Among all work zones, 41.33% of crashes were rear-end crashes.	36,208	7.6264 x 10ˆ-6
Weather-related incidents	Adverse weather conditions such as fog, mist, rain, severe crosswind, sleet, snow, dust, and smoke	22,375	0.0022
Road conditions	Crashes related to improper lane marking and pavement conditions	656	6.5600 x 10ˆ-5

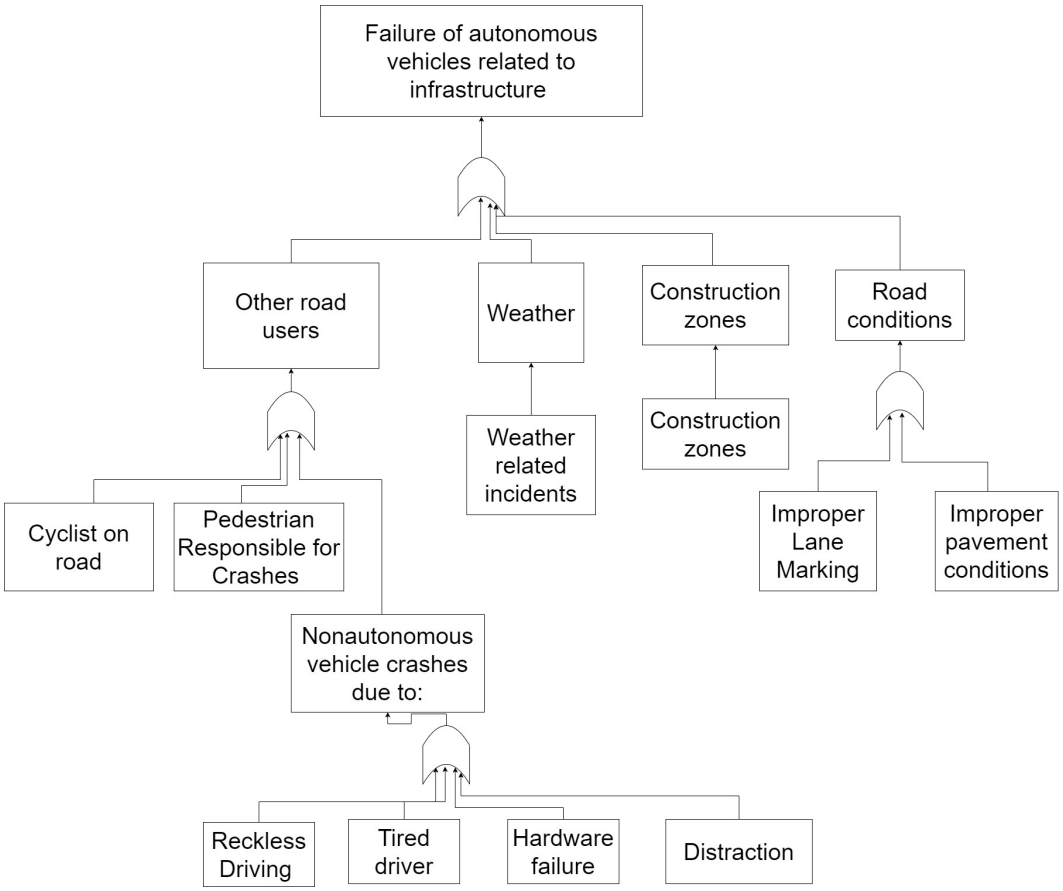

Figure B.1: Fault Tree Analysis of autonomous vehcicle failure related to infrastructure *Image made with draw.io*

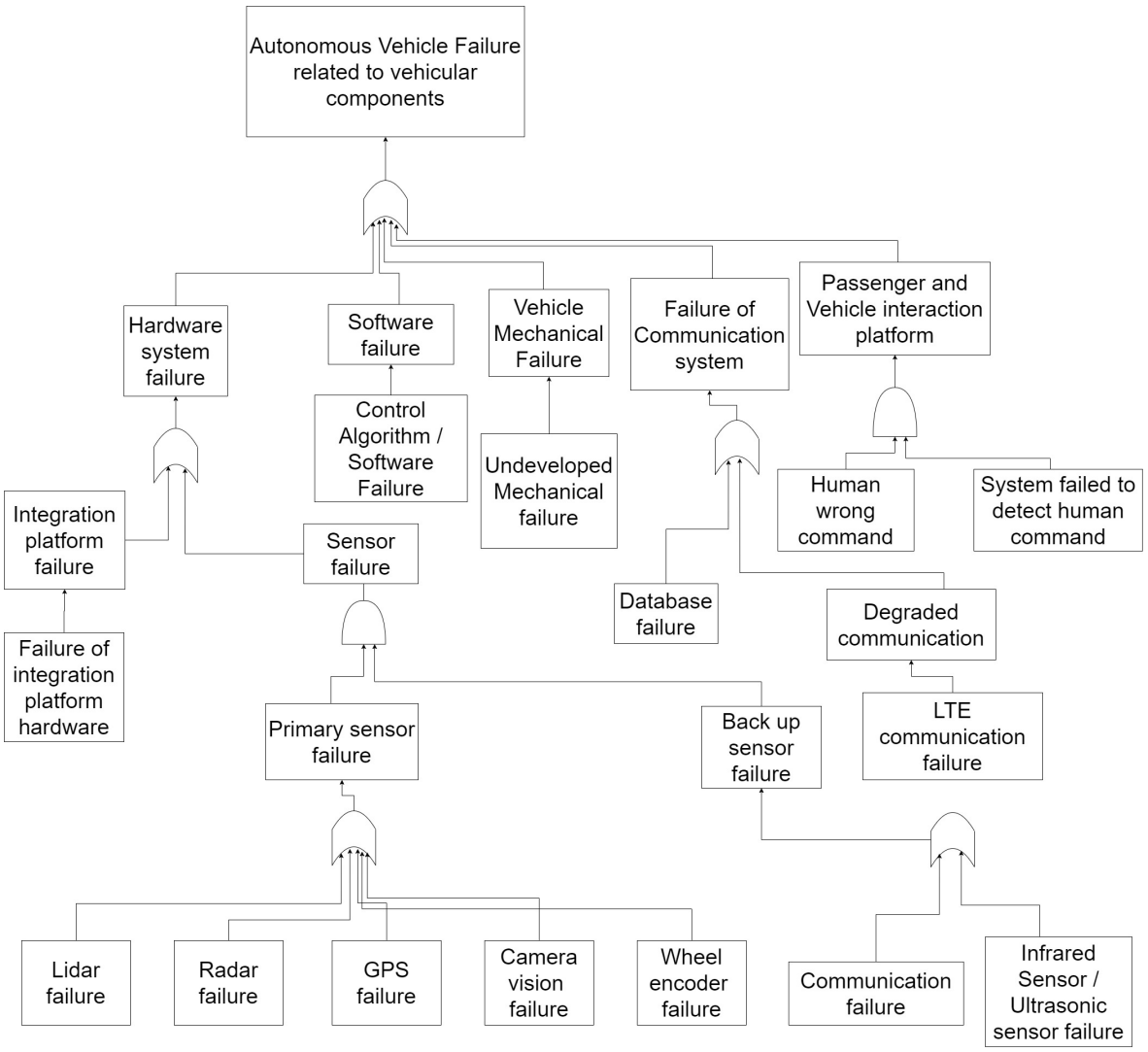

Figure B.2: Fault Tree Analysis of autonomous vehcicle failure related to vehicular components *Image made with draw.io*

Appendix C

Identified hazards in automated cars

Environment	System	Subsystems
1. Driver and passengers protection not met by regular safety standards due to new seatings or design 2. The temperature of the environment above or below the operational use of the systems	3. Malfunction or failure of the computer (controller of subsystems) 4. Malfunction or failure of safety protocols (after an accident or in an unusual situation handing over the control to the driver or relocate the vehicle to a safer area) 5. Data not processed (e.g. images, conversion of signals, etc.) 6. Malfunctioning or failure of low and high speed automated driving 7. Not able to mitigate collisions 8. Not able to stop automated assistance or driving 9. No ability to detect malfunctions	10. Malfunctioning or failure of sensors, cameras, radars, GNSS 11. Malfunction or failure of collision avoidance technologies such as blind-spot detection and lane control systems 12. Automated subsystems not able to apply the required force needed to actuator systems such as braking and steering 13. Malfunction or failure of automated technologies such as automatic parking and braking systems, automotive engine control circuitry

Figure C.1: Functional Hazards

Environment	System	Subsystems
a) Slippery roads compromising the response of system or subsystems b) Road, signs, obstacles, other vehicles or pedestrians not detected due to low visibility in intense weather conditions c) Bad repairs are done to the car due to unexperienced repair shops or lack of training available d) Poorly process yellow lights considering the distance, speed, and other factors to avoid collisions with other drivers behind e) Not able to interact with other vehicles and share information to avoid accidents	f) Damaged of the computer due to its location (not enough protected) g) The system is not designed to address possible malfunctions or failures of subsystems or the system in general h) The software of the system hacked or compromised i) The system not updated with the necessary upgrades j) Limitations of reacting to rear-end type of collisions k) No response of the system when a strange object or event is detected (e.g. emergency vehicles approaching and clear the road to allow their pass) l) Not able to communicate accurately the actual information of the systems and car state m) Data collection compromised n) Process of actions not fast enough to avoid collisions o) Not violate traffic laws when required (e.g. avoid emergency vehicles when approaching) p) The response of the car according to what is detected but causes a bigger accident q) Not able to communicate malfunctions to driver	r) Sensors, cameras, radars, GNSS misplaced or loose s) No detection of objects or events that are not common t) Limitations of detecting to rear-end type of collisions u) Subcomponents did not design to withstand operational conditions (temperature, weather, etc.)

Figure C.2: Operational Hazards

Environment	System	Subsystems
I. Compromised signs, road marks that not allow the correct identification by the computer II. Inexperienced or uneducated drivers III. Interaction with other reckless vehicle drivers	IV. Driver does not take control of the vehicle when needed (system compromised) V. Accidental deactivation of automated help by the driver VI. Lack of knowledge to operate the system and the scope of the system by the driver	VII. Lack of knowledge to operate the subsystems by the driver VIII. Accidental (des)activation of specific automated components by the driver or passengers

Figure C.3: Operational Hazards

Appendix D

Hazard mitigation categories

SEVERITY CATEGORIES		
Description	**Severity Category**	**Mishap Result Criteria**
Catastrophic	**1**	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.
Critical	**2**	Could result in one or more of the following: permanent partial disability,injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than $10M.
Marginal	**3**	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M.
Negligible	**4**	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $100K.

Figure D.1: Severity categories

PROBABILITY LEVELS			
Description	**Level**	**Specific Individual Item**	**Fleet or Inventory**
Frequent	**A**	Likely to occur often in the life of an item.	Continuously experienced.
Probable	**B**	Will occur several times in the life of an item.	Will occur frequently.
Occasional	**C**	Likely to occur sometime in the life of an item.	Will occur several times.
Remote	**D**	Unlikely, but possible to occur in the life of an item.	Unlikely, but can reasonably be expected to occur.
Improbable	**E**	So unlikely, it can be assumed occurrence may not be experienced in the life of an item.	Unlikely to occur, but possible.
Eliminated	**F**	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.

Figure D.2: Probability levels

Appendix E

Design Structure Matrices

Human	Car drivers (private): car owners	Professional service drivers (taxi, limo, bus, truck)	Insurance companies	Aftermarket and auto repair shops	Car manufacturers	Energy and fuel consumption companies
Car drivers (private): car owners			Paying insurance	Buying car and maintenance procedures, providing feedback	Buying car	Buying Energy/fuel
Professional service drivers (taxi, limo, bus, truck)			Paying insurance	Buying car and maintenance procedures, providing feedback	buying car	Buying Energy/fuel
Insurance companies	Providing help in case of accidents	Providing help in case of accidents				
Aftermarket and auto repair shops	Providing safe, well working car	Provide safe, well working car				
Car manufacturers	Providing safe, well working car	Providing safe, well working car		Providing parts, needed knowledge		
Energy and fuel consumption companies	Provinding energy/fuel	Provinding energy/fuel				

Figure E.1: Human interaction

Technical System	Car	Engine	Lidar units (sensors)	Cameras	Radar	Global Navigational satellite system	Computer
Car		Consumes work					
Engine	Provides work						
Lidar units (sensors)							Provide environment scan
Cameras							Provide environmnent visuals
Radar							Provide distances to objects
Global Navigational satellite system							Provides location and route
Computer	Driving						

Figure E.2: System interaction

Environment	Road	Marks	Signs	Other Vehicles	Obstacles	Parking	Weather	Regulations
Road								
Marks	Safety, regulating							
Signs	safety, regulating							
Other Vehicles								
Obstacles								
Parking								
Weather	changing conditions							
Regulations	Safety							

Figure E.3: Environment interaction

Car drivers (private): car owners	Comfortability	Safety	Safety					Safety
Professional service drivers (taxi, limo, bus, truck)	Comforability	Safety	Safety					Safety
Insurance companies				Help incase of accidents				
Aftermarket and auto repair shops								Safety
Car manufacturers								Safety
Energy and fuel consumption companies								
Human/Environment	Road	Marks	Signs	Other Vehicles	Obstacles	Parking	Weather	Regulations

Figure E.4: Human-Environment interaction

Car	Transportation	Transportation		Maintenance	Selling	
Engine				Maintenance		providing energy
Lidar units (sensors)						
Cameras						
Radar						
Global Navigational satellite system	Determining destination					
Computer						
Technical system/Human	Car drivers (private): car owners	Professional service drivers (taxi, limo, bus, truck)	Insurance companies	Aftermarket and auto repair shops	Car manufacturers	Energy and fuel consumption companies

Figure E.5: System-Human interaction

Car								Safety
Engine								
Lidar units (sensors)	scanning	scanning	scanning	scanning	scanning	scanning	scanning	
Cameras	visualising	visualising	visualising	visualising	visualising	visualising	visualising	
Radar				measuring	measuring			
Global Navigational satellite system	choosing							
Computer								Safety
Technical system/Environment	Road	Marks	Signs	Other Vehicles	Obstacles	Parking	Weather	Regulations

Figure E.6: System-Environment interaction