



Dependability Assurance for Vehicle Autonomy

Thesis on a Novel Method to Approach Assurance Cases

submitted by

Luis Pedro Cobos Yelavives

ESR 14, SAS European Training Network

supervised by:

Dr. Giedre Sabaliauskaite (Coventry University)

Dr. Jeremy Bryans (Coventry University)

Dr. Farhan Ahmad (Coventry University)

Dr. Alastair Ruddle (HORIBA MIRA Limited)

Autumn 2022

HORIBA MIRA Limited, England, UK



The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 812788 (MSCA-ETN SAS). This publication reflects only the authors' view, exempting the European Union from any liability. Project website: <http://etn-sas.eu/>.

Acknowledgements

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 812788 (MSCA-ETN SAS). This publication reflects only the authors' view, exempting the European Union from any liability. Project website: <http://etn-sas.eu/>.

The research was done through Horiba-MIRA Ltd. in the position of host institution providing a workplace in CCAAR (Centre for Connected Autonomous Automotive Research) and VRES (Vehicle Resilience) to promote the growth and results of the research. Academically-wise the degree was done with the University of Coventry in the Centre of Future Transports and Cities. Two secondments were provided to aid the research, one in Belgium at KU Leuven and the other one in Holland at RH Marine.

I would like to express my gratitude to everyone at Horiba-MIRA, my employer and host institution for its support during the research, and to all the colleagues in the company that helped me as the results would not have been the same without them, and specifically Dr. Alastair Ruddle for mentoring me in this research. Also, a big thanks to everyone in the Safer Autonomous System Consortium for their support in the ideas exposed on this thesis and the relevant advice. And special thanks to my director of studies at Coventry University Dr. Giedre Sabaliauskaite.

Last but not least I want to thank my family, especially my father, Dr. Carlos R. Cobos, who encouraged me in engineering, science and research, and who taught me how to question things and fight for my goals. And of course, MSc. Claudia Pijoan, my partner, my teammate, my rock, my motivation to everyday be better, and the person that always has my back; none of this would have been possible if she wasn't by my side.

Summary/Abstract

Ensuring very high levels of dependability will be essential to achieve societal acceptability for automated driving. The safety assurance case is a well-established concept and the notion of a cyber security assurance case is emerging. However, wider dependability assurance cases will be needed for high levels of driving automation. In order to address dependability, the assurance cases for automated driving will need to be extended considerably beyond those currently constructed for safety in automotive applications. There is a need to address a wider range of quality aspects, such as reliability, availability, cyber security, safety of the intended functionality and fail-operational functionality. In particular, methods will be needed to allow such assurance cases to accommodate artificial intelligence technologies and machine learning, which are increasingly being used to support the higher levels of driving automation. Furthermore, a rolling programme of software updates is expected to become the norm for future vehicles in order to maintain cybersecurity against unforeseen emerging threats and to maintain or improve vehicle functionality, as well as to enable the use of software upgrades to achieve a “software defined vehicle”. This situation raises a wide range of challenges for validation, assurance and certification, which will need to become a much more wide-ranging and dynamic activity in future.

Considering Cybersecurity, Functional Safety, Safety of the intended Function, and overall Vehicle Safety is essential for getting the expected results in reliability and dependability. Knowing how these differ and their links to each other is important to create a valid “big picture”. This thesis aims to develop a method that can be presented as a cybersecurity case in accordance with the relevant safety and cybersecurity standard, but is also a method that manages to link vehicle safety and vehicle security. The method tries to reduce the inherit bias presented in functional safety and other audit biases by using induction and deduction to challenge claims and ideas. The method itself can be backed up by different work products created in the industry, such as safety and security analysis or assessments, to support its ways of challenging ideas and deducing things are safe as reasonably possible.

The method presented in this thesis is described and later evaluated through examples and applications, always focused on highly connected autonomous vehicles. One of this is a pilot demonstration of a safety critical system on a connected highly autonomous vehicle, that applies most of the theoretical concepts described throughout the document. The method is evaluated and discussed contemplating the examples and understanding what it might need if it is to become an industry standard.

This project was created to generate results that can be used in conjunction to other results in the *Safer Autonomous Systems* project of the European Union’s Horizon 2020 research and innovation program. The method idea has been discussed in conference papers, with experts in Functional Safety, Cybersecurity, and Connected Autonomous Vehicles at Horiba-MIRA, and with experts of Autonomous Systems Assurance at KU Leuven (Belgium) and RH Marine (Netherlands).

Abbreviations

ADAS	Advanced Driver-Assistance Systems
ADT	Attack-Defence-Tree
AI	Artificial Intelligence
ASIL	Automotive Safety Integrity Level
BOM	Bill of Materials
CAN	Control Area Network
CAV	Connected Autonomous Vehicle
CSMS	Cybersecurity Management System
ECU	Electronic Control Unit
E/E/PE	Electrical/Electronic/Programmable Electronic
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ETA	Event Tree Analysis
EV	Electric Vehicle
FMEA	Failure Mode and Effect Analysis
FS	Functional Safety
FTA	Fault Tree Analysis
GTR	Global Technical Regulations
GSN	Goal Structured Notation
HARA	Hazard Analysis and Risk Assessment
HAZOP	Hazard and Operability
ISO	International Standards Organisation
NCAP	New Car Assessment Program
OEM	Original equipment Manufacturer
OTA	Over the Air
PSS	Passive Safety System
UNECE	United Nations Economic Commission for Europe

UN R	United Nations Regulation
SOTIF	Safety of the intended functionality
SRS	Supplemental Restrain System
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-everything
VMs	Vehicle manufacturers

Definitions

Assurance	Justifiable grounds for confidence that the risks of using a product, process or service are acceptable to the stakeholders [1].
Assurance audit	Independent review of the evidence presented by a supplier to demonstrate that appropriate measures have been successfully implemented to ensure that the risks of using a product, process or service are acceptable to the stakeholders [1].
Assurance case	A documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding the properties of a product, process or service are adequately justified for a given application in a given environment [1].
Assurance framework	A structured means of identifying and mapping the main sources of evidence for assurance [1].
Attack objective	Any outcome of a cyber attack that may result in one or more forms of damage (safety, privacy, financial or operational) to the legitimate stakeholders [1].
Availability (system)	Ability to maintain a product, process or service in a functioning state.
Availability (data)	Ability to provide the data required by a product, process or service as and when required by authorized individuals, entities, or processes [1].
Certification	The provision of an official document attesting that a supplier has collated or provided convincing evidence that appropriate measures have been successfully implemented to ensure that the risks of using a product, process or service are acceptable to the stakeholders [1].
Confidentiality (data)	Data is not made available or disclosed to unauthorized individuals, entities, or processes.
Cyber attack	Any attempt to gain unauthorized access to and/or control of the data held within, received by (from sensors and/or communications), or transmitted from (via actuators and/or communications) a product, process or service, including both intentional and unintentional interference with the normal operation of the product, process or service [1].
Cyber resilience	Ability to ensure the continued execution, or timely resumption, of the essential functions of a system, safely and securely, accommodating/mitigating foreseeable safety hazards and other potential threats (operational, financial, privacy) resulting from cyber-related failures or interference with the normal operation of a product, process or service, and enabling a graceful degradation of performance otherwise [1].
Cybersecurity	Freedom from unacceptable risk of fraudulent financial transactions, compromised privacy, impaired system services, and physical injury or damage to health, property or the environment that could result, either directly or indirectly, from unauthorized monitoring and/or control of the data entering, leaving, or held within a product, process or service [1].
Cybersecurity risk	Combination of the likelihood of occurrence of a successful attack on a system and the potential severity of the impact for the stakeholders, such that combination of the lowest severity and the lowest likelihood imply the lowest risk while combination of the highest severity and highest likelihood imply the highest risk and other combinations result in intermediate risk levels [1].

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 812788 (MSCA-ETN SAS). This publication reflects only the authors' view, exempting the European Union from any liability. Project website: <http://etn-sas.eu/>.

Dependability	Ability to perform (i.e. deliver required functionality, safely and securely), as and when required [1].
Functional Safety	Absence of unreasonable risk due to hazards caused by malfunctioning behaviour of Electrical/Electronic/Programmable Electronic (E/E/PE) systems [2][3].
Integrity (data)	Maintaining and assuring the accuracy and completeness of data held by a product, process or service over its entire lifecycle.
Intended use	Set of use cases (comprising stakeholders, applications and environments) for which a supplier has developed a product, process or service [1].
Intentional misuse	Any reasonably foreseeable or unforeseeable uses of a product, process or service that differ from the supplier's intended use, and which are intended to achieve unlawful gain or malicious advantage for one individual or group at the expense of another individual or group [1].
Likelihood	A measure (qualitative or quantitative) of the probability of successfully mounting a cyber attack against a product, process or service [1].
Operational assurance	Justifiable grounds for confidence that the risks of continuing to use a product, process or service remain acceptable to the stakeholders throughout its life [1].
Operational readiness	Justifiable grounds for confidence that reasonably foreseeable threats have been considered in the design and development phases, such that the cybersecurity risks of using the product, process or service are acceptable to the stakeholders [1].
Reasonably foreseeable use	Use of a product, process or service that differs from the supplier's intended use (including aspects of intentional misuse), but which is readily predictable from known human behaviour (e.g. using a screwdriver as a chisel, bradawl, lever, stirrer, weapon etc.) [1].
Resilience	The persistence of dependability in the face of change or adversity [1].
Robustness	Ability to withstand an unexpected internal or external threat or change without degradation in system performance [1].
Safety	Freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment, resulting from failures or interference with the normal operation of a product, process or service [1].
Severity (cybersecurity)	Estimate of the potential impact on the stakeholders of fraudulent financial transactions, compromised privacy, impaired system services, and physical injury or damage to health, property or the environment that could result, either directly or indirectly, from a successful cyber attack on a product, process or service [1].
Stakeholder	Any person, organization, social group, or even society at large, that has an interest in, or is directly or indirectly affected by, the functioning of a particular product, process or service [1].
Threat	Potential source of damage to the stakeholders, in terms of compromised safety, privacy, financial or operational performance, that could result from the exploitation of one or more vulnerabilities of a product, process or service by a threat agent in order to achieve a particular attack objective [1].
Threat agent	Any person, organization, social group, or nation, that has an interest in undertaking cyber attacks [1].
Unforeseeable use	Any uses of a product, process or service that differs from the supplier's intended use, including aspects of intentional misuse, that are not readily predictable from knowledge of human behaviour [1].

Unintended use	Any reasonably foreseeable or unforeseeable uses of a product, process or service that differ from the supplier's intended use, including intentional misuse [1].
Validation	Confirmation, through the provision of objective evidence, that the requirements for a specified intended use or application have been fulfilled [1]. (i.e. Did we build the right system?)
Verification	Confirmation, through the provision of objective evidence, that the specified design requirements have been fulfilled [1]. (i.e. Did we build the system right?)
Vulnerability	Any design, or implementation error, or other weakness, of a product, process or service that could be exploited to gain unauthorized access to and/or control of the data held within, received by (from sensors and/or communications), or transmitted from (via actuators and/or communications) the product, process or service [1].

Table of Contents

	Page
Acknowledgements	ii
Summary/Abstract.....	iii
Abbreviations	iv
Definitions	vi
Table of Contents	ix
1 Introduction.....	1
1.1 Motivation	1
1.2 Aim, Objectives and Research Questions	2
1.3 Novelty and Contributions of the Research.....	3
1.3.1 Novelty.....	3
1.3.2 Contributions.....	3
1.4 Support and Corroboration of the Research	3
1.4.1 HORIBA MIRA	4
1.4.2 SAS Consortium	4
1.4.3 Coventry University	5
1.4.4 Publications in Conferences	5
1.5 Thesis Structure.....	8
2 Theoretical framework.....	9
2.1 Autonomous Driving and Connected Cars.....	9
2.1.1 Driving Automation.....	9
2.1.2 Decision Making in Road Vehicles	10
2.1.3 History and state of the art	15
2.2 Supporting Technologies	16
2.2.1 Connected Vehicles - V2X.....	16
2.2.2 Artificial Intelligence, Machine Learning and Neural networks	20

2.2.3	Simulation, Validation & Testing	21
2.3	Safety and Security	21
2.3.1	Safety	22
2.3.2	Security	26
2.3.3	Trust, Reliability and Availability	29
2.4	Dependability and Assurance.....	30
2.4.1	Assurance Cases	31
2.4.2	Safety and Security Analysis Techniques	35
2.4.3	Incorporation of Safety Aspects of Cyber Security into Safety Cases.....	39
2.4.4	Automated generation Safety Cases	40
2.4.5	Limitations of Assurance Cases	41
2.5	Legality of autonomous vehicles.....	41
2.5.1	Safety and Security	41
2.5.2	Insurance and Liability	42
2.6	Over the Air Updates	43
2.6.1	Benefits and challenges	46
2.6.2	Over the Air Updates Security	47
2.7	Related Projects	49
2.7.1	Pegasus	49
2.7.2	Uptane	50
2.7.3	Trust Vehicle Project.....	50
2.7.4	AutoNet2030	50
2.7.5	Maven	50
2.7.6	V-DAS	50
2.7.7	SAS	51
2.7.8	Peter.....	51
2.7.9	Impact of related projects.....	51

3	Methodology	52
3.1	Approach and Aims	52
3.1.1	Proposed Requirements for a Cybersecurity Case	53
3.1.2	Proposed Method	53
3.2	Related Work	54
3.2.1	Works that Inspired the Proposed Method	54
3.2.2	Works Similar to the Proposed Method	55
3.3	Background information	57
3.3.1	Risk Management and Analysis	57
3.3.2	Relevance and Compatibility with the standards	58
3.3.3	Threat Modelling and Attack-Defence Trees	59
3.3.4	GSN, Eliminative Argumentation and Confidence Maps	61
3.4	Proposed Method Design and Structure	62
3.4.1	Required Inputs	66
3.4.2	Step by Step Build up	66
4	Illustrative Examples	69
4.1	Example 1: Art Heist	69
4.2	Example 2: Traffic Signal Recognition System.....	70
4.2.1	System description	70
4.2.2	Attack Tree	71
4.2.3	Development of a cybersecurity case	72
5	Real World Application.....	74
5.1	Autonomous Marine Vessel.....	74
5.1.1	System description	74
5.1.2	Marine Vessel Safety and Security	75
5.2	Comparison with the Automotive Domain	76
5.3	Identification of Risks and Threats	77

5.3.1	Safety Marine Vessel Safety Identification of potential hazards (Safety)	77
5.3.2	Marine Vessel Security: Identification of Threats (Security)	78
5.4	Application of the Method	79
6	Test Case as a Pilot demonstration	83
6.1	Test Bench for Test Case	83
6.1.1	Setting up the server	84
6.1.2	Setting up the Client	85
6.1.3	Outlay of the Test Bench	86
6.2	Test Case: Assurance case of OTA Update on a safety critical system (Airbag ECU)	88
6.2.1	Concepts and Background	88
6.2.2	Context for the test case	91
6.3	Application of Assurance case into pilot demonstration	94
6.3.1	Existing work products to support the application	94
6.3.2	Layout of the case for the demonstration	94
6.3.3	Pilot Demonstration Application	95
7	Summary of the evaluation of the method	101
7.1	Results from the examples	101
7.2	Evaluating the Real-World Application	101
7.2.1	Comparing the results against various safety and security analysis work products	101
7.2.2	Analysis of results	102
7.3	Evaluating the Pilot demonstration	103
7.3.1	Comparison with the objectives	103
7.3.2	Comparing the results against other work products	103
7.3.3	Analysis of results	104
7.4	Overall remarks of the method	105
7.4.1	Meeting the Regulations	105
7.4.2	Limitations and Weaknesses	105

7.4.3	Key Contributions and Highlights	105
8	Conclusion	107
8.1	Possible Adaptations, Extensions and Future Work.....	107
8.1.1	Marine Vessel, Aircraft or Train Applications.....	107
8.1.2	Considering Vehicle AI Systems.....	108
8.2	Reach	108
8.3	Remaining challenges and obstacles	108
8.4	Summary of contributions	109
	References.....	110
	INDEX – Table of figures, equations and graphs	119
1.	Table of figures	119
2.	Table of tables.....	120
3	Table of Equations	120
	Appendix A – Links of Interest.....	121
	Knowledge base of European Projects regarding connected and highly autonomous vehicles:.....	121
	Marine Conventions.....	121
	Download links for the testbench source codes	121
	Appendix B – ECE Regulations.....	122
	Appendix C – GTR Regulations	124
	Appendix D – Enlarged Method Diagrams.....	125
	REALWORLD APPLICATION.....	126
	Pilot Demonstration.....	128
	Appendix E – Confidential supporting information for AI Marine System. FMEA & Attack Trees	130
	FMEA Document.....	131
	Attack Tree	133
	Appendix F – Confidential supporting information Safety Critical System. HARA, TARA, GSN and ADT.....	135
	Automotive HARA.....	136

GSN Safety Case.....	140
Attack-Defence Tree	142
Appendix G – Ethics Certificate	144
Appendix H – Copyright and permission of co-authors on paper content	145

1 Introduction

This document aims to expose the ideas of an assurance case that considers safety and security of the vehicle. This assurance case can be used for the purpose of a cybersecurity case to comply with standards. The assurance case uses inductive logic to promote critical thinking, changing the perspective of the evaluator with the intention to reduce bias.

1.1 Motivation

This research came to be as part of the EU Research and Innovation Horizon Programme in a project named Safer Autonomous Systems (SAS). The project aims to provide and collect evidence through research and methods of the safety and reliability of autonomous systems to be able to establish human trust on the systems. In order to achieve this the project is divided into 6 work packages (WP 1-6) and 15 Early-stage researchers (ESR 1-15). This research was created to work as the last research of WP 3 “Assurance Strategies” and assigned to ESR 14 “Luis Pedro Cobos” under the topic Dependability Assurance for Vehicle Autonomy. The objective of ESR 14 is to develop research and create a pilot demonstration of evaluating assurance on an autonomous vehicle. Other than that, the research of ESR 14 must also help in completing the Overall Project Objectives and cooperate in working with the other ESRs to complete the final WP.

In the direction of the objective of creating a pilot demonstration the research was oriented to Connected Highly Autonomous Vehicles, their technologies, and their regulations. The electrification and evolution of technology has made previously known mechanical combustion machines such as vehicles targets to cybersecurity problems, and therefore the world of regulations and standards is responding to cybersecurity. To establish human trust on Connected Autonomous Vehicles it is important to consider the full spectrum of safety and security; vehicle safety is a very well-developed practice and remains one of the main objectives of the automotive industry. Considering where cybersecurity and safety link can be essential in providing assurance, and to improve assurance it is important to critically think how it is evaluated or if any bias exist. Creating a method to visually and logically understand this, while adhering and proving compatibility with legislation and regulations is a potential game changer. With the idea of a method to show assurance for safety and security in automotive a secondment opportunity provided the chance to apply the method on a vehicle of a different industry.

Considering the experience and expertise of ESR14 on vehicle safety and the development of vehicle features oriented to functions, it became a logical process to try and develop the pilot demonstration in this direction.

As the ideas developed on creating a good pilot demonstration, the way of updating vehicles over-the-air, and the potential inhouse knowledge in Coventry University, and a secondment at KU Leuven, lead to the creation of a test bench to be applied on a safety critical system and the pilot demonstration.

1.2 Aim, Objectives and Research Questions

- **Aim** - To develop a unified and holistic approach to developing a range of assurance cases that could address a range of aspects of dependability for highly automated and fully autonomous vehicles.

- **Objectives:**
 - ▣ Review of autonomous vehicle technologies, existing regulations, available functions; and relevant techniques from functional, safety cyber security, other sectors affecting automotive.
 - ▣ Identification of approaches for accommodating non-deterministic and evolutionary features of artificial intelligence technologies.
 - ▣ Development of a common framework for developing wider dependability assurance cases.
 - ▣ Use the information on this literature review in a pilot demonstration of proposed approach.
 - ▣ Apply proposed approach to Over the air updates.

- **Research Questions:**
 - ▣ How can the classic automotive industry approach of passive and active safety, adapt itself to include emerging ideas like cybersecurity?
 - ▣ How can a cybersecurity case be presented?
 - ▣ What would be a holistic approach to represent an assurance case that links vehicle safety and security accomplishments?
 - ▣ Why are over the air updates valid for safety critical functions?

1.3 Novelty and Contributions of the Research

Novelty and contribution are closely linked, the novelty is more closely related to the highlight of what makes the research unique, and the contribution are the detail of the impact it has had and hopes moving forward.

1.3.1 Novelty

The novelty of this project comes from using an assurance case that is able to comply with recent regulations, and at the same time use inductive reasoning to try and reduce biasing in assurance cases. It also innovates in attempting to make sure that the method is able to link safety and security concepts. The method itself is unique and the position of the author and development of the method was evolved through publishing conference papers.

1.3.2 Contributions

More than just being unique as expressed in the novelty, the thesis and the author are expected to give some contributions to the scientific and academic communities. Most of the theoretical concepts that are explained throughout the thesis, have been taught as guest lectures for Master's degree students in two universities in Spain, that accepted the collaboration of the author and the SAS project. Concepts of connected car and vehicle electronics were transmitted to Coventry University students when an opportunity to teach during one semester was given to the author. As for contributions to science and the automotive industry, the development of method that can be used as a cybersecurity case and the compatibility with cybersecurity standards while following other relevant regulations and safety standards. There was also an effort made to make the method interdisciplinary, so it can be used for safety and security, it can be used in other industries, and helps visualize the factors that need safety and security assessments. Finally results presented in this research are part of a bigger scale project it will also become part of the SAS final report.

1.4 Support and Corroboration of the Research

With a project like this it is important to maintain it grounded to reality and be sure it follows, regulations, rules and best practices. In the benefit of such a network of field professionals and papers have tracked the progress of the project to maintain it peer reviewed and well assessed.

1.4.1 HORIBA MIRA

Throughout preparation of this thesis, Horiba-MIRA colleagues within the company continuously evaluated the project and helped correct the procedure while giving input. These people are:

- **David Ward** - *Functional Safety Lead*: Evaluated the method 4 times, giving input on how to use the supporting evidence correctly and efficiently and making sure functional safety aspects were correct, and that the regulations were interpreted correctly.
- **Tim Edwards** - *Chief Engineer CAV*: Evaluated the examples to make sure of their technical viability and gave input on the context for all the examples.
- **Paul Wooderson** - *Chief Engineer Cybersecurity*: Evaluated the method 2 times providing improvements in how to assess the mitigations of the method. Also provided help in complying with cybersecurity standards and making the cybersecurity case.
- **Edith Holland** - *Chief Engineer SOTIF*: Evaluated the method once and assessed in the correct way of linking SOTIF with functional safety.
- **Anthony Baxendale** - *Head of R&D*: Overall review of the method from a research and development perspective and its potential uses.
- **Anthony Martin** - *Head of Vehicle Resilience*: Support with literature and background regarding assurance, compliance, and resilience.

1.4.2 SAS Consortium

As part of the SAS Consortium the project received contributions from senior members of the different companies and other ESRs. These people and their contributions are the following:

- **Jeroen Boydens** - *Senior Professor of Information Technologies at KU Leuven*: Coordinator of the SAS project and main supervisor of the secondment at KU Leuven, provided support in creating a test bench and evaluating the example.
- **Jens Vankeirsbilck** - *Expert researcher on distributed and Secure software at KU Leuven*: Helped by verifying update protocols and any assumption regarding the CAN network were correct.
- **Ehab el Amam** - *Lead Consultant Safety and Security at RH Marine*: Main supervisor of the secondment at RH Marine, contributed with the relevant work product documentation and assessing the correct analysis of such.
- **Tianlei Miao** - *Research Autonomous Driving at RH Marine*: Overview of marine regulations mentioned in this document and adjustments to the marine vessel example regarding AI.

- **Orian Dheu** - *Research Law and Liability of Autonomous Systems at KU Leuven*: Overview assessment of sections regarding liability and regulations.
- **Fang Yan** - *Goal Structuring Notation Research at York University*: Provided functional safety cases for some the examples and evaluated the use of Goal Structuring notation in the method.

1.4.3 Coventry University

Members of the Centre for Future Transport and Cities at Coventry University are motivated to contribute with each other to collaborate in knowledge and enhance the quality of the research. This research was enhanced by the following people:

- **Kacper Sowka** - *Researcher at FTC*: Contributed with the generation and assessment of Attack-Defence Trees.
- **Shahid Mahmood** - *Researcher at FTC*: Helped assess the basis for building the test bench, and helped with understanding and operating UPTANE.
- **Siraj Shaikh** - *Lead at FTC*: Evaluated and suggested how to orient examples and timings.
- **Rhys Kirk** - *Researcher at FTC*: Help with instructions of management of networks on Linux to help the work bench.

1.4.4 Publications in Conferences

As a result of this research several publications were produced. Therefore, his thesis refers to/includes contents from the following publications in conferences:

- Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS) 2021, Setubal, Portugal
 - **Conference Paper title:** “Requirements for a Cybersecurity Case Approach for the Assurance of Future Connected and Automated Vehicles.”
 - **Role:** Main Author /Presenter
 - **Abstract:**

Cybersecurity is an issue of increasing concern for emerging connected vehicles. Ensuring public trust in future connected and automated vehicles will require very high levels of confidence in their dependability, which will include cybersecurity assurance. In functional safety engineering, the safety case has become a widely used approach to describing and documenting safety assurance arguments and their supporting evidence. The use of a similar security case can also be considered in cybersecurity engineering, but there are significant differences between safety and cybersecurity. Cybersecurity impacts include, but are not limited to, possible safety issues. Furthermore, the cybersecurity threats arise from the ingenuity of human attackers, and available technology, with the result that they are constantly evolving. This paper proposes the use of an assurance case approach for cybersecurity and outlines the requirements that are considered to be necessary for the development of such a cybersecurity case.

- **Overview:** This paper sets the stage for the needs to construct the method, the current state of the technology and the requirements.

- 31st European Safety and Reliability Conference (ESREL), 2021, Angers, France

- **Conference Paper title:** “Cybersecurity Assurance Challenges for Future Connected and Automated Vehicles”
- **Role:** Main Author /Presenter
- **Abstract:**

Increases in the connectivity of vehicles and automation of driving functions, with the goal of fully automated driving, are expected to bring many benefits to individuals and wider society. However, these technologies may also create new cybersecurity threats to vehicle user privacy, the finances of vehicle users and mobility service operators, and even the physical safety of vehicle occupants and other road users. Assuring the cybersecurity of future vehicles will therefore be key to achieving the acceptability of these new automotive technologies to society. However, traditional prescriptive assurance methods will not work for vehicle cybersecurity, due to the evolving threats, through-life software updates, and the deployment of artificial intelligence techniques. Cybersecurity regulations that are goal-oriented and risk-based, like those increasingly used in safety engineering for complex systems, are now mandated in recent vehicle type approval regulations. This results in many new assurance challenges, which will not be limited purely to cybersecurity. In particular, emerging standards have proposed that an assurance case approach should be adopted in relation to cybersecurity. This paper therefore proposes a novel cybersecurity case framework that adapts existing approaches from safety engineering, emphasizes the limitations of the analysis through eliminative argumentation, and merges in the attack-defence tree techniques used in cybersecurity engineering, with the aim of providing a better reflection of the some of the uncertainties in the cybersecurity risk analysis.

- **Overview:** This paper is used to introduce the method as a cybersecurity case that also encompasses safety.

- SAE World Congress 2022, Detroit, USA

- **Conference Paper title:** “Requirements for the automated generation of attack trees to support automotive cybersecurity assurance”
- **Role:** Second Author /Presenter
- **Abstract:**

As the need for automotive assurance continues to grow, it becomes necessary to develop approaches which can provide assurance cases in a systematic and efficient manner. In the case of cybersecurity, this problem is exacerbated by the increasing complexity of vehicular onboard systems, their inherent obscurity due to their heterogenous architecture, emergent behaviours, and the disparate motivations and resources of potential threat agents. Furthermore, the advancement of connected autonomous vehicles (CAV) may allow external attackers to leverage the naïve trust ECUs have for adjacent devices to compromise the safety and security of the vehicle. To that end, there is an increased interest in automatically producing threat models such as attack trees, which usually rely on intensive expert driven construction or rudimentary formally defined processes, to identify potential threats to a vehicle. Therefore, this paper will explore the ways in which such an automated scheme could be applied for a practicable identification and analysis of potential attack paths. Although ISO/SAE 21434 recommends the development of an assurance case for cybersecurity, the precise nature of a cybersecurity case is not explicitly defined within the standard. Therefore, this paper also explores the combination of threat modelling techniques with assurance case techniques adapted from accepted practice in vehicle safety for functional safety (per ISO 26262) while taking into consideration the relevant standards.

 - **Overview:** This paper shows examples of the method and how implements attack trees, and pushes the idea of a holistic assurance case that implements cybersecurity
- 2nd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 2022, Mauritius, Maldives
 - **Conference Paper title:** “Application of an Automotive Assurance Case Approach to Autonomous Marine Vessel Security”
 - **Role:** Main Author /Presenter
 - **Abstract:**

The increase of autonomy in autonomous surface vehicles development brings along modified and new risks and potential hazards, this in turn, introduces the need for processes and methods for ensuring that systems are acceptable for their intended use with respect to dependability and safety concerns. One approach for evaluating software requirements for claims of safety is to employ an assurance case. Much like a legal case, the assurance case lays out an argument and supporting evidence to provide assurance on the software requirements. This paper analyses safety and security requirements relating to autonomous vessels, and regulations in the automotive industry and the marine industry before proposing a generic cybersecurity and safety assurance case that takes the general graphical approach of Goal Structuring Notation (GSN).

 - **Overview:** This paper is all about how the method works on automotive examples and how to apply it to other types of vehicles

1.5 Thesis Structure

The thesis is divided in 8 chapters. The introduction is the first chapter, and its objective is to set-up the reader for the project.

Chapter 2 covers the background theoretical concepts, the state of the art and a review of available literature. This is a chapter that establishes most of the concepts used further on. It starts with how the vehicles work and the technologies they include, then it specifies safety, security and other assurance concepts. Finally, it talks about legal issues and existing relevant projects.

Chapter 3 is about the developed methodology. The chapter starts by explaining how the method will go beyond other research and what research is used to support it. Then it explains the logic and creates a step by step build up.

Chapter 4 shows two small scale examples. The first example is fairly simple and not tied to automotive to help understand the method. The second example uses an automotive system and starts the use of external documentation, referred as work products, to help build the assurance case.

Chapter 5 features a real-world application of the method on a vehicle outside the automotive industry. The method here is used to evaluate autonomous marine vessel. It also presents the challenge of adapting the method from automotive standards to another industry.

Chapter 6 unveils the pilot demonstration. It explores the creation of a test bench and how it is used for software updates. Then it introduces a safety critical system and creates a context for the experiment on the pilot demonstration. Using various work products within the industry the method gets the most development in its execution in this section.

Chapter 7 considers the previous three chapters and evaluates the method. The method evaluation is done in relation to the objectives, work products and supporting documentation. To cap it all off it considers the future works and possible adaptations before giving some final remarks.

Chapter 8 concludes the thesis by explaining the expected reach of the method, the fulfilled objectives and the remaining challenges and obstacles.

2 Theoretical framework

The goals of autonomous driving are to significantly reduce the number of accidents in traffic as well as to increase comfort and create solutions for individual transport in daily life. With the emergence of connected cars and the tendency for autonomous features until the eventual fully autonomous cars, it is normal to wonder if they are reliable. For the sake of public acceptance a product should be viewed positively and trusted by people but change and new things are always hard to come by. Creating a responsible assurance method that considers safety and security might be the missing piece to lead the society in a way more open to autonomous vehicles. This Theoretical framework is the collection of background information, previous research, literature review, paradigms, and theoretical considerations on which the current research project is based.

2.1 Autonomous Driving and Connected Cars

The world is not shy of the emerging automated driving vehicles; they are becoming more of a reality with each passing moment. Although most of the established vehicle manufacturers have active development programmes on this topic, it has also garnered interest from a number of new entrants.

The world does not have legally worldwide accepted definition of what an autonomous system should consider. The most common definition of an autonomous vehicle is that it is a vehicle that is capable of sensing its environment and moving safely with little or no human input by combining a variety of sensors that let the vehicle perceive its surroundings and an advanced control system that interpret sensory information leading to a proper navigation or path following [4][5][6]

2.1.1 Driving Automation

Over recent years the automotive industry has been adding increasingly complex driving automation features to vehicles, leading to the advanced driver-assistance systems (ADAS) that are currently on the market. Examples that are already found in many vehicles include parking sensors, electronic stability control, traction control and cruise control. More sophisticated systems include adaptive cruise control (ACC, which enhances cruise control by maintaining a safe following distance), lane departure warning (LDW), lane keeping and lane change assistance, as well as pre-crash support such as forward collision warning and automatic emergency braking (AEB). There are middle difficulty functions like the detection, classification and understanding of surrounding objects as pedestrians, bicycles, motorcycles, other vehicles (car, truck, SUV), lamp poles as other street objects, etc. Then there are more complex features like the traffic jam pilot

that enables the vehicle to follow the car ahead while being aware of the traffic lights etc., or the self-parking features (which can do parallel parking for drivers who lack the necessary skills).

However, ADAS functions are only the beginning of automated driving, and driving automation actually describes a spectrum of vehicle capabilities (summarized in Table 1) that has been classified in SAE J3016 [7]. These range from human driven vehicles with only rudimentary ADAS (Level 0) through to full driving automation under all conditions with no requirement for a human driver (Level 5).

Table 1: SAE Levels of Driving Automation (based on SAE J3016 [7]).

Feature	Driver Support Features			Automated Driving Features		
	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Control scope	Warnings and only momentary assistance	Steering OR brake/ throttle support	Steering AND brake/ throttle support	Can drive vehicle for limited conditions	Can drive vehicle for limited conditions	Can drive vehicle under all conditions
Driver input	Always required	Always required	Always required	May be requested to resume	Not required under some conditions	Never required
Sample systems	Blind-spot warning, AEB, LDW	Lane keeping OR ACC	Lane keeping & CC	ATraffic jam pilot	Automated local taxi (fixed route)	Driving anywhere, under all conditions

2.1.2 Decision Making in Road Vehicles

The implementation of driving automation can be summarized as a sequence of high-level functionalities between the sensing and actuation tasks that include perception, prediction, and planning (see Figure 1).

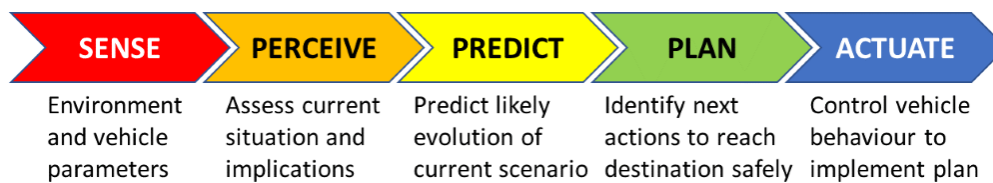


Figure 1: Role of AI in driving automation

- **Sense:** This is the entry phase of the AI here the AI recognizes vehicle parameters (Speed, functions activated, etc.) and its surroundings, to do so it uses GPS data search for a location, it uses the cameras it has to “see” its surroundings, and it use the sensors (infrared, LIDAR, etc.) to feel its surroundings how far are they, are they on a straight line, etc.
- **Perceive:** Here the AI understands its current situation, it takes everything in the sense face and uses it together, using the camera and sensors it now knows what objects are in front and how far they

are. With its GPS location it understands exactly where on a road it is and what type of road it is on (highway, avenue on a city, street in a small town, a rural road, etc.). It now also understands why the vehicle is at a certain speed, or the steering wheel has a certain yaw. In this face everything that it sensed in the previous phase gives the AI the info to be able to completely assess its surroundings. Most vehicles use a process known as data fusion or info fusion, to compile everything it sensed into a real perception.

- **Predict:** This phase is what really puts the neural network to test. The method normally used by neural networks is direct perception, here it concludes around 14 possible outcomes [8] of its surrounding, and a way to achieve this.
- **Plan:** In this phase it plans the next move it will execute and makes a decision; the decision is based on the options it has predicted would happen. To put it mildly and simply it just uses its knowledge base, to decide the most possible and safest outcome. But the real decision making to decide the real plan is a bit more complex than that, as it requires probability, the internal knowledge base and the AI limitations it has.
- **Actuate:** This is the final phase and the name is as simple as its function, it executes an action.

2.1.2.1 Parts of an autonomous vehicle

An autonomous vehicle is a complex conjunction of different components that can automate driving tasks (see Figure 2) [9]. The competitions Formula Student [10] and DARPA Urban Challenge [11] grade the vehicle on its functionality and capabilities, and companies use these competitions to test their ideas. The hardware used by winners of these competitions, listed below, gives a good idea for what components are useful for each element of the driving task. [9]

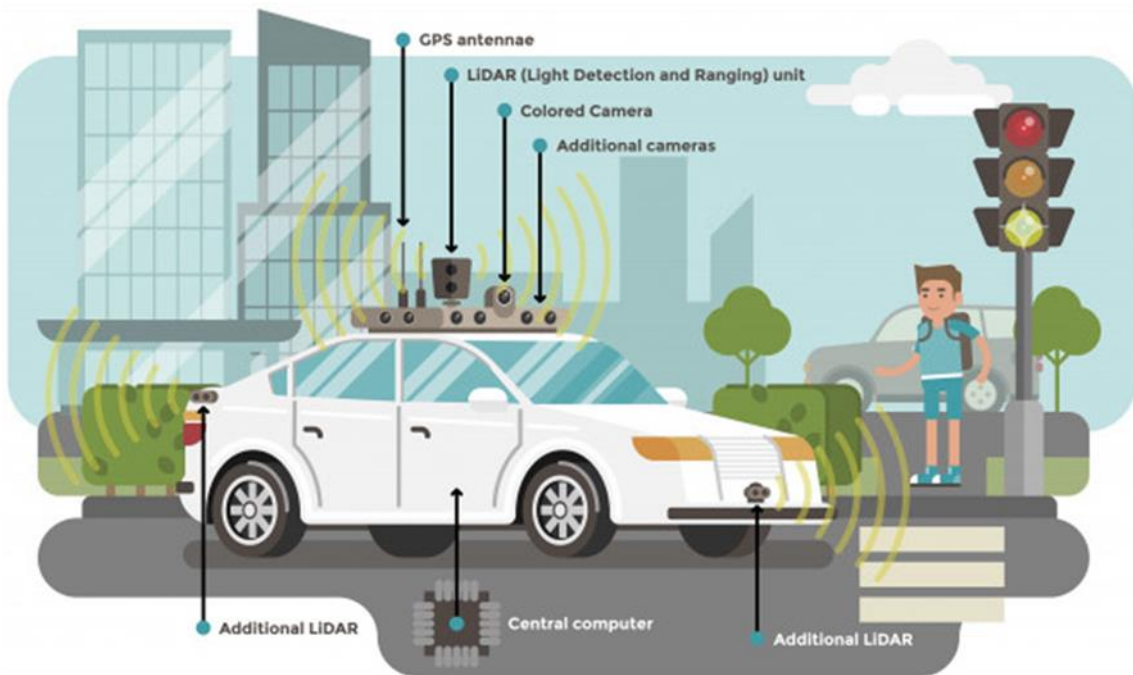


Figure 2 Main driving automation components [12]

- **Actuators:** They help to move the physical parts like the steering wheel, brakes and accelerator. Note that in some commercial vehicles, the acceleration can be control digitally with the ACC, and some now have digital park brakes, and the emergency assist already breaks digitally this can reduce the number of actuators needed if there is a possibility to connect digitally, but before a digital connection to any of this a safety consideration has to be made to always give a superior priority to the safety idea.
- **GPS:** An antenna and a digital map to identify the coordinates of a global position system are the basis of helping the vehicle understand its location. The coordinates can be Latitude/Longitude or UTM (Universal Transverse Mercator coordinate) if a flatted up terrain is required, UTM coordinates are relative to zones so most of the time a conversion must be made between both systems must be made for the most exact precision and make it redundant. [13]
- **Camera:** The tendency is to high resolution RGB cameras, (even tough older prototypes have worked with greyscale they tend to be decreasing). A camera helps understand through image processing what the vehicle has in front, as the image sharpens it facilitates to understand the boundaries and divide the elements. Once the elements are divided it is time to categorize and identify them.
- **Radar:** It is used to detect objects and the distance between them, radars work pinging out radio waves then measuring what is reflected back, the radar frequencies are calibrated to detect other vehicles, pedestrians, bikes, or obstacles. They can be used for front assist and parking. [14]

- **Infrared Sensor:** An infrared sensor can be used to produce imagery primary thermal imaging, this kind of image in conjunction with a camera (through data fusion) can easily help with the classification of objects[15].
- **LIDAR:** Light Detection and Ranging, is a remote sensing method that uses light in the form of a pulsed laser to measure ranges (variable distances) to the Earth. These light pulses combined with other data recorded by the airborne system — generate precise, three-dimensional information about the shape of the Earth and its surface characteristics (definition by the American Geoscience Institute). To put it in a simpler way it does a 3D scanning of the surroundings using light. Contrary to what Elon Musk claims, most of the research uses LIDAR technologies to better perceive the surroundings of a vehicle [16]. The LIDAR helps create for the vehicle a 3D imaging of the surrounding, especially a spatial approach of the surroundings.

2.1.2.2 Data Fusion

Data Fusion, also known as “info fusion”, is the process in which in real-time the data from all data sources is interpreted by the AI. The AI accomplishes this by arranging and overlapping the data of the different sensors to map and fully discern a clear picture. The objective is to provide redundancy and be able to categorize and classify each object sensed by the different sensors. This technique is necessary and relevant because the ideal conditions are never met in real life and it is important to assure the system with as much information as possible. [17][18] Other than the perfect summer day with no wind or rain very bright and not many surroundings there will always be a problem and each sensor has a weakness:

- **Camera:** No matter how precise the camera is, lighting will be the primary weakness of that camera. As the environment grows the darker the precision and the movement will reduce the resolution of such camera and also its field of view.
- **Radar:** Standard radars use for ADAS function operate with 77GHz mm Wave, and even when it is not affected by weather (rain or wind), radar is limited by its field of view and it’s reach. It is not acceptable solely rely on them because, a radar works at the speed of sound not the speed of light, the further it goes the longer it takes to return, meaning the AI is already thinking while the RADAR is still collecting information.
- **Infrared:** Detecting thermal imaging works, but it is more precise with living objects than inert objects, plus extreme weather reduces the accuracy of thermal readings

- **LIDAR:** LIDARs are fragile, but the main enemy of the LIDAR is the weather rain and strong winds will deceive the LIDAR sensor and produce a messy image scan of the surroundings, making it a bit disoriented or curved, and even causing some bizarre issues.

The redundancy that data fusion produces can be seen for example while driving at night the camera is unreliable, but the LIDAR and the radar should suffice. In case of a thunderstorm with heavy rain during the day while passing to a small town, the camera combined with the infrared sensor and the radar would give the vehicle a clear idea of pedestrians crossing during the rain.

The results of data fusion through the multiple sensors helps the AI determine what is a false reading, and generate a true trustworthy measurement, by mapping its surroundings and ruling out what does not fit.

2.1.2.3 Decision Making

When the time comes for an autonomous vehicle to make the final decision of what manoeuvre it will make it has to follow a process and certain rules. This decision-making process is mathematically known as *Markov decision making process*, a discrete-time stochastic control process that states a continuous modelling of situations where outcomes are partly random and partly under the control of a decision maker. In other words, to start the AI will be creating a series of steps to follow during a trajectory and organizing them as a mathematical series getting ready to execute action A+1 while doing action A. Every time it proceeds to the next action in the series it must verify the conditions to execute this step remain (for example be obstacle free), if this fails the series must be overridden by a new manoeuvre and its series. The creation of this series works and stores with an algorithm known as path planner or way mapper. The speed, path and yaw angle of the steering are planned in parallel, through a method known as *path-velocity decomposition*. The vehicle is limited by its internal rules, one of the things is that using location with a V2X technology to know the speed limit so while this marks the top speed it would reach an equation to control throttle while steering also exists in the action code, therefore this also subjects the AI to another speed control (see Equation 1). Another limitation programmed into the AI could be its predisposition to lane change, and when it finally decides to take over another vehicle (a certain time, an under-speed trigger etc.). So, to summarize the decision making is constantly working and making calculations for the next immediate movement side by side while sending the movement info and controlling that the status of the corresponding action with the perceptions and the new plan of action. The path storing and the actions and calculations are relative the process unit, yet anyhow they are faster and more precise than a human driver.[9][19][20][21][22]

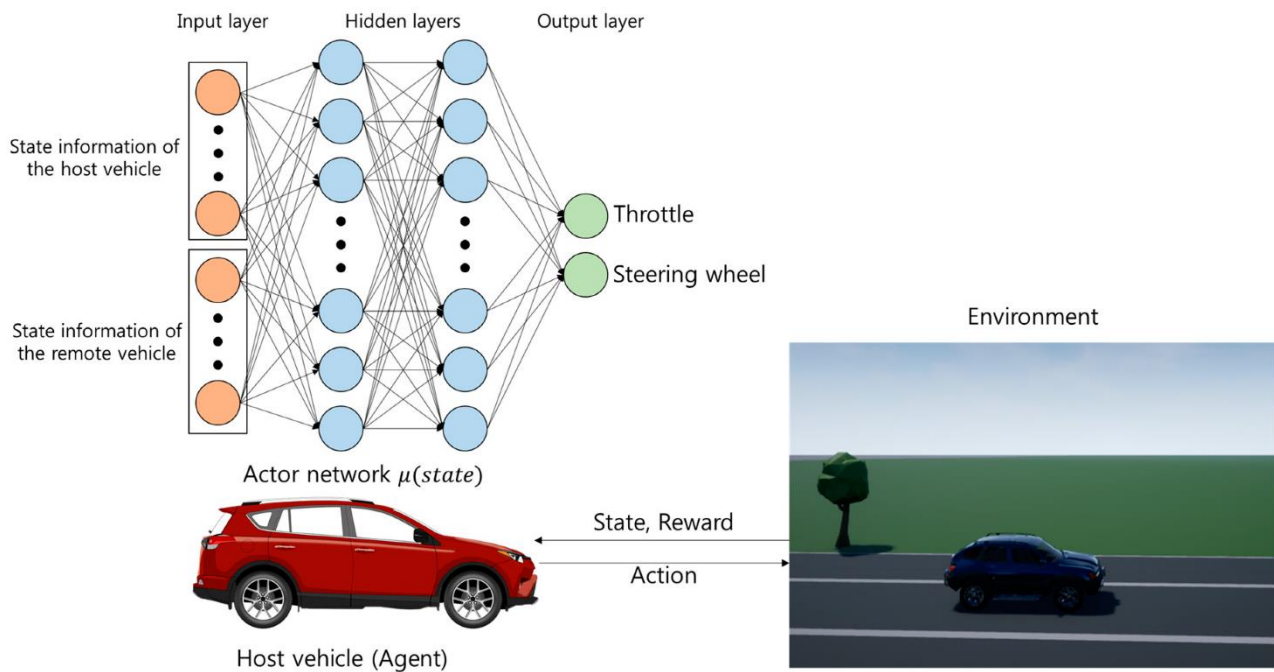


Figure 3 Architecture of decision making of an autonomous car [20]

Equation 1 Equation to obtain the throttle percentage speed while steering.

$$T = T'(1 - |S|)$$

This is done to prevent the car from oversteering drifting or turning at an inadequate speed. Reducing the speed based on the turning angle of the tyres is achieved at high speed being limited by the function where S is the steering from simulation data and T' is throttle percentage at an steering angle of zero. [8]

2.1.3 History and state of the art

People are familiar with what is happening in recent times; for example, Uber has had its automated driving project running [23], and WAYMO has been shown to be quite capable in their demonstrations [24]. Nonetheless, automated driving projects already have a history going back to 1977, with the Automated Highway System (AHS) in California and the Tsukuba car in Japan [25]. The latter functioned by following white street markers and was able to reach speeds of up to 20 miles/hour on a dedicated test course.

During the 1980s Ernst Dickmanns and his group at the University Bundeswehr Munich built the world's first real robot cars, using saccadic vision, probabilistic approaches such as Kalman filters, and parallel

computers. Until 1995 Dickmanns lead the pan-European Prometheus project, the largest robot car project ever to that point with a budget of almost a billion USD, resulting in a prototype that was able to move on empty roads at a top speed of 96 km/hour. In the late 1980's the Carnegie Mellon University, Pittsburgh started and successfully developed the first auto steering, even when acceleration and break needed human assistance, it is the birth of the concept used today [26]. During the 1990's the USA responded to the Prometheus program with a budget increase to their AHS program. The AHS projected concluded in 1997, ending the project and inspiring many small private projects, and leading in the 2000's to the media acclaimed DARPA challenge, a prize competition for autonomous vehicles [27]. In 2005 in Europe the birth of European Land Robot Trials (ELROB) happened, it consisted of demos of autonomous off-road vehicles, and some very promising concepts.

Many of the people who were an integral part of history are still there to see the legacy continue: some have become professors and others have moved to private companies developing autonomous systems. The thing is that if such advancements were made in those times, the evolved world of information technologies (IT) that gives us faster processing speeds, higher fidelity image processing, and more exact calculations: the developments these days are sky rocketing.

2.2 Supporting Technologies

This section describes emerging and existing technologies that support driving automation.

2.2.1 Connected Vehicles - V2X

The connected car is the current world, and everyone wants a bite, this section deepens into it. A connected car is a vehicle capable of communicating bidirectionally with other systems outside of the car. Connected car protocols are known as Vehicle to everything (V2X) or, Car2X and C2X [28]. There are two types of application of V2X:

- Single vehicle applications: This type of applications handle information obtained for the vehicle to use by itself.
- Cooperative Safety and efficiency applications: Are use cases in which a vehicle learns something that it could also potentially communicate to another vehicle or entity and that might also help other users.

The original standard is based on a Wi-Fi offshoot, IEEE 802.11p (part of the IEEE's WAVE, or Wireless Access for Vehicular Environments program). Integrated in Dedicated Short-Range Communications (DSRC) in the US, and ITS-G5 in the European Cooperative Intelligent Transport Systems (C-ITS) initiative, it underpins the use but is considered a successful start into paving the way for V2X in 5G. Meaning there are 2 ways of deploying V2X, by Wireless networks or cellular networks, even though the 2 ways incompatible with each other, a vehicle could still be prepared to communicate with both. Its original purpose is to increase the

safety of the vehicle by expanding its field of vision to more than just what it perceives with sensors, into a concept that it can digest through connecting with other information systems [29][28][30]

V2X is known for the following specific types of communication (Figure 4):

- **V2I:** Vehicle to infrastructure, is the communication between a traffic infrastructure like a traffic sign, traffic light or a parking spot, and the vehicle, providing information of what interaction is possible.
- **V2N:** Vehicle to network, is the communication between the vehicle and a denominated cloud network, to sync or download traffic updates (weather effects or accidents) or media content (music, podcasts, maps).
- **V2V:** Vehicle to vehicle, is the communication between two vehicles, sharing the information of its current actions like speed, location, direction of travel, braking, vision, and loss of stability.
- **V2P:** Vehicle to pedestrian, is the communication between the vehicle and a vulnerable road user or multiple vulnerable road users. It sends warnings to the road user of an approaching vehicle, and warnings to the vehicle of vulnerable road users that it communicates with.
- **V2D:** Vehicle to device, is the communication between the vehicle and a portable smart device linked to the vehicle itself. This lets the applications in the device work as key for the vehicle or open tolls or car washes and make the payments.
- **V2G:** Vehicle to grid, is the communication between a plug-in electrical vehicle and an electric grid, allowing bidirectional communication with the grid without affecting its performance while creating a balance within the local environment permitting the store and discharge of electricity generated from renewable energy sources such as solar and wind, with output that fluctuates depending on weather and time of day.

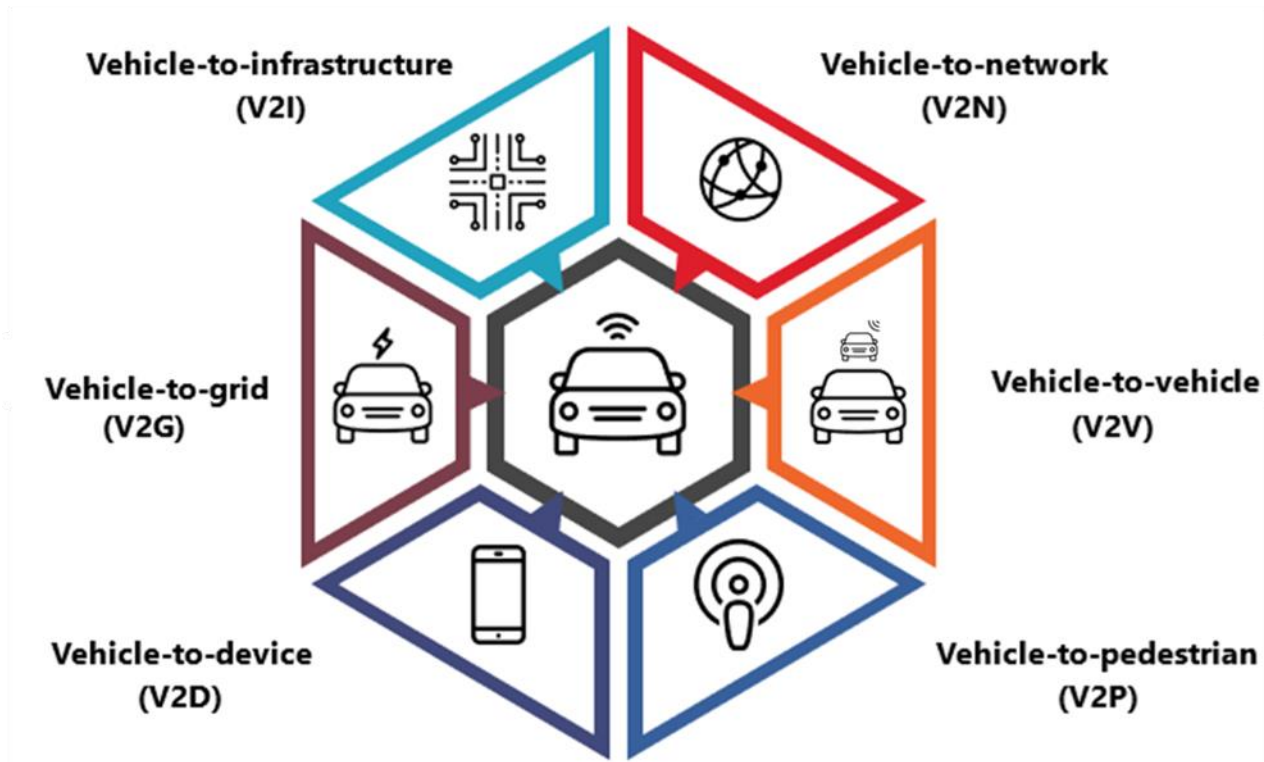


Figure 4 Division of V2X Technologies

In Table 2 some examples of applications of V2X can be seen as well as how these are beneficial and what kinds of channels can they use. This can also help us understand that even if 5G seems like the option that has the most followers there are also other ways.

Table 2 Example uses of V2X technologies

	Road Safety Applications	Traffic Management Applications	Comfort and Infotainment Applications
Potential Benefits	<ul style="list-style-type: none"> • Collision avoidance (safe distance) • Road sign notifications (curve speed warning) • Incident management (emergency vehicle warning) 	<ul style="list-style-type: none"> • Traffic management (intelligent traffic flow control) • Road monitoring (vehicle tracking) 	<ul style="list-style-type: none"> • Entertainment (music download) • Comfort (parking booking)
Channel Models	<ul style="list-style-type: none"> • DSRC • WAVE • Wi-Fi • Cellular Network 	<ul style="list-style-type: none"> • DSRC • WAVE • Cellular Network • ZigBee 	<ul style="list-style-type: none"> • DSRC • WAVE • Cellular network • WiMAX

As Table 3 sums up most of the current status of the V2X, some very interesting advancements have been made. The USA has been experimented mostly with V2X in Dedicated Short-Range Communications and has mostly concluded that 5G is a far better option with development centres like TOYOTA and GMC backing up the idea. In Europe the industry is trying to promote the development of V2X technologies to secure jobs and development, while also experimenting with 4G and 5G, as an Example SIEMENS has worked with Volkswagen Automotive group on successful trials of V2X technologies for easy deployment in their newest cars. In Asia specifically China with the deployment of 5G V2X experimentation has begun soaring. V2X will probably be a standard safety feature in the coming years.[30][31][32]

Table 3 Current Status of the V2X technologies

Current Implementations	Current Challenges
<ul style="list-style-type: none"> ❑ Downloading of maps, weather data, and accident notifications ❑ Info of electromechanical components through CAN ❑ Emergency call system (e-call) ❑ Seemingly compatible mobile phone connection and UI ❑ Vehicles with wireless connectivity ❑ Software locks from the grid 	<ul style="list-style-type: none"> ❑ The infrastructure (for V2I) it hasn't been built nor is widespread ❑ The cellular network connection has to be independent of the e-call system ❑ Access in remote or unpopulated areas ❑ Security issues such as future proofing ❑ Security issues: data integrity protection, Access Control and Hacker Attacks preventions

2.2.2 Artificial Intelligence, Machine Learning and Neural networks

The Oxford dictionary defines artificial intelligence as the theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages. AI in the automotive is made to discern a path to reach and objective and make decisions along the way. For an AI to work and continue working during its life cycle it might need to be updated, but it also requires machine learning. Machine learning is an ability of AI intelligence to automatically improve (there the “learn” as it is the human term of such action) from experience without the explicit need of being programmed for that specific action[33]. Neural Networks are a series of coded algorithms that aim to recognize relationships in sets of data through a process vaguely inspired by the biological neural networks that constitute human brains, albeit more Boolean based, and by being that way it deletes the randomness of instincts or feelings [34] [35] The process of machine learning in combination with a neural network is very helpful during testing as while a specific scenario was never programmed, based on previous experience and what it already has as its rules it will perform well on an unknown scenario[33][36]. An AI is set to work at its processing speed, so as the code is more efficient and the processor is faster the results are better. When it comes to its programming architecture a thing an AI must have in consideration with its processing speed is that it has to be aware of falsification and be ready for failure prevention. By falsification it refers that a variable is not detected an even through redundancy it gets misclassified, correcting this misclassification at the first chance it gets solves the falsification [35]. A real

time self-monitor is also a feature that might use the processor but it is of a great help to the AI as it helps it to continuously be on the defence and correcting them [37] [34] [35]. So the AI will have to handle its methods to be safe while proactively improving its response to scenarios, but also it is important to not forget that decision making and data fusion will also depend on the AI, so a capable processing capability is the key for a efficiently and safely programmed successful AI.

2.2.3 Simulation, Validation & Testing

There is a perception that all scenarios and possibilities should be tested in real-life. Even though the possibilities of existing scenarios in the world is infinite, and testing infinity is impossible some even dare to propose. One of the best takes on tackling the issue is through simulation. A simulation can help detect errors early on and save up costs of prototyping. A simulation also offers a wider range of possibilities to test different scenarios and even create combinations that do not exist in real life. For final purposes and to prevent tempering or biasing a random track can be made to run for the simulation. A system similar to what is used in NCAP for pedestrian protection or ADAS can be used to give the final legal approval on the driving software. The NCAP regulation for this case makes some worst-case scenarios mandatory and randomly takes the non-worst cases to extrapolate [38][39]. And even if this would conclude the test for the AI, there would probably still be a requirement for some mileage to be done before classifying it fully viable. Using the resource of simulation and a lighter test tracked validation can also even help track training and correcting the AI on the spot. Even though similar and more detailed ideas are proposed by people like Harsha Jakkanahalli Vishnukumar [39], and the AIRSIM project [40], this are quite far from getting universal praise and acceptance.

2.3 Safety and Security

Most of the advancements in the field of autonomous cars are created with the idea that a self-driving car is safer than a human driver. Statistically without human error and a competent AI, it will be true that it is safer for an autonomous system to control than a human driver, yet it is also true that an AI cannot comprehend the randomness that human behaviour is (humans have emotions, and shifting moral behaviours based on their surrounding environment and past experience, to get to know all of this and how their emotions and individuality will affect the human rather than its instincts make it a mathematical random variable for any prediction), so it is indeed safer if all drivers are autonomous or human, not a combination. Security comes in hand of making things safer, a secure system is protected from maliciousness directly improving safety, so

it is important to consider. Technology seems to be pointing and pushing to a human driverless future but only time will tell if it really is safer and securer.

2.3.1 Safety

This section takes in account research about safety as a feature of the vehicle, something more in line with the approach of classical (passive and active safety). The classic definition of **Safety** is concerned only with physical harm to organisms and the environment.

2.3.1.1 Passive Safety

Passive safety refers features or systems work when they are called to action by an accident or any other trigger event. They work with the objective to minimize damage and reduce the risk of injury during the time of impact and save lives. All things that are programmable in passive safety are set to automatically deploy when correctly trigger. The design of the chassis and framework are elements of passive safety, as they are designed to always save the interior cockpit absorbing all impact in other elements. Airbags are the prime example of passive safety; they are design to cushion impacts and reduce injuries. Seatbelts have been a staple for quite a while and are attributed to saving many lives. There are other passive safety things like the active bonnet and the pedestrian protection design, or how the pre-crash algorithm unlocks doors and slightly opens the windows to release airbag gases and allow breathing. [41][42]

2.3.1.2 Active Safety

On the other hand, active safety refers to systems and features that are always present while driving, and as such are continuously running in the background activating and deactivating during the ride. Most if not all ADAS functions have a role of active safety. Other than ADAS functions like the ACC, the forward collision warning and the lane departure warnings, things like the electronic stability and traction control or the ABS and breaking are part of the active safety of the vehicle, as their function is that of active safety. [42]

2.3.1.3 Beyond Active and Passive Safety

Safety regards protection from unintentional failures and accidents, while security aims to grant protection from ill-intentioned threats. Safety is clearly of paramount importance, so for an AI system to be effective in automated driving it must be capable of driving safely. A number of major research efforts, such as Pegasus project [43], have attempted to define this. However, what can be considered as safe enough still remains unclear [44] and there is no binding legal agreement on what the rules are, with the result that the necessary

standards are not quite there yet. Other than just driving safety elements like airbags and seatbelts will continue to exist, talking about reducing them to even airplane level standards should be out of the question.

Attacks from hackers or terrorist can be a risk for an electronic autonomous not correctly secured system; at the same time the implications of possible system failures must also be considered, in terms of functional safety (ISO 26262 [45]), as well as safety hazards resulting from functional insufficiencies or by reasonably foreseeable system misuse that are addressed in SOTIF (safety of the intended function, ISO/PAS 21448 [46]). While these standards are relatively mature for more conventional vehicles, further development will be required to adapt them for AI-based automated driving functions.

a. Functional Safety

Functional safety is a subset of safety, concerned only with the safety implications of failures in the functions of programable electronic systems. Functional Safety is the absence of unreasonable risk due to safety hazards resulting from malfunctions of electronic systems. Automotive Functional Safety is regulated by ISO 26262[45]. Making anything "safe" (i.e. eliminating the risks) is not practicable. The pragmatic approach is to assess and mitigate the risks such that the residual risks are at an acceptable level. Hazard and risk analysis is carried out to identify hazards and classify their associated risks in order to determine whether additional safety measures are required to reduce these risks to acceptable levels.

b. SOTIF

SOTIF - safety of the intended functionality, Is the absence of unreasonable risk due to safety hazards resulting from functional insufficiencies of the intended functionality or from reasonably foreseeable misuse by a person. The term "misuse" here really means "unintended use", rather than deliberate misuse with malicious intent. SOTIF is specified in ISO/PAS 21448. ISO/PAS 21448 requires that whether a failure is random or systematic it must be traceable. The objective is to make unavoidable failures "safe". Making anything "safe" (i.e. eliminating the risks) is not practicable. The pragmatic approach is to assess and mitigate the risks such that the residual risks are at an acceptable level. (ISO/PAS 21448 [46]).

As Figure 5 illustrates, faults lead to errors and errors to failures, and a problem with the code is inherited to the component, therefore a problem with a component is inherited into the car itself.

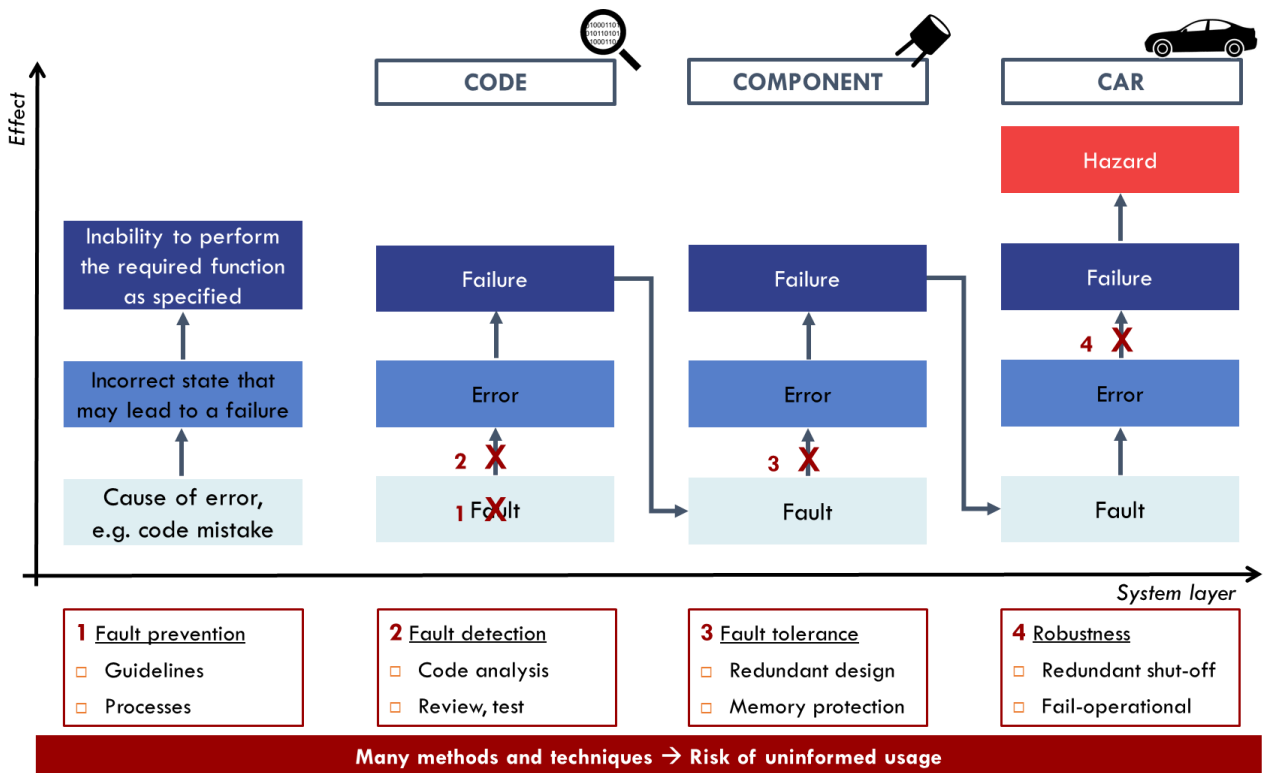


Figure 5 SOTIF errors and its effects and development

SOTIF is has been developing for the past few years. And several techniques and technologies can help us out with the concept quite a lot, Table 4 summarizes some of this technologies and methods. [47]

Table 4 State of the art of SOTIF

Technology	Methods
<ul style="list-style-type: none">□ Measures against random HW failures□ Measures against systematic failures (System, HW, SW)□ Development of safety concepts□ Implementation of safety mechanisms	<ul style="list-style-type: none">□ FTA (Fault tree analysis)□ FMEA (Failure Mode and Effects Analysis)□ FMEDA (Failure modes, effects, and diagnostic analysis)□ Analysis of dependent failures□ ASIL decomposition

c. *ASIL*

The integrity requirements for safety measures are categorised in terms of ASILs. ASIL is the abbreviation for Automotive Safety Integrity Level. ASIL works as a risk classification standard proposed in ISO 26262[45]. Table 5 summarizes and represents how classes and ranks are awarded and how are they functionally classify them. Table 6 on the other hand provides a perspective of hypothetical examples and their approaches and levels.

Table 5 ASIL levels

Conceptually, Risk = f (Severity, Probability)

ISO 26262 risk parameters and classification				
Table 1 – Classes of severity				
	Class			
	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Table 2 – Classes of probability of exposure regarding operational situations					
	Class				
	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

Table 3 – Classes of controllability				
	Class			
	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

ASIL mapping to risk parameter combinations

ASIL Levels:
 ASIL is categorised in four levels (A–D) to specify the required integrity of safety measures to be applied to an item or element of a system to avoid unreasonable risk (with D representing the most stringent requirements and A the least stringent).
 • ASIL is NOT the risk level, but it is related to the risk level.
 • QM (“Quality Management”), denotes no requirement to comply with ISO 26262. Nevertheless, the corresponding hazardous event can have consequences with regards to safety and safety requirements can be formulated in this case. The classification QM indicates that quality processes are sufficient to manage the identified risk.

Table 6 ASIL example

MALFUNCTION of ADAPTATIVE FRONT STEERING	Operational situation			E	C	S	ASIL
	Speed	Environment	Surface				
No superimposition	>100 km/h	Highway	Wet Asphalt	E3	C1	S3	A
Steering Inversion	>50 km/h <100 km/h	Road	Dry Asphalt	E4	C1	C3	D
Oversteering	>50 km/h <100 km/h	Road	Dry Asphalt	E4	C1	S1	QM

Exposure:
E3: 1 – 10% of average operating time
E4: >10% of average operating time

Controllability (Average Driver):
C1: Hazardous situation is simply controllable
C3: Hazardous situation is not controllable

Severity:
S1: Minor injuries
S3: Critical injuries

2.3.2 Security

Security is classically known as the protection against deliberate threats. Vehicle Security are the measures designed to reduce the risk of car related crime. For example, alarms and immobilisers may be programmed to prevent the engine ignition without the detection of the original key or transponder by isolating at least

two of the operating circuits, while an alarm may block the car and disconnect it until it is correctly disarmed. As tech evolves and the vehicles are more electronic dependant treats to its electronics and programming arise, EMC and cybersecurity are concepts that must be part of the current and future vehicle.[42][48]

2.3.2.1 Cyber Security

When talking about cybersecurity as a concept of safety is going beyond the classic vehicle safety. **Cybersecurity** has a much wider scope than safety, being concerned not just with the safety implications of deliberate attacks on data, but also with other potential implications such as privacy (including IPR protection), financial fraud, and the availability of non-safety functions.

As the deployment of wireless connectivity and environment sensors rises in automated vehicles they are expected to become increasingly susceptible to faults and failures due to cyber-attacks. Such attacks may be achieved by external manipulation (e.g. jamming, spoofing, replay etc. see Figure 6) of sensor inputs, GNSS data, and V2X communications [49]. Access to in-vehicle networks may also enable direct control of vehicle functions. Recommendations relating to vehicle cybersecurity are already available (e.g. SAE3061 [50]) and more comprehensive standards are currently in development. However, AI-based systems will have unique vulnerabilities. For ex-ample, corruption of the training data for AI systems is a conceivable attack.

The need to monitor and mitigate vehicle cybersecurity breaches raises the need for dedicated security operations centres, which would provide monitoring of the operation of large numbers of vehicles. Cyber-attacks on vehicles are more likely to be identified by their impact on physical traffic flow than by anomalous system behaviour, since manipulation of the vehicle inputs (including GNSS and V2X signals) can modify behaviour without the need to interfere with internal system behaviour.

The main threats of cyber security are authenticity, availability, data integrity, confidentiality. Authenticity or identification means data was generated by legitimate entities and the location matches, ensuring integrity. Availability means information is exchanged, processed, and accessed in real time. Data integrity or data trust means anything received is unaltered during transmission. Confidentiality or privacy is never disclosed to someone unauthorized.[49]

Security attacks

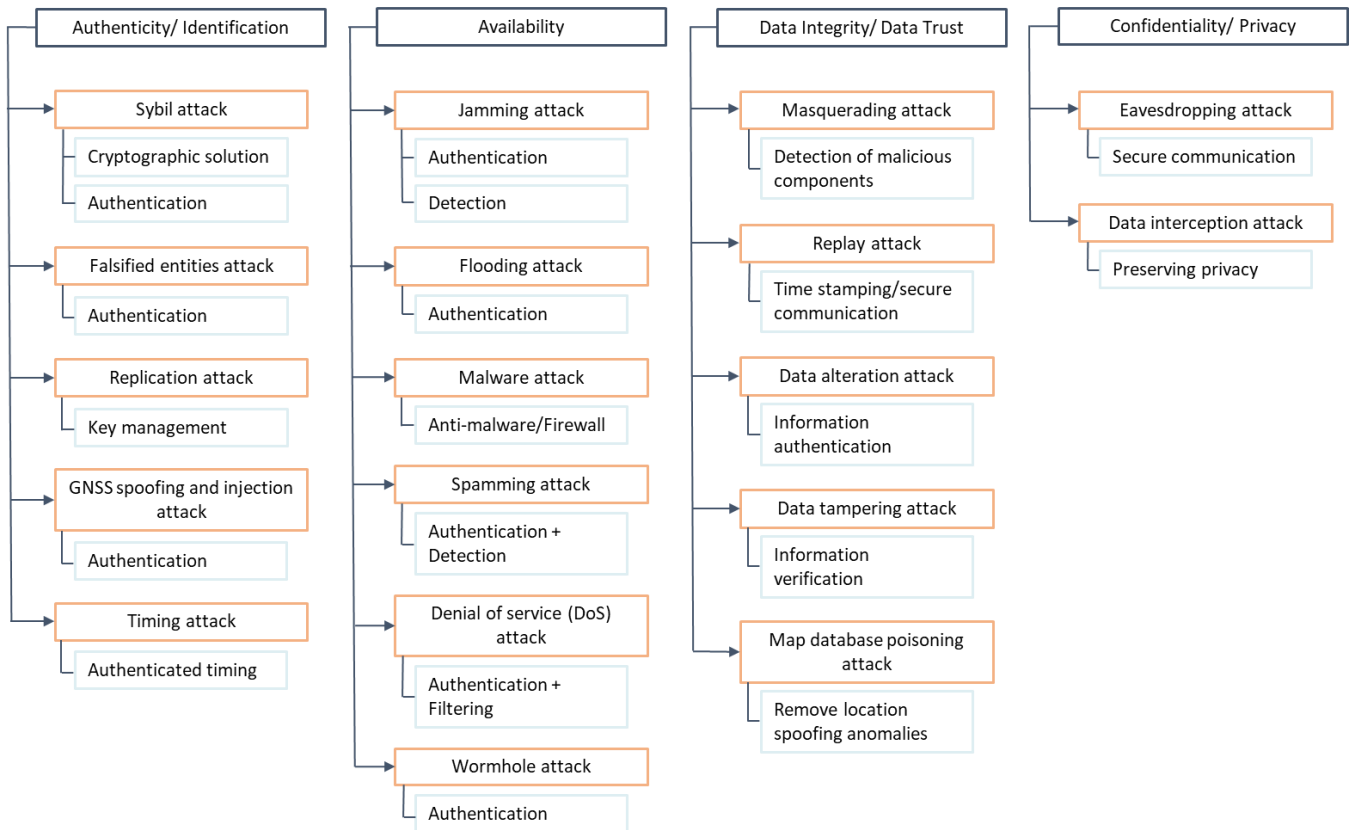


Figure 6 Types of cybersecurity attacks and counters

A further consequence of cybersecurity concerns, as well as of increasing reliance on software controls, is that the need for software updates will become increasingly common. Consequently, over-the-air (OTA) updates, which would avoid the need to visit a service centre for wired downloads, are a topic of considerable interest in the automotive industry. Furthermore, the ability to modify vehicle software could also be of interest as a new business opportunity, by providing the possibility of remote vehicle upgrades and/or differentiation, resulting in a “software defined vehicle”. However, OTA updates are also a potential source of new safety issues, as well as providing a further entry point into vehicle systems for malicious attackers.

A security case could be considered that, similarly to the safety case provides a convincing and valid argument that a specified set of critical claims regarding the properties of a product, process or service are adequately justified for a given application. However, in the case of cyber security it is not possible to be certain about the “environment” (i.e. human attackers), only that it will change over the long operational life of a product such as a vehicle. Consequently, the security case will need to be much more dynamic than a traditional

safety case. Furthermore, with evolving software, the safety case will similarly need to be adapted throughout the vehicle lifetime.

2.3.2.2 Intentional Electromagnetic Interference

A known problem in cyber security is jamming or problems with EMC (electromagnetic Compatibility). Jamming happens when a strong signal or impulse overrides or causes malfunction, on functions and components. Electronic Counter Measures, also known as ECM are the military responses to jamming. An EMP (electro magnetic pulse) is a short burst of electromagnetic energy creating an electromagnetic field that affects electronic components, though mostly man made it can be created by natural causes. The effects of an EMP on a fuel vehicle wouldn't be as severe, but as more vehicles rely heavily on electronics and electric and hybrid vehicles are a thing the effects of an EMP could actually affect functioning and be deadly (for more info about the threats of an EMPs see: <http://www.empcommission.org/>). In the case of civilian vehicles an interesting solution that could work is replace the CAN interface with something more secure and anti-jamming like the USA military does. [51][52]

2.3.3 Trust, Reliability and Availability

The trust on autonomous systems is deeply rooted in human acceptance, and its success will depend on trust. Sometimes releasing a technology ahead of its socially accepted time might not be the best strategy, a great example are touch screens, in the 1990's PDA (Personal Digital Assistants) companies were pushing for the technology with a limited acceptance and now a days everyone seems to have a touchscreen smart phone. Trust will come when reliability is achieved, or believed by society, and its availability is widespread. Reliability is the quality of being trustworthy or of performing consistently well. Availability on the other hand is the degree to which a system, subsystem or equipment is obtainable and has an ease of use an access.

Any change in something that has been done the same way since its conception is viewed with great scepticism. Many people regard the prospect of widespread deployment of automated vehicles with alarm, and not purely on the grounds of technological capability. Human driving has been something that has been experienced by most people and changing this suddenly could do more harm than good: both sociologically (by taking jobs) and in terms of trust [53].

Even though automated driving is theoretically safer than human driving, and 90% of accidents are due to human error, the distance covered by humans in vehicles is more than that of autonomous cars, and there is

not have enough statistical evidence of everyday applications in a human-AI environment or AI-AI environment to completely confirm that they are safer [53]. Another important detractor from trust is mode confusion [54]. Mode confusion occurs when the human operator is confused about the current mode of the system, or cannot remember how the system will react in the current mode [55].

It has been suggested that the best strategy is for manufacturers to slowly build acceptance and need in their technologies, thereby making them a customer standard in no time [56]. For example, people currently trust Amazon's Alexa and Apple's Siri with a lot of information in exchange for the performance of menial tasks. Nonetheless, a system such as a vehicle has much higher potential to cause significant harm and damage, with the result that robust technical arguments are required to build trust in automated driving technologies.

2.3.3.1 Vehicle Resilience

Vehicle resilience is a safety management philosophy that emphasises complex sociotechnical systems into making a vehicle to recover from difficulties. In the past, incidents have prompted safety concerns. Resilience Engineering (RE) enhances safety systems by taking a proactive approach to safety. The notion of resilience engineering has been accepted as a new tool for proactive safety in safety management. When a system is under duress, resilience refers to managing unforeseen changes and prospering. Responding, monitoring, anticipating, and learning are the cornerstones of a system's resilience. When a robust system drifts towards harmful activities, it must monitor its condition and adjust its bounds. A robust system requires managing the decision-making process when the goals and priorities are clearly established. Instead of regarding performance and safety as mutually incompatible, RE enhances a system's performance by correlating them. RE has been used as a safety management technique in a variety of industries, with positive results. Aviation, automotive, healthcare, petrochemical plants, manufacturing, trains, and construction are among these domains. [57]

2.4 Dependability and Assurance

For CAVs to be successfully adopted there is a need to establish public trust in them. To be trusted they need to be dependable, and their dependability needs to be assured. Dependability is the ability to perform (i.e. deliver required functionality, safely and securely), as and when required; and assurance is the set of justifiable grounds for confidence that the risks of using a product, process or service are acceptable to the stakeholders [1]. Dependability encompasses operational aspects (availability, reliability, durability, maintainability) as well as safety and security.

An autonomous vehicle is considered dependant if it follows these aspects: [58]

- **First** it has a flexible system design.
- **Second** it has an adaptive graceful degradation.
- **Third** it has an effective use of sensor/actuator modalities and does not lead to passenger harm.

Traditional approach for simple systems has been to identify performance criteria and test methods for specific functions in standards. Establishing assurance is then a simple case of demonstrating compliance with standards. This simplified approach of achieving regulations like the UNECE is reviewed further on the next chapter.

Technological change is increasingly rapid, so standards that reflect specific technologies struggle to keep pace and are unlikely to reflect emerging technologies. AVs are complex Cyber-Physical Systems (CPSs), having hardware and software, and so they become vulnerable not only to failures, but also to cyberattacks. Complex systems that are heavily reliant on software and that may also interact with other systems to provide enhanced functionality, are now also capable to be modified to alter functionality during their life cycles via updates [59]. This happens within a competitive industry that is always releasing new services and features and complying with assuring people's safety is more of a requirement than an ethical responsibility. Increasingly, assurance is moving towards providing evidence to support claimed achievement of more abstract goals than compliance with prescriptive tasks. In functional safety, for example, it is recognised that complete safety is impracticable, being unachievable in practice and unaffordable if it was possible. In functional safety, therefore, the overall goal is to identify the safety hazards associated with possible failure of the functions of programmable electronic and electrical systems, and then ensure that the safety risks are at levels that are acceptable to society. This may require additional risk mitigation measures to be implemented in pursuance of achieving the necessary risk reduction. Assurance is then based on collating the evidence for this in a "safety case". The main point is that the evidence is generally more subjective in this situation than the more objective "pass the test" evidence of traditional assurance. It has more of the flavour of a court-room argument, where the evidence is intended to establish guilt as "beyond reasonable doubt" (in the UK, at least) – so while not necessarily certain, considered to be extremely likely. In fact, it may well go to court if there is an accident involving an automated vehicle!

2.4.1 Assurance Cases

An assurance case is a living document assuring a system's critical properties. The most common way to do it is through a safety case. Assurance cases work under the notion of CAE (claim, argument, evidence), the

elements needed to assure the system is hazardless. The use of safety cases is a valuable tool. In safety engineering it is common practice to construct a “safety case” to support assurance claims. The safety case comprises a documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding the safety properties of a product, process or service are adequately justified for a given application in a given environment. Typically, this will include performance validation data. [60]

Safety cases for the automotive industry are essential saving lives. Passive and active safety maybe perceived by the trained naked eye when they fail while functional safety or cybersecurity might be harder. While developing a safety case before getting to the evidence, safety arguments, claims or requirements, is important that to have the homologation requirements as prerequisites and the objectives for risk mitigation this are known as *predefined safety requirements* [60]. (Figure 7, shows an example of the creation of safety case as shown by [61]). Also, it is important to comply with standards, manufacturer standards and ISO style standards; and that the safety process takes in account its contextual limitation, plus the requirements of other safety processes as for example and active bonnet and how it is trigger. The evidence of safety arguments may come from testing or simulation, but it may also be inherited from claims of compliance with a standard, for example ASIL level. A safety argument is the essence of a safety case; a multi-stage, hierarchical construct, broken down into a network sub-claims with their own arguments and evidence; while it is totally dependent to the context of the case (a context-free safety case is unreasonable), it serves as the idea that links the evidence and the claims. A safety claim is an idea that is supported by enough evidence and should be a requirement of the vehicle [62]. A safety case must be clear communicating the ideas to be convincingly and acceptable; and by acceptable it does not mean absolutely safe, as that is theoretically impossible, but safe enough to tolerable risk [63]. The probabilistic approach and the concept of *As low as reasonably possible* (ALARP), is an idea that started by the British government to secure and save lives on the oil and gas industry, and from there it extended like wildfire to the other industries in the European Economic Area that might need them (railway, automotive, Aerospace, etc.).

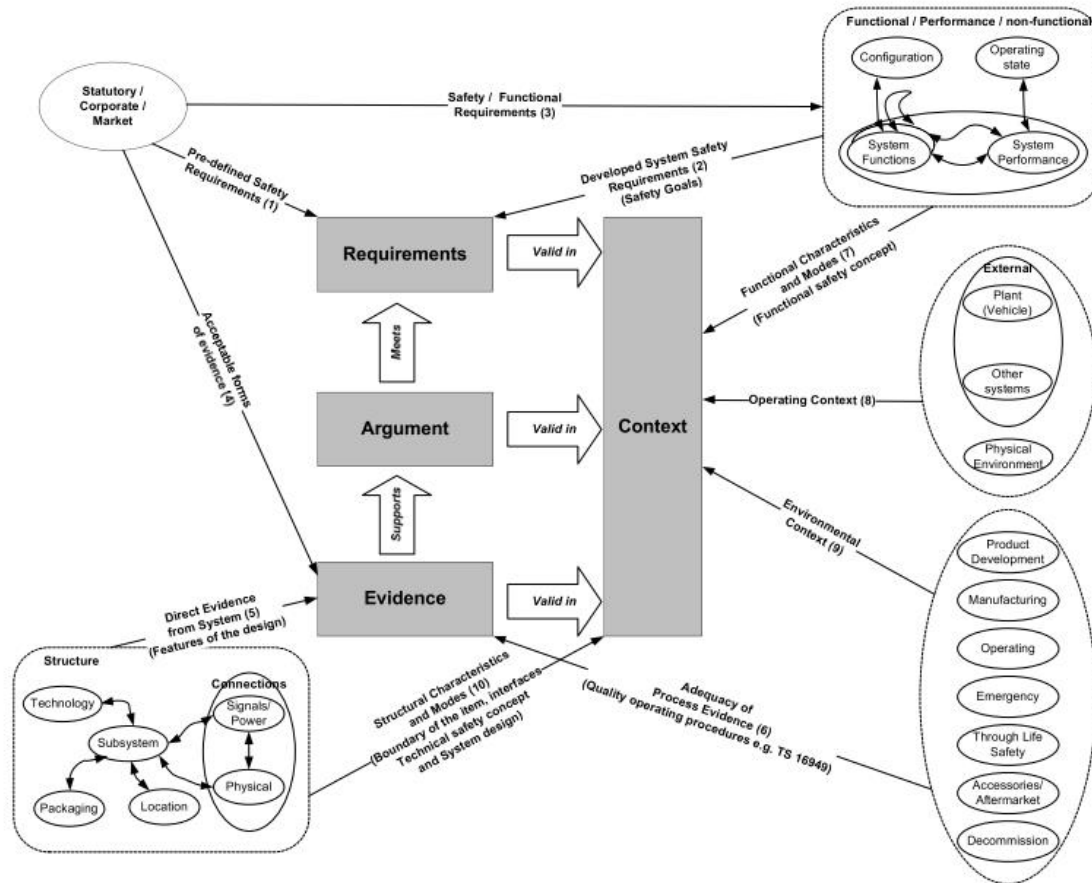


Figure 7 Safety Case Dependencies (based on [61])

Safety cases can be categorized in three types: Generic product Safety Case (GPSC) independent of application and can be re-used for different independent applications, Generic application Safety Case (GASC) for a class or type of application with common functions, and Specific application Safety Case (SASC) for a specific application used for only one particular installation.[64]

Techniques useful in safety cases include Dempster–Shafer theory (DST) also sometimes referred as evidence theory, and it consists of a general framework that deals and reasons with uncertainty through understanding connections to other frameworks[65]. Another method commonly uses in creating a safety case is through FMEA (Failure Mode and Effects Analysis) this structured technique approach aims to discovering any potential failures that may exist within development process or the design of a product [66][67]. A popular and very engineer like approach is FTA (Fault tree analysis), a graphical input that heavily relies in the use of Boolean relationships to bring to light the reasons and causes of system level failures [62][66][67]. Other

techniques like probabilistic risk assessment (PRA), Objective Quality Evidence (OQE), Hazards and Operability Analysis (HAZOP), Cost-Benefit Analysis (CBA) work with ALARP.[64][68]

Building a safety case requires a significant amount of resources. Creating a good safety case takes time and people that in the current state of the industry it may be hard to justify and are easy targets for budget cuts. Using too much time and resources in these activities is not what industry executives view as the best investment [60]. The proposal of the agile safety cases saves time in two essential ways; one is reusing opportunities, previous work and experiences to save time and use all of those to start creating the next safety case; the other one is to create templates for different types of application. Working with templates or other works tend to increase the understanding of the systems and efficiency. Safe Scrum is a tool in a work in progress state that could eventually be useful. [64] The planning and initial phases of the safety case are important to create awareness and a real scope of the safety case. A continuous follow-up and progression of the safety case seem to be part of the recipe for success. Reducing extra effort and time is what the industry aims for, but the idea of creating safety cases just to pass a certification, regulation or requirement, instead of creating a safety case to make the product or process safe, defeats the true objective of the safety case[60].

As per Iso 26262 and the MISRA safety analysis, it is important in assurance cases for functional safety, in this methods controllability is set in classes and risks are set into groups. [69] The MISRA documents aims to identify the need to protect vehicle software from unauthorized access that could compromise the performance of safety-related systems. On the MISRA method risks are classified in combination with severity and probability; acceptable risks are classified in anything from R0 to R7, anything above R7 called R7+ in a non-acceptable risk.[70]

With the dependencies of connected vehicles to electronics and software, safety is not possible without cybersecurity. [71] Although there is overlap, safety is mainly about faults (through time, misconfiguration, strain etc.) and security focuses on protecting against someone who wants to deliberately induce those faults; therefore, in order to apply real safety, the system has to be secure. Creating assurance cases for security is more fluid task then in safety because the threat landscape changes so quickly.

A way to approach how to do an assurance case for a security scenario is doing a black box approach (external security) and a white box approach (internal security). Then a Threat Analysis and Risk Assessment (TARA) should be performed to identify the possible threats against the target which can lead to security incidents. To prevent safety violations from happening as a direct consequence of a security vulnerability a Hazard Analysis and Risk Assessment (HARA) should be made and analyse the results in terms of security. For TARA

to go with HARA different testing techniques and best practices must be held consecutively. Since most black box approach tests are doing post development, they are considered penetration tests, and preparing for them in the assurance case ground is important before testing. [73] A security assurance case just like a safety case takes a tremendous amount of time to prepare, and the people working on them need training. And even when assurance cases in the safety department are used often; when it comes to security it is more limited, this brings concerns over if a security case could be a risk by itself and the long going debate of the effectiveness of security by obscurity.[74]

2.4.2 Safety and Security Analysis Techniques

There are different techniques and ways to prove that a system is as hazardless as desired. An assurance case based on correctly linking claim, argument and evidence. This section reviews different techniques for creating assurance cases, propose arguments and claims, and show proof of evidence.

There are over 86 methods of safety and cybersecurity co-engineering methods that mix and match various techniques. Out of these methods just 20 are compliant with safety-security regulations and standards. And not even half of the methods are capable of communicating the results clearly to stakeholders. [75] This section focuses on explaining relevant techniques to support dependability and assurance.


2.4.2.1 Argumentation strategies

Arguments in assurance cases is a link between the evidence and a claim. There are two kinds of induction are commonly used in argumentation: enumerative induction and eliminative induction. In enumerative induction enumerative induction, confidence increases as confirming examples are found. On the other hand, eliminative induction finding the truth and full confidence by using evidence to eliminate false cases of success, therefore confidence is constructed based on the variety of instances that support it. The process is an idealization there is always some uneliminated (residual) doubt in an argument. [76]

2.4.2.2 Goal Structuring Notation

GSN (Goal Structuring Notation) is a safety case form that visualizes an argument structure that supports a claim to be true. In the industry in which safety assurance is critical, standards such as IEC 61508 (general), ISO26262(automotive), DO-178C(airplane), etc require documentation of "Safety Cases", and GSN is the standard format to document the cases graphically.[63]

Table 7 Structures of GSN

Vanilla GSN Symbols	Description
 <p> {Goal Identifier} <Goal Statement> </p> <p> {Strategy Identifier} <Strategy Statement> </p> <p> {Solution Identifier} <Solution Statement> </p> <p> {Context Identifier} <Context Statement> </p> <p>©goalstructuringnotation.info</p>	<p>A goal, rendered as a rectangle, presents a claim forming part of the argument.</p> <p>A strategy, rendered as a parallelogram, describes the nature of the inference that exists between a <i>goal</i> and its supporting <i>goal(s)</i>.</p> <p>A solution, rendered as a circle, presents a reference to an evidence item or items.</p> <p>A context, rendered as shown left, presents a contextual artefact. This can be a reference to contextual information, or a statement.</p>

The “vanilla GSN” defined above in Table 7 has extensions that make the safety case building more effective this extensions include: maintenance of arguments, modular safety cases, assurance case patterns and more. As a techniques that is easily perceived accepts advanced concepts, it has been appearing in the domains of safety and security. [63] [77]

The latest standard of GSN released in 2021, [78] defines the addons that can be applied to increase the complexity and deepen the assurance case process. The first add-on is known as *Argument Pattern Extension*, that lets represent arguments as abstract patterns rather than merely arguments. The second add-on *Modular Extension* that lets partitions on the assurance case to later interact in an overall argument. The third extension, *Confidence Argument Extension*, considers that an Assurance Claim Point (ACP) is associated with an assertion. The final add-on is the *Dialect Extension*, this testing truth, logically disputing and constructively criticising; this extension would consider the basis eliminative argumentation as confidence maps.

2.4.2.3 Attack Trees and Attack-Defence Trees

Attack trees (ADT) provide a formal, methodical way of describing the security of systems, based on varying attacks. Attack-Defence trees (ADT) are an extension of attack trees that provide counter measures to attacks. Basically, represent attacks against a system and the defences that a defender can employ to protect

the system; in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes. [79]

To create attack trees:

- Identify the possible attack goals.
- Let each goal forms a separate tree (although they might share subtrees and nodes).
- Think of all attacks against each goal.
- Add them to the tree and repeat.

ADT's is represented in a logical way and follows the node flow in one direction. It is a popular technique for analysing threats in cybersecurity.[79]

{Appendix E provides an example of an Attack Tree}

2.4.2.4 Systems-Theoretic Accident Model and Processes

Systems-Theoretic Accident Model and Processes (STAMP) is an accident causality model based on systems theory and systems thinking, represents a paradigm shift in accident modelling and hazard analysis. STAMP shifts emphasis from failure prevention to identification and enforcement of constraints on system behaviour and component interactions; meaning that events leading to losses occur as a result of ineffective enforcement of safety constraints.[80]

2.4.2.5 Failure Modes and Effects Analysis

Failure Modes and Effects Analysis (FMEA) is hazard and reliability analysis technique, mainly used at the design stage, due to its proactive emphasis on prevention; its main advantage is that provides a mean to compare, from a risk point of view. When developed it becomes a systematic method organized in tables and flowcharts. FMEA essentially contains at least the following things:

- Steps in the process.
- Failure modes.
- Failure causes and effects.
- Detection, occurrence, and severity.

2.4.2.6 **Fault Tree Analysis**

Fault Tree Analysis (FTA) is also hazard analysis technique created to evaluate the unique interrelationship of events that lead into states of failure, undesired, or unintended. It works in a deductive form from the root to the nodes, and uses logical gates (and, or, nor, etc) to interconnect events.[81]

2.4.2.7 **System-Theoretic Process Analysis**

System-Theoretic Process Analysis (STPA) is a hazard analysis technique developed with the idea of being more comprehensive with autonomous vehicles and better identifying the systemic and interaction related problems of complex software in intensive electric and electronic systems.[82]

2.4.2.8 **TARA**

In automotive threat analysis and risk assessment (TARA) is commonly used for analysing security threats. As common of a risk assessment method it begins with asset identification. Assets scenarios and impacts are categorized in confidentiality, integrity, and availability (C, I, A) ratings. With that impacts are measured between negligible to severe and assigned one of the four following categories: safety, financial, operational, and privacy (S, F, O, P). In addition to impact, attack feasibility is determined. Finally, impact and feasibility values are used to determine cybersecurity risk level. [83]

2.4.2.9 **EVITA**

A TARA method meaning E-safety vehicle intrusion protected applications its main focus is on how intra vehicular operations work and how they are trustworthy of protecting data. Mainly its goal is to make the on-board architecture of vehicles secure by design. Works with the analysis of existing threat scenarios, by creating security anchors with trust hardware security modules, while following existing requirements. [84][85]

2.4.2.10 **STRIDE**

In the field of TARA and based threat modelling, another method is Microsoft's STRIDE; whose name is an acronym for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service (DoS) and Elevation of privilege. In addition to Authorization, Authentication, and Non-Repudiation (AAN), this methodological approach seeks to guarantee that an application satisfies the security standards of Confidentiality, Integrity, and Availability (CIA). Security subject matter experts create a data flow threat diagram initially in the

cybersecurity process. The application is then examined by system engineers and/or other subject matter experts utilising the STRIDE approach. [86]

2.4.2.11 AVES

The Automated Vehicles Safety and Security Analysis Framework (AVES) has the objective of mixing 4 relationship matrices with a Safety and Cybersecurity Deployment (SCSD) model to facilitate the risk analysis of autonomous vehicles. Matrix 1 contains hazards and the threats of the targeted vehicle plus the associated risks and regulated requirements, Matrix 2 contains safety and security countermeasures, Matrix 3 contains the links of the countermeasures and Matrix 4 contains the recorded status countermeasures. The 4 matrices are set on a meta-model that analyses the vehicle's development lifecycle and the standards. AVES is implemented in eleven stages, and aims to work on the different levels of vehicle autonomy.[87]

2.4.2.12 HARA & SAHARA

Hazard Analysis and Risk Assessment (HARA) is commonly used in Functional Safety. The goal of HARA is to identify failures that might lead to E/E system hazards and estimate the risk that comes with them. A Security-aware hazard analysis and risk assessment (SAHARA) is an extended HARA added with STRIDE-based security, that considers the ASIL levels. It gives provide hazards and risks deeply oriented with the well-known ASILs letting the user have a better minded or oriented result. The inclusion of STRIDE, a security model developed at Microsoft, makes SAHARA a well oriented method for risk analysis. STRIDE is a system that gets its name from the threats it focuses on: Spoofing, Tampering, Repudiation, Information disclosure (privacy breach or data leak), Denial of service, and Elevation of privilege.[88]

2.4.3 Incorporation of Safety Aspects of Cyber Security into Safety Cases

A risk-based approach like the one exposed in safety cases seems inherently well suited to cybersecurity, where the threat (the equivalent of a hazard in safety) is not readily defined. Some threats will be foreseeable so can (and should) be addressed before product launch, but unforeseeable threats are highly likely. They depend on human ingenuity and motivation to interfere with the correct functioning of programmable electronic systems. The unforeseeable threats can only be responded to reactively, so assurance inevitably becomes an ongoing process throughout the life of the vehicle.

The incorporation of security into the safety assessment has impacts on verification and validation according to the British standard PAS 11281:2018[89]; the things to consider are:

- The Integration and interaction of requirements.
- Supply-chain integrity.
- Post-deployment malicious events that may arise or change in nature in an ever evolving environment.
- Reduced lifetime of installed equipment for security control.
- Threats to the effectiveness and independence of safety fences.
- Design changes and patches to address the operational use.
- Possible exploitation and confidentiality of information.
- Trustworthiness of the evidence offered.

When considering the implementation of safety and security together, most approaches are considering functional safety, and as a result do not handle indirect threats like kidnapping. Assurance cases also do not take in account fraud. A full approach should be considered wider.

2.4.4 Automated generation Safety Cases

The use of software and automatic simulation of arguments and scenarios for the creation and use of safety cases are a way out that does not just come up with many ideas of what is unsafe, it can also test worst case scenarios, defining the real worst case: and software should not have confirmation bias, a current problem with safety case creation and something hard to avoid if humans create the software (as it will have this bias). Confirmation Bias is a tendency of the human brain to favour the information that would confirm their preconceptions falsely making a hypothesis true. The value of a safety case comes when its objective is to be safe and a safety engineer tries to prove how it is unsafe, these 2 contrasting opinions are in a way a form of combating confirmation bias; yet another problem is the idea of the ALARP concept blinds the creator of the safety case from the real worst case scenarios. The use of a safety case software that builds safety cases and validates them (by itself) reduces the human error, while improving the time it requires to build a safety case; and makes the use of templates and previous ideas more efficient. There is great software for safety case building in GSN format like AsthaGSN, but scenarios where an AI generates a full safety case is something that has not been made possible yet. Even though Astah and SafeScrum are great tools that use templates to their advantage there is still work to be done to make this software neat enough before self-generation.[68][64]

2.4.5 Limitations of Assurance Cases

The problems faced in assurance are not just finding the leverage and balance between safety and cyber security, but making it blend seamlessly. And even though a united holistic approach is the best idea to not just comply with rules but to make things safer there is more work to be done. Some of the challenges faced are:

- Linking to an evidence, while being able to identify bias.
- How to handle the non-deterministic behaviour of AI systems – how can the safety of these be argued and what kind of evidence would be required to support these arguments?
- How to handle evolving systems – e.g. due to SW updates or unsupervised learning by AI?
- How to give a more balanced view in the safety case (Maybe calling it a risk case rather than a safety case; but perhaps showing the failure of arguments for “non-safety” could help[68]).
- Assurance cases need a better and more explicit handling of uncertainty.
- There needs to be a deeper understanding of where formal methods might add value.

An assurance case should cover what is foreseeable. When the unforeseen is encountered it then becomes foreseeable, and existing assurance cases should be updated to reflect it and future assurance cases should take it into account as now part of the foreseeable through “lessons learned”.

2.5 Legality of autonomous vehicles

2.5.1 Safety and Security

The world as currently known lives in as a society that has rules, these rules lead to laws and regulations. The vehicle industry has no escape from those. For example, the vehicle manufacturers are bound by the ECE regulations in many regards. The ECE regulations are still recorded under this name because they were developed by the Sustainable Transport Division of the United Nations Economic Commission for Europe, as the ECE rules for commercial vehicles. As of the year 2010[90] World Forum for Harmonization of Vehicle Regulations adopted all the ECE for the world. These regulations for example dictate how headlamps should illuminate, lumens, valid positions, etc. {UN R1, 20, 31}. These regulations are based on the knowledge developed by engineering of safety and common sense. There exist regulations for seat belts and child chairs

{UN R14, 16-17}, collisions {UN R32-33, 93-95}, fuel tanks {UN R34}. Appendix B has all the ECE regulations.[91]

The harmonization of the ECE rules was to help the Transatlantic Trade and Investment Partnership in 2013, but it also led the way to directly link with the GTR (Global Technical regulations). World Forum for Harmonization of Vehicle Regulations also manages these regulations. The Global Technical Regulations are developed under the 1998 international Agreement on vehicle construction to which the EU is a Contracting Party. This Agreement currently has 38 Contracting Parties (including the EU, Japan, Russia, Korea, China, India and the United States of America) [91][92]. This regulations include testing requirements before a vehicle's market release for example, simulations and tests for crash{GTR 5,7,14}, or requirements for cyclist and pedestrian protection{GTR 9}.

The World Forum for Harmonization of Vehicle Regulations uses the previous regulations to help countries develop their legal inspections and their follow up of the requirements, for example the MOT (Ministry of Transport) inspection in the UK or the ITV (Inspección técnica de vehículo) in Spain.

It must be kept in mind is that UNECE/GTR regulations are a minimum, and as technology advances so should they. The latest meeting to update will happen on the 26th of august during year 2022 and will be regarding vital topics for this literature review, Topics are on the improvement the UNECE regulation UN R155 on cybersecurity approvals and UN R156 on software update approvals. Consumer tests (like NCAP) and insurance company tests are based on GTR to qualify and rate the vehicles. This private test due increase the requirements over the minimum and make the standards more aggressive. As of recent year, more manufacturers aim to not just achieve the legal standards but perform well in this consumer tests.

2.5.2 Insurance and Liability

A question that is probably on the mind of anyone reading this is "In case of an accident, who is to blame and how will that be legally handled?". Fear not, it is a common question, as technology prepares to face the world the legal world is slowly trying to adapt. A factor that does not work in favour of autonomous systems is the criminal liability in accidents, especially those that lead to death or damage. These takes to the questions of who the blame on, the owner of the product or the company that created it. Autonomous systems raise high hopes due to their numerous societal benefits, these socio-technical artefacts also raise many challenges, both technical and non-technical. Safety is one of the most pressing ones. Without sufficient safety, public trust in these systems will not gain enough traction to be effectively deployed. Safety can be incentivized and mandated through different mechanisms. For instance, ex ante safety requirements

and processes are essential building blocks in order to foster trust in autonomous systems. The law may play an important role in framing these safety requirements both during development and deployment phase.

Currently, there are many legal obstacles for deploying autonomous systems into the real world. The mere legality of such systems is questioned[93]. For instance, self-driving vehicles are not yet fit for most road traffic rules. Adaptations will be made necessary. However, some countries have started initiating experimental frameworks in the interest of manufacturers to test their vehicles in real life conditions (See for instance Belgium and France which have introduced experimental frameworks for testing to be carried out.). Certification and approval schemes for autonomous systems will also have to be adapted, due to their intrinsic features, namely their dynamicity and self-learning nature. But these legal considerations are not the only ones that may hamper the development and deployment of autonomous systems.

Indeed, fostering trust in autonomous systems through ex ante safety requirements and assurance frameworks, approval schemes and legal frameworks is not enough. Ex post compensation mechanisms for damages caused by autonomous systems will become another crucial element in the trust building exercise. Currently, there is a multiplicity of liability regimes which vary from one sector to another. As an example, AXXA has proposed a policy for insuring vehicles[94]. These systems' dynamicity, autonomy, data reliance and opacity will greatly challenge the implementation of current liability paradigms.

For instance, when fault liability applies, the victim may find it technically difficult (if not impossible) and costly to identify the source of the damage and attribute it to one or several parties. Indeed, with such systems being for most part autonomous, ascribing liability to a human agent may become difficult[95]. Moreover, establishing causation, a usual prerequisite of applying liability, will become extremely burdensome. However, in some instances, strict no-fault liability regimes may continue to apply (minus certain amendments)[96]. Furthermore, many authors have noted that such technologies may ultimately shift the control from the human operator towards the machine, resulting in a liability shift towards the manufacturer[97]. Product liability is said to have a more prominent role in future litigation suits.

2.6 Over the Air Updates

Software is always updated in a PC, PLC, etc., it gives maintenance fixes minor or problematic bugs and keep things fresh. Now a day's everyday vehicles have a lot of software that are updated for example the infotainment systems or the digital cock pits. This update can be more frequent, efficient and faster (due to smaller size) if they are done by connecting online and installing in the background. An over-the-air update is the wireless delivery of new software or data to a device. It can be use by the original equipment

manufacturer (OEM) to fix, block or upgrade the vehicle. (Figure 8). Even though this may cause mundane trouble for the users like the blocking of the fast charging on a second hand first edition TESLA [98].

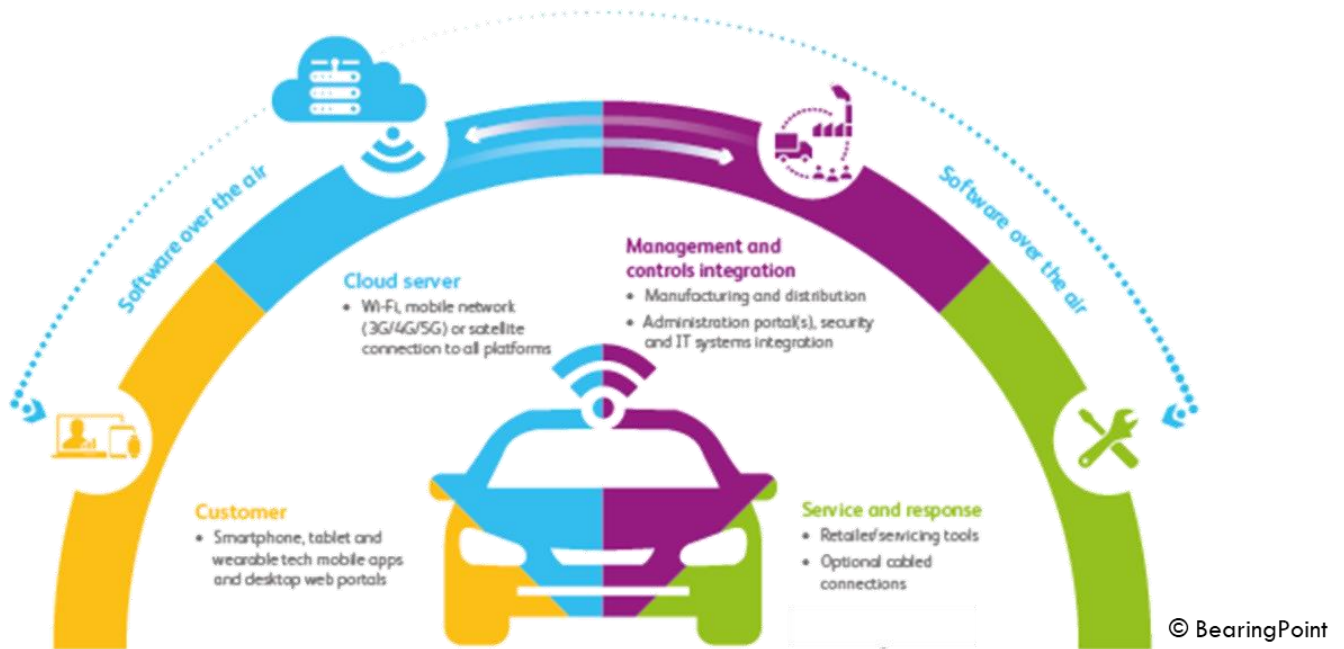


Figure 8 Reach of over the air updates [99]

A vehicle electronic component wise is made of different central units in charge of controlling each vehicle function or set of functions, this unit is known as electronic control unit (ECU). ECUs communicate with each other through a central gateway unit wired to different buses (like CAN or LIN) that allows communication flow within different units. The conditions to achieve and perform a wireless SW update requires the Diagnostic Tester (DT), an element possessing the current and newer software versions and all required keys to authorize the update, to connect the vehicle using its Wireless Vehicle Interface (WVI) to the OEM using automotive diagnostic protocols such as Unified Diagnostic Services (UDS). Once this is done the process can be summarized in 3 steps[100]:

- (i) Initialize the update process and validate and authorization for the SW update
- (ii) Transfer the binary to the ECU
- (iii) Override and flash the ECU.

This steps normally happen locally and remotely in an authorized garage or a service centre, where the DT and the car's WVI are interconnected using Wi-Fi or the requirement of the WVI to connect[100][101]. An example of this could be the ECU updates done by the VW Group's ODIS tool.

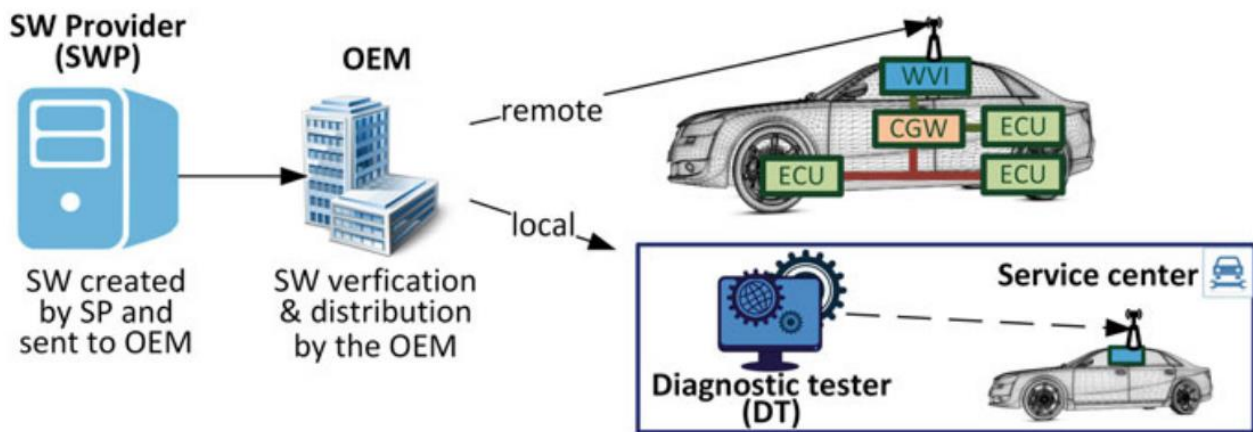


Figure 9 A new SW version is created by the SW provider (SWP), verified and distributed by the OEM and finally installed on the concerned ECU of a vehicle[100]

Firmware over the air updates (FOTA) has been in the telecom industry wide spreader since the 2000's. It has been implemented in the automotive industry and for OEMs works as a standard and fast way to approach the update of ECU's. In the industry and the growing implementation of connected cars, 30% of the car bill of material (BOM) account for software and ECUs [101]. FOTA is vital to be able to deliver vehicles since prototypes, and plays a major role between the start of production and when the units are actually sold.

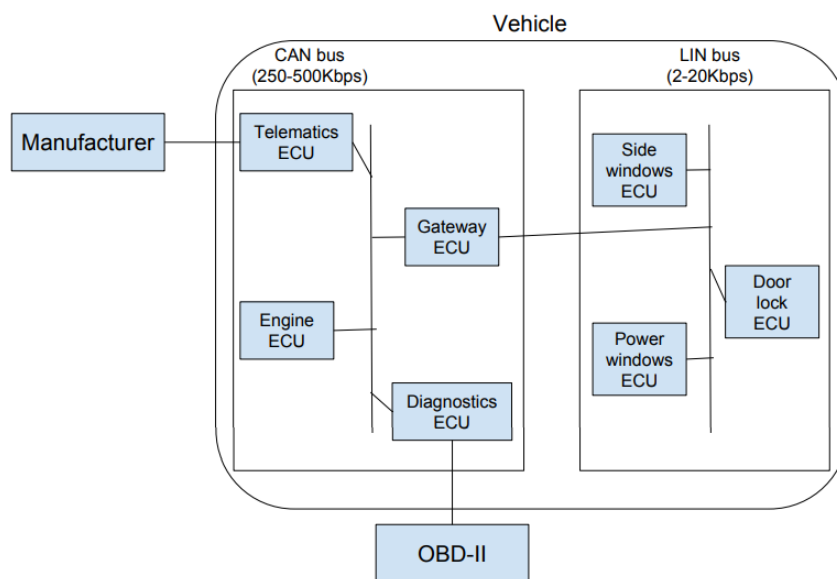


Figure 10 Example of how ECUs are distributed in a vehicle [102]

2.6.1 Benefits and challenges

Even though its uses are wide range of options the most probable reasons to perform an update on a ECU are:

- patch security issues.
- patch safety issues.
- patch functional performance issues.
- Add new or enhanced functions or features.

2.6.1.1 Benefits

There are many benefits for the manufacturer of the vehicle to perform updates over the air, that has made it a *defacto* technique to enumerate some:

- Ease the process of warranty and recalls.
- Can be location independent, so no recalls to factory and close to the user also reduces transportation and allocated space.
- Can be executed simultaneously in many vehicles.
- Software packages are maintained and stored by the OEM, therefore dealers can access the ones needed without maintaining their private repository.
- Leads to forced updating, meaning it can happen even if the client is not actively participating.
- Improves safety by reducing the time a vehicle has been flagged for recall is driven.

2.6.1.2 Challenges

As it has benefits it also has some challenges here the challenges have been sorted in categories:

- Technical Challenges
 - The download and update protocol must be secure
 - It must have secure components to communicate wirelessly to the gateway
 - Should be correctly encrypted and decrypted
 - Prepare for updates to be available in correspondence to battery capacity
- Customer Challenges

- The customer must be notified of any software update
- There should be information of any update available to the customer
- Process Challenges
 - Software updates should remain as low as possible, continuous updates make clients lose confidence on the product
 - Understanding the status of the vehicle before applying the update (if ignition is needed, if an update can be done directly to the latest or are certain versions required first, etc)
- Component Challenges
 - Enough storage should exist to manage the delta after multiple updates
 - The OEM must certify the communication protocol is supported for more than 10 years and the updates available for at least 25 years
- Company Challenges
 - The development of an update system for prototypes is expensive
 - The vehicle should always operate safely after any update to avoid legal claims
- Dealer Challenges
 - Dealers must be trained to perform *day one* patches updates
 - The dealers might lose revenue source (mostly due to lesser repair times)

2.6.2 Over the Air Updates Security

A mentioned problem of over the air updates was how to make them secure, so how can OTA be secure? There are 2 main ways to do so . Blockchains (BC) and Certificate-Based Approaches, and both approaches seem to have similar properties with respect to the added latency as well as the total number of exchanged packets. [100]

The BC technology was first introduced in 2008. It is well known as an essential part of Bitcoin cryptocurrency network, but BC has also been used in other non-monetary like healthcare data exchange or video game match making, due to its security, privacy, and decentralization features. The secure nature of BC originates from the consensus algorithm employed for appending new blocks into each block decentralizing in the process while changing and reallocating the needed private keys.[100]

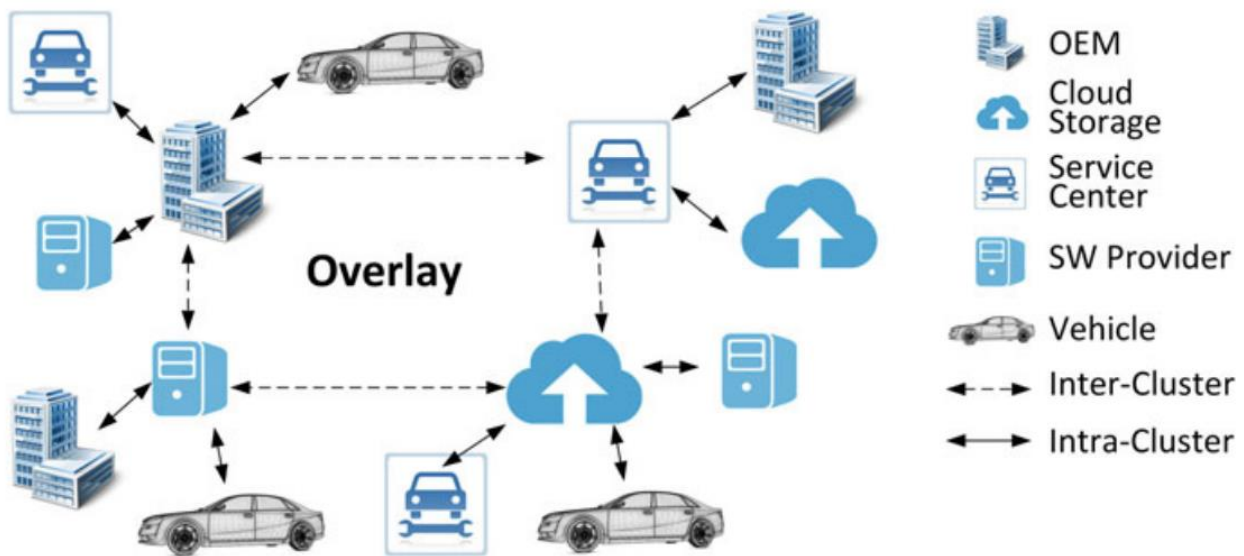


Figure 11 BC Approach [100]

Certificate based approach like Uptane happen when there is a certificate to check the keys and updates are dependent on whether it is signed or unsigned. Uptane is an American update method that achieves to do it in the most secure way possible. Using *The Update Framework* (TUF) and a comprehensive and broad threat model, securing even small details for interventions between the reception and the signing. Uptane has 4 roles under the TUF framework Standard: root, timestamp, release, and target. This are used to sign and securely verify the updates. It also has 5 identified ways in which ECU updates are attacked and is prepared to avoid them. The first one is to prevent the read of the updates, preventing reverse engineering and access to the data and intellectual property. The second one is preventing interception or anyway the information may be altered in between modifying, overwriting, and signing. Third is the prevention of denying an update because an attacker might want to stop fixing issues or vulnerabilities. Fourth is preventing a denial of functionality, this means to avoid losing its functions, logging unknown errors, or looping. And the fifth is preventing control access, this means not letting anything unauthorized be able to ever run, preventing any attacker from making an ECU work their way.[102]

Role	Purpose
root	Serves as the certificate authority for the repository. Distributes and revokes the public keys used to verify the root, timestamp, release, and targets role metadata.
timestamp	Indicates whether there is any new metadata or image on the repository.
release	Indicates which images have been released at the same time by the repository.
targets	Indicates metadata such as the cryptographic hashes and file sizes of images. May delegate this responsibility to other, custom-made roles.

This figure illustrates the four basic roles that must exist on a TUF-securd repository: the root, timestamp, release, and targets roles. The root role serves as the certificate authority: it distributes and revokes the public keys used to verify metadata produced by each of these four roles (including itself). The timestamp role indicates whether there are any new metadata or images on the repository. The release role indicates which images have been released by the repository at the same time. The targets role provides metadata, such as hashes and file sizes of images, and may delegate the responsibility of signing metadata about images to other, custom-made roles. For example, in the figure, the targets role has delegated all images that match the filename pattern "A.*" to the A1 role, and all images that match the filename patterns "B.*" and "C.*" to the BC role. In turn, the A1 role delegates a subset of its images (in this case, only the "A.pkg") to the A2 role. A delegation binds the public keys used by a delegatee to a subset of the images these keys are trusted to sign. This means that the targets role would distribute and revoke the public keys for the A1 and BC roles, whereas the A1 role would do the same for the A2 role.

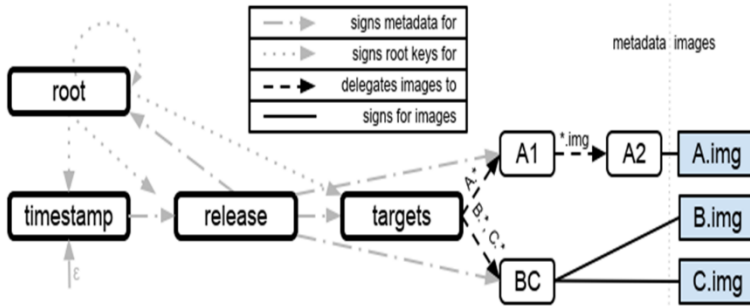


Figure 12 TUF standard applied to UPTANE framework [102]

2.7 Related Projects

There has been a wide variety of projects that are delivering results for the industry. This chapter takes a brief overview of some of the projects

2.7.1 Pegasus

A German funded project, PEGASUS goal is to deliver standards for automated driving. The project concluded by the middle of 2019, releasing an extensive report of highly automated driving functions. Based on the ideal "While driving, one simply switches to the autopilot, sits back, reads, etc." Like in Sci-Fi media. The project emphasises on how the technology technically exists at the present moment and could be adapted and use for this, yet its road usability is the question. The research focuses on the requirements on autonomous vehicles, and if their systems and methods are actually safe and reliable. It is believed by the researchers that without people behind the wheel, it will not work, because the transfer of responsibility from the driver to the automated system comes with high demands, since the humans no longer have to continuously monitor their driving task and can devote themselves to other activities. This leads to an analysis of the human role in the autonomous system process.[103]

2.7.2 Uptane

Is an American open source project hoping to standardize vehicle secure software over the air updates. Uptane began under a non-profit consortium called the Uptane Alliance. The goal is to create a design which protects software delivered over-the-air to the computerized units of automobiles. Mainly created to thwart attacks from malicious actors who can compromise servers and networks used to sign and deliver updates. It has been widespread and accepted, and it is currently used by many large OEMs.[104]

2.7.3 Trust Vehicle Project

Also known as OMG is an Austrian project focused on the use of ADAS in difficult weather and mixed traffic scenarios. The project finalized in July of 2020. It has been crucial in the systematic identification of critical road scenarios, and what are the weak spots of different sensors and actuators in each scenario. It also provides a great analysis of driver failures and HMI relevant to it, plus taking in account possible trajectories on counter plans. [105]

2.7.4 AutoNet2030

A project set to finish before 2020 and be deployed before 2030. Centralizes on the idea of a decentralized decision-making process to use on path following, lane assist, and cruise control. As an ongoing deployment the research reach is not yet conclusive, but the findings for highly autonomous systems are relevant specifically for traffic use and V2X technologies. As of November 2020 the site seems to be defunct.[106]

2.7.5 Maven

Maven is a significant project focused on signal recognition for autonomous driving functions, understanding different signs in different countries and the road structures. It is a great step forward in autonomous systems, as it had created a good database and tried various examples.[107]

2.7.6 V-DAS

A project that sounds like lives if pronounced in Spanish, therefore its origin is from Spain. This project lead by Spanish technology centre VICOMTECH. The project finalized in 2019. It focused mainly on technologies to reduce accidents and improve road safety. The project deepened into a cloud based V2X to improve the ADAS algorithms, and had a plan for each sensor that contributes to driving in a SAE level 3 or 4 vehicle.[108]

2.7.7 SAS

It is a Marie Curie Award project and it is the project that sponsors this PhD. SAS means safer autonomous systems. The project focuses on more than just the automotive industry, with the argument of improving assurance and securing it even when removing the human in the loop systems. The project aims are to identify ways to establish people's trust in autonomous systems by making these systems demonstrably safer. [109]

2.7.8 Peter

PETER Pan-european training-network of electromagnetic risk management is also Marie Curie Award project similar to SAS focusing on security issues relating to electromagnetic risks. Its goal is to obtain a functional hazard analysis method adapted for considering electromagnetic effects, while integrating computational electromagnetics results into risk analysis. [110]

2.7.9 Impact of related projects

All of the projects mentioned above are relevant to the research in the way that this research was developed under the SAS project. The mentioned projects are ordered from the ones that have already had a great amount of impact to unfinished projects whose impact will be seen in the future. The projects mentioned here are either still ongoing or were going on at some point of the SAS project.

3 Methodology

3.1 Approach and Aims

A security case is one type of assurance case; others include safety cases, reliability cases, and dependability cases, among others. Security isn't listed among the reliability qualities, but as a part of dependability[111]. Instead, integrity, confidentiality, and availability are the appropriate terms to use when discussing security. Security does not exist as a separate term since defining what a secure system means is challenging due to the wide range of security concerns. The use of a cybersecurity case to document compliance with cybersecurity goals is suggested in ISO/SAE 21434 [112], but no further information is provided (While no information is directly provided, there have been examples created on how it can be done). As the safety case is already widely used for functional safety in the automotive industry, this provides a natural basis for developing an assurance case for cybersecurity.

UN-ECE regulations 155 and 156 (apply on from July 2022 onward, to all UNECE member countries manufacturing vehicles) require Vehicle Manufacturers and OEMs to manage vehicle cybersecurity and the safety and security of software updates (respectively) in order to obtain type approval. UN-ECE type approval is required in order to sell vehicle in Europe and many other territories.

Regulation 155 concerns vehicle cybersecurity management and its requirements are reflected in the ISO/SAE 21434. Unlike ISO/SAE 21434, which does not specify specific processes (but does demand compliance and the creation of work products to verify compliance), UN-ECE-R155 mandates the creation and implementation of a management system that focuses on cybersecurity during the vehicle's whole lifecycle (the so-called Cybersecurity Management System, or CSMS). UN-ECE-R155 involves suppliers of components to get really involved in the CSMS in order to comply.

UN-ECE-R156 defines the safety and security requirements for automotive software updates and the Software Update Management System (SUMS). The main objective of this regulation is clarifying the specific requirements for the management of vehicle updates, the security of their delivery (including by OTA means) and the safety of their implementation, as well as the identification of relevant details such as kernels and software versions. UN-ECE-R156 assumes the vehicle already complies with UN-ECE-R155 and avoids repetition.

3.1.1 Proposed Requirements for a Cybersecurity Case

Based on emerging technological trends in the automotive industry, as well as current functional safety engineering practices, it is considered that an assurance case for automotive cybersecurity should ideally provide the following basic characteristics and requirements:

- Unified approach with functional safety case techniques – to maximise efficiency by exploiting existing familiarity with safety case techniques and facilitating reuse of common evidence where possible.
- Ability to address aspects beyond traditional safety – including availability of mission-critical (rather than safety-related) functions, privacy issues, fraudulent financial transactions, and indirect safety implications (such as kidnapping) that are beyond the remit of more traditional safety analysis.
- Ability to adapt to emerging threats – to cope with the inevitability of threats that were unforeseeable at design time.
- Ability to integrate cybersecurity analysis – as essential sources of argument and evidence.
- Support probabilistic risk analysis – to cope with significant uncertainties.
- Provide explicit visibility of uncertainties.
- Graphical approach – to help cope with scope complexity, and readability.
- Hierarchical structure – to help cope with scope complexity, and readability.
- Living document – will need to be readily adapted throughout development and operational lifecycles to reflect the impact of software updates and security patches.
- Modular construction – to allow the impact of system changes to be assessed efficiently.
- Support for emerging legislation – provide a path for demonstrating compliance with relevant regulations, such as the UNECE Regulations 155–156.

However, some of the above requirements that have been proposed are also intended to respond to some of the criticisms of existing safety case techniques raised by Levenson [68]. In particular, the perceived potential for undesirable confirmation bias and a lack of transparency concerning confidence and uncertainty seem even more relevant in the construction of a cybersecurity case than for a safety case, since there is even less certainty in relation to cybersecurity threats than there is in the safety domain.

3.1.2 Proposed Method

A possible solution to these aspects could be to take the attack-defence trees developed during cybersecurity risk analysis and integrate them into a GSN-type graphical assurance case argument using an eliminative style

of argumentation. The aim of this is to produce a more explicitly “adversarial” case than has traditionally been used in functional safety, in a similar style to the way legal cases are presented and examined in a court of law. In fact, this works in accordance with version 3.0 of the GSN standard [78] complying with the *dialectic extensions* to provide support this style of argument.

It is expected that such cybersecurity case, prepared initially for product launch, would effectively be the first draft of a dynamic assurance case that would be updated through the operational life of the vehicle. Ongoing assurance activities will also be needed to complement the product launch assurance, in the interest of ensuring that cybersecurity assurance is maintained over the operational lifetime of the vehicle as outlined in the UNECE regulations and ISO/SAE 21434 [112]. This will require the development of dedicated vehicle security operations centres to help ensure the through-life cybersecurity performance of vehicles, and methods that facilitate the construction and maintenance of dynamic assurance cases that can be readily modified as new threats are identified and the on-board vehicle software evolves. These requirements will also have a corresponding impact for vehicle safety assurance, in order to respond to a future in which through-life in-service software modifications become the norm, to implement new or improved features, correct faults and patch security. These software updates are expected to be delivered by over-the-air methods, which will themselves require safety and cybersecurity assurance.

3.2 Related Work

In this section the focus is on related work that the method can directly compare to in regard to objectives or works that helped shape the method.

3.2.1 Works that Inspired the Proposed Method

The following documents in Table 8 show techniques that are used for creating the method developed in this thesis. The use of these techniques is covered in “background information”. Furthermore, they were described in the literature review.

Table 8 Works that inspire the method

Title	How it influences the Methodology
Security Assurance Cases: Motivation and the State of the Art- University of York [72]	This document presents the idea of the security case, its objectives requirements and uses
Foundations of Attack--Defense Trees [79]	This document gives the information and the symbols and building of Attack-Defence Trees (ADTs) that would be used in the development of the method

Goal Structuring Notation Community Standard Version 3 [78]	The Document that explains how the standard of Goal Structuring Notation works, the symbols and the way to use it or add information.
Eliminative Argumentation: A basis for arguing system confidence in system properties with induction [76]	The idea of challenging claims and goals and using an inductive logic to developing safety cases comes from this document.

3.2.2 Works Similar to the Proposed Method

This section summarizes similar work and how the presented methodology differs from it or improves it.

Table 9 gives an overview of the related work.

Table 9 Related work

Author	Title	Notable Aspects	Limitations and points that can be expanded on
Chowdhury [113]	Safe and Secure Automotive Over-the-Air Updates (2018)	<ul style="list-style-type: none"> • Use Attack Trees and GSN • Considers ISO regulations for Functional Safety and Cybersecurity • It is a systematic approach • Creates templates 	<ul style="list-style-type: none"> • It does not merge safety and security • It does not consider emerging technologies or future proofing • It does not consider non-safety aspects of security
Nigam [114]	Model-Based Safety and Security Engineering (2018)	<ul style="list-style-type: none"> • Takes ADT and Safety Cases into Assurance Samples • GSN and ADT can work in parallel by translating GSN nodes to ADT • It can create ADTs from FMEAS • It has simple examples that are easy to understand and try to develop • Uses SimuLink for some examples 	<ul style="list-style-type: none"> • The implementation is not seamless letting it be more of conversion • It does not consider issues of vehicle updates nor more recent regulations • It does not consider the ECU systems
Kirovskii [115]	Driver assistance systems: Analysis, tests and the safety case. (2019)	<ul style="list-style-type: none"> • It identifies the scope for life cycle of SOTIF, Functional Safety, and Cybersecurity • It creates an example using the ADAS system through the life cycle • Uses hazard evaluation and probability to determine tests and weak points 	<ul style="list-style-type: none"> • Does not address cybersecurity aspects • It does not include cybersecurity on the safety case as it would be out of its FS and SOTIF scope
Messnarz [116]	Integrating Automotive SPICE, Functional Safety, and Cybersecurity Concepts: A Cybersecurity Layer Model (2016)	<ul style="list-style-type: none"> • Creates an integrated Layered model, that is very good for penetration testing • Consider Functional Safety and Risk Analysis as it develops defence layers 	<ul style="list-style-type: none"> • It does not have a visual representation • Research is set before any cybersecurity standard

Patu [117]	How to develop Security Case by combining real life security experiences (2013)	<ul style="list-style-type: none"> • Defines a security case • Builds a security case using GSN 	<ul style="list-style-type: none"> • Not oriented on vehicle cybersecurity • Suitable for budget informational networks • Does not consider ADT
Dürrwang [118]	Security Evaluation of an Airbag-ECU by Reusing Threat Modelling Artefacts (2017)	<ul style="list-style-type: none"> • Considers all ECUs and can networks relevant • Understands the functioning of the airbag and proposes attacks and testing • Has accurate effective counter measures • It identifies attacks and mitigation 	<ul style="list-style-type: none"> • Lacks integration with overall safety for a safety critical system

In his paper Chowdhury [113] tackles Attack trees that loop feed a GSN safety case, the work considers ISO26262, ISO/SAE 21434, and SAE J3061, including considerations of functional safety and security, but does not consider any future proofing. It does not really merge safety and security; it only puts them together in one model. Also, in this ever-evolving landscape it is not looking outside the safety impacts of cyber security or the emerging technologies. Chowdhury creates templates of some ADT, where he links Claims with evidence or criteria, instead of its attacks and counters. This systematic assurance case templates and his idea of efficiency towards GSN are explained in his earlier papers [119]–[120]. The research also focuses on creating and developing this kind of template for a vehicle update scenarios. The ideas and structures could be used to check OTA assurance cases like the one presented in this thesis.

Vivek Nigam [114] also has an interesting approach, that extracts information from safety cases and attack defence trees and translates them to assurance samples. This differs from the main idea proposed in this thesis, because it implements the attack trees and the GSN side-by-side but connecting the goals. It works more as two parallel safety cases or converting GSN nodes to Attack defence nodes rather than implementing them together. The paper has various examples including a very simple airbag example. It does not focus on considering this on highly autonomous connected vehicles and the implications of adding or updating functions OTA, and its regards to safety ECUs. The final method is based Model-Based Engineering implemented using SimuLink.

OM Kirovskii [115], developed a process to integrate SOTIF and Functional Safety, this is firstly done by finding the common ground. Once the common ground is defined the lifecycle of ADAS system development is analysed. The document proceeds by integrating the life cycles of all disciplines and creating a hazard evaluation. The hazard evaluation using probabilistic data defines the relevant process that requires further

evaluation. This process does not create an assurance case but creates a decisive way of creating hazard analysis mixing SOTIF, FS and cybersecurity.

Messnarz [116] developed a method to integrate cybersecurity concepts into functional safety using a multi-layered model. Vaise Patu [117] in her work explains how to build a cybersecurity case. However, it is just suitable for informational networks with a budget to do so and not specifically vehicles. Jürgen Dürrwang [118] proposes a method of extracting possible attacks of an airbag using threat modelling, giving a good view of attacks and counter measures to a safety critical system.

3.3 Background information

In order to develop the method, this section covers all of the basics need to reinforce the method.

3.3.1 Risk Management and Analysis

The concept of risk is a combination of the likelihood of an event and the severity of its impact on the stakeholders, such that low severity with a low likelihood represents a low risk and high severity with a high likelihood represents a high (and probably unacceptable) risk[121]. Other combinations of severity and likelihood result in intermediate risk levels, and both the severity and likelihood are typically categorized in order to allow them to be mapped to risk categories.

Although the elimination of all risks is impracticable (and would be unaffordable if practicable), risks can be managed to ensure that they are not unreasonable, by creating a risk management plan. In the safety context, a hazard is the source of an accident or incident, and is something that may have repercussions. An incident is an event led by a hazard that does not cause losses, while an accident causes losses; these losses might be economic, health or life related. In cybersecurity, threats, and attacks on the vehicle, perpetrated by malicious individuals, could lead to a variety of possible outcomes, including safety impacts as well as non-safety risks.

Risk analysis is the process of identifying and analysing potential issues that could have a negative impact for the stakeholders. A risk analysis is a vital part of a risk assessment; it is a step in which all risks are identified and categorized, determining how significant each risk is, and hence the potential need for risk reduction measures.

As previously stated, there are various ways to approach risk analysis, especially in cyber security. It should be noted that the severity of impact can only be assessed at system level, where the impact on the

stakeholders can be assessed, whereas the likelihood depends on the individual likelihoods of actions in the chain of events that lead to the specific outcome.

3.3.2 Relevance and Compatibility with the standards

A defining process and what made the cybersecurity case something relevant to OEMs is ISO/SAE 21434 and UNECE Regulation 155, that is heavily backed up by the ISO standard. For the regulation, the cybersecurity case is an essential input to approve a cybersecurity assessment and to the release for post-development. A cybersecurity case is to be created after the assignment, identification, definition and planning of the cybersecurity activities. And even though the standard does not actually identify a specific method to build the case it has a clear objective by conveying that it shall be created to provide the argument for the cybersecurity of the item or component, supported by work products, and that it can be created by combining customer supplier cybersecurity cases but most also support post-development. The standard also clarifies that there are 4 main losses causes by cybersecurity risks that are to be taken in consideration: safety, financial, privacy, and operational. The standard has a clause focused on operations and maintenance, in this section the relation of prerequisites for post development are relevant, and how it must be used in the instant of delivering updates.[122][123]

In the interest of relevance with the standard there are clauses or sections directly linked to the activities. Sections 4, 5, and 6 of ISO 21434 contain the organizational requirements for cybersecurity, including culture, governance, and responsibilities. Section 6 specifically mentions the need of a cybersecurity case. Section 9 details the concept phase, by (1) defining the operational environment, (2) specifying the cybersecurity goals and claims and (3) specifying the cybersecurity requirements. Section 10 aims to verify the cybersecurity requirements, identify and manage vulnerabilities; and provide the evidence that it complies with cybersecurity. Section 11 aims to assure section 10 after the integration of components by validating claims and goals while confirming residual risk is acceptable. Part 13 handles how cybersecurity must be preserved after updates.

The compatibility with functional safety, specifically ISO 26262, is achieved with the correct use of GSN, as the correct modular use of GSN has become a gold standard in automotive functional safety, since its introduction to its uses [124]. When regarding its compatibility with SOTIF, active safety and passive safety, its compatibility becomes inherit from the facts that the components being used have to be in accordance to the UN-ECE rules, and when mandated have gone through an ASIL rating.

The regulations and work packages of functional safety and cybersecurity are connected the Figure 13 works as an extension to the information derived from a figure by David Ward in a paper [125] to include cybersecurity.

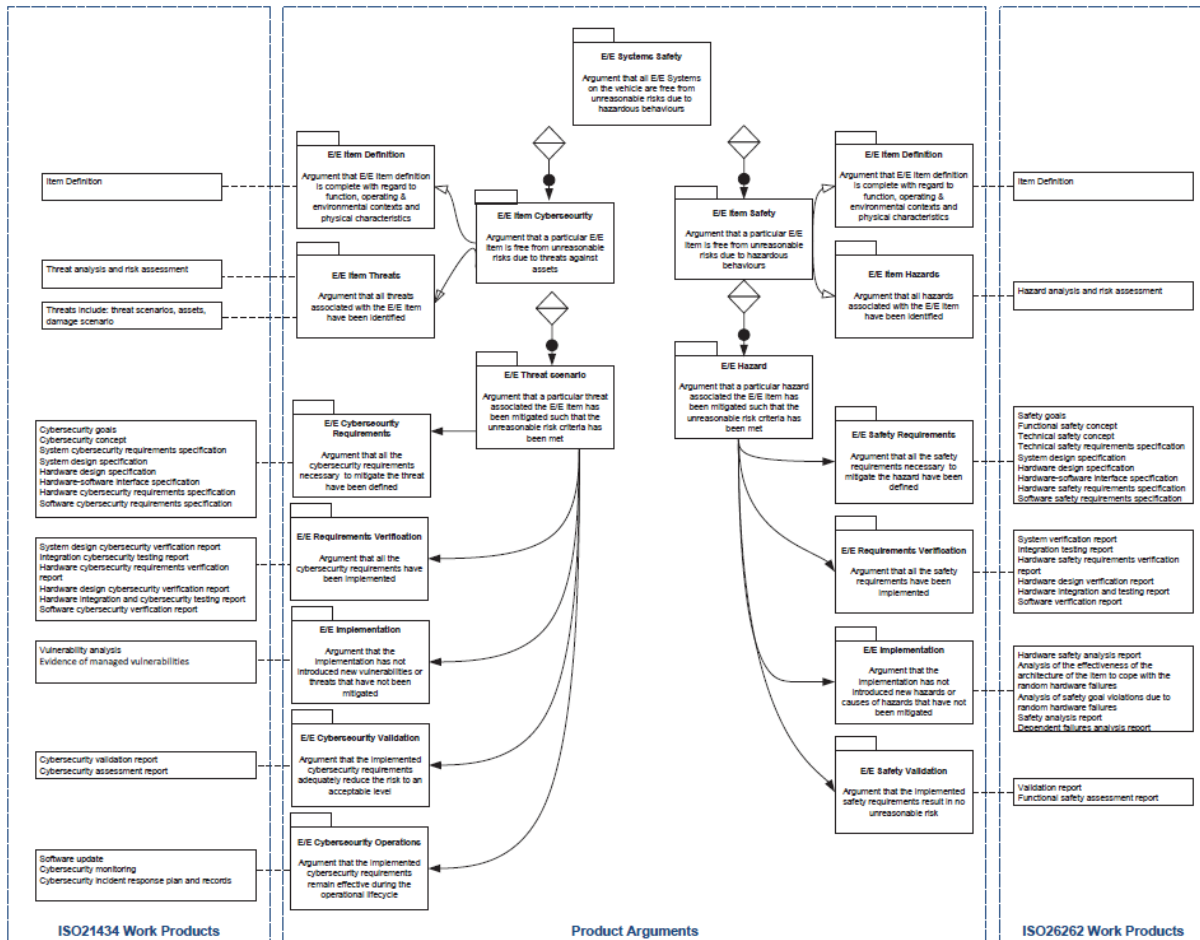


Figure 13 Relation between product arguments and work products of automotive functional safety and cybersecurity

3.3.3 Threat Modelling and Attack-Defence Trees

Threat modelling must satisfy the business objectives and security policies, but it also has to closely follow regulations and standards. When doing so it is important to consider the robustness of the vehicle, its surrounding environment, and the motivations of attackers. Attack trees are a popular technique for analysing threats and identifying counter measures in cybersecurity, that provides a methodical, graphical way of modelling possible cybersecurity threats to systems [79]. Attack Trees consist of the possible threats and vulnerabilities, and the way they can be implemented. Attack-Defence Trees (ADT) on the other hand, also include the mitigations and counter measures for the attacks.

The process to create ADTs is as follows:

- Develop a functional model of the system.
- Propose possible attacker goals (i.e., illegal benefit to the attacker).
- Identify possible attack objectives that could allow the attacker to achieve these goals (i.e., possible harm or other loss to stakeholders).
- Identify attack methods that the attacker could use to implement the attack objectives
- Decompose the attack methods into lower-level actions that would be required to achieve a successful attack.
- Identify opportunities to eliminate branches or mitigate the effects by reducing the likelihood of success.
- Let each goal form a separate tree (although they might share sub-trees and nodes).

ADTs are represented in a logical way and follow the node flow in one direction. For each node of an ADT that has more than one branch the relationships between the subsidiary branches may be either disjunctive (OR) or conjunctive, the latter using either a simple AND or a sequential AND (SAND). The SAND approach provides a more compact representation a specific sequence of steps that may be needed to mount an attack [79].

ADT techniques have many advantages, for example they are easy to understand and can be easily shared and explained to people with little experience in security, and can often be reused to address similar threats. The classic structure can be viewed in Figure 14.

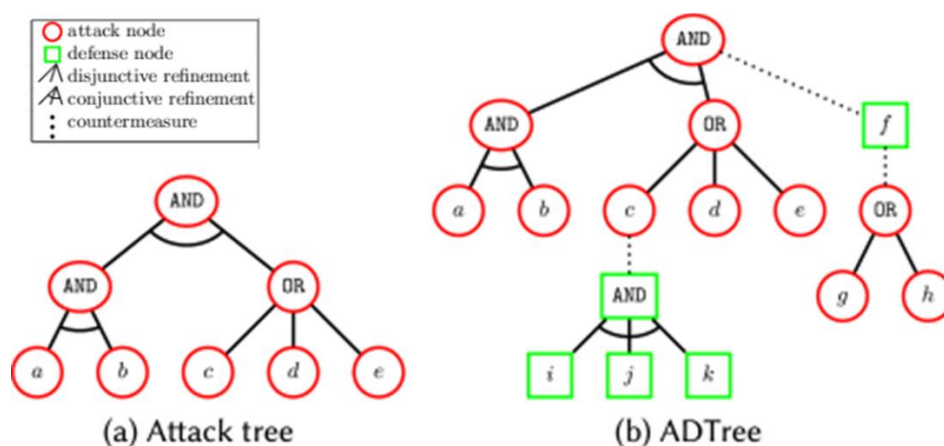


Figure 14 Classic ADT Structure

3.3.4 GSN, Eliminative Argumentation and Confidence Maps

The GSN safety case structure works towards a “goal”, which is a claim, implemented through a “strategy” and supported by “context”, which are arguments that lead to a “solution” (i.e. evidence). The “vanilla GSN” mentioned also has the possibility of extensions that make the safety case building more effective. These extensions include maintenance of arguments, modular safety cases, assurance case patterns, eliminative argumentation and more. As a technique that is easily understood and able to present advanced concepts, it has been appearing with increasing frequency in the domains of safety and security [63].

In “eliminative argumentation” there are three potential types of doubt: doubts about the claim, doubts about the evidence, or doubts about the inference used to link the claim and the evidence. The objective is therefore to identify the relevant doubts about claims, evidence and inferences, and to provide counter arguments against the identified doubts where possible to increase confidence in the assurance case [76].

A graphical representation of an eliminative argument is described as a “confidence map”, as it details the identified doubts concerning an argument and also shows whether these doubts can be countered or if they remain, thus illustrating the confidence that can be attributed to the argument. It should be noted that not all doubts will have the same importance, and appropriate weightings should be. To maintain the clarity of the safety case it has been recommended that the confidence map should be separate from, but linked to, the safety case [126]. Figure 15 shows the symbolism of eliminative argumentation on Figure 16 symbolism “Vanilla GSN”. GSN standard 3 [78] introduces extension for dialectic arguments with a dashed line and an arrowhead that symbolizes a connection to a challenge on the GSN; the other change introduced on the standard that enables crossing out defeated elements is not used in this work in favour of eliminative argumentation symbolism.

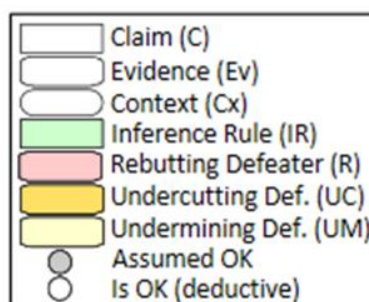


Figure 15 Symbolism for Eliminative Argumentation

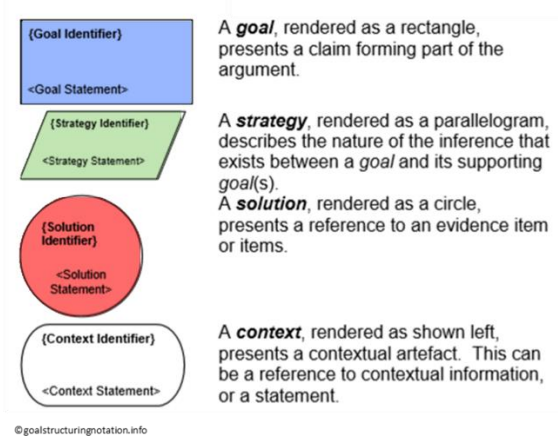


Figure 16 Symbolism for standard GSN

3.4 Proposed Method Design and Structure

A generic Cybersecurity Assurance Case is proposed here that takes the general graphical approach of GSN, whilst applying the additional symbolism of confidence maps from eliminative argumentation [76], and also integrating the structure of ADTs to augment and amplify the arguments. The symbols used in the generic illustration presented here are summarized in Figure 17, and their meanings are discussed further below.

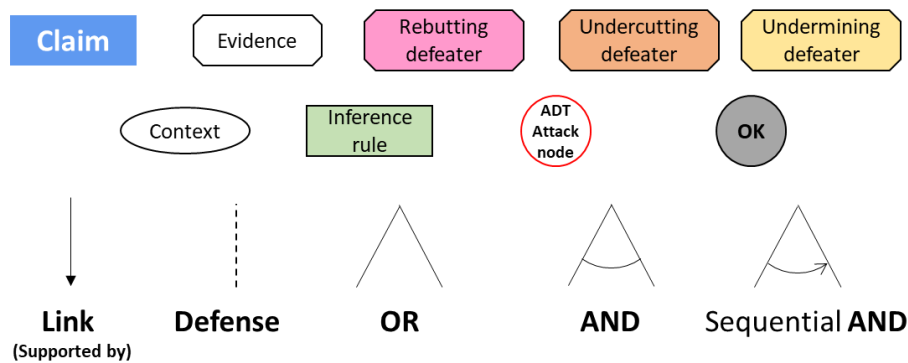


Figure 17 Key to symbolism used in the proposed methods

Arguments taking account of the potential for unforeseeable cybersecurity risks and the requirements for a through-life cybersecurity management system (denoted by CSMS in the diagram) are presented in Figure 18. The system description, which provides the context for the assurance case, is indicated by a white ellipse. The *claims* are represented by blue rectangles, which are justified by *inference rules* represented by green

rectangles. The claims may be challenged by *rebutting defeaters*, the inference rules by *undercutting defeaters*, and the evidence by *undermining defeaters* [127]. These challenges may be responded to by using further claims, inferences and evidence. The need for a robust threat analysis approach is also included in Figure 19, along with the treatment of a threat judged to be of inherently acceptably low risk, and considering a cybersecurity management system (CSMS). Lines of argument that are considered to have been acceptably resolved are indicated by the grey circles.

The diagram is continued in Figure 20, which illustrates approaches for threats involving attack trees that could contain disjunctive and conjunctive relationships (the latter including both simple and sequential AND possibilities). These could be addressed either by outright elimination of possible attack steps (denoted by "ATK" and represented by circles with red boundaries), or at least mitigating the vulnerability to reduce the anticipated likelihood of success to a sufficiently low level to achieve an acceptable level of residual risk. These requirements for defence are indicated by dashed lines terminating in claims for possible successful elimination (denoted "ELIM" in a blue rectangular box) or mitigation countermeasures (denoted by "MIT" in a blue rectangular box), which therefore represent sub-claims that must be supported by appropriate evidence.

It should be noted that if an OR node occurs in an attack tree fragment then all of the options must be addressed with suitable countermeasures in order to achieve complete resolution. If there is an AND or SAND node, however, then mitigating any of the contributors could be sufficient to achieve the necessary risk reduction (in the ADT fragment denoted "ATK x" in Figure 20, one of the required contributors is simply eliminated, thereby disabling that attack path). In practice, the requirements for mitigation might well be identified at lower levels of a specific attack tree network than is shown in the very abstract (non-specific) illustration presented here.

To understand the order and usage of the method, here are some simple guidelines and an easy way to remember the shapes and usage of the method:

- A context {white oval} can be placed anywhere it defines or limits the contextualization, by formatting the statements and ideas that limit and contain argument.
- A goal {blue rectangles} are the claims of an argument and the main debatable object of this assurance case. They are the initial structure and continue to be the main point of diversion within the assurance case. When an ADT branch happens, mitigations and defences become claims, and therefore goals, by themselves. They are followed by inferences or rebutting defeaters.

- Evidence {White polygons} provide factual information that validate. They are bound to follow goals or defeaters before being validated by an “OK”.
- Inference Rules {green rectangles} present a possible scenario that support a claim and tend to start using the word “if”. As the name implies an inference rule is a condition that is supporting a claim through reasoning the basis of the evidence. They follow either goals or rebutting defeaters.
- Rebutting defeaters {pink polygons} challenge the claims, by claiming a counter-condition or scenario, they tend to start with the word “Unless”. They follow claims and are followed by inferences when an acceptable condition can be deduced or inferred; or may be followed by an ADT where necessary to develop the argument through attack.
- Undercutting defeaters {Orange polygons} challenge the inferences and tend to start with “but”, they aim to point out how the inferences could be less of effective or weaken the logical conclusion on which the inference was reasoned. They follow inference rules and are to be followed by evidence to clarify. They follow inferences and are to be followed by another inference or evidence.
- Undermining defeaters {Yellow Polygons} challenge the evidence and tend to start with “However” or “Still”. They lessen the effectiveness, power, or ability of the evidence by pointing out how that evidence might be void. They follow evidence and should be followed by further evidence.

The idea is that this approach could be implemented into a future cybersecurity case framework, and more specific examples are developed in the line of the research. The demonstration is shown in Figure 18 (and in more detail in Figure 19 and Figure 20) follows all the guidelines previously mentioned and works as an introduction to the method.

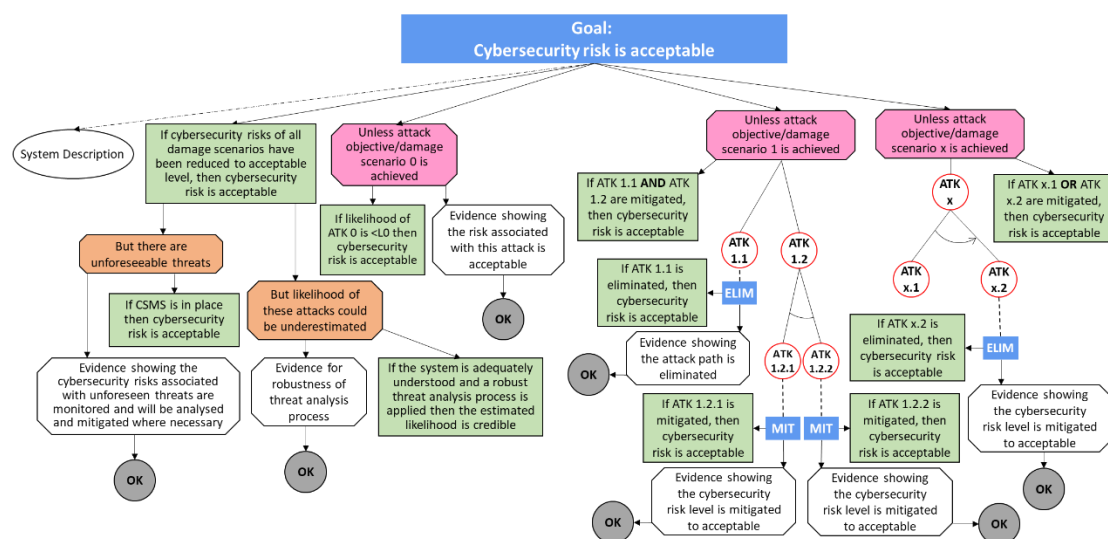


Figure 18 Demonstration

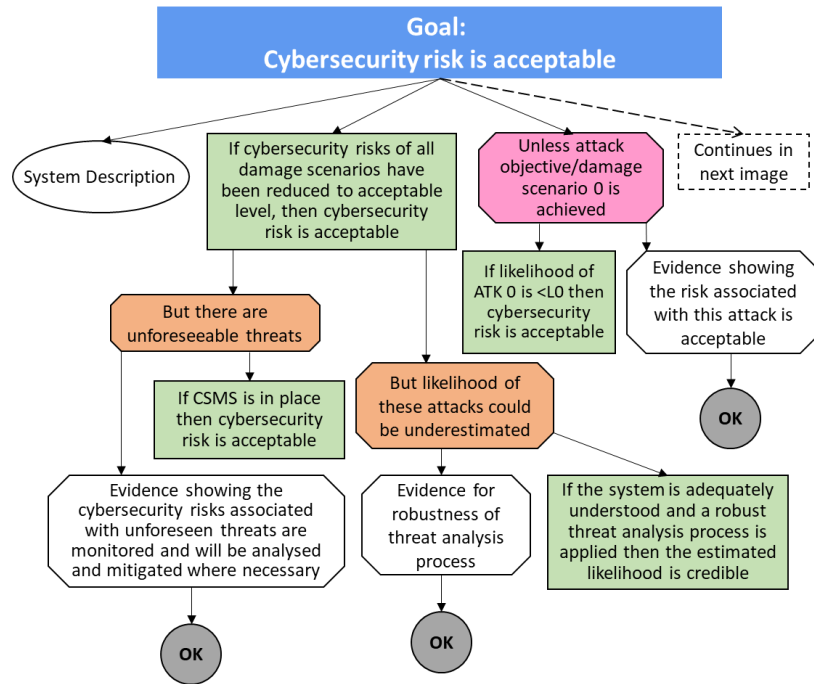
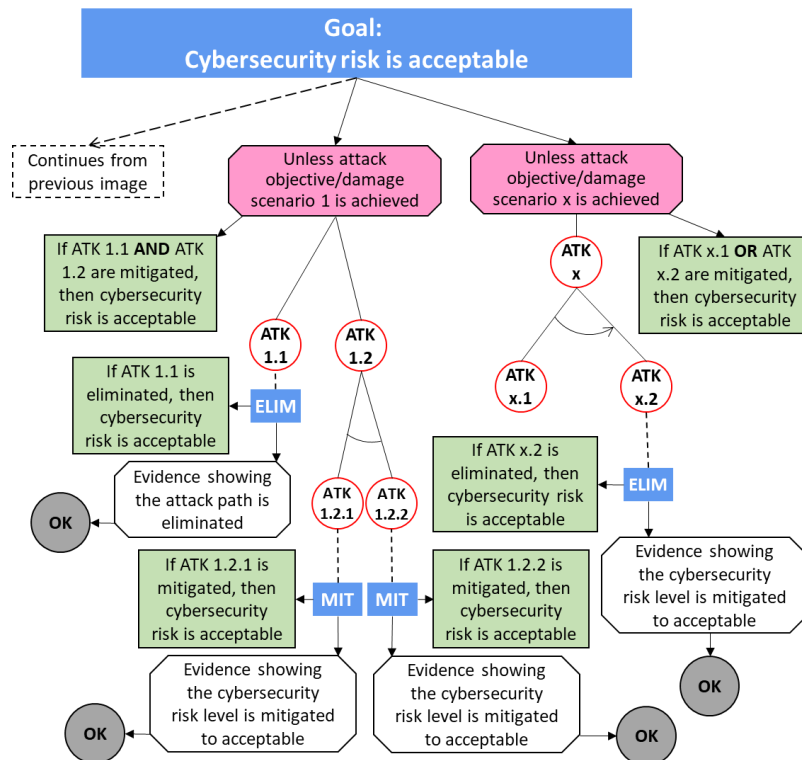


Figure 19: Demonstration part 1



3.4.1 Required Inputs

The method explained is a holistic assurance case that considers elements of safety and security, to produce a logical and efficient diagram to follow. The process leading to being able to generate all of these requirements relies on organizational safety and security, the culture of safety and security within manufacturing process and proper life cycle management from concept phase till postproduction phase; this industrial and organizational processes are bigger than the scope of this document, that just aims to focus on a new approach on assurance cases. As a regular assurance case it requires some information bestowed upon it before hand, then it can be summarized in the following points:

- **Identifying hazards:** As implied if there are no hazards identified there will be no assurance case as the goals and claims aim to ensure they are as hazardless as possible. (Activities and methods necessary could be, but not limited to: HAZOP, Fault Tree Analysis, etc.).
- **Extent of harm:** Deciding who might be harmed, when, and how. (Activities and methods necessary could be, but not limited to: Asset definition, damage scenarios, ASIL analysis, etc.)
- **Evaluation of risks:** All the risks associated with the identified hazards. (Activities and methods necessary could be, but not limited to: Risk Matrix, TARA, Risk determination analysis etc.).
- **Mitigation strategies:** Deciding on the necessary control and security measures, necessary to counter, deter, stop or mitigate threats. (Activities and methods necessary could be, but not limited to: Attack path and feasibility rating, adversary-driven state-based system security evaluation, quantitative cyber risk reduction estimation methodology, etc.).
- **Evidence:** As not all evidence should be implied, many should come from statistics or testing. Documentation must be clear on recording those findings and implementing them. (Necessary activities and methods could be, but are not limited to: Vehicle & component Testing, Statistical Data, etc.).
- **Evaluating and monitoring:** Progress and changes should be maintained under observation as ongoing basis, any change should be considered and assessed properly in accordance with all previously mentioned requirements. (Necessary activities and methods could be, but are not limited to: product Life cycle assessment, product update process, etc.).

Even when the above-mentioned requirements are essential for building a safety case it is also important to consider legal requirements and following certain standards. Compliance with the various standards has been previously mentioned, and it is emphasized here to clarify its importance and significance in the process of creating the vehicle [123].

3.4.2 Step by Step Build up

In furtherance of making the process tangible and the possibility to create an assurance case in this style, three phases are to be established: start, building, and verification and maintenance. The second phase or building phase should be repeated iteratively until the process is completed.

3.4.2.1 Start Phase

This phase is the beginning part, it is important to set the main goal and have all the sub goals clear, plus all context must be defined. Information for the goals, context and any argumentation or evidence should be clear before proceeding to the next step.

3.4.2.2 Building Phase

This phase is made of several steps, these steps are to be repeated over and over until all branches are concluded. In this part of the process all open elements must be reconsider until all branches are deemed OK, and therefore closed.

1. Interconnect any non-connected context that is relevant to the “Goal” on the topmost part that it is not yet completed.
2. Set any strategies in the form of inference rules {Green Polygon} relevant to this “Goal”.
3. Put any rebuttal that the claim “Goal” may face as a rebuttal defeater {Pink Polygon}.
4. Check if any inference can be undercut by an undercutting defeater {Orange polygon}; when an undercutting defeater follows an inference, the inference gives context and works as a strategy, like in the vanilla GSN, letting the undercutting defeater be more direct.
5. Try to link any relevant evidence {White Polygon} to any open defeater or inference.
6. Check if the evidence can be undermined if it can be it shall be placed with an undermining defeater {Yellow Polygon}.
7. Review open rebuttal defeaters if they invoke a possible attack path develop the attack tree regarding it.
8. Develop the attack tree until attacks are mitigated or eliminated, any mitigation or elimination of a threat will become a sub goal {Blue rectangles} and should be reviewed next as a starting goal.
9. Check if there is any evidence {White Polygon} or inference {Green Polygon} relevant to an open defeater and link it.
10. Check if evidence that could not be undermined or inferences that where not challenged can be deducted as safe as possible with an “OK” {grey circle}.
11. Make sure the current branch has reached an “OK” and restart the building phase from a goal in any unclosed branch.

3.4.2.3 Verification and Maintenance Phase

During this phase it is important first to review the resulting diagram everything has been correctly validated with paths being ensured with an “OK” through validation or deduction. Any change, upgrade or update of the system should be analysed in this phase and when required return to the building phase.

4 Illustrative Examples

With the objective of illustrating the proposed method and to see how it works a couple of synthetic examples were analysed. The examples go from easy to complex in order to raise the comprehension level.

4.1 Example 1: Art Heist

The first example is maintaining a special valuable work of art safe and secure in an art exhibition when it closes each night. The statement for this example to work is as follows: There is a museum holding an extremely valuable work of art that is sought by many, the museum treasures the art piece as its most valuable possession and plans to keep it secure by all means necessary. A resulting assurance case is shown in Figure 21.

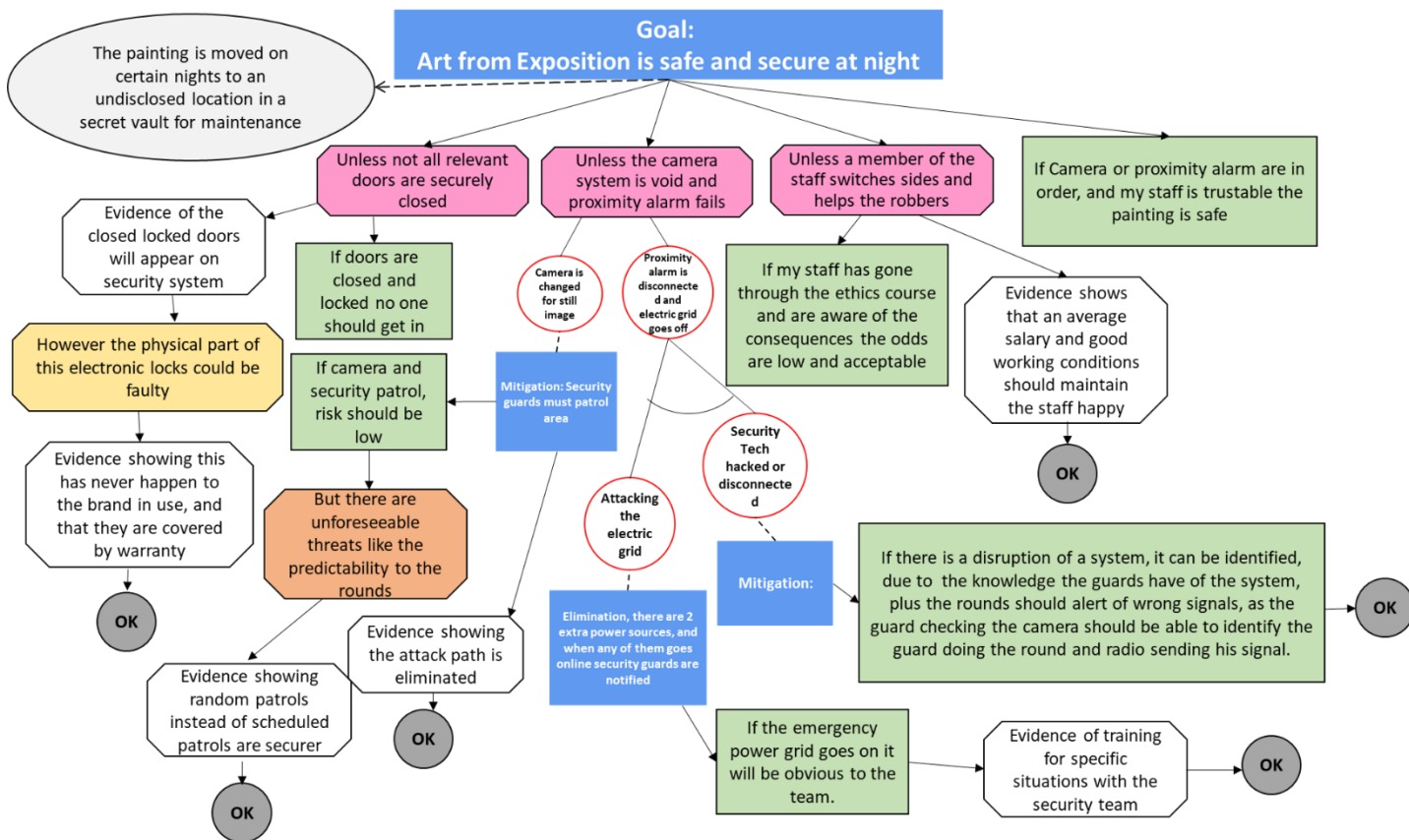


Figure 21: Security case for the “Art Heist” example

The example provides a simple way of how the security team of the art exhibition will deal with threat that a valuable painting may be a target for thieves an art gallery is tasked with safeguarding a valuable painting, the examples go around how it can be kept away from being snatched.

In Figure 21, the top-level claim (goal) is that the painting is secure at night. As a context there is an explanation about the painting's secret maintenance. The inference supporting this claim is based on trust on the system and the employees. This claim, with an inference already, is challenged by three rebutting defeaters. The first one on the left is about the doors and access points, here there is evidence and inferences that are eventually challenged by a undermining defeater that is set to rest by more evidence. The middle rebutting defeater gets a debatable argument through an attack and is developed with an ADT structure. From the ADT structure 3 goals can be obtained by either mitigation or elimination, and the first one of these goals gets an inference that is challenged by an undercutting defeater, while the other ones are dimmed ok through an inference or evidence. The final rebutting defeater on the left leads to an inference and evidence to be qualified as OK.

4.2 Example 2: Traffic Signal Recognition System

This example is created from an attack tree proposed in a presented at the SAE World Congress 2022.

The signal recognition system used in the following attack tree is simplified to just focus on a small number of cybersecurity threats. With what is shown in the attack tree, a cybersecurity case is portrayed as a response.

4.2.1 System description

The function of the system (see Figure 22) is to identify what traffic signals are is being presented to a vehicle, in real time, based on a number of inputs.

The required inputs are:

- colour and monochrome camera images of traffic lights and other road signs that are in view.
- GNSS data for the current location.
- an up-to-date map that includes traffic signalling data.
- Data from the onboard database to compare and contrast.

The output is a list of road signals currently being presented to the vehicle.

It requires a camera for a visual input on traffic signals and traffic lights, a colored image should be store along a greyscale image for the camera to work correctly and for redundancy in the recognition, because even when traffic lights have a position, and most signs are associated to a shape, colour can be used to verify. The system requires a location service, this is used so the system can know if such traffic signalling is valid in the current location. The system also has an onboard database that compares via internet connection to an off-board server database that is frequently updated, database on board can be updated to match. The 3 mentioned inputs are processed within the ECU in order to make a decision of what traffic signal is being given in real time.

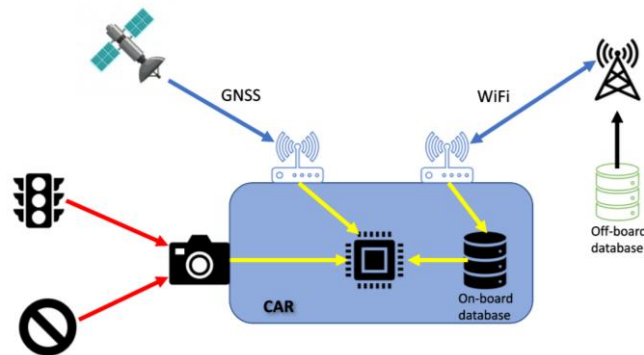


Figure 22: Elements on a Traffic Signal Recognition System

4.2.2 Attack Tree

The attack tree (see Figure 23) was created from the system description in the previous sub-section.

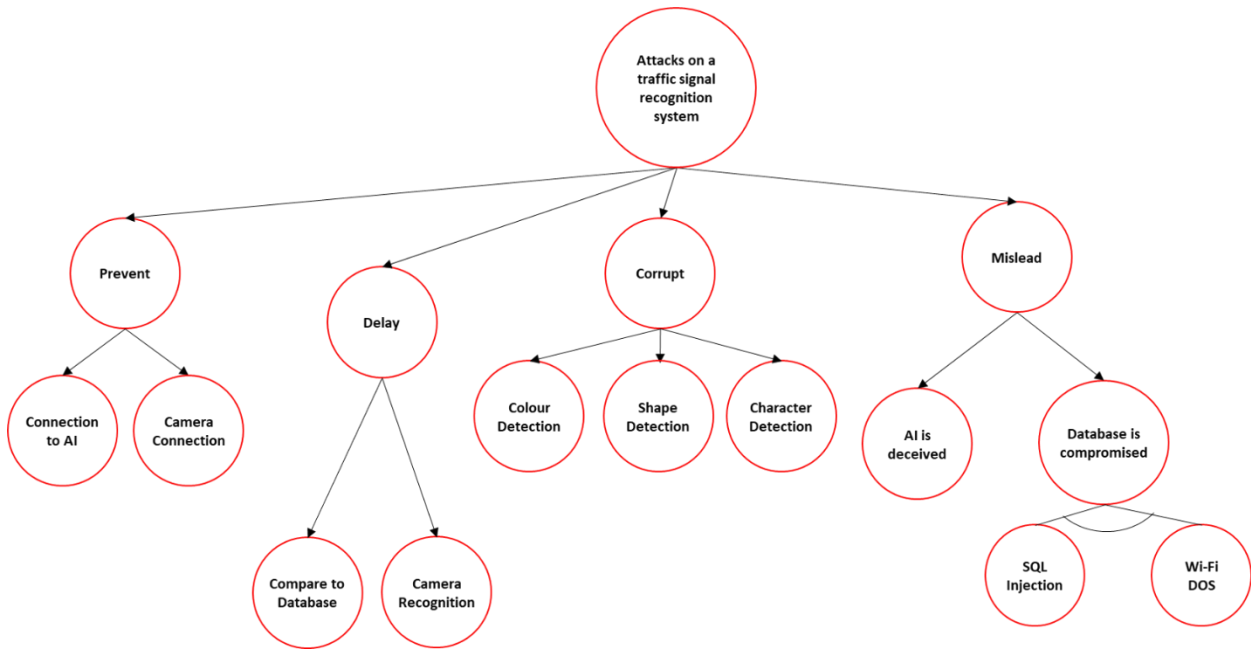


Figure 23 Attack tree for a traffic signal recognition system

4.2.3 Development of a cybersecurity case

The idea of knowing the main attacks from the attack tree, and using the step by step building up of the method through the 3 phases previously mentioned, leads to a cybersecurity case as follows. The attack tree on Figure 23 was used to develop the mitigations needed to complete the assurance case shown in Figure 24.

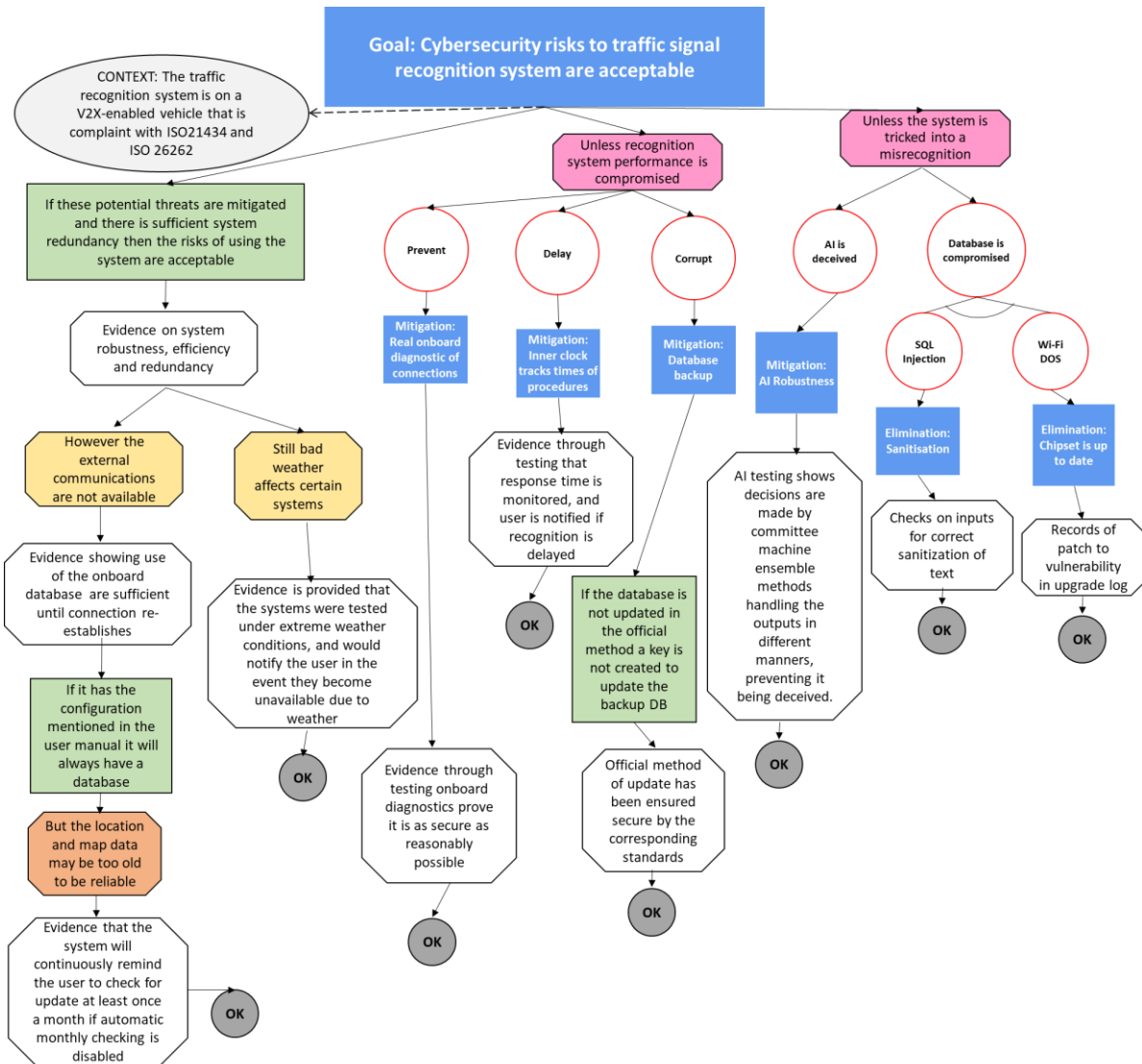


Figure 24 Cybersecurity Case for a Traffic recognition system

The cyber security case illustrated in Figure 24 uses an attack tree of to identify potential threats. These identified threats are used as claims supporting the rebuttals to the main goal. The structure of the attack tree is followed by arguments that transform into new goals as they are strategically mitigated or eliminated. These new goals are further justified and provided with evidence in order to deem them as safe and secure as reasonably as possible. Reaching a level of acceptability for the claims sourced from the attack trees can be achieved by directly backing them with evidence or proposing a reasonable deduction through inferences corroborated with evidence.

5 Real World Application

This example was created in a secondment at RH Marine where the inner workings of an Autonomous Sailing Vessels (ASV) were analysed and the work products (security and safety analyses) developed by the company for their autonomous sailing project (an ADT and a FMEA, respectively) were used to produce a viable and peer reviewed collaborative assurance case.

5.1 Autonomous Marine Vessel

This example explores Artificial intelligence in an autonomous transportation application while also using the method outside the automotive sector. ASV are gaining increasing attention worldwide due to the potential benefits of improving safety and efficiency.

5.1.1 System description

The degree of automation in navigation today means that many manned vessels operate in autopilot mode from one waypoint to the next, ensuring their movement on the planned trajectory. This is simply ensured by connecting the GNSS (global navigation satellite system) receiver with autopilot and gyro-compass. This information is passed to the autopilot as a new course to the target and compared with the current course, which gives the basis for calculating the correction to the rudder/thruster. While an autonomous sailing system consists of environment perception, situational awareness, decision making, and controlling, which enables more intelligent functions like environment detection, obstacle recognition, collision avoidance, and control.

An effective perception of the environment is the precondition of safe sailing. For ASV, typically, there are multiple sensors used onboard. One is the automatic identification system (AIS), through which ships can broadcast static information (e.g. vessel identification number, ship name), dynamic information (e.g. position, speed), and other relevant information to each other. Besides, the vessels can also perceive their environment including other ships by means of exteroceptive sensors such as radar, lidar, and camera. Using these sensors, usually AI-based methods are required for obstacle recognition, classification and tracking. Single sensors always have limitations since different types of sensors have different features such as ranges, sensitivity to precipitation conditions, light levels, and measurement accuracy. Sensor fusion can lead to better perception by utilizing the data from multiple sensors.

Another important aspect of the ASVs is a collision avoidance system with effective and robust collision avoidance algorithms to ensure vessel safety during automated sailing. Apart from the above main purpose, Collision avoidance takes account of concerns such as the dynamics of the own ship, the external environment disturbances, movement and intention prediction of target vessels, as well as compliance with the International Regulations for Preventing Collisions at Sea (COLREGs)[128]. Considering all the concerns above results in a significant computational load, especially in complex scenarios. Ensuring real-time performance is another critical factor in the practical system.

5.1.2 Marine Vessel Safety and Security

Ships are the most secure and ecologically friendly mode of commercial transportation. Almost all shipping operations have long been committed to safety, due to the innate possibility of danger. The shipping industry was one of the first to establish universally accepted worldwide safety standards. [129] Because shipping is fundamentally international, it is governed by a number of United Nations bodies, including the International Marine Organization (IMO), which has produced a comprehensive set of worldwide maritime safety laws. On the other hand, all governments demand that ships and other maritime constructions flying their flag meet specific criteria.

A non-governmental regulating organisation known as classification society, is an organized operation in the marine industry, including vessel and offshore structure development, which aim to represent the interests of ship builder and operators. These societies oversee the development of rules for the design and classification of ships and offshore structures. IMO and national governments are influenced by the classification societies, when deciding on regulations. Ship surveyors, naval architects, and a wide range of certified marine engineers are used by classification societies. These professionals are in charge of monitoring ship building and maintenance, as well as conducting required surveys of ships currently in operation to ensure that standards are fulfilled [130]. To improve stability, safety, and cleaner emissions, classes are designed to control the structure and design of all vessel types. To that aim, classification societies agree on technical standards, supervise designs, and double-check computations to guarantee that the rules are followed. Qualified personnel are assigned to inspect ships and structures during construction and commissioning, as well as to survey vessels (including submarines) on a regular basis to verify that they continue to meet all requirements. They are also in charge of classifying offshore constructions such as oil rigs, platforms, and other structures. Propulsion systems, navigation devices, pumps, valves, and other equipment are all included by this survey.

The 3 largest classification societies are DNV, (Det Norske Veritas,) Nippon Kaiji Kyokai, and ABS (the American Bureau of Shipping)[131] The main Regulations followed by all classification societies are:

- **SOLAS** (International Convention for the Safety of Life at Sea) Established in 1974 and updated to date defines and clarifies the minimum standards of safety equipment on board.
- **MARPOL** (International Convention for the Prevention of Pollution from Ships) Available since 1978 discloses the requirements necessary to prevent pollution from occurring yet accidental or as a result of routine operations.
- **COLREG** (Convention on the International Regulations for Preventing Collisions at Sea) Accepted since 1972, and mainly achieves what the road safety rules do on cars.
- **ISPS** (The International Ship and Port Facility Security Code) From 2002 onward is the gold standard of marine vessel safety it has been updated to also include cybersecurity.

5.2 Comparison with the Automotive Domain

As the marine industry has its regulations the requirements are identified in a goal based manner similar to automotive cyber security; an expected result but not an specific method. The maritime industry does not have standards similar to SOTIF or functional safety, neither do they have a sector-specific cybersecurity standard.

In comparison to the Automotive industry, this example can be compared to a level 4 autonomy vehicle.

Regarding safety the automotive industry is bounded by the UN-ECE regulations plus ISO 26262 for Functional Safety and ISO 21448 for Safety of the intended function (SOTIF). These regulations also not just are legally binding but needed to compare and be compatible with all other vehicles. Other than the regulations automotive vehicles are set on consumer tests like NCAP to see if they are more than the standards and regulations and how they rank. So even when there are many regulations, standards, and consumer tests on automotive, marine manages to achieve the same objective through its organizations and has been doing it since before cars. Tools like a FMEA are used in vehicle safety in addition to a HARA, ASIL, as for functional safety (FS) these tools are applied to a Goal Structured Notation (GSN) safety case. Considering that for the current scenario there is an existing FMEA, it will be used to create the safety objectives ala FS trying to not forget the vital parts of SOTIF. Therefore, by narrowing the ideas from the FMEA it is possible to convert them into goals or claims that fit the method for the assurance case. The FMEA will also help to counterclaim and argument this goals and eventually deduce evidence regarding its status.

Security and cybersecurity specifically become harder to manage as technology and automatization develop farther, the vehicle industry normally follows ISO21434 and the mandatory UN regulation 155. Both the standard and the regulation require a safety case, and to do so a holistic approach that can consider the links with safety is effective. When it comes to marine industry IMO Resolution MSC. 428(98) introduced in 2021 has various cybersecurity requirements for ships. The main difference is that IMO requires the owners to assess the cyber risks while the automotive industry expects it from the developers. With an attack tree, things that are linked to security become more apparent and logically perceivable. The threats of an attack tree can seamlessly transfer into the assurance case.

5.3 Identification of Risks and Threats

By identifying the safety and security concerns the idea takes a shape similar to how it is done in automotive. Using this notion it should be possible to create an assurance case that can work as a cybersecurity case that incorporates safety. Using the FMEA and the attack tree , supplied as a work product, is possible to extrapolate safety and security concepts and help build on the assurance case. While no specific standard exists, it does not mean that this elements are not taken in consideration, the elements are consider through the life cycle and the documentation exists to back it up.

5.3.1 Safety Marine Vessel Safety Identification of potential hazards (Safety)

This section identifies the safety hazards, regarding any hazard that may cause a physical harm or loss inherently from the AI. The main hazards from the AI that are identified in a FMEA are the following:

- The loss of the Vessels Ability to maintain its position
- Problems relevant to the ability to self-drive
- Unavailability of the control systems
- Communication problems
- Failure of collision avoidance (Other vessels and shore)
- Non functionality of alarms and problem detection systems
- Incorrect lighting or identification
- Safety of the crew and evacuation methods

5.3.2 Marine Vessel Security: Identification of Threats (Security)

Regarding security threats the most important factors to consider and that are the backbone to an attack tree regarding cybersecurity of an attack tree are:

- **Confidentiality Issues:** This considers that the information regarding the vessel loses the secrecy of the private information it possesses.
- **Attacks on the AIS:** May be due to spoofing either the closest point of approach (CPA) or Search and Rescue Transponder (SART). Also an inaccurate understanding of the weather will affect how the AIS responds.
- **GPS Attacks:** Anything from spoofing to eavesdropping on the location can have dire consequences in helping the vessel orientate.
- **Radar System Attacks:** Any potential attack on the radar system will cause the effect of blinding the vessel.
- **Access to the Network or Server Issues:** The server provides access to information pertinent to decision making, limiting this access disables control and service.
- **Limiting the Availability:** Reducing availability of essential functions.
- **Problems with the physical bridge or Workstation:** This would not permit a manual override to save the vessel.

5.4 Application of the Method

Applying the method produces an assurance case with the following appearance shown Figure 25 while the next 3 figures will show the different segments individually and at a different scale for more detail.

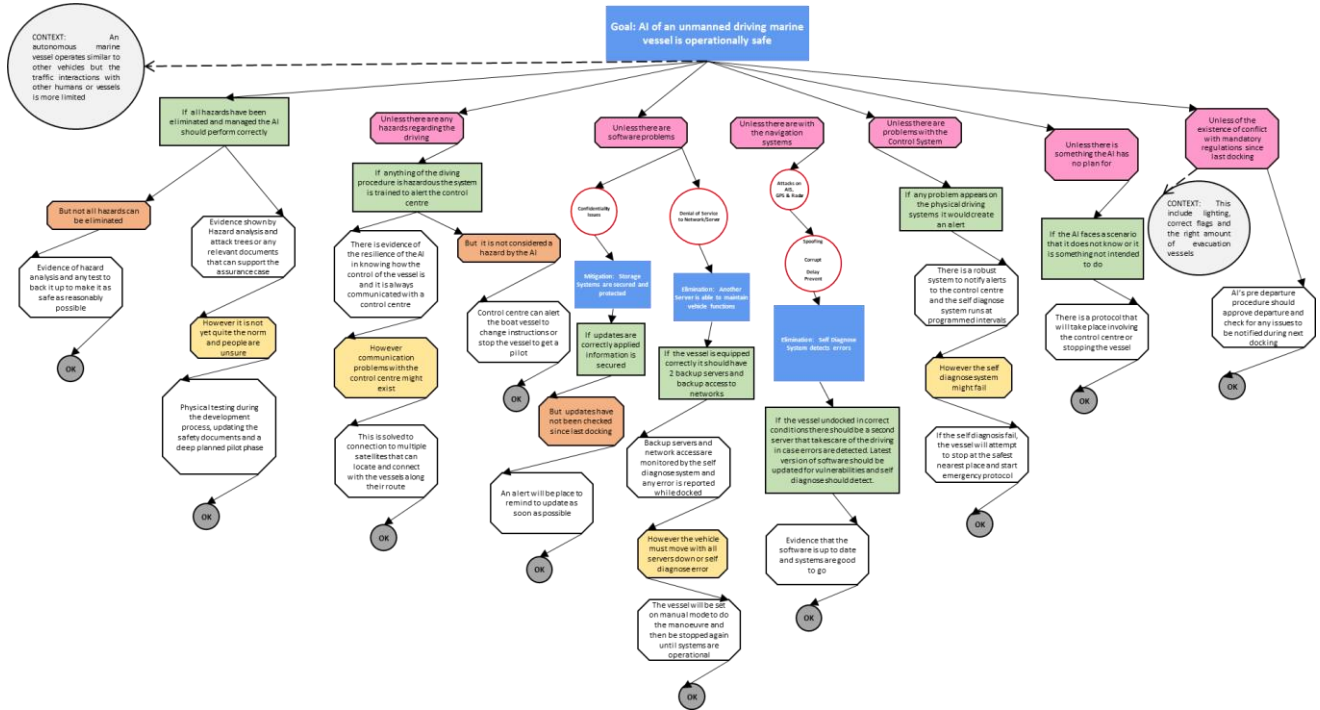


Figure 25 Application of the method to an ASV (Extended size image on Appendix D – Enlarged Method Diagrams)

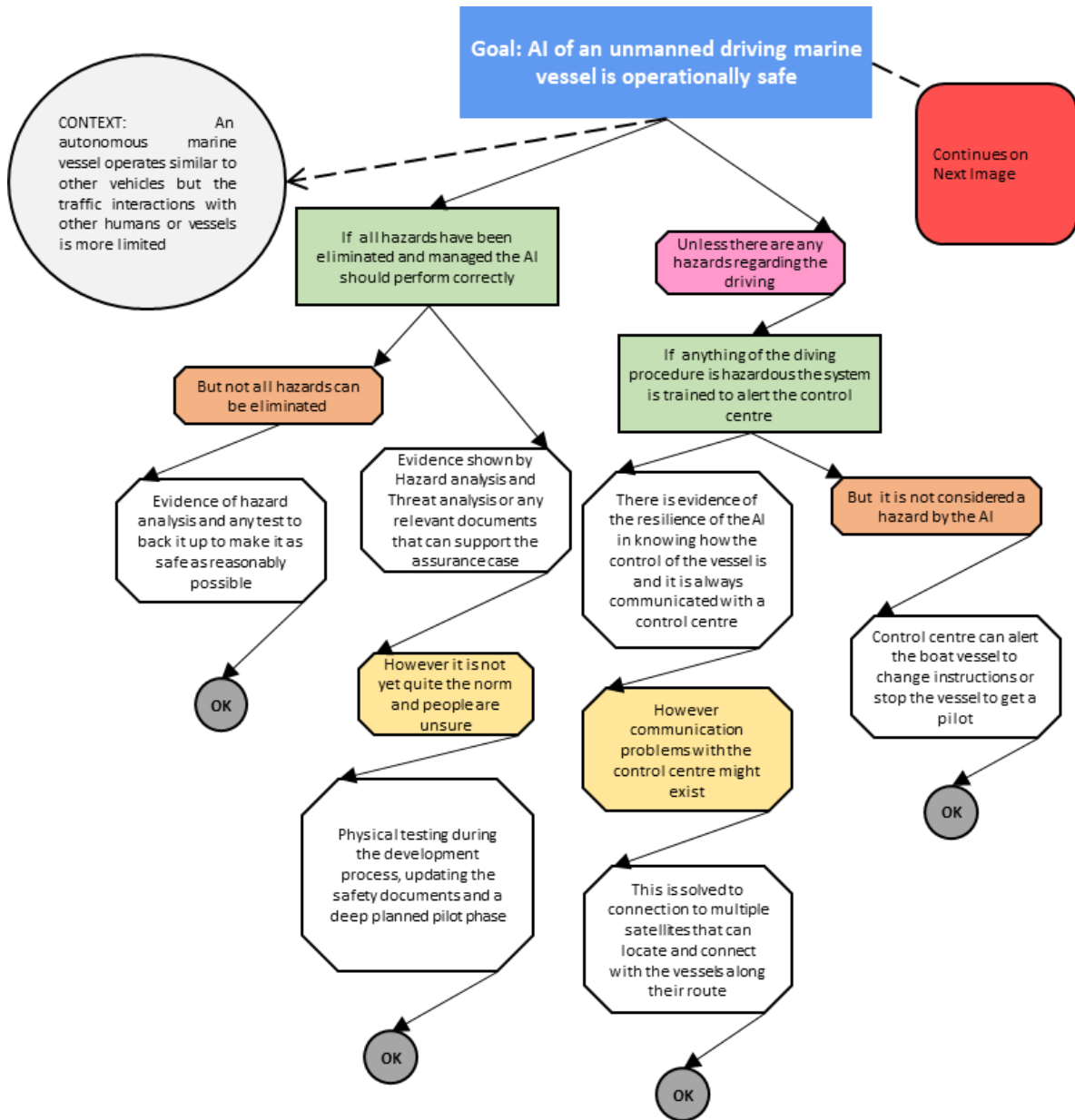


Figure 26 Enhanced size detailed diagram part 1 of 3

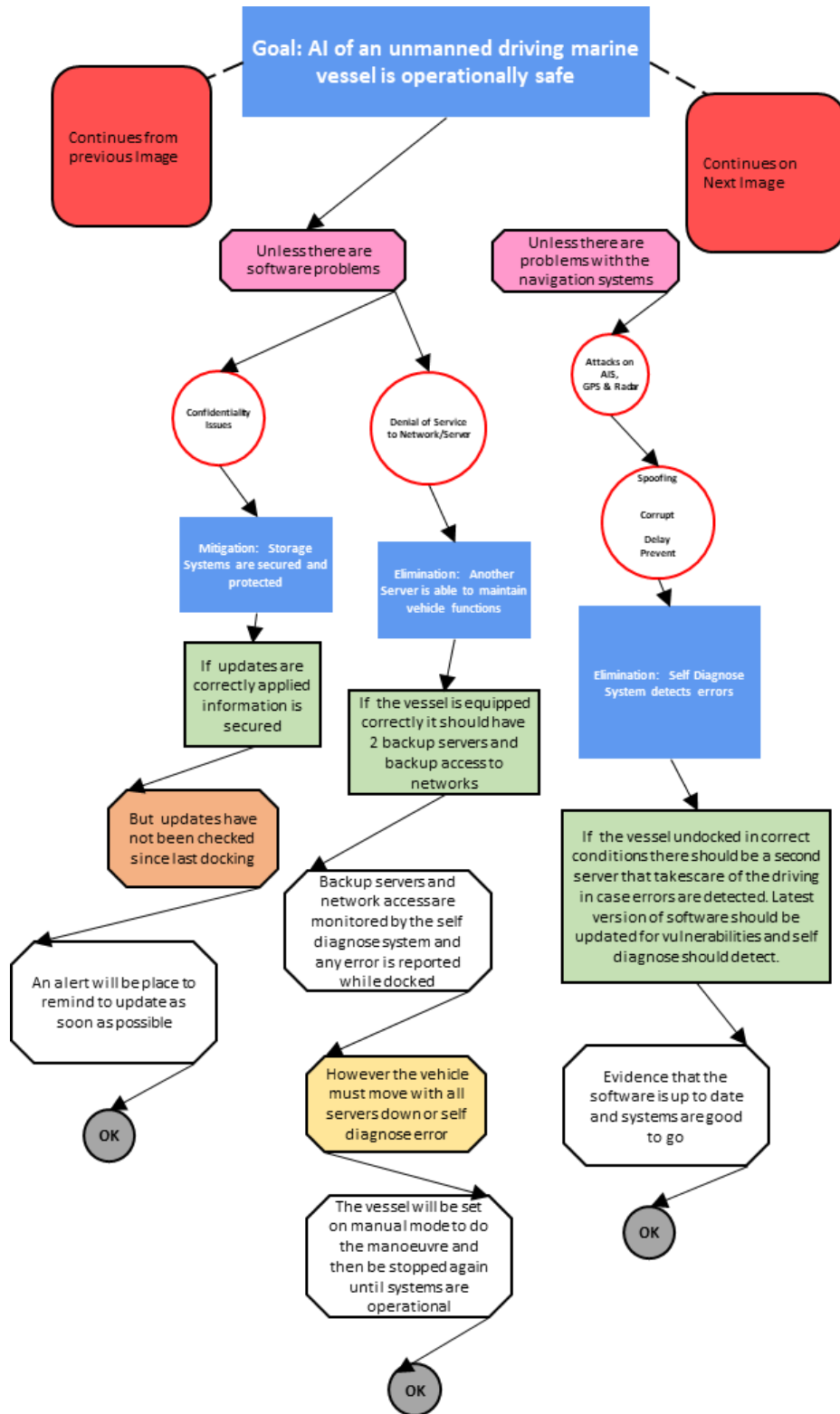


Figure 27 Enhanced size detailed diagram part 2 of 3

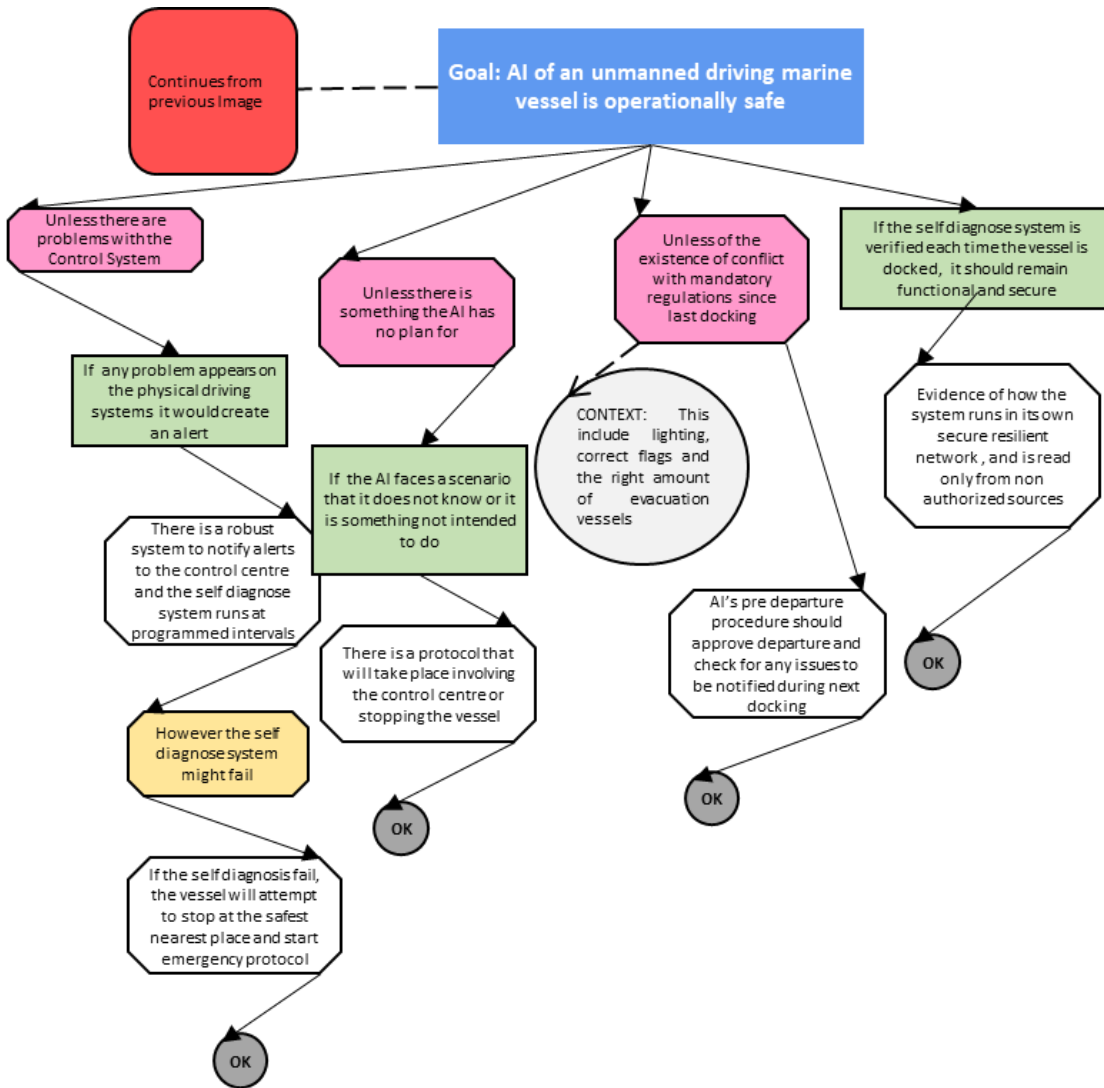


Figure 28 Enhanced size detailed diagram part 3 of 3

6 Test Case as a Pilot demonstration

In order to try the method with more than examples and to its fullest extent, this part will delve into the test bench that inspired the test case and the necessary background to build it. A similar test bench was created and developed at Coventry University by Shahid Mahmood[132], but due to the changes of integrity and Linux packages, it could not be cloned it had to be built from the start. This running Uptane is used to do a small test to see how OTA updates happen, and how it will affect a safety critical system like and airbag if it is updated. The idea that updating a safety critical system can go wrong and its cascading effects can set the basis for dangerous events that put lives at risk.

6.1 Test Bench for Test Case

To develop a more practical part to the concept and the test case a test bench was created. The main idea of the test bench is to run the Uptane standard for over the air updates(OTA). A well known application that implements OTA security with a certificate-based approach, this means there is a certificate to check the keys and updates are dependent on whether it is signed or unsigned. Uptane is an American update method that achieves to do it in the most secure way possible. OTA updates in Uptane work using The Update Framework (TUF) in combination with a comprehensive and broad threat model. It is composed of the 4 roles in TUF: root, timestamp, release, and target; used securely verify the updates, plus also signing them digitally. Uptane is protected against the 5 most common malicious attacks during updates, this are:

1. Preventing updates to be read outside Uptane
2. Preventing interception and modification
3. Preventing the denial of service
4. Preventing a denial of functionality
5. Preventing control access

The idea of UPTANE in the project was to create a test bed that was to be tested through bit flipping, and that would enable extra support for the assurance cases being developed. Coventry University had developed a test bench like this, yet it is more than 5 years old, it has proved challenging to install outdated software and resources, and hardware wise has been impossible to replicate. It worked using the initial [UPTANE demo](#), that has been archived since early 2019. Even though the old demo is defunct, the UPTANE framework is alive and kicking. The physical elements would remain fairly the same (some physical specs are updated), but to do so an OTA server that is compatible with the newest UPTANE must be created. The structure of putting

a full OTA project would look something like the following Figure 29 but the objective is something simpler. The key idea is that it needs two parts a server side and a client side.

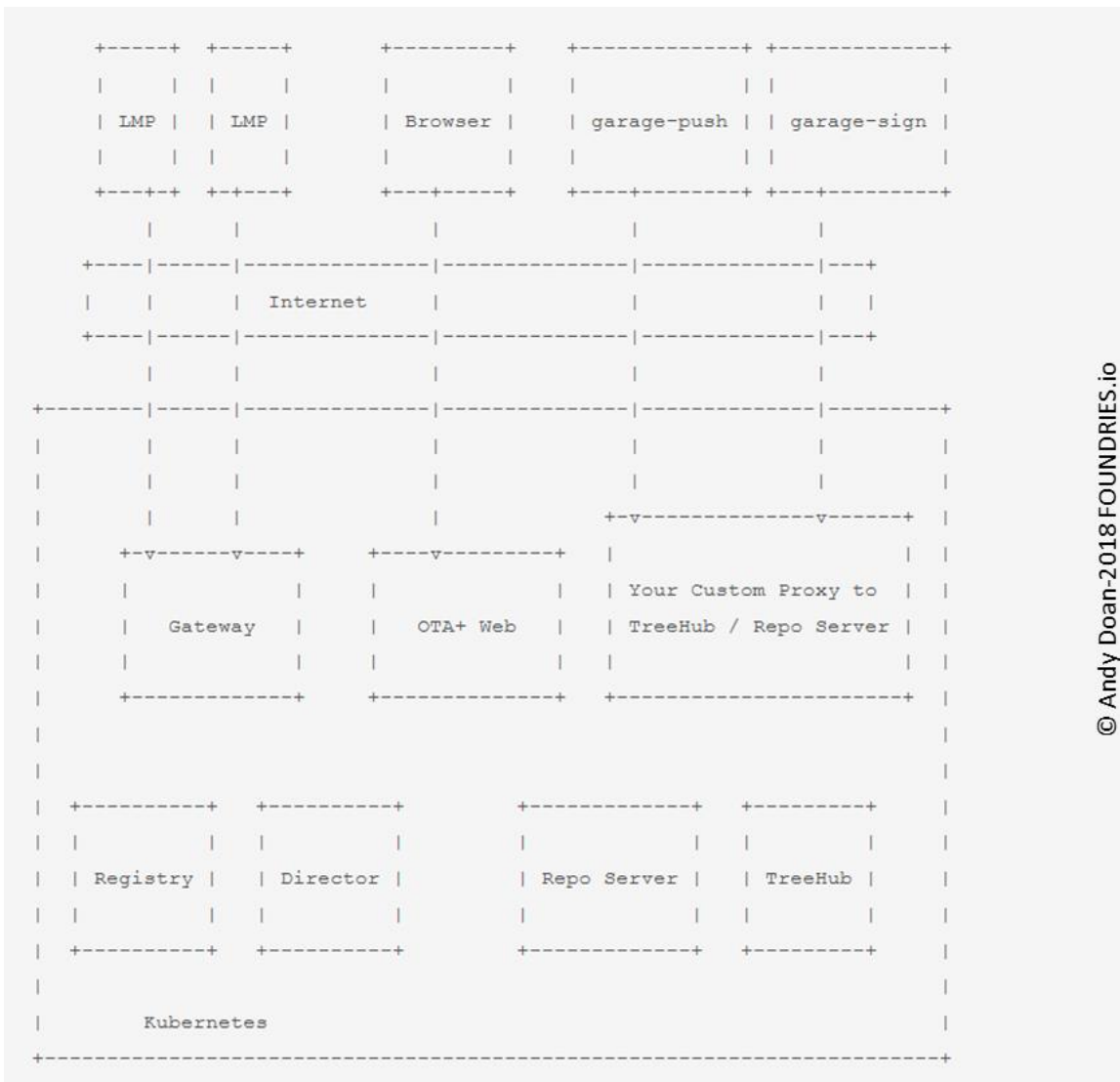


Figure 29 Structure of a complete OTA server project [133]

6.1.1 Setting up the server

To set up the server there are 2 options one is [HERE OTA CONNECT](#), which is a paid service, and the other is [OTA Community Edition](#), a open-source server software that supports devices compatible with mainly used for experimenting.

As the objective is to experiment OTA Community Edition, is the most suitable choice. The open-source server software to allow over-the-air (OTA) updates of compatible clients. It is comprised of a number of services which together make up the OTA system. The source code for the servers is available on [Github](#) and is licensed under the MPL2.0 (as is the code in this repository). Docker container images of the latest build are available on [Docker Hub](#). This repository contains scripts to launch the open-source OTA Community Edition software under the [Kubernetes](#) orchestration system on a single machine (minikube). Note that the OTA Community Edition doesn't use authentication nor any other security provision needed for a production system. It is meant to run locally/inside of a firewall.

6.1.1.1 System Requirements

All of the system requirements were achieved with a laptop provided by Coventry University. The system requirements on the testbench server are:

- More than 100GB of hard drive space for images and data related to the clients and updates
- More than 8GB of RAM to run and software
- Wireless and ethernet connection
- Linux Ubuntu 16 or more
- Required tools to run the scripts in the current repository:
 - [minikube](#)
 - [kubect](#)l (version >= 1.16)
 - [kops](#) (version >= 1.16)
 - [jq](#)
 - [httpie](#)
 - [VirtualBox](#)

6.1.2 Setting up the Client

The client is who is being updated or used as reference to update. Clients use [Aktualizr](#), the C++ implementation of [Uptane](#) OTA update client. The client is intended to be installed on any devices connected to the server and that are going to interact directly with OTA updates from an Uptane-compatible OTA server. The recommended and most built is done by using the [meta-updater](#) layer in a [Yocto environment](#). With the possibility of using [aktualizr](#) as a stand-alone system tool or, integrated with [libaktualizr](#) into a larger project.

The clients use raspberry pi 4 model b. A [raspberry pi image](#) can be built for HERE OTA using a simple process. Raspberry pi images built for HERE are compatible with the open-source experimental server.

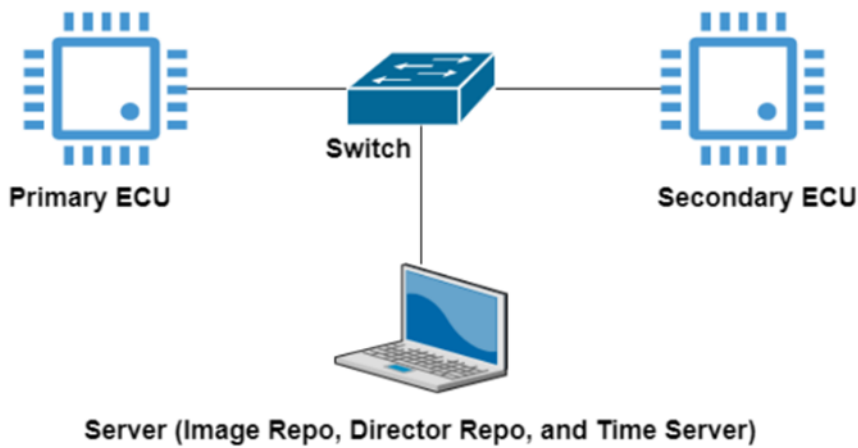
The client is responsible for:

- Communicating with the OTA server
- Authenticating using locally available device and user credentials
- Reporting current software and hardware configuration to the server
- Checking for any available updates for the device
- Downloading any available updates
- Installing the updates on the system, or notifying other services of the availability of the downloaded file
- Receiving or generating installation reports (success or failure) for attempts to install received software
- Submitting installation reports to the server

The client is intended to maintain the integrity and confidentiality of the OTA update in transit, while communicating with the server over a TLS link. The client is expected to run either as a system service(one that would periodically checking for updates), or in a way that it can be triggered by another system.

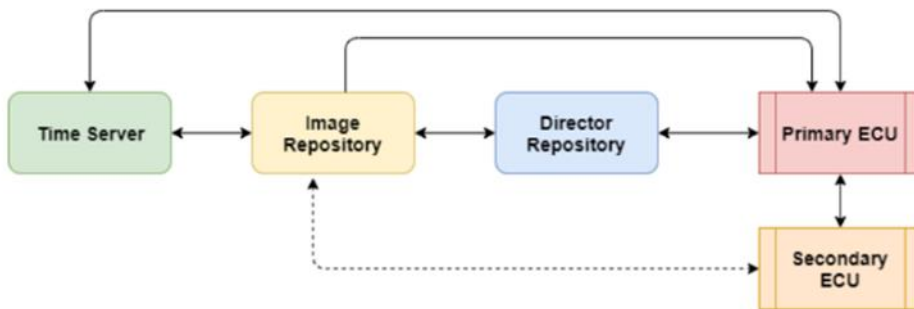
6.1.3 Outlay of the Test Bench

Having the client and server side means that a complete test bench can be built. The test bench uses a laptop as a server and two raspberry pi as clients. It uses router as a switch, to connect each raspberry pi to the laptop through ethernet. It is possible to connect a real ECU to a raspberry pi using the ODB 3 component of a raspberry pi. A more elegant idea than bit flipping was discovered between the tools of the OTA server and it is better and more easy to use than bit flipping. As per the original testbench by S. Mahmood [132] Figure 30 shows the basic network structure of the test bench; Figure 31 shows how the images are handled in Uptane, and how this flow of information works on the test bench; and Figure 32 shows the original test bed in Coventry university correctly labelled. Figure 33 shows the updated interface in the most recent test bench as in contrast the original Coventry University test bench that lacked a user interface.



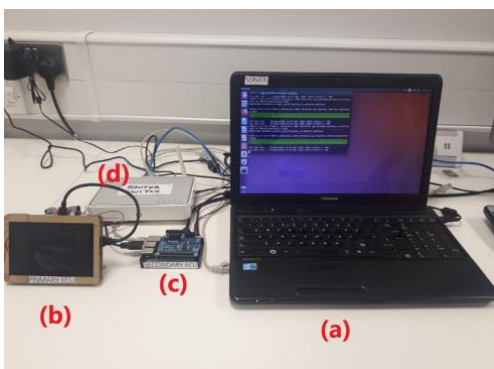
© Coventry University -2020

Figure 30 Network Diagram of the OTA Test Bench [132]



© Coventry University - 2020

Figure 31 Information flow from primary ECU to secondary ECU in the test bench [132]



The testbed for the testing of OTA software update system for automobiles. The setup comprises of (a) a laptop computer (hosting server components for the Uptane framework), (b) the primary ECU, (c) the secondary ECU (both of which implemented on Raspberry Pi 3 micro-controllers), and (d) a switch for interconnecting the components.

Used with the Permission of ©Shahid Mahmood

Figure 32 Details of the testbed at Coventry university. [132]

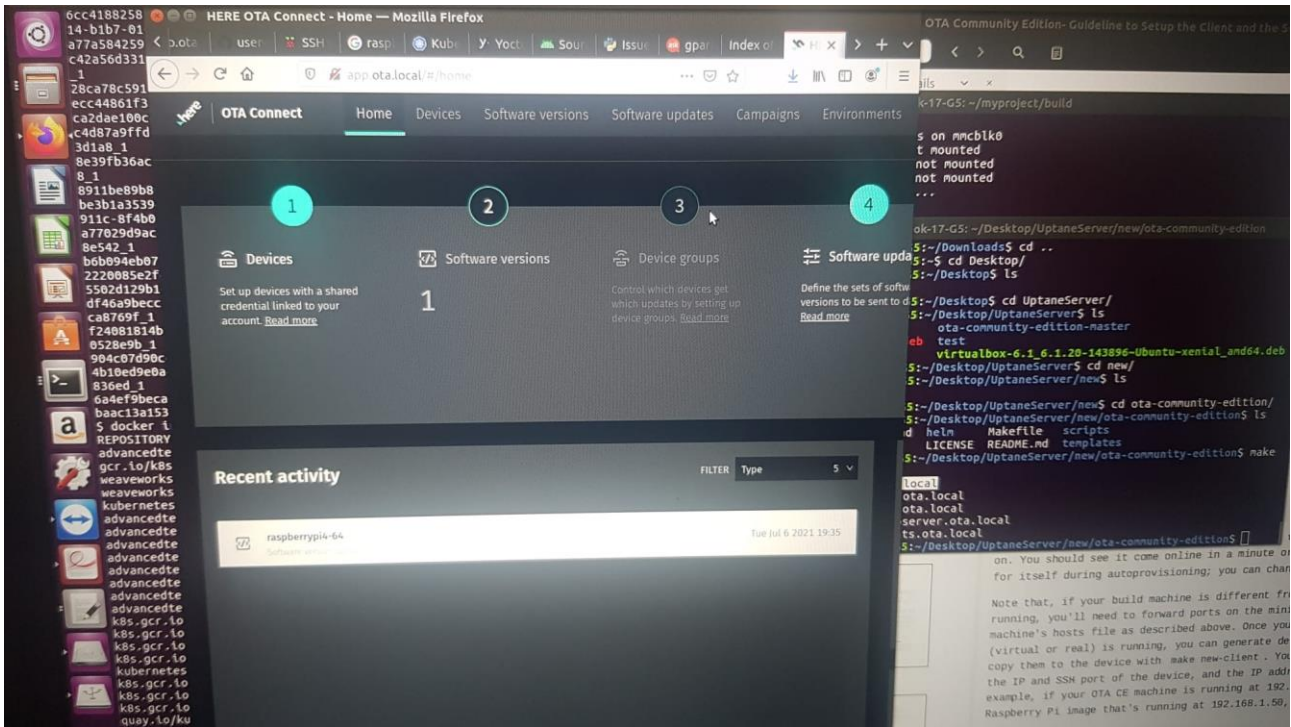


Figure 33 Current user interface in the newest version of Uptane

6.2 Test Case: Assurance case of OTA Update on a safety critical system (Airbag ECU)

6.2.1 Concepts and Background

Before delving into the test case itself and to be congruent within the narrative of the document it is important to understand a few concepts of how car ECU's work.

6.2.1.1 In Vehicle Data Networks and Domains

A vehicle's computer system is made of the combined power of many ECUs working in parallel. The communication between ECUs is mostly done through CAN -Bus. A group of ECU's with related functions form a domain with its own subnetwork. A gateway allows the exchange of signals between domains over a backbone network. A Telematics ECU can serve as a gateway if it is connected to all of the domains. The gateway ECU is a unit that performs a frame or signal mapping function between two communication systems. This kind of gateway ECUs is what are typically installed to handle a direct connection from the vehicle to a source allowing also conversions and CAN communications as per ISO 11898-2 [134]. In the context of automotive vehicle networks there are 5 common types:

- **CAN High**, this type of CAN has rates ranging from 40 kbit/s to 1 Mbit/s, it is by far the most widely used CAN, the current generation is referred as CAN FD for the flexible data rate.
- **CAN Low**, a CAN bus enables bit rates from 40 kbit/s to 125 kbit/s, sometimes known as "fault tolerant CAN," allows communication to continue even if there is a failure on one of the two wires.
- **LIN**, With fewer harness and less expensive nodes, LIN bus networks are lower cost supplement CAN bus networks used on non-critical car operations.
- **FlexRay**, Is a bus that is capable of splitting data rates into static and dynamic and is ideal for safety critical functions.
- **Automotive ethernet**, provide the highest bandwidth and is being rolled out specifically for some ADAS applications.

The conversion into different protocols for each network to get to the Diagnostics OBD-3 port can be seen in Figure 34. Figure 35 and Figure 36 show and explain how a typical CAN network and subnetwork are distributed, in this case for the Land Rover Evoque.

© ElectronicSpecifier.com

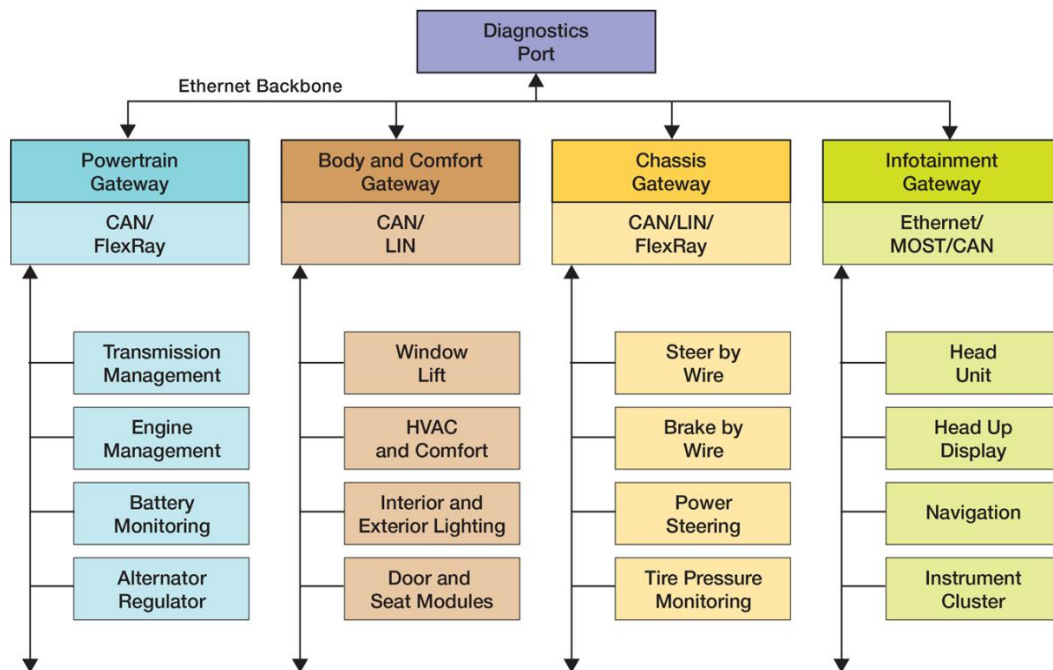


Figure 34 Application domains of vehicle networks [135]

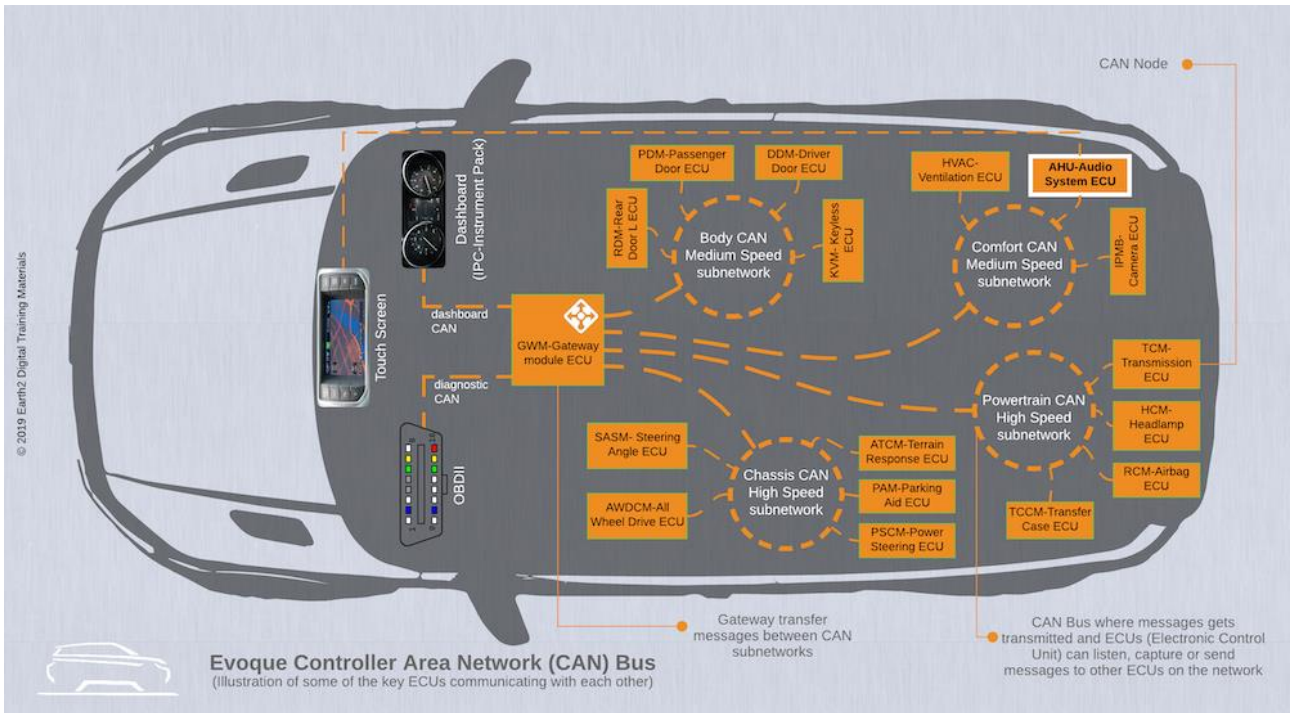


Figure 35 Selected elements of CAN network of the Land Rover Evoque, showing four domains [136]

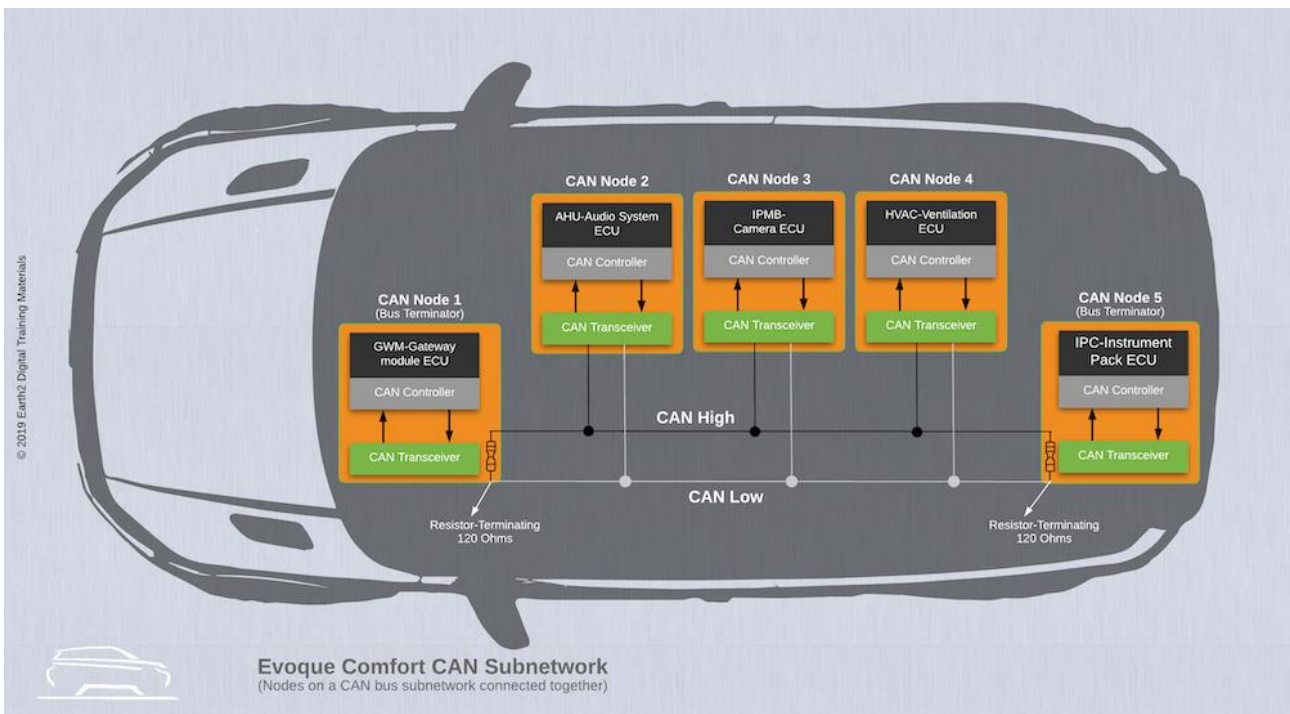


Figure 36 Comfort domain CAN sub-network of the Land Rover Evoque [136]

6.2.1.2 Airbag ECU

The airbag ECU is a safety critical system that is required by law to deploy the airbags in the vehicle. Due to the car development process is one of the ECUs that is updated close to the start of production. The system can be found in the powertrain domain (see bottom right of Figure 35). To ensure its correct functioning it ends up being dependant on the doors and windows, speed and other factors. Due to the nature of the safety brought by the airbags any incorrect deployment that being later, or at a non-crash moment may be fatal for the user. Being the most electronically complex in passive safety due to its electronic management of the sensor and triggers it becomes the ideal target ECU to be attacked in an OTA update to cause harm, and even more ideal as the test subject for the test case.

6.2.1.3 ECU Updates

Conventional wired firmware updates are usually done in a garage by connecting with the gateway via the ODB3 port, and directly sending those updates to the correct ECU. With the introduction of firmware over the air, a gateway should be able to get the updates through its Telematics Control Unit. Updates are to be applied during the times the vehicle is parked. Due to the size or sensitivity of some of the updates they are only applied in recognized networks with accepted keys. ODB3 continues to be an option for updating and the over the air can happen between the device connected to the OBD3 port and the network. For vehicle protection and so there is mainly just one controller manufacturers have opted for the gateway ECU to be the only and main way into the other components. Even though the gateway being the only accessible ECU helps security, it still doesn't make it extremely secure, as the gateway ends up doing functions of a messenger in an update. Automatically triggered big updates may have the inconvenience of excessive battery drain or being interrupted because the car wasn't parked long enough.

6.2.2 Context for the test case

This test case will take into account a simplification of managing the updates directly in a Airbag ECU that has its own gateway ECU protocol (telematics included) in order to simplify the idea of a gateway ECU connecting to all the car and focus directly on a safety critical system, the airbag ECU. To make attacks feasible they are done within the UPTANE environment, as some of the attacks mentioned will be void due to how the Uptane standard works.

6.2.2.1 How Uptane protects the system

For this test case, as previously, the test case considers updates are done using the Uptane framework, developed in collaboration with the United States Homeland Security for the automotive industry and used by many OEMs. Uptane limits the possibility of security incidents during software updates by providing a highly resilient system that prevents hackers from installing unauthenticated, unsigned, out-of-date or otherwise compromised software during the OTA process. Updates security features are a combination of both online and offline. Uptane developer Justin Cappos believes the system is secure enough to not be easily compromised, and is always being updated, making it as secure as reasonably possible and a correct mitigation or inferred solution to relevant branches on the test case.

6.2.2.2 Airbag

The airbag itself interacts with various delicate sensors (a device meant to detect a specific physical parameter through electric input) and actuators (an actuator is a device that produces a motion by converting energy and signals going into the system) that precisely calculated any alteration might lead to an incident

a. How does an air bag work?

An airbag in a vehicle is a Supplemental Restraint System (SRS) the main objective is to prevent the driver and passengers from being ejected from the vehicle, while also cushioning and softening the impact. The airbag is meant to work in conjunction with the seat belt, as when the airbag triggers the seat belt also tightens. In an automobile collision, the driver's speed drops from roughly 20 m/s to 0 m/s in less than a second. This indicates that the rate of change of momentum will be quite rapid, resulting in a significant impact of the driver's body on the steering wheel or dashboard. Airbags lower the driver's body's rate of change of momentum, decreasing the impact of the driver on the car's front interior. Air bags are deployed when a combination of crash signals is detected, signals come from the pressure sensors that can detect a crash and sensors that measure the absorption of energy through deformation in the beam. Precrash signals are detected when the car decelerates at a certain rate, and other sensors at the front transmit prepare for impact, the precrash protocol sends an electronic signal to a heating element in the chemical propellant, causing it to oxidise. This oxidising effect activates the pyrotechnic ignitors that generate instant heat, this causes sodium azide (NaN_3) and potassium nitrate (KNO_3) to decompose into sodium metal and nitrogen gas, which will inflate the vehicles' air bags. Each airbag inflation is dependant of its pyrotechnic ignitor, that works as an inflator, regardless of location and is timed to the vehicle specifics. The gas inside the airbag cools quickly, ensuring that the airbag deflates in time to absorb the impact. Figure 37 shows how an airbag works. Front airbags and side air bags are legal requirements for cars in Europe.

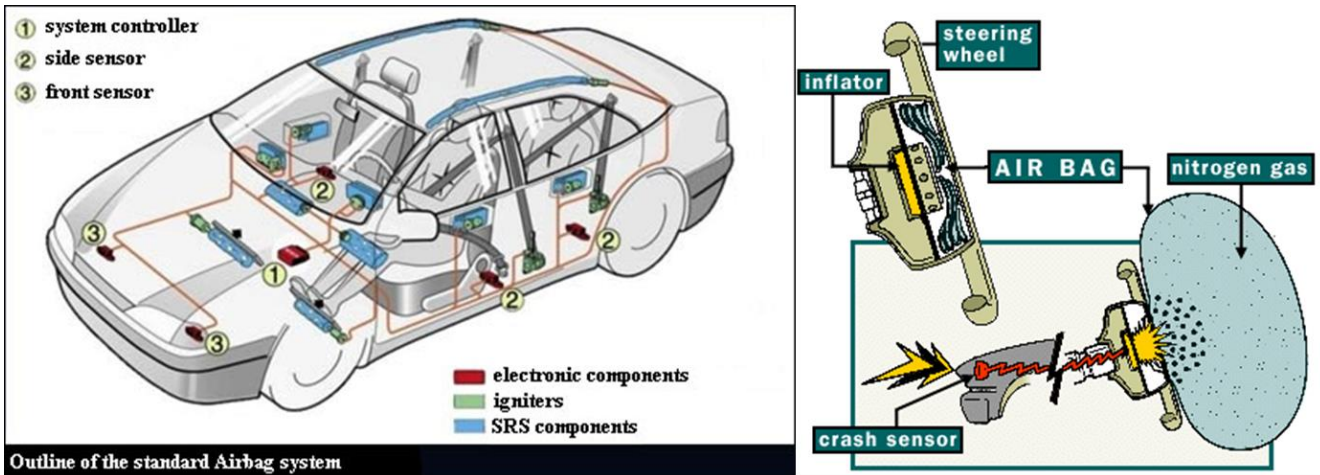


Figure 37 Working and deployment of a vehicle airbag [137]

b. Air bag Attacks

Even when considering that updates are secured via Uptane preventing any new error from actually happening would be impossible [118]. During a malicious attempt on an update, attacks can still happen to the genuine update itself and should still be considered. The example aims to establish that the update is not just safe as an update but that all functionalities and existing attacks remain as secure and safe as reasonably possible.

- **Attacks on the deployment:** All of this relate to affecting the correct deployment of the airbag, from changing inflation time to the triggers.
- **Airbag should not trigger at what is considered a low speed crash in full frontal scenario.** The a faster deformation in stationary would still be considered a full frontal.
- **Attacks on the Sensor detection to spoof a crash:** This considers all and everything that will make the vehicle think there was a crash, be it false positive or false negative.
- **Altering the identification of misuse cases:** By misuse cases it means all the incorrect unintentional wrong uses the vehicle might have that are to not be considered a crash, for example getting hit by a basketball or running over an animal.
- **Tampering the diagnostic services:** This includes messing around with the vehicle to prevent any other services including ignition as it believes airbags have falsely deployed or another in car diagnosis is not recognized as safe.
- **Generating problems on the ventilation system, window opening and vehicle locks or any precrash service in those regards:** Anything relating letting the airbag fumes remain on the vehicle, plus any alteration that would prevent the doors from letting the person leave the vehicle.

- **V2X tricking to deploy airbag or post-crash services:** This would include the e-call system handled by the airbag ECU.

6.3 Application of Assurance case into pilot demonstration

The work products obtained, lead to an assurance case applying the test bench update concept and the test case together in the method developed through this thesis.

6.3.1 Existing work products to support the application

A demonstration of an application as such should not be taken lightly, therefore the following inputs documents were used to develop the assurance case. (see Appendix)

- **An Attack-Defense Tree**, this was created by a fellow researcher of Coventry with the specific scenario in mind
- **GSN Functional Safety case**, A GSN safety case was design for this specific scenario to be evaluated as functional safety case example by a researcher in the university of York, and a collaboration with this project
- **HARA**, Provided by an electric vehicle OEM, it provides all the relevant information of a CAV regarding airbags and ECU updates
- **ASIL**, Created by an OEM dedicated to sport cars, it lays out the evaluation of threats regarding safety critical systems, that are relevant to the electronic elements of active/passive safety.

These work products influence some of the decisions on the example. The diagram featured in Figure 38 is a 2-seater to be congruent with the ASIL analysis, and to be also compatible with the HARA it will be assumed it is an Electric Vehicle with all-wheel drive. The GSN FS case and the Attack Tree consider the vehicle with these specifications.

6.3.2 Layout of the case for the demonstration

The demonstration considers a simplified ECU system where the TELEMATICS ECU and the AIRBAG ECU are set as one. Airbags are set to trigger once any of the actuators perceive deformation beyond the point of no return in forces (all are pressure sensors except the front middle one that would be a pressure + optic sensor). To simplify, all the sensors have an exact point of triggering and are sensitive to force, the system does not consider complex physics of static mechanics, plasticity, deformation, nor will it consider a combination of

optic sensors that track beam deformation or active components of the car that could disassemble at the moment of impact. This simplified layout gives the needed functionality, by taking off the pressure of calculating the complex physics and electronics, and letting the example focus more in its relations of cybersecurity and safety. Figure 38 shows the diagram of sensors and actuators, included for the demonstration, that will have a reaction during a crash. It specifies the ECUs and ODB port in the centre, and identifies all crash sensors as black dots and how they are connected through black lines, it shows the unexpanded airbags as green rectangles.

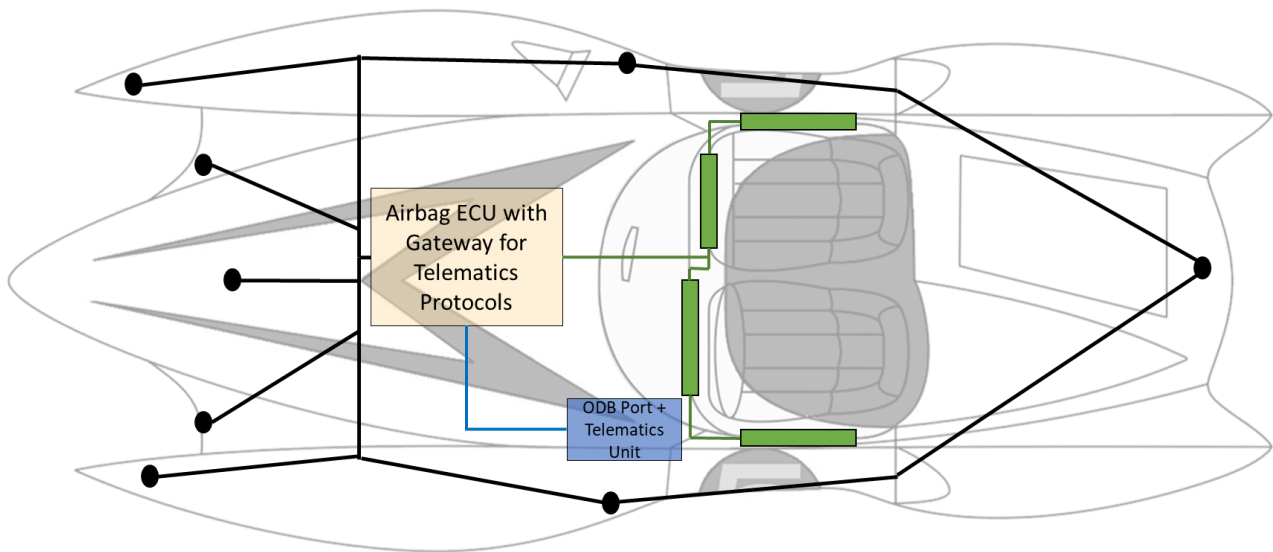


Figure 38 Sensors (Black Points) and Airbags (Green Squares) available

6.3.3 Pilot Demonstration Application

The application of the assurance case method to the update of the safety critical system results in the following diagram Figure 39, for ease of use it will also be segmented (in 4 parts).

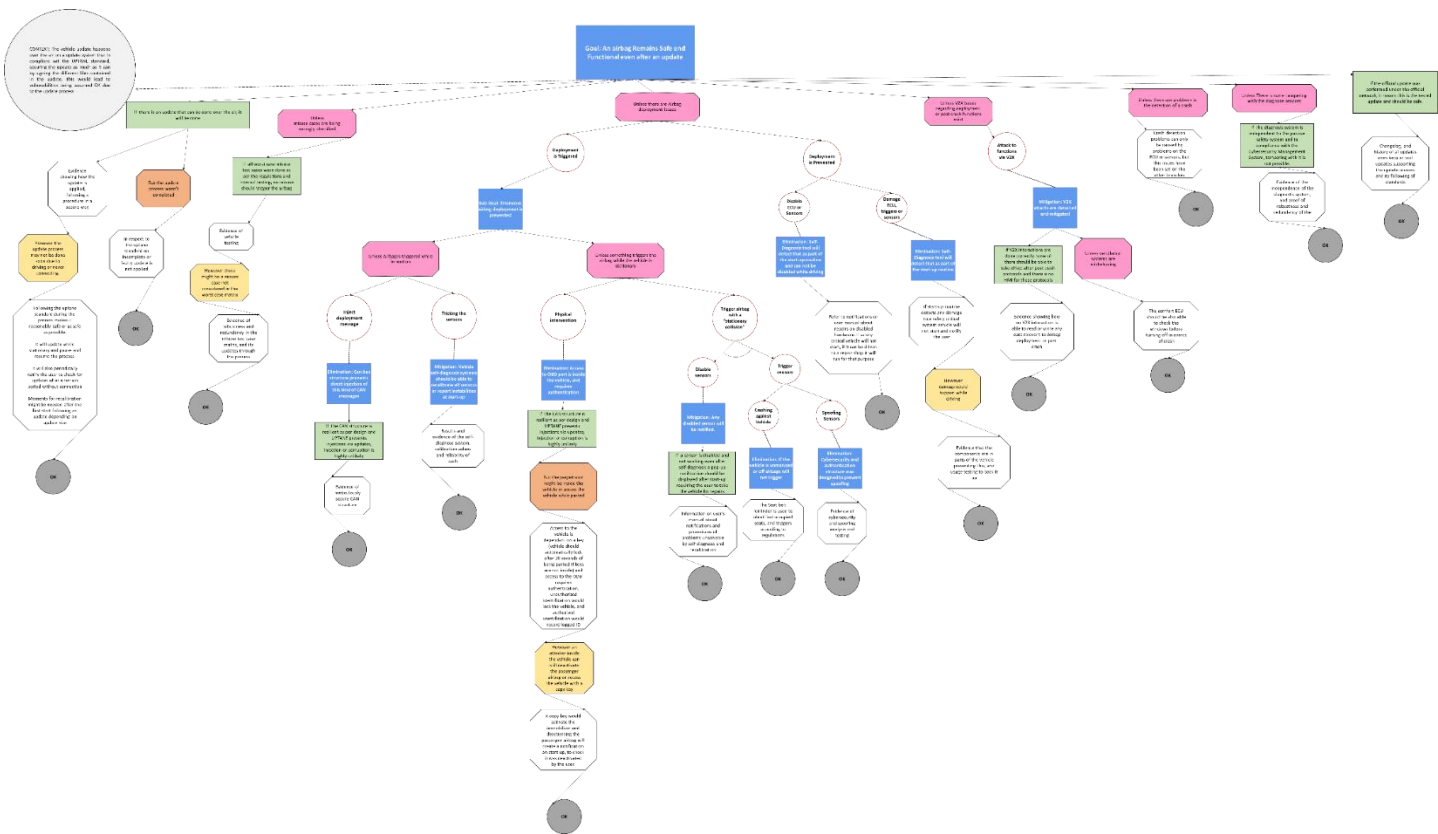


Figure 39 Pilot Demonstration, (Extended size image on Appendix D – Enlarged Method Diagrams)

....

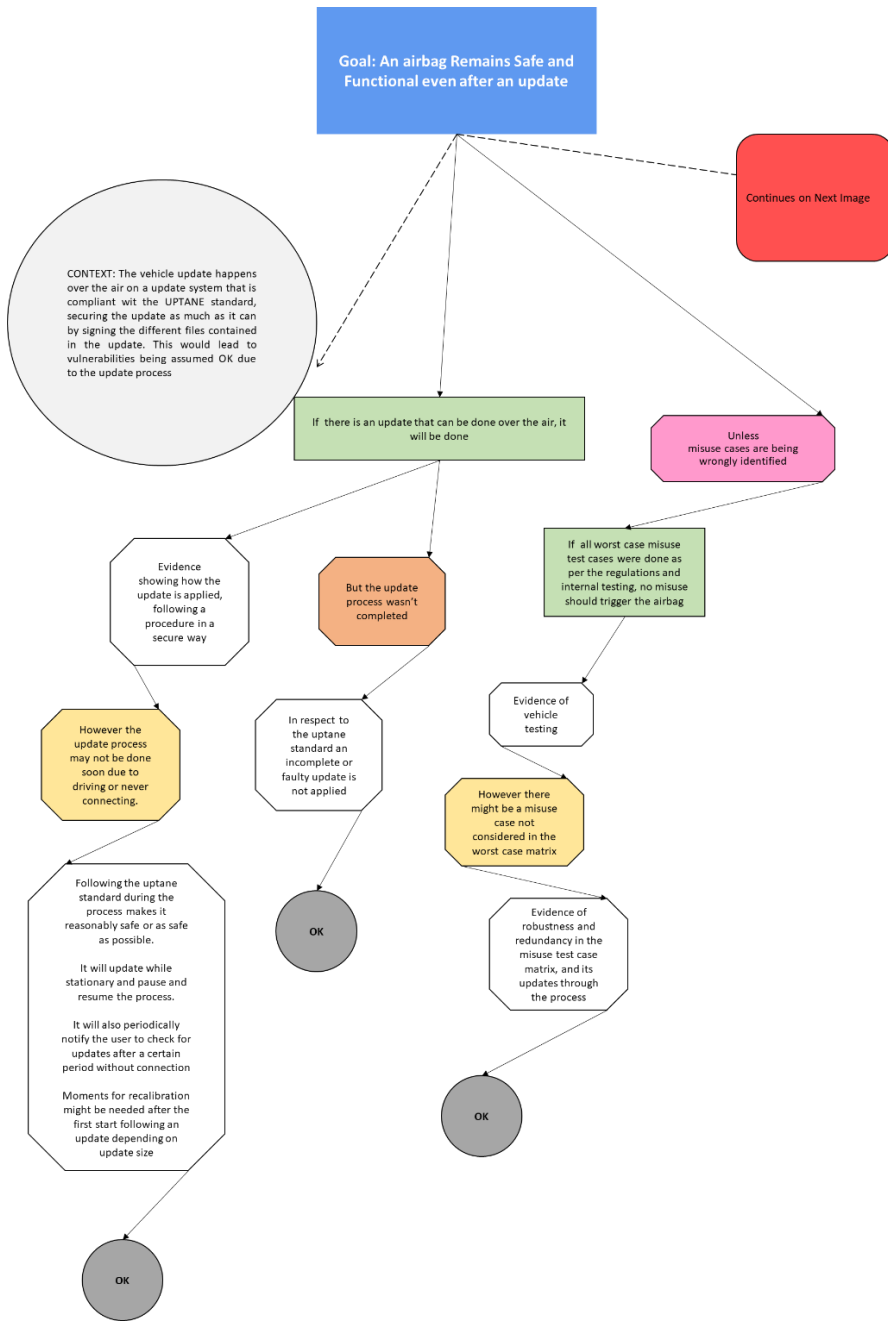


Figure 40 Enlarged image for details part 1 of 4

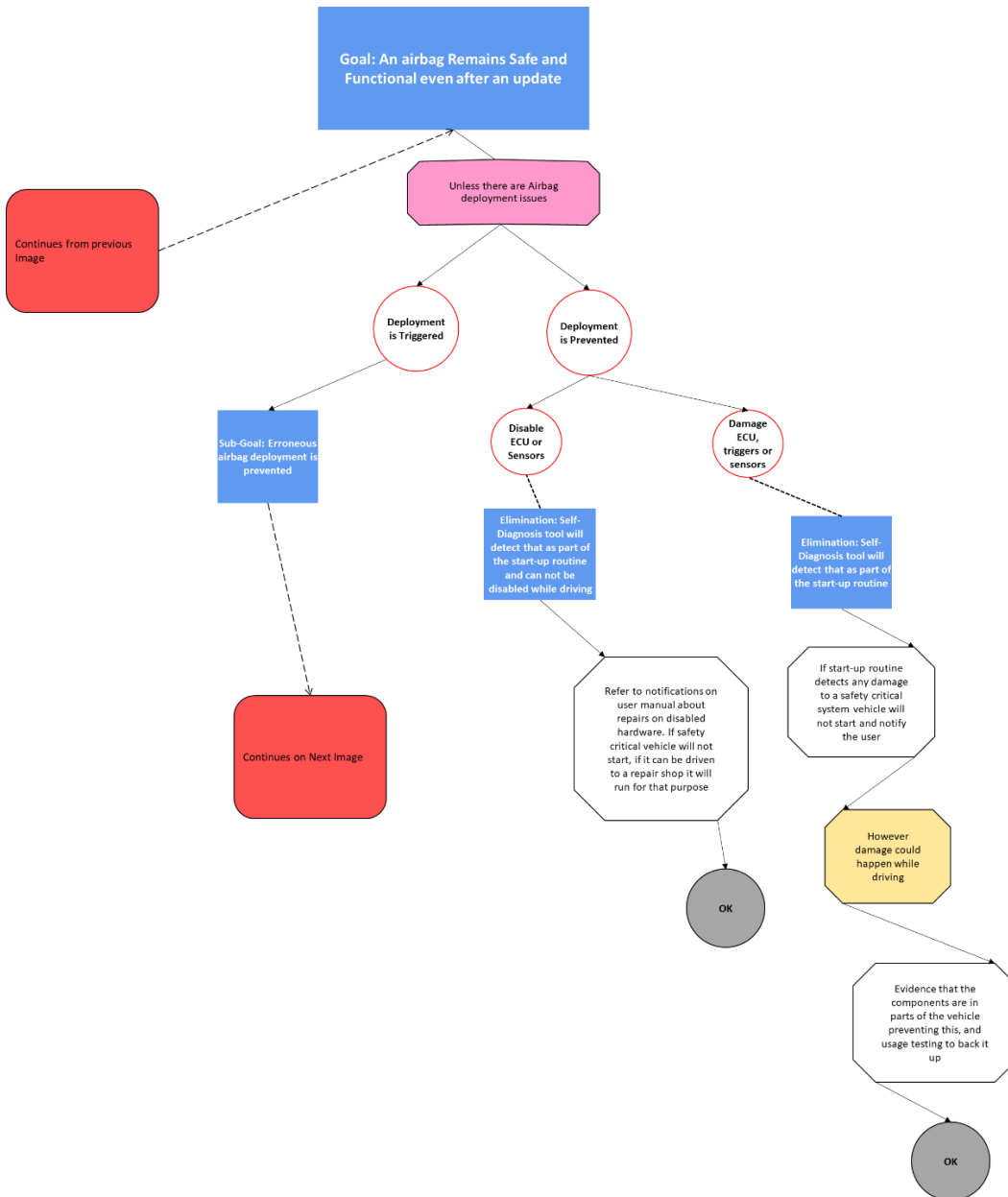


Figure 41 Enlarged image for details part 2 of 4

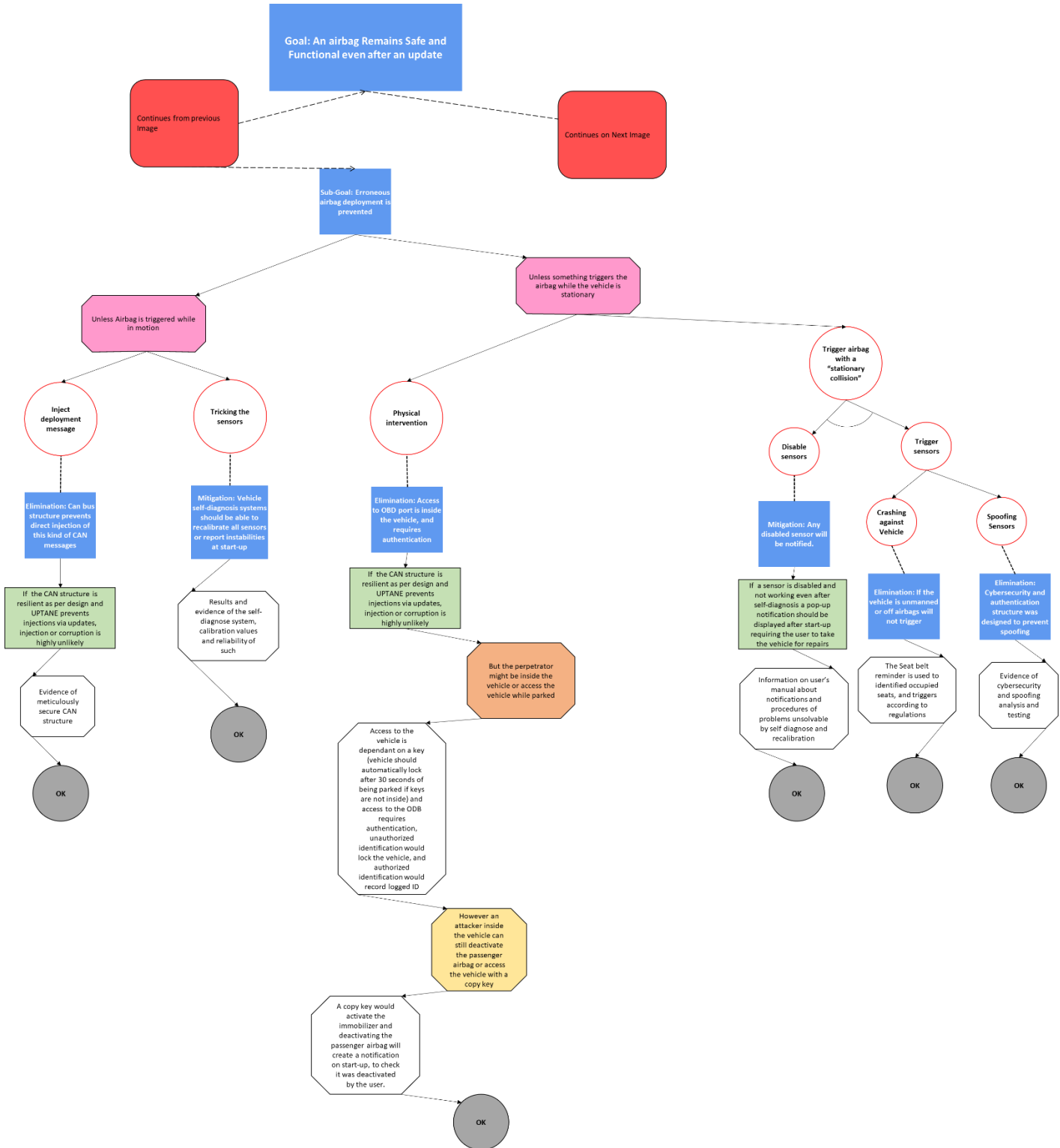


Figure 42 Enlarged image for details part 3 of 4

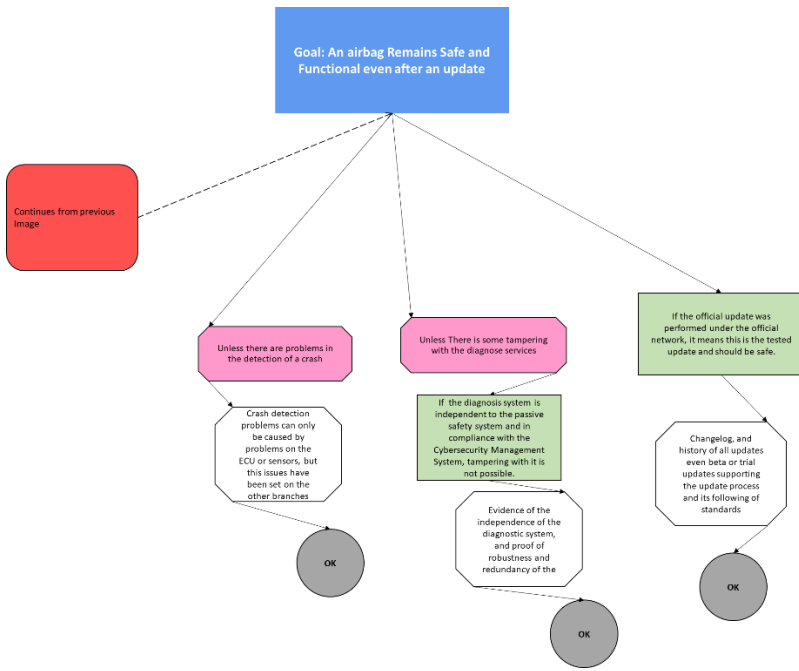


Figure 43 Enlarged image for details part 4 of 4

7 Summary of the evaluation of the method

The evaluation of the method was performed through the examples and test case. The test case is the most detailed and serves as the main pillar to explain how the method works regarding existing work products. Even if the examples indeed show the usage of the method, they are mostly illustrative and do not possess the depth, and defined base backed up with work products like the pilot demonstration does.

7.1 Results from the examples

The examples show how the method is used and how it can be used more than in just the automotive domain. The first example works by explaining how challenging the outcomes through logic, will foil a plan to an Art heist like those seen in movies.

The second example is built from an attack tree and incorporates the rest of the ideas from inductive logic. The highlight of this example is how it uses all of the main attacks presented and expands on them with counters, setting them as new goals. Even when not all the attacks have to be specified completely, through the innate reasoning of the method they are set as reasonable by the time they reach the “OK”.

7.2 Evaluating the Real-World Application

The real-world application focuses on a marine vessel, with certain similarities to a CAV, this example visualizes the use of such and the similarities to a land vehicle. It also considers how it differs from what the automotive industry is used to with a different application. It is a good example to analyse the method’s compatibility with AI in a way that simplifies autonomous driving by reducing the number of other vehicles it would interact with.

7.2.1 Comparing the results against various safety and security analysis work products

7.2.1.1 The FMEA

An FMEA sourced from RH Marine provided most of the information needed to produce the assurance case, with the relevant safety and security context established each of the desired goals can be challenged with a relevant threat scenario. The two main branches on the left and the 3 main branches on the right (Figure 26 and Figure 28), alongside the sub goals that are followed by the attacks, show a consistent method of representing threats resolved via the FMEA within the diagram. For the FMEA analysis, it is important to

enumerate as many of the possible failures, and the potential solutions (being backed up by the FMEA) logically deducing the “OK” by adhering to the work products.

7.2.1.2 The ADT

Even when the hazards and threats are identified, the ability to link them to safety and security goals becomes significant, especially in terms of clearly demonstrating the explicit relationship between safety and security in the big picture. In the middle branches that show attacks, the effects of the attack tree are in full view and directly influence the subgoals that appear as mitigations or eliminations. With regard to the possibility enumerating every possible attack mentioned in an attack defence tree within the assurance case, this is not the intended purpose of an assurance case. Instead, the assurance case succinctly demonstrates all relevant claims through logical deduction and reasoning and attempting to fully reason through every little detail in an attack defence tree would prove cumbersome. Instead, the most relevant potential attacks can be integrated into a more compact attack defence tree by summarizing various branches within a more contextually sound and abstract manner, with the main concern being that each branch is logically proven safe and secure. (Notably on Figure 27)

7.2.2 Analysis of results

The comparison of the method with the other work products, proves that the method takes in consideration relevant data to prove assurance from ASILs and HARAs. Significantly, by comparing and contrasting the method with additional work products it can be shown that the method takes in consideration relevant data to demonstrate assurance. Within the automotive industry it is important to rely on a GSN Safety Case, ASILs and HARAs, and similarly in the marine industry it is expected that any analysis or assurance would still comply with its relevant regulations. Additionally, the management of the data and the recollection of such can be considered acceptable by taking in account how the information from the FMEA and the ADT were represented, it also demonstrates that with respect to the available information it can be assured that it is as safe and secure as reasonably possible by clearly demonstrating the safety and security threats and how they are linked and mitigated. This becomes apparent with the use of the relevant attacks as show within the attack section of the diagram. Thus, if the evaluation is performed taking in all the relevant consideration outlined, the result is acceptable as an assurance case, that can be interpreted as an easy-to-follow safety case or cybersecurity case.

7.3 Evaluating the Pilot demonstration

7.3.1 Comparison with the objectives

The closest thing to a hypothesis for the evaluation is considering if the method works as a holistic approach for safety and security. Being so it should be able to cover the main points of the pilot demonstration and match the work products, if the method is able to match the key points of those documents and link them in a traceable way the hypothesis is successful.

From what was expected of the method it is able to use inductive reasoning to say that OTA updates are a viable option for safety critical systems. The central part of the diagram where the attacks are placed provide connected information from all the work products, and it works as the backbone to cement how these updates can be assured. It is also important to remember that the use of UPTANE is essential to ensure the updates in this method as a vital part for the context for the demonstration.

7.3.2 Comparing the results against other work products

7.3.2.1 The ADT

In regard to possible cybersecurity threats of hacking the Airbag ECU or altering the updates themselves, the method covers all major points. When comparing to the ADT presented with the pilot demonstration, all mitigations are presented either as sub goals or deduced safe through a defeater.

For example, all of the attacks on Figure 41 and Figure 42 cover all main attacks from the ADT. And all mitigations are satisfied by the structure of the vehicle network itself and Uptane. Mitigations are also validated by the documentation of the ADT and the framework's modus operandi. Things that are not mentioned but possible from the work products is fulfilled by the context of the demonstration.

7.3.2.2 The GSN Safety Case

Even though the method and the specific test case did not consider connection to other modules and their immediate safety cases, the method does the job of achieving all of the GSN goals in a different way. This can be seen specifically in Figure 40 as all of those goals are relevant to the safety case.

7.3.2.3 HARA

All the hazards within the HARA are considered in the pilot demonstration, and by approaching all of this hazards and ensuring they are as safe as reasonably possible, the method applies the information on the HARA especially in Figure 40 and Figure 43.

7.3.2.4 ASILs

Regarding the ASIL levels it can be observed throughout the diagram that the priority of the ASILs is never altered in the method and that while building the assurance case, maintaining that priority was essential and the method is meant to look at the issues this way.

7.3.3 Analysis of results

The resulting diagram of the method proves the integration of the various work products and manages to present it in a graphical way. As a result, the method indeed covers what the GSN Safety case does and what an ADT does, even when the information is presented and tackled in a different way. Even when the information is tackled in a different way in order to be able to correctly make the connections between modules, specifically for functional safety, it will still be useful that the method works in parallel with a Functional Safety case during the development. The results also show how an over the air update on a safety critical function can be deduced as viable. The viability of updating safety critical functions is still linked to the condition of following the standards and having a secure network and protocol to do so, but with the current technology and standards it can be deduced it is a safe practice.

Having a safety case and an ADT can be very useful for building the assurance case with the method on top. By considering a HARA and an ASIL analysis on top of the GSN safety case and the ADT, the reliability of its logical arguments is reinforced and becomes more intuitive to follow. With this correct implementation it can be presented as a cybersecurity case in accordance to the standard and also be presented as a valuable resource to safety engineers to aid in following the connections within the different disciplines. This can be also great help as during development experts might want to modify their part, tracking changes on safety cases and ADTs, and then applying to the method might be the best way to update. So even when an ADT and a functional safety case are not mandatory to build an assurance case with this method, they work great in parallel and are helpful to each other, and become the most efficient way to track that the method is done correctly. The method helps SOTIF, functional safety and cybersecurity to understand their connections, and updating cybersecurity and functional safety data helps the method be better at deducing assurance.

7.4 Overall remarks of the method

The assurance case can be constructed with knowledge of the system and no supporting documents, but as the complexity of the system grows, having the work products as backup becomes more essential in building a stable assurance case. The examples in this thesis show a growing difficulty and how evidence helps. One of the advantages of the method is that it visually links safety and security. The ability to present and share the method show the capabilities of intuitive understanding of diagrams over complex texts. As a proposed method it can still be improved, yet it has completed the core mission it had.

7.4.1 Meeting the Regulations

- **ISO/SAE 21434:** The assurance case presented on this thesis is compliant with the definition of the cybersecurity case mentioned in the standard. Therefore, it can be used as a cybersecurity case.
- **UN-ECE R155:** Similar as with the ISO regulation the use of a cybersecurity case is compatible with the regulation.
- **UN-ECE R156:** The pilot demonstration deals with over the air updates and is an example that can be used to clarify the essential points in updating a safety critical system

7.4.2 Limitations and Weaknesses

- It has not yet been adopted by an OEM/VMs, nor been used enough to establish the benefits
- The process takes time in understanding the system and the relevant work products, then critical thinking is needed for the assessment.
- Stakeholders and development and manufacture process managers could have a hard time justifying a person for this time- or salary-wise, so cheaper options could be looked at.

7.4.3 Key Contributions and Highlights

- By using inductive reasoning on an assurance case, the evaluator who understands the systems and relevant work products is forced to approach the goals from a different point, a practice that could help combat bias.
- The use of ADTs in conjunction with safety analysis already used in the automotive industry might simplify the presentation of the safety case in accordance to ISO 21434.
- The method is a good way to prepare the systems for an homologation of UN R155 Cybersecurity

- The example regarding OTA updates of a safety critical system can be decomposed to help support evidence for UN R156 regarding vehicle updates.
- If relevant AI safety and cybersecurity analysis work products are available, it should be possible to link the safety and security threats of an AI for autonomous driving and its supporting systems.

8 Conclusion

The fully autonomous connected vehicle is not a thing of the future, the vehicle technology is ready, and it exists. Even when the latter is true infrastructure and law are not yet ready for a wide spread of CAVs, and an important part of making this happen is getting the users to feel trust to the vehicles, and this trust is gained through assurance. The assurance case proposed above can be seen as one small step in a series of various steps needed for society to embrace autonomous vehicles. The assurance case proposed is just part of that big picture to support autonomous vehicles, but it can also play a role in documenting cybersecurity as a valid cybersecurity case. As a cybersecurity case it can directly correlate the threats in a visual way that should be sufficient to comply with the standards.

8.1 Possible Adaptations, Extensions and Future Work

To make the method easier to understand “Assumed OK” and “Deduced OK” from eliminative argumentation were merged into one “OK”, so a possible extension could be to separate them to see the difference more clearly. Another possible adaptation is to use the LINK lines on GSN 3 that are dotted and dotted strike with an “X”, this were avoided to stop confusion as dotted lines were used only for defences and context, yet this expansion can also lead the method elsewhere.

Another possible adaptation is a simplified not colour-coded version where polygons are defeaters without explicitly specifying the kind of defeater as it will be implied with the content. Same thing will happen between strategies and goals as they would be rectangles. The OK and attack will share the circle shape, but even without the colour, the OK text should be enough to differentiate them.

8.1.1 Marine Vessel, Aircraft or Train Applications

As per the real-world application the transversality of the method is a factor that could be researched further. As the rules with different transports change, and some uses are a collective method of transportation, the focus remains the same that the users feel safe and secure, and the proof exists of such. Using the method in conjunction with the work products already developed in the other industries will produce results and the nature of the assurance case might promote different approaches of viewing different issues, opening debates and maybe unbiassing certain ideas.

8.1.2 Considering Vehicle AI Systems

According to the available research, the less careful behaviour of vehicle occupants and road users, system failures, and the absence of control of crash algorithms that evaluate life or death scenarios during inevitable accidents are all potential sources of AV-related safety issues. If the public supports broad deployment, which would give AVs more real-world driving experience, safety performance might improve over time. As a result, most national governments have chosen for light-control-oriented policies in the form of non-mandatory AV testing standards with the goal of stimulating AV development rather than utilising unduly strict procedures to manage safety hazards. Because AV is still in its early stages of development, councils or working groups have been formed to investigate the technology's consequences. Germany has made significant progress in implementing new laws, while nations such as Japan are now working on legislation to control the safety of AV testing. Australia has sought public referendum to address AV safety concerns, indicating a shift toward a more adaptive policy [138]. This reinforces the idea that AI driving systems are backed up by the public or will not be accepted. The real world application shown on this thesis is linked to the AI of a self-driving vessel, and assurance cases can be used as tools to evaluate the AI, and boost confidence, but that alone should not be the only tool to evaluate an AI.

8.2 Reach

During the research period as part of the Safer Autonomous Systems project, the ideas proposed in this work overlapped with those of the other members of the consortium, and the closing of this EU project should be able to disseminate these ideas into a greater audience. The method was teased and presented in conferences with acceptable results and no negative feedback. The publication of the thesis itself should also help the ideas reach a wider audience.

Regarding vehicle safety and security disciplines in the industry the method is aimed to influence and help debate how to challenge cybersecurity problems using reasoning, something that can at least help with the debate of using this or other methods. Another important outreach is the usage of assurance cases in the style of the automotive domain, and the impact that might have.

8.3 Remaining challenges and obstacles

Significant challenges faced in developing assurance cases, for both safety and cybersecurity applications, still remain, include the following:

1. Linking to evidence, while being able to identify bias.

2. Handling the non-deterministic behaviour of AI systems – how can the safety and cybersecurity of these technologies be argued, and what kind of evidence would be required to support these arguments?
3. How to handle evolving systems – e.g., due to SW updates or unsupervised learning by AI?
4. How to provide a balanced view of the limitations of such a case, such as by including and explicitly showing the failure of possible counterarguments, such as for “non-safety”.
5. Assurance cases need to provide a better and more explicit handling of uncertainty and the limitations of the arguments.

8.4 Summary of contributions

- An assurance case method that takes in account aspects of safety and security.
- Examples of the method and building of the assurance case.
- An assurance case that can be used as a cybersecurity case that is compatible with ISO 21434 and helpful for proof in the homologation of UN ECE R 155.
- A method that attempts to solve the bias of assurance cases through inductive reasoning.
- An extensive theoretical background that can be reviewed by other researchers.
- A method that has intention to be compatible with the industry, and was reviewed by many peers.
- Scientific contributions to the EU SAS Project.

References

- [1] A.R. Ruddle et al., “Requirements and timescales for CYB-R: the UK Centre of excellence for road transport cybersecurity resilience”, ResiCAV Project Deliverable 1, 30th March 2020 (available from: <https://zenzic.io/reports-and-resources/>).
- [2] BS EN 61508-1: “Functional safety of electrical/electronic/programmable electronic safety-related systems”, (2010).
- [3] BS ISO 26262: “Road vehicles — Functional safety”, (2018).
- [4] Taeihagh, A., & Lim, H. S. M. (2019). Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews*, 39(1), 103–128.
- [5] Pinto, C. (2012). How autonomous vehicle policy in california and nevada addresses technological and non-technological liabilities. *Intersect: The Stanford Journal of Science, Technology ...*, 5(1), 1–16.
- [6] Kour, R. (2020). *Cybersecurity in Railway : A Framework for Improvement of Digital Asset Security*.
- [7] SAE J3016: “Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems”, (2014).
- [8] Al-qizwini, M., Barjasteh, I., Al-qassab, H., Fellow, H. R., Lqirupdwlrq, H., Surfhhvvhg, L. V, & Wkh, L. (2017). DL for autonomous driving using GoogleNet. *Iv*.
- [9] Hubmann, C., Becker, M., Althoff, D., Lenz, D., & Stiller, C. (2017). Decision making for autonomous driving considering interaction and uncertain prediction of surrounding vehicles. *IEEE Intelligent Vehicles Symposium, Proceedings, July 2019*, 1671–1678.
- [10] Zeilinger, M., Hauk, R., Bader, M., & Hofmann, A. (2017). Design of an Autonomous Race Car for the Formula Student Driverless (FSD). *Proceedings of the OAGM & ARW Joint Workshop*, 3–8.
- [11] Rojo, J., Rojas, R., Gunnarsson, K., & Simon, M. (2007). Spirit of berlin: An autonomous car for the darpa urban challenge-hardware and software architecture. *Technical Semifinalist Paper ...*, 1–25.
- [12] Freepik, Images of self driving cars, <https://www.freepik.com/vectors/self-driving-car>, last accessed 2022/08/18
- [13] Levinson, J., Askeland, J., Becker, J., Dolson, J., Held, D., Kammel, S., Kolter, J. Z., Langer, D., Pink, O., Pratt, V., Sokolsky, M., Stanek, G., Stavens, D., Teichman, A., Werling, M., & Thrun, S. (2011). Towards fully autonomous driving: Systems and algorithms. *IEEE Intelligent Vehicles Symposium, Proceedings, Iv*, 163–168.
- [14] Cisneros, Ó. (2010). Los sistemas de detección de peatones.
- [15] Thakur, R. (2018). Infrared Sensors for Autonomous Vehicles. *Recent Development in Optoelectronic Devices*. <https://doi.org/10.5772/intechopen.70577>
- [16] Coffey, V. C. (2019). Integrated Lidar: Transforming Transportation. *Opt. Photon. News*, 30(9), 40–47. <https://doi.org/10.1364/OPN.30.9.000040>

- [17] Steiner, W., Mehmed, A., & Punnekkat, S. (2015). Improving Intelligent Vehicle Dependability by Means of Infrastructure-Induced Tests. Proceedings - 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, DSN-W 2015, 147–152.
- [18] Cheng, C.-H., Gulati, D., & Yan, R. (2019). Architecting Dependable Learning-enabled Autonomous Systems: A Survey. <http://arxiv.org/abs/1902.10590>
- [19] Hubmann, C., Becker, M., Althoff, D., Lenz, D., & Stiller, C. (2017). Decision making for autonomous driving considering interaction and uncertain prediction of surrounding vehicles. IEEE Intelligent Vehicles Symposium, Proceedings, July 2019, 1671–1678. <https://doi.org/10.1109/IVS.2017.7995949>
- [20] An, H., & Jung, J. Il. (2019). Decision-making system for lane change using deep reinforcement learning in connected and automated driving. Electronics (Switzerland), 8(5).
- [21] Schwarting, W., Alonso-Mora, J., & Rus, D. (2018). Planning and Decision-Making for Autonomous Vehicles. Annual Review of Control, Robotics, and Autonomous Systems, 1(1), 187–210.
- [22] Liu, Y., Wang, X., Li, L., Cheng, S., & Chen, Z. (2019). A Novel Lane Change Decision-Making Model of Autonomous Vehicle Based on Support Vector Machine. IEEE Access, 7, 26543–26550.
- [23] Uber, <https://www.uber.com/gb/en/atg/>, last accessed 2020/05/21
- [24] Waymo, <https://waymo.com/tech/>, last accessed 2020/05/21
- [25] Forrest, A. D. (2007). Autonomous Cars & Society. Worcester Poly-technic Institute-April 2013.
- [26] Pomerleau, D. A., Gowdy, J., & Thorpe, C. E. (1991). Combining artificial neural networks and symbolic processing for autonomous robot guidance. Engineering Applications of Artificial Intelligence, 4(4), 279–285. [https://doi.org/10.1016/0952-1976\(91\)90042-5](https://doi.org/10.1016/0952-1976(91)90042-5)
- [27] Highlights of Robot Car History/ Prof. J. Schmidhuber (2005), < <http://www.idsia.ch/~juergen/robotcars.html> >, last accessed 2020/05/18
- [28] Cui, J., Sabaliauskaite, G., Liew, L. S., Zhou, F., & Zhang, B. (2019). Collaborative Analysis Framework of Safety and Security for Autonomous Vehicles. IEEE Access, 7(March 2018), 148672–148683.
- [29] Wang, P., Di, B., Zhang, H., Bian, K., & Song, L. (2018). Cellular V2X Communications in Unlicensed Spectrum: Harmonious Coexistence With VANET in 5G Systems. IEEE Transactions on Wireless Communications, 17(8), 5212–5224.
- [30] ZD net, Charles McLellan < <https://www.zdnet.com/article/what-is-v2x-communication-creating-connectivity-for-the-autonomous-car-era/> >, last accessed 2020/07/15
- [31] Schoitsch, E. (2016). Autonomous vehicles and automated driving: Status, perspectives and societal impact. IDIMT 2016 - Information Technology, Society and Economy Strategic Cross-Influences - 24th Interdisciplinary Information Management Talks, 405–423.
- [32] Macher, G., Messnarz, R., Armengaud, E., Riel, A., Brenner, E., & Kreiner, C. (2017). Integrated Safety and Security Development in the Automotive Domain. SAE Technical Papers, 2017-March(March).
- [33] Vishnukumar, H. J., Butting, B., Muller, C., & Sax, E. (2018). Machine learning and deep neural network - Artificial intelligence core for lab and real-world test and validation for ADAS and autonomous vehicles: AI for efficient and quality test and validation. 2017 Intelligent Systems Conference, IntelliSys 2017, 2018-Janua(September), 714–721.

- [34] Cheng, C. H., Nuhrenberg, G., Huang, C. H., Ruess, H., & Yasuoka, H. (2018). Towards dependability metrics for neural networks. 2018 16th ACM/IEEE International Conference on Formal Methods and Models for System Design, MEMOCODE 2018
- [35] Cheng, C.-H., Gulati, D., & Yan, R. (2019). Architecting Dependable Learning-enabled Autonomous Systems: A Survey.
- [36] Sun, Y., Huang, X., Kroening, D., Sharp, J., Hill, M., & Ashmore, R. (2018). Testing Deep Neural Networks. 1–28.
- [37] Xiang, W., Musau, P., Wild, A. A., Lopez, D. M., Hamilton, N., Yang, X., Rosenfeld, J., & Johnson, T. T. (2018). Verification for Machine Learning, Autonomy, and Neural Networks Survey. 1–51.
- [38] latest NCAP Protocol <https://cdn.euroncap.com/media/43373/euro-ncap-assessment-protocol-sav901.pdf> , last accessed 2020/05/21
- [39] Vishnukumar, H. J., Butting, B., Muller, C., & Sax, E. (2018). Machine learning and deep neural network - Artificial intelligence core for lab and real-world test and validation for ADAS and autonomous vehicles: AI for efficient and quality test and validation. 2017 Intelligent Systems Conference, IntelliSys 2017, 2018-Janua(September), 714–721. <https://doi.org/10.1109/IntelliSys.2017.8324372>.
- [40] Shah S., Dey D., Lovett C., Kapoor A. (2018) AirSim: High-Fidelity Visual and Physical Simulation for Autonomous Vehicles. In: Hutter M., Siegwart R. (eds) Field and Service Robotics. Springer Proceedings in Advanced Robotics, vol 5. Springer, Cham
- [41] Zobel, R. (1995). Accident data and the passive safety of vehicles or can you rate the passive safety of vehicles from accident data? Proceedings of the International Research Council on the Biomechanics of Injury Conference, 23, 375–388.
- [42] Hojjati-Emami, K., Dhillon, B. S., & Jenab, K. (2012). Reliability prediction for the vehicles equipped with advanced driver assistance systems (ADAS) and passive safety systems (PSS). International Journal of Industrial Engineering Computations, 3(5), 731–742.
- [43] Pegasus Project. <https://www.pegasusprojekt.de/en/information-material>, last accessed 2020/05/21.
- [44] Burton, S., Gauerhof, L., Hawkins, R., Habli, I., Sethy, B.: Confidence arguments for evidence of performance in machine learning for highly automated driving functions. Safecomp 2019 - Workshop on Artificial Intelligence Safety Engineering (Waise) of the 38th International Conference on Computer Safety, Reliability and Security (2019).
- [45] ISO 26262: “Road vehicles — Functional safety”, (2018).
- [46] ISO/PAS 21448: “Road vehicles — Safety of the intended functionality”, (2019).
- [47] Walker, A. (2019). SOTIF the Human Factor. In A. Walker, R. V O’Connor, & R. Messnarz (Eds.), Systems, Software and Services Process Improvement (pp. 575–584). Springer International Publishing.
- [48] Johnson, N., Prof, S., & Kelly, T. (2018). The Practical and Socio-technical Challenges of Safety-Security Co-assurance.
- [49] Cui, J., Liew, L. S., Sabaliauskaite, G., & Zhou, F. (2019). A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. Ad Hoc Networks, 90(December), 101823.
- [50] SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (2016).

- [51] Yağdereli, E., Gemci, C., & Aktaş, A. Z. (2015). A study on cyber-security of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation*, 12(4), 369–381. <https://doi.org/10.1177/1548512915575803>
- [52] Zhao, H., Li, G., Wang, N., Zheng, S., Yu, L., & Chen, Y. (2013). Study of EMC Problems with Vehicles. In Y. Yang, M. Ma, & B. Liu (Eds.), *Information Computing and Applications* (pp. 159–168). Springer Berlin Heidelberg.
- [53] Hancock, P.: Are autonomous cars really safer than human drivers?. <https://theconversation.com/are-autonomous-cars-really-safer-than-human-drivers-90202>, last accessed 2020/05/21.
- [54] Janssen, C. P., Donker, S. F., Brumby, D. P., & Kun, A. L. (2019). History and future of human-automation interaction. *International Journal of Human Computer Studies*, 131(May), 99–107. <https://doi.org/10.1016/j.ijhcs.2019.05.006>.
- [55] Sarter, N. B., & Woods, D. D. (1992). Mode Error in Supervisory Control of Automated Systems. *Proceedings of the Human Factors Society Annual Meeting*, 36(1), 26–29. <https://doi.org/10.1177/154193129203600108>.
- [56] Hengstler, M., Enkel, E., & Duelli, S. (2016). Applied artificial intelligence and trust-The case of autonomous vehicles and medical assistance devices. *Technological Forecasting and Social Change*, 105, 105–120. <https://doi.org/10.1016/j.techfore.2015.12.014>.
- [57] Fanas Rojas, J., Brown, N., Rupp, J., Bradley, T., & Asher, Z. D. (2022). Performance Evaluation of an Autonomous Vehicle Using Resilience Engineering. *SAE Technical Paper Series*, 1, 1–9.
- [58] Kim, J., Rajkumar, R. (Raj), & Jochim, M. (2013). Towards dependable autonomous driving vehicles. *ACM SIGBED Review*, 10(1), 29–32.
- [59] Sabaliauskaite, G., Liew, L. S., Zhou, F., & Cui, J. (2019). Designing safe and secure mixed traffic systems. *Proceedings of IEEE International Symposium on High Assurance Systems Engineering*, 2019-Janua(January), 222–227.
- [60] Palin, R., & Habli, I. (2010). Assurance of automotive safety - A safety case approach. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6351 LNCS, 82–96.
- [61] Dowding, M. (2002). Maintenance of the Certification Basis for a Distributed Control System – Developing a Safety Case Architecture. MSc Thesis, University of York, UK
- [62] Fraade-Blanar, L., Blumenthal, M., Anderson, J., & Kalra, N. (2018). Measuring Automated Vehicle Safety: Forging a Framework. In *Measuring Automated Vehicle Safety: Forging a Framework*.
- [63] Kelly, T., & Weaver, R. (2004). The Goal Structuring Notation – A Safety Argument Notation. *Elements*.
- [64] Stålhane, Tor & Myklebust, Thor. (2016). The Agile Safety Case. 9923. 5-16. 10.1007/978-3-319-45480-1_1.
- [65] Wang, R., Guiochet, J., Motet, G., & Schön, W. (2019). Safety case confidence propagation based on Dempster–Shafer theory. *International Journal of Approximate Reasoning*, 107(February), 46–64.
- [66] Johnson, N., & Kelly, T. (2018). An Assurance Framework for Independent Co-assurance of Safety and Security. *The Safety-Security Challenge*, August, 1–11.

- [67] Johnson, N., & Kelly, T. (2018). Safety-Security Assurance Framework (SSAF) in Practice *. September, 5–6.
- [68] Leveson, N. (2011). Paper on the Use of Safety Cases in Certification and Regulation (Vol. 156).
- [69] Ward, D., Ibarra, I., & Ruddle, A. (2013). Threat Analysis and Risk Assessment in Automotive Cyber Security. *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, 6(2), 507–513.
- [70] Hall, B. (2019). MISRA: Guidelines for Automotive Safety Arguments British Library Cataloguing in Publication Data (Issue September 2020).
- [71] Cheah, M., Shaikh, S. A., Bryans, J., & Wooderson, P. (2018). Building an automotive security assurance case using systematic security evaluations. *Computers and Security*, 77, 360–379.
- [72] Alexander, R., Hawkins, R., & Kelly, T. (2011). Security Assurance Cases: Motivation and the State of the Art. *Www-Users.Cs.York.Ac.Uk*, 1–19.
- [73] Dürrwang, J., Braun, J., Rumez, M., Kriesten, R., & Pretschner, A. (2018). Enhancement of Automotive Penetration Testing with Threat Analyses Results. *SAE International Journal of Transportation Cybersecurity and Privacy*, 1(2), 91–112.
- [74] Alexander, R. D., Hawkins, R. D., & Kelly, T. P. (2017). From Safety Cases to Security Cases. White Rose Research Online Unspecified..
- [75] Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2020). Cybersecurity and safety co-engineering of cyberphysical systems - A comprehensive survey. *Future Internet*, 12(4), 1–17.
- [76] Goodenough, J. B., Weinstock, C. B., & Klein, A. Z. (2015). Eliminative Argumentation: A basis for arguing system confidence in system properties with induction. *Proceedings - International Conference on Software Engineering*, February, 1161–1164.
- [77] Luo, Y., Li, Z., & Van Den Brand, M. (2016). A categorization of GSN-based safety cases and patterns. *MODELSWARD 2016 - 4th International Conference on Model-Driven Engineering and Software Development, Doctoral Consortium, 2016-February(Modelsward)*, 509–516.
- [78] The Assurance Case Working Group. (2021). Goal Structuring Notation Community Standard Version 3. <http://www.goalstructuringnotation.info/>
- [79] Kordy, B., Mauw, S., Radomirović, S., & Schweitzer, P. (2011). Foundations of Attack--Defense Trees. In P. Degano, S. Etalle, & J. Guttman (Eds.), *Formal Aspects of Security and Trust* (Issue C, pp. 80–95). Springer Berlin Heidelberg.
- [80] Stukus, P. D., & Leveson, N. (2017). Systems-Theoretic Accident Model and Processes (STAMP) Applied to a U.S. Coast Guard Buoy Tender Integrated Control System.
- [81] Lee, W. S., Grosh, D. L., Tillman, F. A., & Lie, C. H. (1985). Fault Tree Analysis, Methods, and Applications d A Review. *IEEE Transactions on Reliability*, R-34(3), 194–203.
- [82] Sabaliauskaite, G., Cui, J., & Liew, L. S. (2018). Integrating Autonomous Vehicle Safety and Security Analysis Using STPA Method and the Six-Step Model.

- [83] Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016). A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context. In A. Skavhaug, J. Guiochet, & F. Bitsch (Eds.), *Computer Safety, Reliability, and Security* (pp. 130–141). Springer International Publishing.
- [84] EVITA Project. (2011)E-safety Vehicle Intrusion Protected Applications
- [85] Taeihagh, A., & Lim, H. S. M. (2019). Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews*, 39(1), 103–128.
- [86] Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017). STRIDE-based threat modeling for cyber-physical systems. 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 1–6.
- [87] Sabaliauskaite, G., Liew, L. S., & Zhou, F. (2019). AVES – Automated vehicle safety and security analysis framework. *Proceedings - CSCS 2019: ACM Computer Science in Cars Symposium*, Iso 26262.
- [88] Ma, Z., & Schmittner, C. (2016). Threat Modeling for Automotive Security Analysis.
- [89] PAS 11281: “Connected automotive ecosystems :Impact of security on safety – Code of practice”, (2018)
- [90] The End of the 'ECE' Era, *Driving Vision News*, 29 August 2011(<<https://www.drivingvisionnews.com/the-end-of-the-ece-era/>>) last accessed 2020/08/02
- [91] GTR, <[https://www.hsdl.org/?view&did=751039/](https://ec.europa.eu/docsroom/documents/42306/attachments/1/translations/en/renditions/native#:~:text=Technical%20Regulations%20(GTRs)-,The%20Global%20Technical%20Regulations%20are%20developed%20under%20the%201998%20international,the%20United%20States%20of%20America)> . last accessed 2020/05/21</p>
<p>[92] USA congressional research service, <a href=), last accessed 2020/07/30
- [93] Vellinga, N. E. (2017). From the testing to the deployment of self-driving cars: Legal challenges to policymakers on the road ahead. *Computer Law & Security Review*, 33(6), 847–863. <https://doi.org/10.1016/j.clsr.2017.05.006>.
- [94] AXA, <https://www.insurancejournal.com/news/international/2020/03/20/561794.htm>, last accessed 2020/05/21
- [95] Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology*, 6(3), 175–183. <https://doi.org/10.1007/s10676-004-3422-1>.
- [96] See for instance: E.F.D ENGELHARD, “Annex I EU Common Approach on the liability rules and insurance related to Connected and Autonomous Vehicules”, Report for the European Parliament, 2017, 131 p.
- [97] Wagner, G. (2017). Robot Liability * I . The Concepts of Robots , Autonomous Systems and IoT-Devices II . The European Parliament Resolution of February 2017 III . The Commission Communication on " Building a European Data Economy ". February, 1–24;

- [98] Lambert F, Elektrec, <https://electrek.co/2019/07/22/tesla-removes-free-unlimited-supercharging-used-cars/> , last accessed 2020/11/09
- [99] Software Over the Air Updates, BearingPoint, <https://www.bearingpoint.com/it-it/insights-events/insights/software-over-the-air-sota-an-automotive-accelerator/>, last accessed 2020/11/09
- [100] Steger, M., Dorri, A., Kanhere, S. S., Römer, K., Jurdak, R., & Karner, M. (2018). Secure Wireless Automotive Software Updates Using Blockchains: A Proof of Concept. 137–149.
- [101] Shavit, M., Gryc, A., & Miucic, R. (2007). Firmware update over the Air (FOTA) for automotive industry. SAE Technical Papers, 724
- [102] Karthik, T., Brown, A., Awwad, S., McCoy, D., Bielawski, R., Mott, C., Lauzon, S., Weimerskirch, A., & Cappos, J. (2016). Uptane: Securing Software Updates for Automobiles. 14th Escar Europe 2016, 7058(July), 471–481.
- [103] Pegasus, <https://www.pegasusprojekt.de/> , last accessed 2020/02/15
- [104] Uptane, <https://Uptane.github.io/> , last accessed 2020/10/15
- [105] OMG, www.trustvehicle.eu , last accessed 2020/09/09
- [106] Autonet2030, <https://www.autonet2030.eu/>, last accessed 2020/11/09
- [107] Maven, <http://www.maven-its.eu/> , last accessed 2020/11/09
- [108] VI-Das: Vision Inspired Driver Assistance Systems, <http://www.vi-das.eu/>, last accessed 2020/11/09
- [109] SAS: Safer Autonomous Systems, <http://etn-sas.eu> , last accessed 2020/11/09
- [110] PETER Pan-european training-network of electromagnetic risk management, <https://etn-peter.eu/> , last accessed 2022/05/09
- [111] Avizienis, A., Laprie, J., & Randell, B. (2001). Fundamental Concepts of Dependability. 010028. <http://citeseer.ist.psu.edu/avizienis00fundamental.html>
- [112] ISO/SAE 21434: “Road vehicles –Cybersecurity”, (2021)
- [113] Chowdhury, T. et al. (2018) Safe and Secure Automotive Over-the-Air Updates. In: Gallina B., Skavhaug A., Bitsch F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2018. Lecture Notes in Computer Science, vol 11093. Springer, Cham
- [114] Nigam, V., Pretschner, A., & Ruess, H. (2018). Model-Based Safety and Security Engineering. 1–15.
- [115] Kirovskii, O. M., & Gorelov, V. A. (2019). Driver assistance systems: Analysis, tests and the safety case. ISO 26262 and ISO PAS 21448. IOP Conference Series: Materials Science and Engineering, 534(1).
- [116] Messnarz, R., Kreiner, C., & Riel, A. (2016). Integrating Automotive SPICE, Functional Safety, and Cybersecurity Concepts: A Cybersecurity Layer Model. Software Quality Professional, 18(4), 13–23.
- [117] Patu, V., & Yamamoto, S. (2013). How to develop Security Case by combining real life security experiences (evidence) with D-Case. Procedia Computer Science, 22, 954–959.

- [118] Dürrwang, J., Braun, J., Rumez, M., & Kriesten, R. (2018). Security Evaluation of an Airbag-ECU by Reusing Threat Modeling Artefacts. *Proceedings - 2017 International Conference on Computational Science and Computational Intelligence, CSCI 2017*, 37–43.
- [119] Chowdhury, T., Lin, C. W., Kim, B., Lawford, M., Shiraishi, S., & Wassyng, A. (2017). Principles for systematic development of an assurance case template from ISO 26262. *Proceedings - 2017 IEEE 28th International Symposium on Software Reliability Engineering Workshops, ISSREW 2017*, 69–72.
- [120] Chowdhury, T., Wassyng, A., Paige, R. F., & Lawford, M. (2019). Criteria to Systematically Evaluate (Safety) Assurance Cases. *Proceedings - International Symposium on Software Reliability Engineering, ISSRE, 2019-October(November)*, 380–390.
- [121] Wilhelmsen, C. A., & Ostrom, L. T. (2019). *Risk Assessment: Tools, Techniques, and Their Applications*. Wiley.
- [122] Mohamad, M., Åström, A., Askerdal, Ö., Borg, J., & Scandariato, R. (2020). Security assurance cases for road vehicles: An industry perspective. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3407023.3407033>
- [123] Dantas, Y. G., Nigam, V., & Ruess, H. (2020). Security Engineering for ISO 21434. 1–15. <http://arxiv.org/abs/2012.15080>
- [124] Habli, I., Ibarra, I., Rivett, R. S., & Kelly, T. (2010). Model-based assurance for justifying automotive functional safety. *SAE Technical Papers*, April.
- [125] Palin, R., Ward, D., Habli, I., & Rivett, R. (2011). ISO 26262 safety cases: Compliance and assurance. *IET Conference Publications, 2011(578 CP)*, 1–6. <https://doi.org/10.1049/cp.2011.0251>
- [126] Hawkins, R., Kelly, T., Knight, J., & Graydon, P. (2011). A new approach to creating clear safety arguments. *Advances in Systems Safety - Proceedings of the 19th Safety-Critical Systems Symposium, SSS 2011, MoD 2007*, 3–23.
- [127] The Assurance Case Working Group (2018). Assurance Case Guidance ‘ Challenges , Common Issues Version 1 The Assurance Case Working Group (ACWG). January 2019, page 54.
- [128] He, Y., Jin, Y., Huang, L., Xiong, Y., Chen, P., & Mou, J. (2017). Quantitative analysis of COLREG rules and seamanship for autonomous collision avoidance at open sea. *Ocean Engineering, 140*(October 2016), 281–291.
- [129] Notteboom, T., Pallis, A., & Rodriguez, J.-P. (2022). *Port Economics, Management and Policy (1st ed.)*. Routledge.
- [130] Grinstead, J. (1996). Marine safety regulation in transport Canada: The winds of change. *Marine Technology and SNAME News, 33*(3), 211–217.
- [131] Song, B.-H., Lee, K.-H., & Choi, W.-K. (2018). A Study on the Advancement of the Legal System for Small Fishing Vessels to Ensure Marine Safety. *Journal of the Korean Society of Marine Environment and Safety, 24*(7), 875–888.
- [132] Mahmood, S., Fouillade, A., Nguyen, H. N., & Shaikh, S. A. (2020). A Model-Based Security Testing Approach for Automotive Over-The-Air Updates. *Proceedings - 2020 IEEE 13th International Conference on Software Testing, Verification and Validation Workshops, ICSTW 2020*, 6–13.

- [133] What Is OTA Connect, Andy Doan, <https://foundries.io/insights/blog/ota-part-2/>, last accessed 2022/08/09
- [134] ISO 11898: "Road Vehicles-Controller area network (CAN)", (2016)
- [135] Driving down power, Nat Bowers, <https://www.electronicsspecifier.com/products/power/driving-down-power>, last accessed 2022/08/09
- [136] What is Vehicle CAN bus and why do you need to care, Earth2Digital, <https://www.earth2.digital/blog/what-is-vehicle-can-bus-ecu-evoque-adam-ali.html>, last accessed 2022/08/09
- [137] Airbags, Why Files, https://whyfiles.org/032air_bag/how_work.html, last accessed 2022/08/09
- [138] Taeihagh, A., & Lim, H. S. M. (2019). Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews*, 39(1), 103–128.

INDEX – Table of figures, equations and graphs

1. Table of figures

FIGURE 1: ROLE OF AI IN DRIVING AUTOMATION.....	10
FIGURE 2 MAIN DRIVING AUTOMATION COMPONENTS [12].....	12
FIGURE 3 ARCHITECTURE OF DECISION MAKING OF AN AUTONOMOUS CAR [20]	15
FIGURE 4 DIVISION OF V2X TECHNOLOGIES	18
FIGURE 5 SOTIF ERRORS AND ITS EFFECTS AND DEVELOPMENT	24
FIGURE 6 TYPES OF CYBERSECURITY ATTACKS AND COUNTERS	28
FIGURE 7 SAFETY CASE DEPENDENCIES (BASED ON [61]).....	33
FIGURE 8 REACH OF OVER THE AIR UPDATES [99].....	44
FIGURE 9 A NEW SW VERSION IS CREATED BY THE SW PROVIDER (SWP), VERIFIED AND DISTRIBUTED BY THE OEM AND FINALLY INSTALLED ON THE CONCERNED ECU OF A VEHICLE[100]	45
FIGURE 10 EXAMPLE OF HOW ECUS ARE DISTRIBUTED IN A VEHICLE [102]	45
FIGURE 11 BC APPROACH [100].....	48
FIGURE 12 TUF STANDARD APPLIED TO UPTANE FRAMEWORK [102]	49
FIGURE 13 RELATION BETWEEN PRODUCT ARGUMENTS AND WORK PRODUCTS OF AUTOMOTIVE FUNCTIONAL SAFETY AND CYBERSECURITY	59
FIGURE 14 CLASSIC ADT STRUCTURE.....	60
FIGURE 15 SYMBOLISM FOR ELIMINATIVE ARGUMENTATION	61
FIGURE 16 SYMBOLISM FOR STANDARD GSN.....	62
FIGURE 17 KEY TO SYMBOLISM USED IN THE PROPOSED METHODS.....	62
FIGURE 18 DEMONSTRATION	64
FIGURE 19: DEMONSTRATION PART 1	65
FIGURE 20 DEMONSTRATION PART 2	66
FIGURE 21: SECURITY CASE FOR THE “ART HEIST” EXAMPLE	69
FIGURE 22: ELEMENTS ON A TRAFFIC SIGNAL RECOGNITION SYSTEM	71
FIGURE 23 ATTACK TREE FOR A TRAFFIC SIGNAL RECOGNITION SYSTEM.....	72
FIGURE 24 CYBERSECURITY CASE FOR A TRAFFIC RECOGNITION SYSTEM	73
FIGURE 25 APPLICATION OF THE METHOD TO A ASV (EXTENDED SIZE IMAGE ON APPENDIX D – ENLARGED METHOD DIAGRAMS)	79
FIGURE 26 ENHANCED SIZE DETAILED DIAGRAM PART 1 OF 3	80
FIGURE 27 ENHANCED SIZE DETAILED DIAGRAM PART 2 OF 3	81
FIGURE 28 ENHANCED SIZE DETAILED DIAGRAM PART 3 OF 3	82
FIGURE 29 STRUCTURE OF A COMPLETE OTA SERVER PROJECT [133]	84
FIGURE 30 NETWORK DIAGRAM OF THE OTA TEST BENCH [132]	87

FIGURE 31 INFORMATION FLOW FROM PRIMARY ECU TO SECONDARY ECU IN THE TEST BENCH [132]	87
FIGURE 32 DETAILS OF THE TESTBED AT COVENTRY UNIVERSITY. [132].....	87
FIGURE 33 CURRENT USER INTERFACE IN THE NEWEST VERSION OF UPTANE	88
FIGURE 34 APPLICATION DOMAINS OF VEHICLE NETWORKS [135].....	89
FIGURE 35 SELECTED ELEMENTS OF CAN NETWORK OF THE LAND ROVER EVOQUE, SHOWING FOUR DOMAINS [136]	90
FIGURE 36 COMFORT DOMAIN CAN SUB-NETWORK OF THE LAND ROVER EVOQUE [136].....	90
FIGURE 37 WORKING AND DEPLOYMENT OF A VEHICLE AIRBAG [137].....	93
FIGURE 38 SENSORS (BLACK POINTS) AND AIRBAGS (GREEN SQUARES) AVAILABLE.....	95
FIGURE 39 PILOT DEMONSTRATION, (EXTENDED SIZE IMAGE ON APPENDIX D – ENLARGED METHOD DIAGRAMS)	96
FIGURE 40 ENLARGED IMAGE FOR DETAILS PART 1 OF 4.....	97
FIGURE 41 ENLARGED IMAGE FOR DETAILS PART 2 OF 4.....	98
FIGURE 42 ENLARGED IMAGE FOR DETAILS PART 3 OF 4.....	99
FIGURE 43 ENLARGED IMAGE FOR DETAILS PART 4 OF 4.....	100

2. Table of tables

TABLE 1: SAE LEVELS OF DRIVING AUTOMATION (BASED ON SAE J3016 [7])......	10
TABLE 2 EXAMPLE USES OF V2X TECHNOLOGIES.....	19
TABLE 3 CURRENT STATUS OF THE V2X TECHNOLOGIES.....	20
TABLE 4 STATE OF THE ART OF SOTIF.....	25
TABLE 5 ASIL LEVELS.....	26
TABLE 6 ASIL EXAMPLE.....	26
TABLE 7 STRUCTURES OF GSN	36
TABLE 8 WORKS THAT INSPIRE THE METHOD	54
TABLE 9 RELATED WORK	55

3 Table of Equations

EQUATION 1 EQUATION TO OBTAIN THE THROTTLE PERCENTAGE SPEED WHILE STEERING.	15
--	----

Appendix A – Links of Interest

Knowledge base of European Projects regarding connected and highly autonomous vehicles:

<https://connectedautomateddriving.eu/cad-knowledge-base/>

Marine Conventions

- **SOLAS** [https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-\(SOLAS\),-1974.aspx](https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx)
- **MARPOL**
<https://www.imo.org/en/KnowledgeCentre/ConferencesMeetings/Pages/Marpol.aspx>
- **COLREG** <https://www.imo.org/en/OurWork/Safety/Pages/Preventing-Collisions.aspx>

Download links for the testbench source codes

- Testbench Source Code: <https://github.com/advancedtelematic>
- Actualizr-Uptane source code: <https://github.com/advancedtelematic/aktualizr>

Appendix B – ECE Regulations

<u>UN R0 International Whole Vehicle Type Approval</u>	<u>UN R79 Steering Equipment</u>
<u>UN R1 Headlamps (R2/HS1)</u>	<u>UN R80 Coach Seat Strength</u>
<u>UN R3 Retro-reflecting Devices</u>	<u>UN R81 Motorcycle/Moped Mirrors</u>
<u>UN R4 Rear Plate Lighting</u>	<u>UN R82 Moped Halogen Headlamps</u>
<u>UN R5 European SB Tractor Headlamps</u>	<u>UN R83 Motor Vehicle Emissions</u>
<u>UN R6 Direction Indicators</u>	<u>UN R84 Fuel Consumption Measurement</u>
<u>UN R7 Position, stop and end-outline lamps</u>	<u>UN R85 Net Power Measurement</u>
<u>UN R8 Halogen Headlamps</u>	<u>UN R86 Tractor Lighting</u>
<u>UN R9 Three-Wheeled Cycle Noise</u>	<u>UN R87 Daytime Running Lamps</u>
<u>UN R10 Electromagnetic Compatibility</u>	<u>UN R88 Moped Retro-reflective Tires</u>
<u>UN R11 Door Latches</u>	<u>UN R89 Speed Limitation Devices</u>
<u>UN R12 Steering Mechanism</u>	<u>UN R90 Replacement Brake Components</u>
<u>UN R13 Heavy-Duty Braking</u>	<u>UN R91 Side-Marker Lamps</u>
<u>UN R13-H Light Vehicle Braking</u>	<u>UN R92 Motorcycle RESS</u>
<u>UN R14 Safety-Belt/ISOFIX Anchorages</u>	<u>UN R93 Front Underrun Protection</u>
<u>UN R15 Emission of Gaseous Pollutants</u>	<u>UN R94 Frontal Collision Protection</u>
<u>UN R16 Safety belt systems</u>	<u>UN R95 Lateral Collision Protection</u>
<u>UN R17 Strength of Seats</u>	<u>UN R96 NRMM Emissions</u>
<u>UN R18 Unauthorized Vehicle Use</u>	<u>UN R97 Vehicle Alarms</u>
<u>UN R19 Front Fog Lamps</u>	<u>UN R98 Gas-discharge-light Headlamps</u>
<u>UN R20 Headlamps (H4)</u>	<u>UN R99 Gas-discharge Light Sources</u>
<u>UN R21 Interior Fittings</u>	<u>UN R100 Electric Powertrain Vehicles</u>
<u>UN R22 Helmets</u>	<u>UN R101 CO2 Emissions/Fuel Consumption</u>
<u>UN R23 Reversing Lights</u>	<u>UN R102 Close-Coupling Devices</u>
<u>UN R24 Diesel Engine Emissions</u>	<u>UN R103 Replacement Catalytic Converters</u>
<u>UN R25 Head Restraints</u>	<u>UN R104 Retro-reflective Markings</u>
<u>UN R26 External Projections</u>	<u>UN R105 ADR Vehicles</u>
<u>UN R27 Warning Triangles</u>	<u>UN R106 Agricultural Tires</u>
<u>UN R28 Audible Warning Devices</u>	<u>UN R107 Coach and Bus Construction</u>
<u>UN R29 Commercial Vehicle Cabs</u>	<u>UN R108 Retreaded Tires</u>
<u>UN R30 Pneumatic Tires</u>	<u>UN R109 CV Retreaded Tires</u>
<u>UN R31 Halogen SB Headlamps</u>	<u>UN R110 CNG/LNG System Components</u>
<u>UN R32 Rear-End Collision Protection</u>	<u>UN R111 Tank Vehicle Stability</u>
<u>UN R33 Head-On Collision Protection</u>	<u>UN R112 Asymmetrical Beam Headlamps</u>
<u>UN R34 Fuel Tanks</u>	<u>UN R113 Symmetrical Headlamps</u>
<u>UN R35 Foot Controls</u>	<u>UN R114 Replacement Airbags</u>
<u>UN R36 Bus Construction</u>	<u>UN R115 LPG/CNG Retrofit Systems</u>
<u>UN R37 Filament Lamps</u>	<u>UN R116 Anti-theft and Alarm Systems</u>
<u>UN R38 Rear Fog Lamps</u>	<u>UN R117 Tire Noise, Wet Adhesion, and Rolling Resistance</u>
<u>UN R39 Speedometer Equipment</u>	<u>UN R118 Material Burning Behavior</u>

<u>UN R40 Motorcycle Emissions</u>	<u>UN R119 Cornering Lamps</u>
<u>UN R41 Motorcycle Noise</u>	<u>UN R120 NRMM Net Power/Fuel Consumption</u>
<u>UN R42 Front and Rear Protection</u>	<u>UN R121 Hand Controls, Tell-tales and Indicators</u>
<u>UN R43 Safety Glazing</u>	<u>UN R122 Heating Systems</u>
<u>UN R44 Child Restraint Systems</u>	<u>UN R123 Adaptive Front-lighting Systems</u>
<u>UN R45 Headlamp Cleaners</u>	<u>UN R124 Passenger Car/Trailer Wheels</u>
<u>UN R46 Indirect Vision</u>	<u>UN R125 Driver Forward Vision</u>
<u>UN R47 Moped Emissions</u>	<u>UN R126 Partitioning Systems</u>
<u>UN R48 Installation of Lighting</u>	<u>UN R127 Pedestrian Safety</u>
<u>UN R49 Diesel/CNG/LNG Engine Emissions</u>	<u>UN R128 LED Light Sources</u>
<u>UN R50 Motorcycle Lamps</u>	<u>UN R129 Enhanced Child Restraints</u>
<u>UN R51 Vehicle Noise</u>	<u>UN R130 Lane-departure Warning</u>
<u>UN R52 Small Bus Construction</u>	<u>UN R131 Advanced Emergency Braking</u>
<u>UN R53 Motorcycle Lighting</u>	<u>UN R132 Retrofit Emissions</u>
<u>UN R54 CV Tires</u>	<u>UN R133 Vehicle Recyclability</u>
<u>UN R55 Mechanical Couplings</u>	<u>UN R134 Hydrogen Fuel Cell Safety</u>
<u>UN R56 Moped Headlamps</u>	<u>UN R135 Pole Side Impact</u>
<u>UN R57 Motorcycle Headlamps</u>	<u>UN R136 Electric Motorcycle Safety</u>
<u>UN R58 Rear Underrun Protection Devices</u>	<u>UN R137 Frontal Impact ORS</u>
<u>UN R59 Replacement Silencing Systems</u>	<u>UN R138 Quiet Road Transport Vehicles</u>
<u>UN R60 Motorcycle Controls</u>	<u>UN R139 Brake Assist Systems</u>
<u>UN R61 CV External Projections</u>	<u>UN R140 ESC Systems</u>
<u>UN R62 Handlebar Vehicle Unauthorized Use</u>	<u>UN R141 Tire Pressure Monitoring Systems</u>
<u>UN R63 Moped Noise</u>	<u>UN R142 Tyre Installation</u>
<u>UN R64 Spare Tires</u>	<u>UN R143 HD Dual Fuel Retrofit Systems</u>
<u>UN R65 Special Warning Lamps</u>	<u>UN R144 Accident Emergency Call Systems</u>
<u>UN R66 Coach Superstructure Strength</u>	<u>UN R145 ISOFIX anchorage systems</u>
<u>UN R67 LPG Equipment</u>	<u>UN R146 Motorcycle HFC Safety</u>
<u>UN R68 Maximum Speed Measurement</u>	<u>UN R147 Agricultural vehicle couplings</u>
<u>UN R69 Slow Vehicle Marking Plates</u>	<u>UN R148 Light-Signalling Devices</u>
<u>UN R70 Long Vehicle Marking Plates</u>	<u>UN R149 Road Illumination Devices (RID)</u>
<u>UN R71 Tractor Driver's Field of Vision</u>	<u>UN R150 Retro-reflective Devices (RRD)</u>
<u>UN R72 Motorcycle Halogen Headlamps</u>	<u>UN R151 Blind spot detection</u>
<u>UN R73 CV Lateral Protection</u>	<u>UN R152 Light Vehicle AEBs</u>
<u>UN R74 Moped Lighting</u>	<u>UN R153 Fuel System Electric Power Train Safety</u>
<u>UN R75 Motorcycle Tires</u>	<u>UN R154 WLTP Type Approval</u>
<u>UN R76 Moped Driving/Passing Headlamps</u>	<u>UN R155 Cybersecurity</u>
<u>UN R77 Parking Lamps</u>	<u>UN R156 SW Updates</u>
<u>UN R78 Motorcycle Braking</u>	<u>UN R157 Automated Lane-Keeping Systems</u>

Appendix C – GTR Regulations

[GTR No. 1 Door Locks](#)

[GTR No. 2 WMTC](#)

[GTR No. 3 Motorcycle Brakes](#)

[GTR No. 4 WHDC](#)

[GTR No. 5 OBD](#)

[GTR No. 6 Safety Glazing](#)

[GTR No. 7 Head Restraints](#)

[GTR No. 8 ESC Systems](#)

[GTR No. 9 Pedestrian Safety \(GTR\)](#)

[GTR No. 10 OCE](#)

[GTR No. 11 NRMM Emissions](#)

[GTR No. 12 Motorcycle Controls](#)

[GTR No. 13 Hydrogen/Fuel Cell Vehicles](#)

[GTR No. 14 Pole Side Impact](#)

[GTR No. 15 WLTP](#)

[GTR No. 16 Tires](#)

[GTR No. 17 Motorcycle Evaporative Emissions](#)

[GTR No. 18 L-OBD](#)

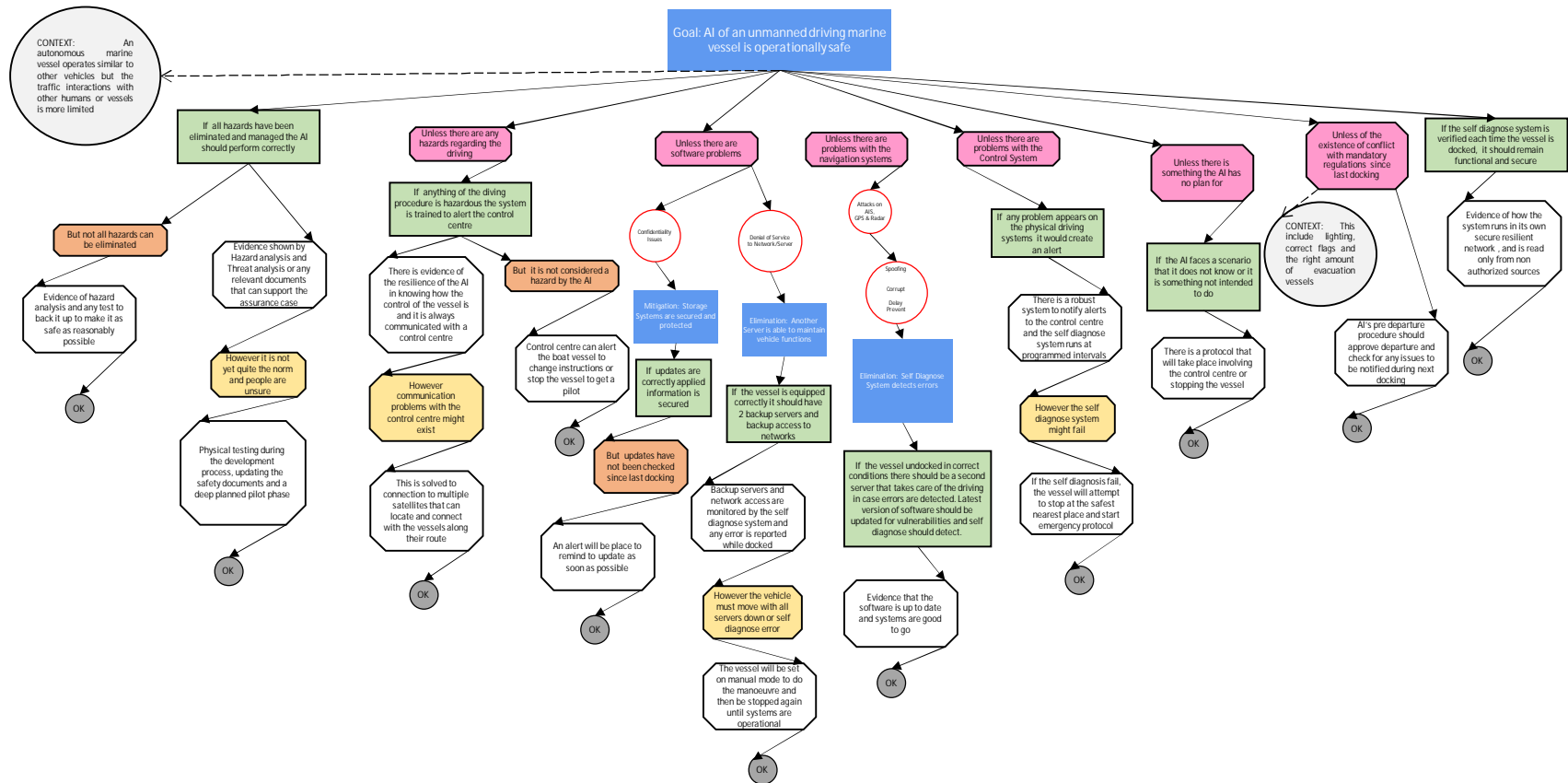
[GTR No. 19 Evaporative emissions](#)

[GTR No. 20 Electric Vehicle Safety](#)

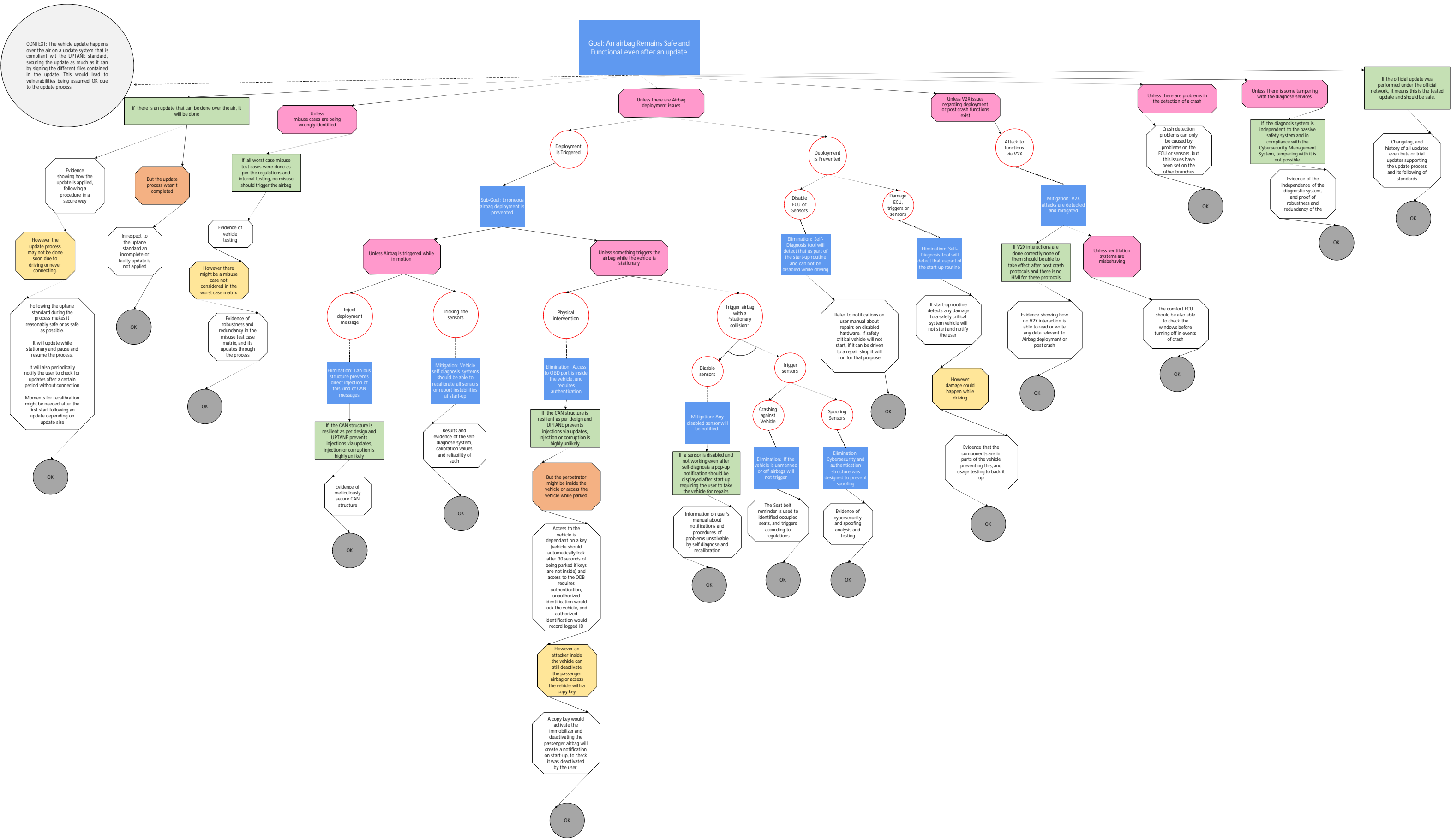
[GTR Regarding Side Impact](#)

Appendix D – Enlarged Method Diagrams

REALWORLD APPLICATION



Pilot Demonstration



Appendix E – Confidential supporting information for AI Marine System. FMEA & Attack Trees

FMEA Document

FMEA

DPT4500 FMEA DP II

ACC

Date

18 December 2020

Reference

P100xxxx-5612-FMEA

FMEA

Main title	Date
DPT4500 FMEA DP II	18 December 2020
Subtitle	Reference number
ACC	P100xxx-5612-FMEA
Special text	
[Special text]	
Version	
1.0	
Total number of pages	
21	
Registration code	
[Registration code]	
Author	
E. El Amam	
Quality control	
[Reviewer]	

FMEA

Table of contents

Figures.....	3
Tables.....	3
Abbreviations.....	5
Updates.....	5
1. Introduction.....	6
1.1 Scope of this document.....	6
1.2 Document overview.....	6
2. DPT4500 Principles.....	7
2.1 Introduction.....	7
2.2 System Architecture.....	7
2.3 UPS Supply.....	9
2.4 System Functions.....	9
2.5 Server Master-Slave behavior.....	9
2.6 Sensor/Sub System Configuration.....	10
2.7 Power Supply Philosophy.....	11
2.8 Network.....	11
3. Analysis.....	12
3.1 Failure classification.....	12
3.1.1 Failure likelihood/probability.....	12
3.1.2 Failure severity.....	13
3.1.3 Failure detection probability.....	13
3.1.4 Risk matrix.....	14
3.2 Demarcation.....	14
4. Conclusions.....	15
4.1 FMEA worksheet summary.....	15
4.2 FMEA result.....	15
Appendix A FMEA Worksheets.....	16

Figures

Figure 1: Typical DPT4500 Configuration.....	7
--	---

Tables

Table 2-1: DPT4500 components within a DPS.....	8
---	---

FMEA

Table 2-2: Non-DPT4500 components within a DPS	8
Table 2-3: DP system power configuration	9

FMEA

Abbreviations

AMCS	Alarm, Monitoring and Control System
COG	Course Over Ground
DGPS	Differential Global Positioning System
DP	Dynamic Positioning Detection Probability
DPCS	Dynamic Positioning Control System
DPS	Dynamic Positioning System
DPT	Dynamic Positioning / Tracking
FMEA	Failure Mode and Effect and Analysis
HMI	Human Machine Interface
IJS	Independent Joystick System
IM	Imtech Marine
MRU	Motion Reference Unit
MSB	Main Switchboard
P	Probability
PC	Personal Computer
PIU	Platform Interface Unit
PLC	Programmable Logic Controller
PMS	Power Management system
PS	Portside
SB	Starboard
SC	Severity Classification
SMC	Ship Motion Control
SOG	Speed Over Ground
STW	Speed Through Water
TCS	Thruster Control System
TFT	Thin Film Transistor
UKC	Under Keel Clearance
UPS	Uninterruptible Power Supply
USBL	Ultra Short BaseLine
VRU	Vertical Reference Unit
VCS	Vessel Control System

Updates

In the table below the corrections are recorded of those parts that have changed since the previous version.

Version	Date	Change/Correction	Reason
1.0	4-Oct-2018		Initial project version

FMEA

1. Introduction

1.1 Scope of this document

This document describes the Failure Mode and Effect Analysis (FMEA) of the applicable elements and functions that are part of the DPT4500 Dynamic Positioning Control System.

A FMEA is obligatory for vessels with the IMO DP equipment Class 2 and 3, e.g. following the BV Rules & Regulations DYNAPOS AM/AT R and DYNAPOS AM/AT RS [1], DNV DYNPOS-AUTR and DYNPOS-AUTRO [2], LR DP(AA) and DP(AAA) [3], ABS DPS-2 and DPS-3 [4].

The objective of this document is to contribute to the process of obtaining a system approval of the DPT4500 Dynamic Positioning Control System, complying with the above mentioned class requirements.

Apart from the specific properties and elements of the Dynamic Positioning Control System (DPCS), ship specific elements (such as redundancy of sensors, actuators, platform automation and power supply) have been taken into account only where this may directly affect the DPCS functionality.

The method used to produce a reliable FMEA has been globally extracted from the Military Standard Procedures for performing a Failure Mode, Effects and Criticality Analysis by the Department of Defense, USA (MIL-STD-1629)[5].

This FMEA covers the typical DP Class 2 configuration of the DPT4500 system.

1.2 Document overview

Chapter 1 contains a general introduction.

Chapter 2 provides a functional description of the typical DPT4500 architecture.

Chapter 3 defines the FMEA categories and classes. Furthermore, some considerations that are essential to the analysis are listed here.

Chapter 4 presents the conclusions of the FMEA.

Appendix A presents the completed FMEA worksheets.

Appendix B presents the control system configuration.

FMEA

2. DPT4500 Principles

2.1 Introduction

The DPT4500 system is derived from the more general Ship Motion Control (SMC) system architecture. This architecture comprises a library of control modules, HMI modules and interface modules as well as a set of certified standard hardware components such as PCs, Control Panels, TFT-displays, etc. These modules can be used to build control systems for controlling any ship motion (as long as the appropriate sensors and actuation devices are present). In case of the DPT4500 system, the implementation is limited to controlling the position and the heading of the ship and to control the forward and lateral speeds of the ship (within the normal DP operating window).

2.2 System Architecture

Figure 1 provides a block diagram of a typical DPT4500 configuration as part of a Dynamic Positioning System.

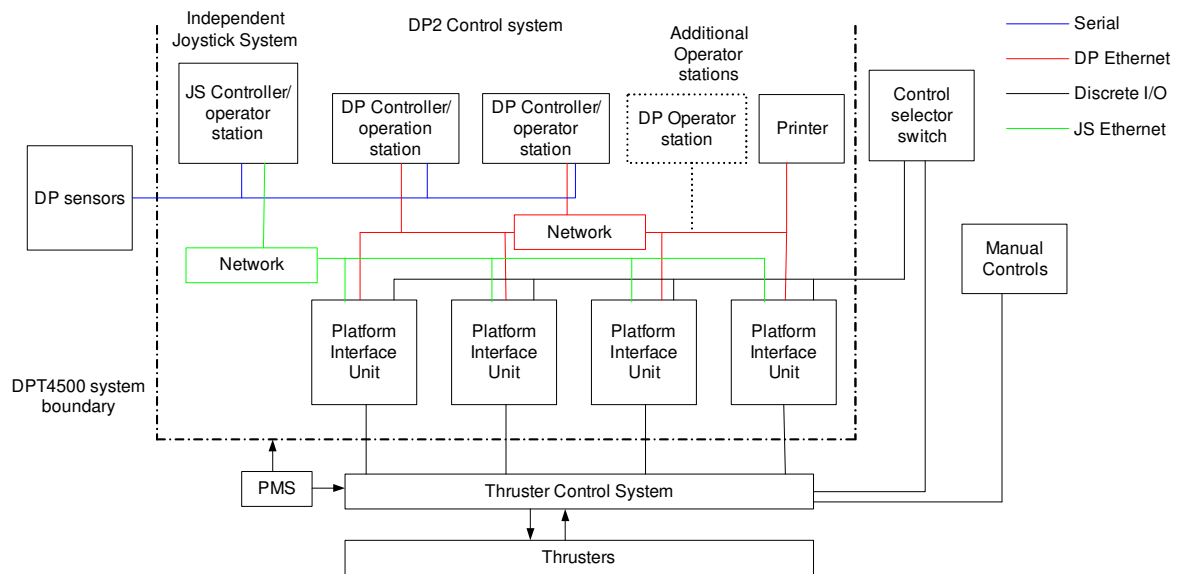


Figure 1: Typical DPT4500 Configuration

Some DPT4500 components play the role of Dynamic Positioning Control System (DPCS), others that of Independent Joystick System (IJS). They are further explained in Table 2-1 here-after.

FMEA

DPT4500 Component	Function
DP Controller	Computer workstation running DPT4500 controller software, infrastructure and communication drivers
DP Operator Station	Kit comprising a computer workstation, a DPT4500 control panel with trackball and joystick, a TFT screen and HMI software
DP Controller/operation station	Combined DP Control Server and DP Operator Station
DPCS Network	Redundant Ethernet switched network for data transfer between the DP Controllers, DP Operator Stations and PIUs
PIU	Platform Interface Unit for interfacing between the DP Network, IJS network and the Thruster Control System.
IJS Network	Single Ethernet network for data transfer between the Independent Joystick System and the PIUs, separated from the DPCS Network
Printer	Provides hard copy screen dumps

Table 2-1: DPT4500 components within a DPS

The DPT4500 system consists of

- Two combined DP Controller/DP Operator Stations
- One Independent Joystick System

See also appendix B for the block diagram of the system.

The DPT4500 interfaces with the components and sensors listed in Table 2-2 below.

Other Component	Function
Control Selection Switch	Operator controllable 3-way switch to select which system is in control: DPCS, IJS or Manual Control System (levers) The contacts to each PIU are assumed to be electrically independent
Thruster Control System	Controlling azimuth thrusters and bow tunnel thruster Providing platform information to the PIUs, and controlling the thrusters from the PIU commands or from the Manual Controls Panel commands
Manual Controls	Panel comprising single levers for (direct) manual control of the thrusters
3x Gyro	Sensor providing at least the ship's heading
3x Position Reference Systems	Sensor providing at least the ship's position, course over ground (COG) and speed over ground (SOG). Combination of 2x DGPS, 1x FANBEAM
2x Wind	Sensor providing at least relative wind speed and direction
2x MRU	Motion reference unit providing at least the ship's roll and pitch angles

Table 2-2: Non-DPT4500 components within a DPS

FMEA

2.3 UPS Supply

The main components of the system will be powered according the table below.

DPT4500 Component	Power Supply
DP Controller/DP Operator station (DPT-001)	UPS 1
Network Switch SW1	UPS 1
Independent Joystick System (JOY-001), Network Switch SW7	UPS 3
DP Controller/DP Operator station (DPT-002)	UPS 2
Network Switch SW2	UPS 2
Printer	UPS 2
PIU1 Propeller PS	UPS 1 & UPS 2
PIU2 Propeller STBD	UPS 1 & UPS 2
PIU3 Sternthruster FWD	UPS 1 & UPS 2
PIU4 Bowthruster FWD	UPS 1 & UPS 2
PIU5 Bowthruster AFT	UPS 1 & UPS 2
UPS 1	230 VAC from Main switch board PS
UPS 2	230 VAC from Main switch board SB
UPS 3	230 VAC from (TBD)

Table 2-3: DP system power configuration

2.4 System Functions

The main operating principles of the DPT4500 system can be summarized as:

- The operator can use the 'DP System in Control' selection switch to select between 'MANUAL', 'DP' and 'JOYSTICK'
- In the position 'MANUAL', the operator is bypassing the DPT4500 System. The system removes it's 'in command' request to the Thruster Control System. The Thruster Control System is to ignore the DPT4500 output and to follow the lever commands
- In the position 'DP', the DPCS is in control, providing manual, automatic and joystick control of the ship's heading, surge, sway and position
- In the position 'JOYSTICK', the Independent Joystick System is in control, providing manual, automatic and joystick control of the ship's heading, surge, sway and position
- In the 'DP' or 'JOYSTICK' position, the Thruster Control System is to follow the DPT4500 commands, unless system failures dictate otherwise

2.5 Server Master-Slave behavior

Master-Slave functionality is only applicable for redundant systems, in this case two DP controllers. Usually, redundant systems focus on hardware failures. The master-slave algorithm in DPT-4500 however, focuses more on functionality degradation.

FMEA

Each DP controller uses the following indications:

- Master On/Off
 - One Server is Master, the other Slave.
An operator can make the other Server Master.

- Standby On/Off
 - Indication that the Standby function is active.
Normally, the Standby indication is "On". This will only change to "Off" only when the fault indication is "On" or by an operator action.
When the Slave is not standby (Standby "Off"), automatic changeover of the Slave to become Master is blocked unless it detects that the Master is not communicating. If the Slave is not standby the Master will generate an alarm.

- Fault On/Off
 - Indication that a serious problem is present.
A serious problem is by definition 'the Server is unable to perform a possible control mode'. Usually, the required sensor information is missing or required actuators are not available.

The following aspects are important to understand Master-Slave behavior:

- The Master determines all settings, including those related to Master Slave settings.
- During startup a server starts as Slave and only becomes Master if it has determined that there is no other system acting as Master.

The Master-Slave switchover consists of two steps. First, the current Master will make itself Slave if the following conditions are met:

- a. The Master has a fault condition.
- b. The Slave is communicating with the Master and has no fault condition.
- c. The Slave standby function is "On".

When these conditions are met, the Master server will make itself Slave. As a consequence, the Slave, seeing no Master, will make itself Master. The control mode will not degrade. When the Slave is not standby, Master-Slave changeover will not occur and the control mode will degrade as a result of the Master fault condition.

A Slave will also make itself Master regardless of its standby & fault state if there are no other DP controllers communicating with the Slave.

To further clarify this procedure:

Assume that the Slave server is Standby and that DP-auto has been selected. In that case, failure of all position reference sensors on the Master will result in a Master-Slave change-over under the condition that a least one position reference sensor on the Slave is still available; DP-auto mode will continue. If all position reference sensors on the Slave fail at the same moment, no switch-over will take place; DP-auto mode will degrade to joystick control.

2.6 Sensor/Sub System Configuration

All sensor/sub system (PMS) data is transmitted via NMEA splitters to all three DPT4500 Controllers (JOY, DPT1 and DPT2). Each splitter is fed from the same UPS as the sensor itself.

FMEA

2.7 Power Supply Philosophy

The power supply arrangement for the DPT4500 control system is defined by the following principles:

- Each DP controller and associated DP HMI and network switch is fed from a dedicated 230VAC UPS with a bypass
- Each PIU and associated network switch is fed from a redundant 24VDC supply, derived from both UPS feeding the DP controllers
- The power supply of the DP sensors is provided by at least 2 UPS, whereby each UPS feeds at least 1 sensor of each type, and the NMEA splitter associated with that sensor.
- The UPS feeding the DP controllers and sensors are fed from different MSBs.

2.8 Network

The DP controllers, PIU's and DP operator stations communicate through Fast Ethernet (100Mb/s) networks. In case of multiple PIUs (used for complying with DP-1/2/3 notation requirements), each PIU is expanded with a network switch, in order to provide a redundant data link to the DP controllers.

Two different topologies are used in the system:

- Single Star
 - o Used for single DP system, independent joystick system
 - o No redundancy
- Redundant Ring
 - o Used between multiple controllers & operator stations and PIUs
 - o Requires "teamed" Ethernet adapters in all the connected PCs
 - o Proprietary ring redundancy protocol used because of fast recovery time (<20ms)

The switches have bandwidth limitation features, in order to protect against network overload.

FMEA

3. Analysis

3.1 Failure classification

The FMEA is a systematic way of finding answers to the following questions:

- Which failures may occur?
- What are the causes?
- What are the effects?
- How serious are they?

The results of these questions for each identified function are put in a table with the following attributes:

- Function
- Failure modes
- Failure causes
- Failure probability
- Failure criticality
- Failure detection probability
- Failure effects
- Failure detection
- Remarks

For most attributes the use and the purpose are clear. In the next section the "Failure probability", "Failure criticality" and "Failure detection probability" are defined in more detail.

3.1.1 Failure likelihood/probability

The failure likelihood is a qualitative prediction to indicate how likely the initiating fault is to occur. Four levels are identified.

This failure probability is listed in the worksheet for each failure mode in column 'P'.

ID	Category	Description
A	Very probable	More than 10 times in the life of a vessel
B	Probable	More than once in the life of a vessel, but less than ten times
C	Foreseeable	Once in the life of a vessel
D	Remote	Once in the life of a fleet
E	Very remote	Not known to have occurred, but could happen

FMEA

3.1.2 Failure severity

A severity classification is assigned to each failure mode giving a qualitative measure of the worst potential consequences resulting from the function failure.

This classification is listed in the worksheets for each failure mode in column 'SC'.

ID	Category	Description
I	Minor	Does not significantly affect the DP system No effect on DP redundancy Continued safe operation not at risk
II	Severe	Does affect DP system, vessel still in position Less or no redundancy Vessel can remain on DP for a limited period
III	Major	DP system affected, positioning poor Insufficient equipment on line DP operations must stop Continued safe operation ceases to be possible
IV	Catastrophic	Total loss of DP No equipment online Safe operation has ceased

3.1.3 Failure detection probability

For each single failure mode the probability of failure detection is quantified by a percentage (rough estimation):

Value	Description
0	Cannot be detected
50	May take long before the operator identifies the problem from the information provided by the DPS
90	The system detects the problem, but there is a chance that the operator will overlook the problem
99	The system detects the problem and it is unlikely that the operator will overlook the problem

FMEA

3.1.4 Risk matrix

To judge the risks of the failure modes, the following risk matrix is used:

Consequence	Probability				
	A Very probable	B Probable	C Foreseeable	D Remote	E Very Remote
I Minor	Yellow	Green	Green	Green	Green
II Severe	Red	Yellow	Green	Green	Green
III Major	Red	Red	Yellow	Green	Green
IV Catastrophic	Red	Red	Red	Yellow	Green

Risk level	Consequence
Low	Not considered significant risk
Medium	Acceptable provided risk reduction measures are available
High	Unacceptable

3.2 Demarcation

In the analysis only those components of the DPS are considered that are essential for DP operations. Meaning that from the components listed in Table 2-1 and Table 2-2 the following are left out: Manual Control Panel, printer.

It is assumed that the ship is active in DP class 2 mode. Therefore, the initial condition is:

- All DPS components are compliant with DP(AA)requirements
- All DPS components are working correctly without any problems
- The DPCS is up and running, and in control of heading and position (DP-Auto)
- The Consequence Analysis function is activated
- The weather conditions are such that the ship can continue DP operation in case of any single failure in the power generation & distribution systems or thrusters
- All failure modes described consists of a single failure

The following types of failures are considered in the analysis.

Component failures:

- breakdown of a hardware component of the DPCS

Interface failures:

- loss of a signal to/from an external system interfaced to the DPCS
- loss of a signal to/from internal components of the DPCS
- incorrect behavior of a signal interfaced to the DPCS

Power supply failure:

- loss of power supply to parts of the DPCS

FMEA

4. Conclusions

4.1 FMEA worksheet summary

The following table shows the distribution of the failure modes/causes combinations identified in the FMEA worksheets across the previously described risk matrix.

Consequence	Probability				
	A Very probable	B Probable	C Foreseeable	D Remote	E Very Remote
I Minor		9	2	10	1
II Severe		10	15	10	7
III Major					1
IV Catastrophic					2

The most dangerous failure modes/causes identified in the worksheets according to the risk matrix are all failures of category B II.

All failures in this category lead to the loss of redundancy (loss of a single thrusters, DP controller or operator station), but do not jeopardize the immediate operation. Therefore, the operator has sufficient time to take action, and these failure modes are considered to have an acceptable risk.

The following possible single failures were identified in the DP control system:

1. Overload of the DPCS network
2. Failure of the control selector switch

Overload of the DPCS network can only occur as a result of the combination of a hidden fault in the software of the switches used, resulting in a common mode failure of the bandwidth limitation functionality in all the switches, and at the same time a failure in the DPT4500 software leading to huge increase of the network traffic, creating such an overload that communication between DP controllers and PIUs is lost. Furthermore it has been proven that the DPCS will keep working correctly at a much higher network load (>95%) than normally is the case. Therefore this failure mode is considered to have acceptable risk.

See also the System Description for more details concerning the DPCS network.

The control selector switch is an obvious single point of failure, but is outside the scope of the DPT4500 system. Only the effect of the selector failure on the PIU inputs is considered. The DPT4500 system has a number of safeguards to deal with failures of the control selector switch. Therefore this failure mode is considered to have acceptable risk. See the System Description for more details.

4.2 FMEA result

According to the estimation of probability and severity of the failure modes in the worksheets (Annex A), no unacceptable situation with a dangerous risk level can occur.

FMEA

Appendix A FMEA Worksheets

Function	ID	Failure Mode	Failure Cause	P	SC	DP	Failure Effect and End Effect	Failure Detection	Remarks
Power Supply	1	UPS PS input voltage failure	Any	C	II	99	<ul style="list-style-type: none"> DPT-001 now supplied from UPS System no longer DP2 compliant 	DPCS alarm indications: <ul style="list-style-type: none"> Mains fail UPS PS 	UPS device generates also audible alarms UPS supply lasts at least 30 minutes after which ID 3/21 occurs
	2	UPS SB input voltage failure	Any	C	II	99	<ul style="list-style-type: none"> DPT-002 now supplied from UPS SB System no longer DP2 compliant 	DPCS alarm indications: <ul style="list-style-type: none"> Mains fail UPS SB 	UPS device generates also audible alarms UPS supply lasts at least 30 minutes after which ID 4/22 occurs
	3	UPS PS output voltage failure	Any	C	II	99	<ul style="list-style-type: none"> DPT-001 offline Automatic changeover to hot-standby DP Controller System no longer DP2 compliant 	DPCS alarm indications: <ul style="list-style-type: none"> Link Server ⇔ UPS PS down Link Server1 ⇔ Server2 down Connection with Server 1 down Workstation alarm 	Same effect as ID 21
	4	UPS SB output voltage failure	Any	C	II	99	<ul style="list-style-type: none"> DPT-002 offline System no longer DP2 compliant 	DPCS alarm indications: <ul style="list-style-type: none"> Link Server ⇔ UPS DB down Link Server1 ⇔ Server 2 down Connection with Server2 down Workstation alarm 	Same effect as ID 22
System in Control selection mode	5	Control Selection Switch fails to "JOYSTICK" for individual PIU	Electro/mechanical failure	E	II	50	<ul style="list-style-type: none"> IJS in control of individual PIU thruster Individual thruster follows lever setpoint (via IJS) Reduced DP-AUTO capability 	DPCS alarm indications: <ul style="list-style-type: none"> DP2 consequence Both DPCS and IJS in control Alarm on IJS Thruster Not Available indication for individual PIU thruster.	Applicable for each individual PIU

FMEA

	6	Control Selection Switch fails to "MANUAL" for individual PIU	Electro/mechanical failure	E	II	50	<ul style="list-style-type: none"> Individual thruster follows lever (direct control) Reduced DP-AUTO capability 	DPCS alarm indications: <ul style="list-style-type: none"> DP2 consequence Thruster Not Available indication for individual PIU thruster 	Applicable for each individual PIU
	7	Control Selection Switch fails at "DP" for individual PIU	Electro/mechanical failure Failure of PIU Input Channel	E B	II	99	<ul style="list-style-type: none"> DPCS not in command of individual PIU thruster Individual thruster follows lever (direct control) Reduced DP-AUTO capability 	DPCS alarm indications: <ul style="list-style-type: none"> DP2 consequence Alarms on IJS PLC failure Thruster Not Available indication for individual PIU thruster	Applicable for each individual PIU
	8	Control Selection Switch selects "DP" and "JOYSTICK" for individual PIU	Electro/mechanical failure Failure of PIU Input Channel Incorrect status information	E E E	II		<ul style="list-style-type: none"> DPCS and IJS not in command of individual PIU thruster Individual thrusters follows lever 	Result equals 5	Applicable for each individual PIU
Thruster selection	9	'Cmd Request' signal to TCS lost for individual thruster	Electro/mechanical failure Failure of PIU Output Channel TCS failure	D B D	II	99	<ul style="list-style-type: none"> 'Cmd Request' not acknowledged by TCS Thruster no longer available to DPCS Reduced DP-AUTO capability Thruster will follow lever position (direct control) 	DPCS alarm indications: <ul style="list-style-type: none"> PIU ready alarm DP2 consequence Thruster Not Available indication for individual PIU thruster	
	10	'Thruster Ready' signal from TCS lost for individual thruster	Electro/mechanical failure Failure of PIU Input Channel TCS failure	D B D	II	99	<ul style="list-style-type: none"> Thruster no longer available for DPCS Reduced DP-AUTO capability Thruster will follow lever position (direct control) 	DPCS alarm indications: DP2 consequence <ul style="list-style-type: none"> Thruster Not Available indication for individual PIU thruster 	
	11	'Thruster Cmd Ack' signal from TCS lost for individual thrusters	Electro/mechanical failure Failure of PIU Input Channel TCS failure	D B D	II	99	<ul style="list-style-type: none"> Thruster no longer available for DPCS Reduced DP-AUTO capability Thruster may not follow DPCS setpoint depending on TCS 	Same as ID 9	
	12	'Thruster Ready' signal lost for all thrusters	TCS failure	E	IV	99	<ul style="list-style-type: none"> No thrusters available for DPCS Total loss of DP capability All thrusters will remain at last known DP auto setpoint until selector switch is set to manual. 	<ul style="list-style-type: none"> DPCS alarm indications: DP control configuration alarm Thruster Not Available indication for individual PIU thruster. 	Situation can only occur in case of a common failure mode in the TCS across all thrusters. TCS is considered not DP2 worthy.

FMEA

	13	'Thruster Cmd Ack' signal lost for all thrusters	TCS failure	E	IV	99	<ul style="list-style-type: none"> No thrusters available for DPCS Total loss of DP capability All thrusters will remain at last known DP auto setpoint until selector switch is set to manual 	DPCS alarm indications: <ul style="list-style-type: none"> DP control configuration Thruster ready alarming Thruster Not Available indication for individual PIU thruster 	Situation can only occur in case of a common failure mode in the TCS across all thrusters. TCS is considered not DP2 worthy.
	14	'Power Reduced' signal from TCS fails active for individual thruster	Electro/mechanical failure Failure of PIU input channel TCS failure	D B C	I	90	No effect on control strategy	Indication on DPCS mimic	
	15	'Power Reduced' signal from TCS lost for individual thruster	Electro/mechanical failure Failure of PIU input channel TCS failure	D B C	I	90	Possibly Degraded DP performance due to follow-up error	Possibly unexpected reduction of thrust by TCS. In that case, mismatch between requested and actual thrust, where large differences will initiate a thruster follow-up alarm.	
	16	'Actuator Max' signal from TCS incorrect high.	Electro/mechanical failure Failure of PIU input channel TCS failure	D B D	I	95	Possibly Degraded DP performance due to follow-up error	Possible too late consequence alarm/ Thrusters follow-up error when difference between setpoint/actual value becomes too big Operator must compare PMS data with DP input data	
	17	'Actuator Max' signal from TCS incorrect low.	Electro/mechanical failure Failure of PIU input channel TCS failure	D B D	I	95	Possible too early Consequence alarm Possible Degraded DP capability	Operator must compare PMS data with DP input data. Thruster limits indicated on DPCS mimic.	Severity depends on the value of the incorrect actuator max signal.
	18	Failure of individual PIU	Power failure CPU failure	C D	II	99 99	<ul style="list-style-type: none"> 'Cmd Request' to TCS removed. Communication between DPCS/IJS controllers and PIU lost Reduced DP capability Thruster will follow lever position (direct control) 	DPCS alarm indications: <ul style="list-style-type: none"> Link PLC PIU down DP 2 consequence Alarms on IJS 	
Thruster Control	19	Thruster setpoint to TCS incorrect	Electro/mechanical failure PIU output channel failure TCS failure	C B D	II	50	Reduced DP-AUTO performance	<ul style="list-style-type: none"> DPCS alarm indications: Possible thruster follow-up alarm 	Depending on the incorrect setpoint value, the DP consequence alarm might be triggered

FMEA

								<ul style="list-style-type: none"> Discrepancy between command and feedback indication on DPCS mimic Possibly out of range detection by TCS. 	
	20	Thruster feedback from TCS incorrect	Electro/mechanical failure PIU input channel failure TCS failure	C B D	II	50		<ul style="list-style-type: none"> DPCS alarm indications: Possible thruster follow-up alarm Discrepancy between command and feedback indication on DPCS mimic Possibly out of range detection by TCS 	
DP Controller	21	Master DP Controller failure	Power failure CPU failure Electro/mechanical failure	C B C	II	99	<ul style="list-style-type: none"> Automatic changeover to hot-standby DP Controller Current Operator Station remains in control 	DPCS alarm indications: <ul style="list-style-type: none"> Connection server 1 down Link server 1 ⇔ Server 2 down Workstation alarm 	Where the Controller and Viewer are combined in one PC, the viewer will automatically fail as well. Refer to ID 23 for further details.
	22	Slave DP Controller failure	Power failure CPU failure Electro/mechanical failure	C B C	II	99	<ul style="list-style-type: none"> Slave not hot-standby, backup DP controller lost 	DPCS alarm indications: <ul style="list-style-type: none"> Connection server 2 down Link server 1 ⇔ Server 2 down Workstation alarm 	Where the Controller and Viewer are combined in one PC, the viewer will automatically fail as well. Refer to ID 23 for further details.
DP HMI	23	DP Viewer failure	Power failure CPU failure Electro/mechanical failure	C B C	II	99	<ul style="list-style-type: none"> Dead screen Operator commands through DP Control Panel, Joystick and Tracker Ball no longer possible Operator is to switch-over to backup Operator Station and make that station the 'Station in Control' No effect on DP performance 	Dead screen. DPCS alarm indications (on other Operator Station): <ul style="list-style-type: none"> Workstation alarm Joystick X,Y,R alarm No control position active Alarm indication on DP Control Panel.	DP operator station was in control prior to failure.
	24	Display failure	Power failure Electro/mechanical failure	C C	II	99	<ul style="list-style-type: none"> Dead screen 	Dead screen	DP operator station was in control prior to failure.

FMEA

							<ul style="list-style-type: none"> Operator is to switch-over to backup Operator Station and make that station the 'Station in Control' No effect on DP performance 		
	25	Tracker Ball failure	Electro/mechanical failure	D	I	99	<ul style="list-style-type: none"> Operator commands through the display no longer possible Operator is to switch-over to backup Operator Station and make that station the 'Station in Control' No effect on DP performance 	No proper response on the display when using the tracker ball	DP operator station was in control prior to failure.
	26	Control Panel failure	Electro/mechanical failure	D	I	99	<ul style="list-style-type: none"> Operator commands through the Control Panel no longer possible Joystick control no longer possible Operator is to switch-over to backup Operator Station and make that station the 'Station in Control' No effect on DP performance 	DPCS alarm indications: <ul style="list-style-type: none"> DPT Panel error Joystick error Joystick X,Y,R alarm 	DP operator station was in control prior to failure.
	27	Joystick failure	Electro/mechanical failure	D	I	99	<ul style="list-style-type: none"> Joystick control no longer possible. Operator is to switch-over to backup Operator Station and make that station the 'Station in Control' No effect on DP performance 	DPCS alarm indications: <ul style="list-style-type: none"> Joystick error Joystick X,Y,R alarm 	DP operator station was in control prior to failure.
DPCS Network	28	Failure of individual Main Network Switch	Power failure	B	I	99	Network communication is re-routed through other Main Network Switch	DPCS alarm indications: <ul style="list-style-type: none"> Switch network alarm Workstation alarm. 	
			CPU failure	B					
	29	Failure of individual PIU Network Switch	Power failure	C	II	99	<ul style="list-style-type: none"> Network communication with PIU lost. 'Cmd Request' to TCS removed PIU output channels set to 'default' Thruster no longer available to DPCS Thruster will follow lever position (direct control) 	DPCS alarm indications: <ul style="list-style-type: none"> Link Server ⇔ PLC down Switch network alarm Consequence analysis alarm 	
CPU failure			B						
30	Main network switch connection failure.	Electro/mechanical failure (wire break)	D	I	99	Same as ID 26	Same as ID 26		No alarms on IJS
		Network link overload	E						

FMEA

	31	PLC PIU network switch connection failure	Electro/mechanical failure (wire break)	D	II	99	Same as ID 27	Same as ID 27	No alarms on IJS
			Network link overload	E					
	32	DP control network overload	Software failure	E	III	99	<ul style="list-style-type: none"> No/unreliable communication between DP controllers & thrusters 'Cmd Request' to TCS removed. PIU output channels set to 'default' Thrusters no longer available to DPCS. All thrusters will remain at last know DP auto setpoint until selector switch is set to manual 	DPCS alarms indications: <ul style="list-style-type: none"> Link sever⇔PLC alarming Switch/Network alarm DP degradation alarm 	<ul style="list-style-type: none"> Not considered to be a single point of failure (see Chapter 4) Operator can switch to Independent Joystick to safely abort DP operation
Ship's State Sensors (Gyro, position, wind, motion reference)	33	Individual sensor data Individual sensor lost	Sensor failure	B	I	99	<ul style="list-style-type: none"> Sensor information lost Automatic switch-over to other sensor if Alternative is available For pos-ref sensor in group of 3 or more: Sensor automatically disabled average calculation No effect on DP performance 	DPCS alarm indications: Sensor message invalid alarm	
			Communication failure	B					
	34	Individual sensor data incorrect	Sensor failure	B	I	95	<ul style="list-style-type: none"> Operator must select other sensor if 1 other is available For pos ref sensor in a group of 3 or more: Sensor automatically disabled from state calculation No effect on DP performance 	DPCS alarm indications: Sensor deviation alarm (if deviation greater than preset alarm limit)	
Power Management System	35	No data from PMS	PMS internal error	D	II	99	<ul style="list-style-type: none"> PMS communication alarm DP2 Consequence alarm 		



Imtech Marine & Offshore B.V.

Sluisjesdijk 155
P.O. Box 5054
3008 AB Rotterdam
The Netherlands
Harbour number 2137
T +31 (0)10 487 19 11
F +31 (0)10 487 17 02
www.imtech.eu/marine

FMEA

RADAR 4500 Development

Project: RADAR 4500
Projectnumber: 390196
Main title: FMEA
Sub title: RADAR 4500 Development
Special remark:
Issue: 1.1
Date: 03-Aug-2010
Total number of pages: 15
Registration code: 390196-FMEA/1.1

Name

Signature

Author: E. El Amam / S.A. de Meijer

Quality control:

Acknowledge:

Table of contents

Title page	
Administrative page	
Figures	3
Tables	3
References	4
Abbreviations	4
Modifications	4
1. Introduction	5
1.1 Scope of this Document	5
1.2 Document Overview	5
2. Radar System	6
2.1 Main Function	6
2.2 System Configuration	6
3. FMEA Principles	7
3.1 Failure classification	7
3.1.1 Failure probability	7
3.1.2 Failure severity	7
3.1.3 Failure detection probability	8
3.1.4 Risk matrix	8
3.2 Demarcation	8
Appendix A: Worksheet	10
Appendix B: Block Diagram of Reference System	15

Figures

Figure 2-1: Typical RADAR 4500 system configuration	6
---	---

Tables

No table of figures entries found.

References

- [1] Main title : System/Equipment Specification
 Sub title : RADAR 4500
 By : Imtech Marine & Offshore
 Ref. : 390196-SES
- [2] Main title : System Block Diagram of Equipment under Test at QinetiQ
 Sub title : RADAR 4500
 By : Imtech Marine & Offshore
 Ref. : 390196-RADAR-4500-QINETIQ-LDS-100
 Rev. : 1.0
 Date : 18-Nov-2009

Abbreviations

AIS	Automatic Identification System
(D)GPS	(Differential) Global Positioning System
DVI	Digital Visual Interface
EM	Electromagnetic
EuT	Equipment under Test
FMEA	Failure Mode and Effect Analysis
IM&O	Imtech Marine & Offshore
LAN	Local Area Network
NMEA	National Marine Electronics Association
PC	Personal Computer
PLC	Programmable Logic Controller
PSU	Power Supply Unit
RADAR	Radio Detection and Ranging
SCU	Scanner Control Unit
VDR	Voyage Data Recorder

Modifications

Issue	Date	By	Description
1.0	08-Apr-2010	EhAm	First release.
1.1	03-Aug-2010	SiMe	References to RADAR 4600 changed into 4500. Preface omitted, Scope of Document adapted. Basics of FMEA procedure added, including boundary conditions for this particular exercise. System configuration in chapter 2 elaborated. FMEA worksheet moved to Appendix A.

1. Introduction

1.1 Scope of this Document

This document describes the Failure Mode and Effect Analysis (FMEA) of the “RADAR 4500” Radar System of Imtech Marine & Offshore (IM&O).

Although a FMEA is typically used as a tool in the design phase, the main purpose of this FMEA is to identify area's that may have been underexposed in the test procedures, and that require additional attention during the verification phase of the RADAR 4500 product.

1.2 Document Overview

Chapter 2 describes the basic system functions, the typical RADAR 4500 system configuration, and the specific system configuration that is used as reference for this FMEA.

Chapter 3 lists the FMEA principles, in terms of failure categories and classes. Furthermore, some considerations that are essential to this analysis are described here.

Appendix A presents the completed FMEA worksheet.

Appendix B presents the block diagram of the specific radar system configuration used as reference in this FMEA.

2. Radar System

2.1 Main Function

Basically, a marine radar is to provide bearing and distance of ships and land targets in vicinity from own ship for collision avoidance and navigation at sea.

This basic function is enhanced by adding target tracking capabilities, the presentation of planned routes, chart information and AIS data of other ships, and various tools that support the navigator in his task.

2.2 System Configuration

A simplified block diagram of a typical RADAR 4500 system configuration is given in Figure 2-1.

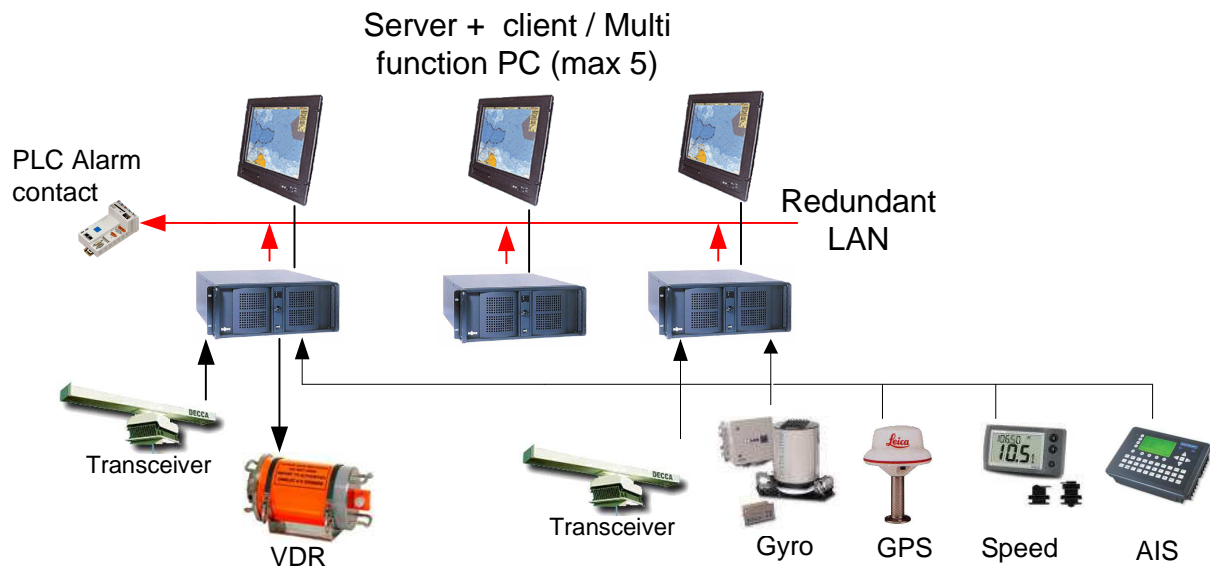


Figure 2-1: Typical RADAR 4500 system configuration

The RADAR 4500 system can be configured to meet customer requirements, and can be equipped with radar transceivers of different type and make. As a consequence, specific system configurations may differ in detail from the typical configuration as shown in Figure 2-1. More details on radar system configurations can be found in [1].

For the FMEA, the system configuration as used for certification tests has been taken as reference. This configuration includes transceivers of different type and make. Details of this configuration can be found in [2]. A copy of this block diagram is enclosed in Appendix B.

3. FMEA Principles

3.1 Failure classification

The FMEA is a systematic way of finding answers to the following questions:

- Which failures may occur?
- What are the causes?
- What are the effects?
- How serious are they?

The results of these questions for each identified function are put in a table with the following attributes:

- Function (or equipment component)
- Failure modes
- Failure causes
- Failure probability
- Failure criticality
- Failure detection probability
- Failure effects
- Failure detection
- Remarks

For most attributes the use and the purpose are clear. In the next section the “Failure probability”, “Failure criticality” and “Failure detection probability” are defined in more detail.

3.1.1 Failure probability

The failure probability is a qualitative prediction to indicate how likely the initiating fault is to occur.

Four levels are identified.

This failure probability is listed in the worksheet for each failure mode in column ‘P’.

ID	Category	Description
A	Very probable	More than 10 times in the life of a vessel
B	Probable	More than once in the life of a vessel, but less than ten times
C	Foreseeable	Once in the life of a vessel
D	Remote	Once in the life of a fleet
E	Very remote	Not known to have occurred, but could happen

3.1.2 Failure severity

A severity classification is assigned to each failure mode giving a qualitative measure of the worst potential consequences resulting from the function failure.

This classification is listed in the worksheets for each failure mode in column ‘SC’.

ID	Category	Description
I	Minor	Does not significantly affect the system. Has no effect on system redundancy. Continued safe operation is not at risk.
II	Severe	Does affect the system and causes loss of functionality. Affects system redundancy.
III	Major	Causes loss of essential system functionality.
IV	Catastrophic	Total loss of system functionality.

3.1.3 Failure detection probability

For each single failure mode the probability of failure detection is quantified by a percentage (rough estimation):

Value	Description
0	Cannot be detected.
50	May take long before the operator identifies the problem from the information provided by the system.
90	The system detects the problem, but there is a chance that the operator will overlook the problem.
99	The system detects the problem and it is unlikely that the operator will overlook the problem.

3.1.4 Risk matrix

To judge the risks of the failure modes, the following risk matrix is used:

Consequence	Probability				
	A Very probable	B Probable	C Foreseeable	D Remote	E Very Remote
I Minor					
II Severe					
III Major					
IV Catastrophic					

Risk level	Consequence
Low	Not considered significant risk
Medium	Acceptable provided risk reduction measures are available
High	Unacceptable

3.2 Demarcation

Since this FMEA is primarily intended to support the verification process, and not as a tool in the design process, the categorization of failure probability, failure severity and failure detection probability are left open for now.

When evaluating failure modes, the initial condition of the radar system shall be considered to be as follows:

- a. All transceivers are connected, and up and running.
- b. Radar server computers are up and running.
- c. Radar client computers and display units are up and running.
- d. Peripheral equipment is up and running.
- e. Power supplies connected to the radar system are up and running.

Appendix A: Worksheet

Component	Id	Failure mode	Failure Cause	P	SC	DP	Failure Effect and End Effect	Failure Detection	Remarks
1. Furuno X/S-band scanner	1	Total loss of functionality	Electrical power failure				Scanner stops turning, Scanner stops transceiving	No Radar video	For the S-band scanner the probability of an electrical power failure is larger as there is an extra component: the PSU
			Electro/mechanical failure						
	2	Incorrect command signal	Signal failure				Scanner stops turning, Scanner stops transceiving	No Radar video	
			Connection failure						
	3	Incorrect trigger signal	Signal failure				Scanner stops transceiving	No Radar video, Alarm no trigger signal	
			Connection failure						
Radar power module failure									
2. Sperry X/S –band Scanner	4	Total loss of functionality	Electrical power failure				Scanner stops turning Scanner stops transceiving	No Radar video	For the S-band scanner the probability of an electrical power failure is larger as there is an extra component: SCU
			Electro/mechanical failure						
	5	Incorrect command signal	Signal failure				Scanner stops turning Scanner stops transceiving	No radar video	
			Connection failure						
	6	Incorrect trigger signal	Signal failure				Scanner stops transceiving	No Radar video, alarm no trigger signal	
			Connection failure						
3. Monitor	7	Total loss of functionality of monitor 1	Electrical power failure				Dead screen, operator commands through tracker ball not possible.	Dead screen	
			Electro/mechanical failure						

Component	Id	Failure mode	Failure Cause	P	SC	DP	Failure Effect and End Effect	Failure Detection	Remarks
3. Monitor	8	Total loss of functionality of monitor 2	Electrical power failure				Dead screen, operator commands Through tracker ball not possible.	Dead screen	
			Electro/mechanical failure						
	9	Total loss of functionality of monitor 3	Electrical power failure				Dead screen, operator commands through tracker ball not possible	Dead screen	
			Electro/mechanical failure						
	10	Incorrect video signal (DVI)	Signal failure				Dead screen	Dead screen	
4. Speaker	11	Loss of sound	Electrical power failure				Speaker doesn't produce sound	No alarm sound generated when an alarm is present.	
			Electro/mechanical failure						
			Incorrect signal						
5. PC	12	PC1 total loss of functionality	Power failure				Communication from and to PC 1 not possible S-band scanner stops turning S-band scanner stops transceiving Communication loss with Moxa board	No Radar video at S-band Dead screen Alarm link PC1 <-> PC2 Alarm link PC1 <-> PC3	
			Electro/mechanical failure						
	13	PC2 total loss of functionality	Power failure				Communication from and to PC 2 not possible	Dead screen No (Sensor information on radar servers?) Alarm link PC2 <-> PC1 Alarm link PC2 <-> PC3	
			Electro/mechanical failure						
	14	PC3 total loss of functionality	Power failure				Communication from and to PC 3 not possible X-band scanner stops turning X-band scanner stops transceiving Communication loss with Moxa n port	Dead screen No Radar video at X-band Alarm link PC3 <-> PC1 Alarm link PC3 <-> PC2	
			Electro/mechanical failure						
	15	Incorrect heading marker signal	Signal failure				Server commands scanner to stop turning and to stop transceiving Scanner stops turning Scanner stops transceiving	No Radar video Alarm no heading marker	Different probability for Furuno, or Sperry radar, as an extra component(radar power module) is present for Furuno Larger probability for Furuno?
			Connection failure						

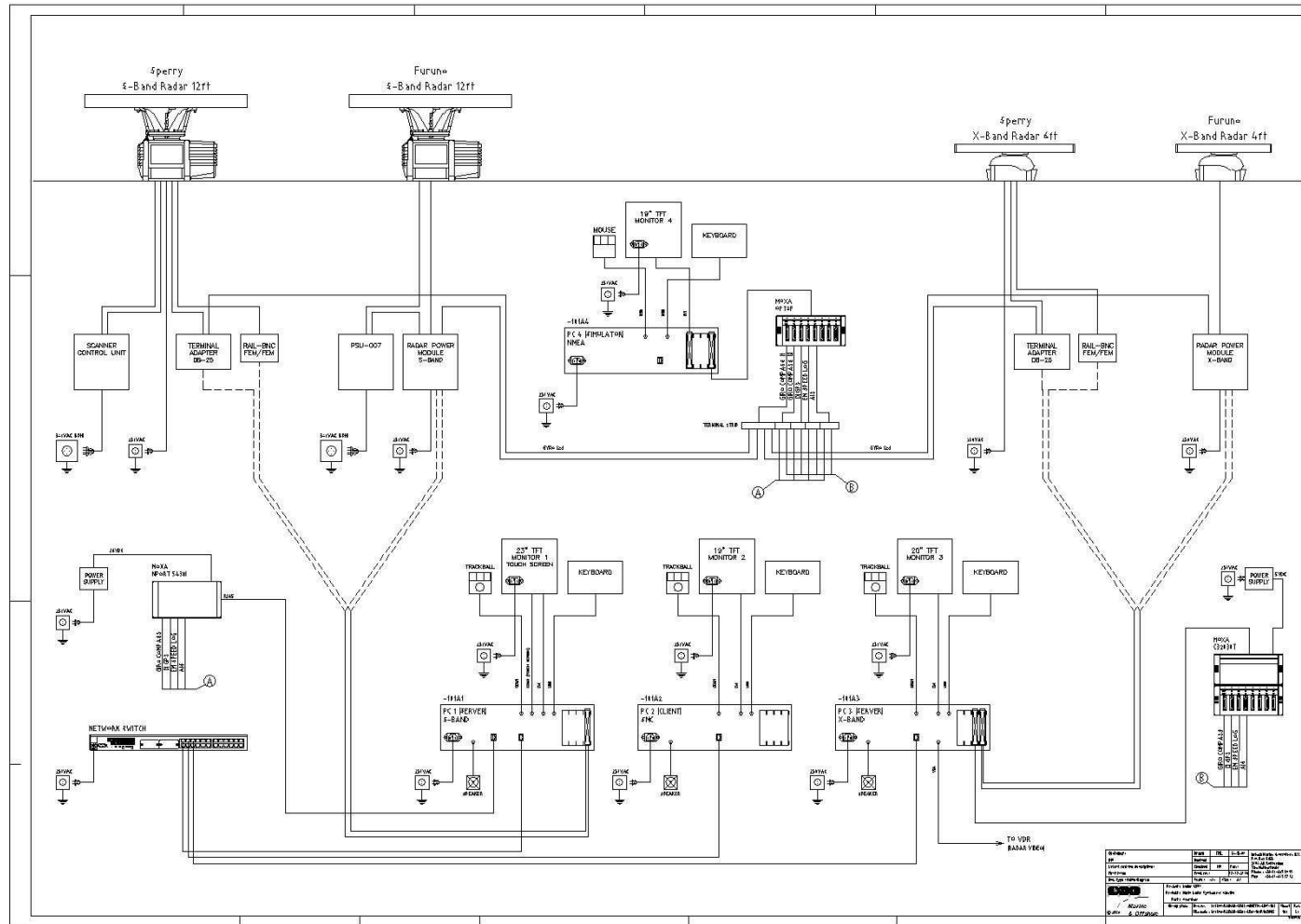
Component	Id	Failure mode	Failure Cause	P	SC	DP	Failure Effect and End Effect	Failure Detection	Remarks
5. PC	16	Incorrect azimuth signal	Signal failure				Server commands scanner to stop turning and to stop transceiving Scanner stops turning Scanner stops transceiving	No Radar video, Alarm no azimuth signal	Different probability for Furuno, and Sperry, as an extra component(Radar power module) is present for Furuno Larger probability for Furuno?
			Connection failure						
	17	PC1 incorrect Gyro signal	Signal failure				No heading shall be shown, North Up shall not be possible	Alarm gyro failure	If signal is delayed w.r.t. other sensors, an alarm is advisable/ time synchronization
			Connection failure						
	18	PC1 incorrect (D)GPS signal	Signal failure				No GPS available → no Chart underlay possible	Alarm (D)GPS failure	If signal is delayed w.r.t. other sensors, an alarm is advisable/time synchronization
			Connection failure						
	19	PC1 incorrect EM Speed Log signal	Signal failure				No EM Speed log available → Sea stabilized mode not possible	Alarm EM Speed log	If signal is delayed w.r.t. other sensors, an alarm is advisable
			Connection failure						
	20	PC1 incorrect AIS signal	Signal failure				No AIS signals available → no AIS information request is possible	Alarm AIS failure	If signal is delayed w.r.t. other sensors, an alarm is advisable
			Connection failure						
	21	PC2 incorrect gyro signal	Signal failure				No heading shall be shown, North Up shall not be possible	Alarm gyro failure	If signal is delayed w.r.t. other sensors, an alarm is advisable/ time synchronization
			Connection failure						
	22	PC2 incorrect (D) GPS signal	Signal failure				No GPS available → no Chart underlay possible	Alarm (D)GPS failure	If signal is delayed w.r.t. other sensors, an alarm is advisable/ time synchronization
			Connection failure						
23	PC2 incorrect EM Speed Log	Signal failure				No EM Speed log available → Sea stabilized mode not possible	Alarm EM Speed Log failure	If signal is delayed w.r.t. other sensors, an alarm is advisable/ time synchronization	
		Connection failure							Automatic switch-over to other sensor if alternative is available

Component	Id	Failure mode	Failure Cause	P	SC	DP	Failure Effect and End Effect	Failure Detection	Remarks
5. PC	24	PC2 incorrect AIS signal	Signal failure				No AIS signals available → no AIS information request is possible	Alarm AIS failure	If signal is delayed w.r.t. other sensors, an alarm is advisable/ time synchronization
			Connection failure				Automatic switch-over to other sensor if alternative is available	Alarm AIS + extra info w.r.t. connection	
	25	PC3 incorrect Gyro signal	Signal failure				No Heading shall be shown, North Up shall not be possible	Alarm Gyro failure	If signal is delayed w.r.t. other sensors, an alarm is advisable/ time synchronization
			Connection failure				Automatic switch-over to other sensor if alternative is available	Alarm Gyro + extra info w.r.t. connection	
	26	PC3 incorrect (D)GPS signal	Signal failure				No GPS available → No chart underlay possible	Alarm (D)GPS failure	If signal is delayed w.r.t. other sensors, an alarm is advisable/ time synchronization
			Connection failure				Automatic switch-over to other sensor if alternative is available	Alarm (D)GPS + extra info w.r.t. connection	
	27	PC3 incorrect EM Speed Log signal	Signal failure				No EM Speed Log available → Sea stabilized mode not possible	Alarm EM Speed Log failure	If signal is delayed w.r.t. other sensors, an alarm is advisable/ time synchronization
			Connection failure				Automatic switch-over to other sensor if alternative is available	Alarm EM Speed Log + extra info w.r.t. connection	
	28	PC3 incorrect AIS signal	Signal failure				No AIS signals available → no AIS information request is possible		If signal is delayed w.r.t. other sensors, an alarm is advisable/ time synchronization
			Connection failure				Automatic switch-over to other sensor if alternative is available		
	29	PC1 all NMEA (Moxa) signals lost(except direct gyro)	Electro/mechanical failure				Automatic switch-over to other NMEA signals(Moxa N-port)	Alarm all NMEA signals via Moxa	If signal is delayed w.r.t. other sensors, an alarm is advisable/time synchronization
	30	PC2 All NMEA (Moxa) Lost (except direct gyro)	Electro/mechanical failure				Automatic switch-over to other NMEA signals	Alarm for all these NMEA signals	If signal is delayed w.r.t. other sensors, an alarm is advisable/time synchronization
PC1 failure			Alarm for all these NMEA signals , Alarm link PC1 <-> PC2 Alarm link PC1 <-> PC3						
31	PC3 all NMEA (Moxa) lost (except direct gyro)	Electro/mechanical failure				Switch over to NMEA signals via Moxa Nport if applicable	Alarm for all these NMEA signals	If signal is delayed w.r.t. other sensors, an alarm is advisable/time synchronization	
		PC1 failure				Alarm for all these NMEA signals, Alarm link PC1 <-> PC2 Alarm link PC1 <-> PC3			

Component	Id	Failure mode	Failure Cause	P	SC	DP	Failure Effect and End Effect	Failure Detection	Remarks
5. PC	32	PC1 all NMEA (Moxa N-port) lost (except direct gyro)	Electro/mechanical failure				Switch over to NMEA signals via Moxa if applicable	Alarm for all these NMEA signals	
			Power failure						
			PC 3 failure						
	33	PC2 all NMEA (Moxa N-port) lost (except direct gyro)	Electro/mechanical failure				Switch over to NMEA signals via Moxa N-port if applicable.	Alarms for all these NMEA signals Alarm link PC3 <-> PC1 Alarm link PC3 <-> PC2	
			Power failure						
			PC 3 failure						
	34	PC3 all NMEA (Moxa N-port) lost (except direct gyro)	Electro/mechanical failure				Automatic switch over to other NMEA signals	Alarms for all these NMEA signals	
Power failure									
35	PC1 Loss of network connection	Connection failure				No connection with PC2 and PC3 → No NMEA data, via Moxa,	At PC2 and PC3: Alarm link PC1 <-> PC2 Alarm link PC1 <-> PC3		
36	PC2 Loss of network connection	Connection failure				No connection with PC1 and PC3	At PC1 and PC3: Alarm link PC2 <-> PC1 Alarm link PC2 <-> PC3		
37	PC3 Loss of network connection	Connection failure				No connection with PC1 and PC2	At PC1 and PC2: Alarm link PC3 <-> PC1 Alarm link PC3 <-> PC2		
38	Loss of connection PC1, PC2, PC3	Network overload				No connections between the PCs	Alarm link PC1 <-> PC2 Alarm link PC2 <-> PC3 Alarm link PC1 <-> PC3		
		Network switch failure							
6.Trackerball	39	Tracker ball failure	Electro/mechanical failure				Operator commands through the display no longer possible	No proper response on the display when using the tracker ball.	

Software functions	Id	Failure mode	Failure Cause	P	SC	DP	Failure Effect and End Effect	Failure Detection	Remarks
1. Time synchronization	1	Incorrect synchronization	<>				No connections between the PCs	<>	
			<>						

Appendix B: Block Diagram of Reference System



Revizija	Revizija	Revizija	Revizija
01	02	03	04
01	02	03	04
01	02	03	04
01	02	03	04

Attack Tree



Appendix F – Confidential supporting information Safety Critical System. HARA, TARA, GSN and ADT

Automotive HARA

Vehicle Use	Operational Situation Description	Exposure - Duration		Exposure - Frequency		General Comments
		Rationale	Ranking	Rationale	Ranking	
Post crash	Vehicle involved in an accident, post crash scenario, first responders present			Assumed to occur less often than once a year for the great majority of drivers	E1	
	Vehicle involved in an accident, post crash scenario			Assumed to occur less often than once a year for the great majority of drivers	E1	

Function Tab ID	CoC	Assumption ID	Hazardous events ID	Assumption	Controllability ranking affected?	Domain	CoC Name & Title	FuSa engineer (Tech Review Lead)	Comments	Date of Comment
F.31	OTA	F_31_A1	N/A	Assumption: Incomplete Firmware Update is assumed subset of Incorrect Firmware update. As Incomplete task will not change current version to requested version and it will create firmware version mismatch fault code. This fault code will be mitigated by the same mitigation strategy with incorrect firmware update.	No	Core Systems Telematics	Lead Engineer	System Owner	Approved	09/07/2020
F.31	OTA	F_31_A2	N/A	Assumption: An OTA update is designed to occur while stationary while Parked with user content in Standby Power Mode	No	Core Systems Telematics	Lead Scientist	System Owner	Approved	15/07/2020

ASIL Analysis

Risk Assessment - F.11 - Passive safety

Vehicle Level FuSa Function	Hazard Name	Operational Situation(s)	Hazardous Event	Potential Harm	ID	Clarifications	FF ID	Functional failures	External Mitigation (e.g. driver action or observation or other vehicle systems)	S	E	C	ASIL	Rating Explanation / Justification	Safety Goals Traceability
F.11 PASSIVE SAFETY	H11.1 Driver subject to exacerbated injuries	Collision (front) with another vehicle or infrastructure	H11.1 Driver subject to exacerbated injuries whilst collision (front) with another vehicle or infrastructure	Driver impacts steering wheel during collision. Could result in broken nose or head severe injury	H.11.1.1	Latent fault where the airbag does not deploy when expected if the conditions are met	F.11_Interior_2.1 F.11_Interior_2.4 F.11_Interior_2.7	(due to lack of airbags activation) (due to insufficient airbag activation) (due to late airbag activation)		S3	E1	C3	A	S - Lack, late or insufficient deployment could exacerbate injuries (assumed worst case life threatening spinal injuries or head injury as a result). E - Actual scenario of a collision is likely to be less than once a year (by frequency). C - Uncontrollable and unexpected by the driver (taking into consideration only the failure of the airbag and not controllability of the original collision)	SG11.1
	H11.1 Driver subject to exacerbated injuries	Collision (side) from another vehicle or infrastructure	H11.1 Driver subject to exacerbated injuries whilst collision (side) from another vehicle or infrastructure	Driver has a side shock which could cause injury to the person's neck, head, chest, legs, or abdomen/pelvis.	H.11.1.2	Latent fault where the airbag does not deploy when expected if the conditions are met	F.11_Interior_2.1 F.11_Interior_2.4 F.11_Interior_2.7	(due to lack of airbags activation) (due to insufficient airbag activation) (due to late airbag activation)		S3	E1	C3	A	S - Lack, late or insufficient deployment could exacerbate injuries (assumed worst case life threatening spinal injuries or head injury as a result). E - Actual scenario of a collision is likely to be less than once a year (by frequency). C - Uncontrollable and unexpected by the driver (taking into consideration only the failure of the airbag and not controllability of the original collision)	SG11.1
	H11.1 Driver subject to exacerbated injuries	Collision (front) from another vehicle or infrastructure	H11.1 Driver subject to exacerbated injuries whilst collision (front) from another vehicle or infrastructure	The lack of a pre-tensioner removes the potential to reduce any injury caused during collision by a poorly positioned driver In severe crashes, when a car collides with an obstacle at high speed, the lack of a load limiter removes the potential to reduce any injury caused by the driver seatbelt.	H.11.1.3	At this point the assumption is being made that airbags cannot be used as an external mitigation to lack of pre-tensioners due to the control being from the same ECU.	F.11_Interior_3.1 F.11_Interior_5.1	(due to lack of pre-tensioners activation) (due to lack of load limiters activation)		S1	E1	C3	QM	S - Pre-tensioners can reduce and prevent severe injuries, non deployment does not allow for injury prevention E - Actual scenario of a collision is likely to be less than once a year (by frequency). C - Uncontrollable and unexpected by the driver (taking into consideration only the failure of the pre-tensioner and not controllability of the original collision)	N/A
	H11.2 Occupants subject to exacerbated injuries	Collision (front) with another vehicle or infrastructure	H11.2 Occupants subject to exacerbated injuries whilst collision (front) with another vehicle or infrastructure	Passenger hits dashboard/coast to coast screen during collision. Could result in broken nose or head severe injury	H.11.2.1	Latent fault where the airbag does not deploy when expected if the conditions are met, or they do not operate in the design intent and prevent harm	F.11_Interior_2.1 F.11_Interior_2.4 F.11_Interior_2.7	(due to lack of airbags activation) (due to insufficient airbag activation) (due to late airbag activation)		S3	E1	C3	A	S - Lack, late or insufficient deployment could exacerbate injuries (assumed worst case life threatening spinal injuries or head injury as a result). E - Actual scenario of a collision is likely to be less than once a year (by frequency). C - Uncontrollable and unexpected by the passenger (taking into consideration only the failure of the airbag, not driver's ability to avoid collision)	SG11.1
	H11.2 Occupants subject to exacerbated injuries	Collision (side) from another vehicle or infrastructure	H11.2 Occupants subject to exacerbated injuries whilst collision (side) from another vehicle or infrastructure	Passenger has a side shock which could cause injury to the person's neck, head, chest, legs, or abdomen/pelvis.	H.11.2.2	Latent fault where the airbag does not deploy when expected if the conditions are met, or they do not operate in the design intent and prevent harm	F.11_Interior_2.1 F.11_Interior_2.4 F.11_Interior_2.7	(due to lack of airbags activation) (due to insufficient airbag activation) (due to late airbag activation)		S3	E1	C3	A	S - Lack, late or insufficient deployment could exacerbate injuries (assumed worst case life threatening spinal injuries or head injury as a result). E - Actual scenario of a collision is likely to be less than once a year (by frequency). C - Uncontrollable and unexpected by the driver (taking into consideration only the failure of the airbag, not driver's ability to avoid collision)	SG11.1
	H11.2 Occupants subject to exacerbated injuries	Collision (front) with another vehicle or infrastructure	H11.2 Occupants subject to exacerbated injuries whilst collision (front) with another vehicle or infrastructure	The lack of a pre-tensioner removes the potential to reduce any injury caused during collision by a poorly positioned passenger In severe crashes, when a car collides with an obstacle at high speed, the lack of a load limiter removes the potential to reduce any injury caused by the passenger seatbelt.	H.11.2.3	At this point the assumption is being made that airbags cannot be used as an external mitigation to lack of pre-tensioners due to the control being from the same ECU.	F.11_Interior_3.1 F.11_Interior_5.1	(due to lack of pre-tensioners activation) (due to lack of load limiters activation)		S1	E1	C3	QM	S - Pre-tensioners can reduce and prevent severe injuries, non deployment does not allow for injury prevention E - Actual scenario of a collision is likely to be less than once a year (by frequency). C - Uncontrollable and unexpected by the occupant	N/A
	H11.2 Occupants subject to exacerbated injuries	Collision (front) with another vehicle or infrastructure	H11.2 Occupants subject to exacerbated injuries whilst collision (front) with another vehicle or infrastructure	A childseat with a child inside is put to the front passenger seat. The airbag should be disabled but it is not. OR it is enabled back undemandably. The airbag deploys when the vehicle has been involved in a crash. Could result in severe injury.	H.11.2.4	In the Chinese and European market front passenger airbag disabling is done by the driver manually via a hard switch. In the US and Canadian market it is done automatically.	F.11_Interior_4.1 F.11_Interior_4.2	(due to lack of front passenger airbag disabling) (due to undemanded front passenger airbag enabling)		S3	E1	C3	A	S - Lack, late or incorrect deployment could exacerbate injuries (assumed worst case life threatening spinal injuries or head injury as a result). E - Actual scenario of a collision is likely to be less than once a year (by frequency). C - Uncontrollable and unexpected	SG11.11 SG11.12
	H11.2 Occupants subject to exacerbated injuries	Collision (front) with another vehicle or infrastructure	H11.2 Occupants subject to exacerbated injuries whilst collision (front) with another vehicle or infrastructure	An adult sitting on the front passenger seat. The driver thinks that he/she enabled the airbag by pressing the button, but it hasn't been enabled OR it is disabled back undemandably. The airbag doesn't deploy when the vehicle has been involved in a crash. Passenger hits dashboard/coast to coast screen during collision. Could result in broken nose or head severe injury	H.11.2.5	In the Chinese and European market front passenger airbag enabling is done by the driver manually via a hard switch. In the US and Canadian market it is done automatically.	F.11_Interior_4.1 F.11_Interior_4.2	(due to lack of front passenger airbag enabling) (due to undemanded front passenger airbag disabling)		S3	E1	C3	A	S - Lack, late or incorrect deployment could exacerbate injuries (assumed worst case life threatening spinal injuries or head injury as a result). E - Actual scenario of a collision is likely to be less than once a year (by frequency). C - Uncontrollable and unexpected by the occupant	SG11.1
	H11.3 Vehicle path deviation	All driving scenarios	H11.3 Vehicle path deviation whilst all driving scenarios	Driver, occupants or other road users subject to possibly high speed impact	H.11.3.1	Driver temporarily stunned and hands pushed off the steering wheel	F.11_Interior_2.2	(due to undemanded driver airbags activation)		S3	E4	C3	D	S - worst case would result in collision with other vehicles or infrastructure and may be fatal E - Could happen during any driving scenario (by frequency) C - Uncontrollable by the driver, they can try to brake but are not aware of the vehicle surroundings due to lack of road visibility.	SG11.5a
	H11.2 Occupants subject to exacerbated injuries	All driving scenarios	H11.2 Occupants subject to exacerbated injuries whilst all driving scenarios	Pre-tensioner merely tightens the seatbelt across the occupants lap, no injury expected	H.11.2.6		F.11_Interior_3.2	(due to undemanded pre-tensioner activation)		S0	E4	C2	NA	S - No injuries expected E - Could happen during any driving scenario (by frequency) C - 90% of people are expected to maintain control of the vehicle	N/A
	H11.4 Emergency service/maintenance personnel injury	Maintenance	H11.4 Emergency service/maintenance personnel injury whilst maintenance	Limbs caught by very fast moving seatbelt mechanism, light injury to hand	H.11.4.1		F.11_Interior_3.2	(due to undemanded pre-tensioner activation)		S1	E3	C2	QM	S - Could cause injury to hands if holding the seatbelt when it is triggered E - E3 as maintenance technician not expected to be in vicinity of pre-tensioner more than a few times per month C - Maintenance personnel familiar with working procedures established to mitigate unintended firing of airbags and pre-tensioners	N/A
	H11.4 Emergency service/maintenance personnel injury	Response post-crash or maintenance	H11.4 Emergency service/maintenance personnel injury whilst response post-crash or maintenance	Side curtain airbag deploys undemandably or late after the impact	H.11.4.2		F.11_Interior_2.2	(due to undemanded airbag activation)		S2	E3	C3	B	S - Could cause serious injury but probably not fatal E - E3 as first responder/maintenance technician not expected to be in vicinity of airbag more than a few times per month C - Uncontrollable (without adding procedural mechanisms)	SG11.5c
	H11.4 Emergency service/maintenance personnel injury	Response post-crash or maintenance	H11.4 Emergency service/maintenance personnel injury whilst response post-crash or maintenance	Airbag deploys undemandably or late due to partial deployment in an impact	H.11.4.3		F.11_Interior_2.2 F.11_Interior_2.11	(due to undemanded airbag activation) (due to partial airbag activation)		S2	E3	C3	B	S - Could cause serious injury but probably not fatal E - E3 as first responder/maintenance technician not expected to be in vicinity of airbag more than a few times per month C - Uncontrollable (without adding procedural mechanisms)	SG11.8
	H11.2 Occupants subject to exacerbated injuries	All driving scenarios	H11.2 Occupants subject to exacerbated injuries whilst all driving scenarios	Small child on a passenger seat and impacted by the airbag	H.11.2.7		F.11_Interior_2.2	(due to undemanded airbags activation)		S3	E4	C3	D	S - Injury could be fatal for a small child in a car seat E - Could occur undemanded in any drive cycle with worst case being E4 (by frequency) C - Uncontrollable and unexpected by the occupants with potentially fatal impact	SG11.6
	H11.2 Occupants subject to exacerbated injuries	All driving scenarios	H11.2 Occupants subject to exacerbated injuries whilst all driving scenarios	Front passenger could be injured by the frontal airbag going off, could cause minor injury not fatal	H.11.2.8		F.11_Interior_2.2	(due to undemanded airbags activation)		S1	E4	C3	B	S - Minor injuries if the passenger was jolted, may depend upon their position when the airbag goes off. E - Could occur undemanded in any drive cycle with worst case being E4 (by frequency) C - Uncontrollable and unexpected by the occupants.	SG11.6
	H11.2 Occupants subject to exacerbated injuries	All driving scenarios	H11.2 Occupants subject to exacerbated injuries whilst all driving scenarios	Occupants could be injured by the side curtain airbag going off, could cause minor injury not fatal	H.11.2.9		F.11_Interior_2.2	(due to undemanded airbags activation)		S1	E4	C3	B	S - Minor injuries if the passenger was jolted, may depend upon their position when the airbag goes off. E - Could occur undemanded in any drive cycle with worst case being E4 (by frequency) C - Uncontrollable and unexpected by the occupants.	SG11.5c
	H11.5 Driver misinformed	Collision (one or more occupants not restrained by seatbelt)	H11.5 Driver misinformed whilst collision (one or more occupants not restrained by seatbelt)	Occupant could be thrown from seat due to lack of seatbelt	H.11.5.1	One or more occupants not restrained by seatbelt	F.11_Interior_1.1	(due to lack of seatbelt warning)		S3	E1	C0	NA	S - Could possibly be fatal with the occupant being thrown from their seat E - Actual scenario of a collision is likely to be less than once a year (by frequency) C - FMVSS 208 requires seatbelt buckle warning to be provided. CO assigned in accordance with ISO26262 Ed.1 Part 3, clause 7.4.3.8	N/A
	H11.6 Driver, occupants injury subject to exacerbated injuries	Vehicle braking	H11.6 Driver, occupants injury subject to exacerbated injuries whilst vehicle braking	Driver, occupants or other road users subject to possibly high speed impact due to driver falling to brake as his/her leg is pushed away from brake pedal	H.11.6.1	Driver feet pushed away from brake and accelerator pedals	F.11_Interior_2.2	(due to undemanded knee airbag activation)		S3	E4	C3	D	S - worst case would result in collision with other vehicles, infrastructure or pedestrians/cyclists and may be fatal E - Could happen during any driving scenario including deceleration C - Driver not expected to regain longitudinal control in sufficient time to avoid collision, but may be able to steer around an object if not overly distracted by the deployed KAB.	SG11.6
	H11.6 Driver, occupants injury subject to exacerbated injuries	Collision (front) from another vehicle or infrastructure	H11.6 Driver, occupants injury subject to exacerbated injuries whilst collision (front) from another vehicle or infrastructure	Driver or passenger is injured due to second stage airbag deployment when conditions were just for stage 1 deployment.	H.11.6.2		F.11_Interior_2.10	(due to excessive airbag activation stage 1 and stage 2, when conditions where just for stage 1)		S3	E1	C3	A	S - Stage 2 deployed in addition to stage 1 for a driver/passenger that is of little weight/size deployment could exacerbate injuries (assumed worst case life threatening injuries) E - Actual scenario of a collision is likely to be less than once a year (by frequency). C - Uncontrollable by the driver or occupant	SG11.2

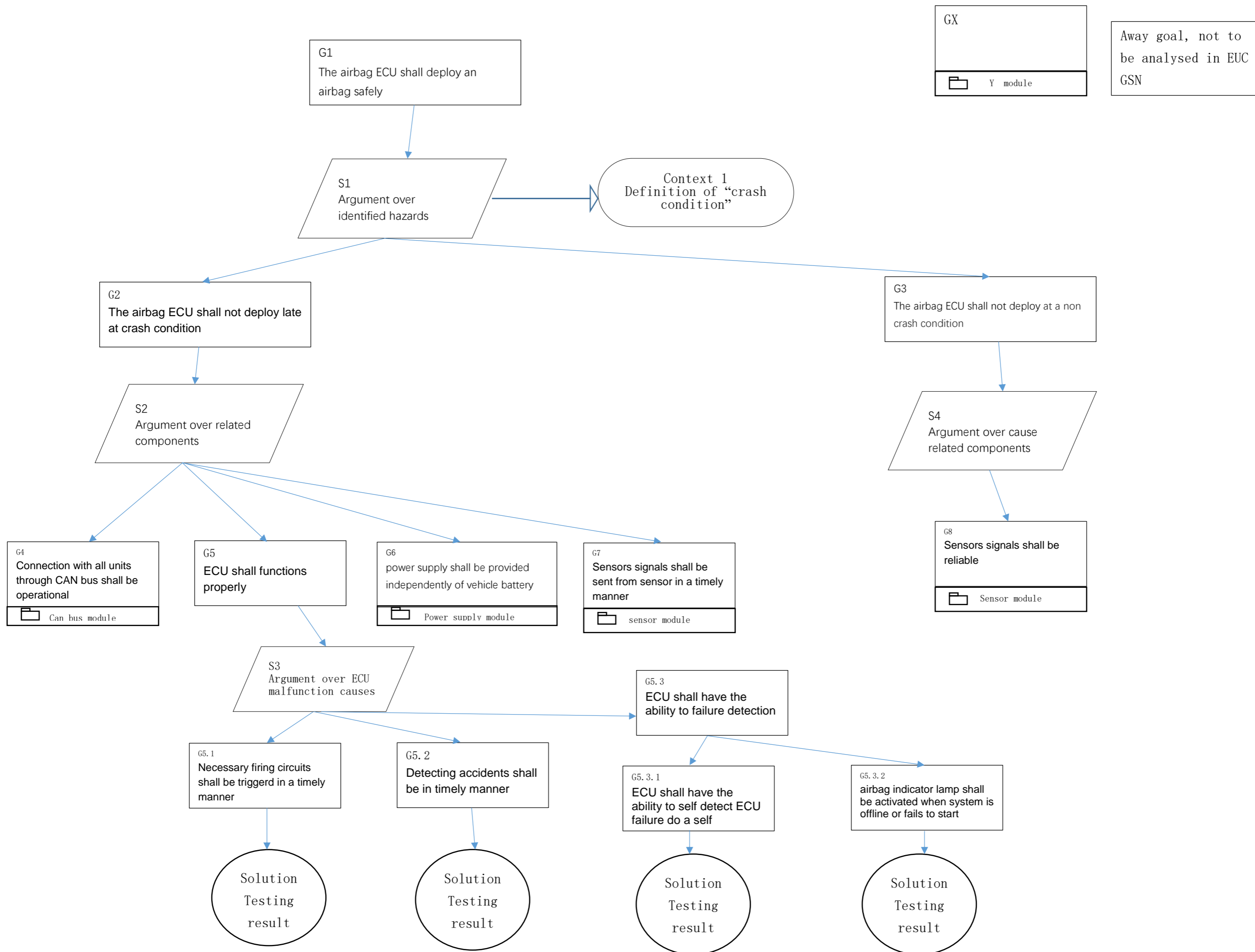
Risk Assessment - F.31 - OTA UPDATE

Vehicle Level FuSa Function	Hazard Name	Operational Situation(s)	Hazardous Event	Potential Harm	ID	Clarifications	FF ID	Functional failures	External Mitigation (e.g. driver action or observation or other vehicle systems)	S	E	C	ASIL	Ratings Explanation / Justification	Safety Goals Traceability
F.31 OTA update F.31_OTA_1 Provide Firmware update orchestration	H31.1 - Impaired driver visibility H31.2 - Driver distraction H31.3 - Driver misinformed H31.4 - Incorrect or lack of information/ warning to other road users H31.5 - Driver/occupants subject to exacerbated injuries (no airbags) H31.6 - Loss of drive H31.7 - Reduced Deceleration H31.8 - Undemanded Deceleration H31.9 - Vehicle path deviation H31.10 - Vehicle roll-away H31.14 - Rapid release of energy H31.21 - Restricted ingress/egress of the vehicle	Vehicle driving on a motorway or dual carriageway with central reservation	H31.1 - Impaired driver visibility H31.2 - Driver distraction H31.3 - Driver misinformed H31.4 - Incorrect or lack of information/ warning to other road users H31.5 - Driver/occupants subject to exacerbated injuries (no airbags) H31.6 - Loss of drive H31.7 - Reduced Deceleration H31.8 - Undemanded Deceleration H31.9 - Vehicle path deviation H31.10 - Vehicle roll-away H31.14 - Rapid release of energy H31.21 - Restricted ingress/egress of the vehicle whilst vehicle driving on a motorway or dual carriageway with central reservation	A loss of modules could lead to loss of propulsion, braking, steering, etc	Hz.31.1.1		F.31_OTA_1.1	(due to undemanded OTA Firmware update)		S3	E4	C3	D	S - Collision with oncoming traffic or pedestrian or off-road infrastructure at medium/high speeds E - Any driving scenario C - There is potentially no controllability from the driver if the modules reset	SG31.1
	H31.1 - Impaired driver visibility H31.6 - Loss of drive H31.8 - Undemanded deceleration H31.10 - Vehicle roll-away H31.11 - Incorrect direction of movement H31.12 - Vehicle Thermal Event or rapid release of energy H31.13 - Burns H31.14 - Rapid release of energy H31.15 - Vehicle stranded H31.16 - Insufficient acceleration H31.17 - Excessive acceleration H31.18 - Undemanded acceleration H31.9 - Vehicle path deviation H31.20 - Limb entrapment H31.21 - Restricted ingress/egress of the vehicle H31.22 - Occupant/emergency service/maintenance personnel injury H31.23 - Compressed air provided under too much pressure H31.24 - Crushing injury	Vehicle stationary and transitioning into drive for the vehicle's first drive cycle	H31.1 - Impaired driver visibility H31.6 - Loss of drive H31.8 - Undemanded deceleration H31.10 - Vehicle roll-away H31.11 - Incorrect direction of movement H31.12 - Vehicle Thermal Event or rapid release of energy H31.13 - Burns H31.14 - Rapid release of energy H31.15 - Vehicle stranded H31.16 - Insufficient acceleration H31.17 - Excessive acceleration H31.18 - Undemanded acceleration H31.9 - Vehicle path deviation H31.20 - Limb entrapment H31.21 - Restricted ingress/egress of the vehicle H31.22 - Occupant/emergency service/maintenance personnel injury H31.23 - Compressed air provided under too much pressure H31.24 - Crushing injury whilst vehicle stationary and transitioning into drive for the vehicle's first drive cycle	Incorrect software across the modules could lead to undemanded or incorrect propulsion, braking, steering, etc	Hz.31.1.2		F.31_OTA_1.10	(due to incorrect OTA Firmware update) (due to incomplete OTA Firmware update)		S3	E3	C3	C	S - Collision with oncoming traffic or pedestrian or off-road infrastructure at medium/high speeds E - By duration, OTA updates could occur between 1-10% of the vehicle life C - There is potentially no controllability from the driver if the modules' software is incorrect	SG31.2

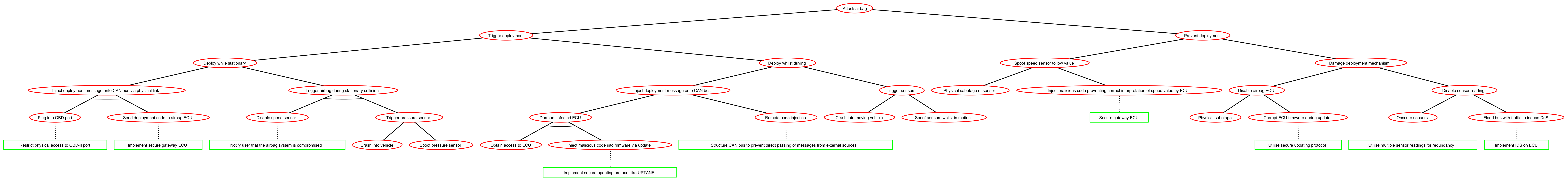
Vehicle Safety Goals

SG No.	Safety Goal	ASIL	Safety Goals Violations	Safe state	Notes	JAMA ID
VEHICLE OCCUPANT SAFETY						
SG11.1	The Rivian vehicle shall avoid exacerbated injuries to the vehicle occupants due to lack of activation of airbags in the event of vehicle collision	A	(due to lack of airbags activation) (due to insufficient airbag activation) (due to late airbag activation) (due to lack of front passenger airbag enabling) (due to undemanded front passenger airbag disabling) (due to excessive LV from the DC/DC converter) (due to loss of LV from the DC/DC converter) (due to Incorrect prioritisation of HV power budget) (due to excessive heating of the DC/DC converter) (due to insufficient cooling of the DC/DC converter) (due to excessive cooling of the HV Battery) (due to excessive heating of the HV Battery) (due to insufficient cooling of the HV Battery) (due to insufficient heating of the HV Battery)		This SG covers functional failures from F.17 - Energy Management	
SG11.2	The Rivian vehicle shall avoid exacerbated injuries to the vehicle occupants due to incorrect activation of airbags in the event of vehicle collision	A	(due to excessive airbag activation stage 1 and stage 2 , when conditions where just for stage 1)			
SG11.5a	The Rivian vehicle shall avoid vehicle path deviation (>0.35m)due to undemanded driver airbag activation	D	(due to undemanded driver airbags activation) (due to excessive LV from the DC/DC converter)		This SG covers functional failures from F.17 - Energy Management	
SG11.5c	The Rivian vehicle shall avoid injury to vehicle occupants or service personnel due to undemanded side curtain airbag activation	B	(due to undemanded airbags activation) (due to excessive LV from the DC/DC converter)		This SG covers functional failures from F.17 - Energy Management	
SG11.6	The Rivian vehicle shall avoid injury to vehicle occupants due to undemanded frontal airbag activation	D	(due to undemanded airbags activation) (due to excessive LV from the DC/DC converter)		In FTA consider 1st and 2nd stage deployment (partial), with the 2nd stage also being late This SG covers functional failures from F.17 - Energy Management	
SG11.8	The Rivian vehicle shall avoid impact or laceration injuries to service personnel due to post-collision airbag activation	B	(due to undemanded airbag activation) (due to partial airbag activation) (due to excessive LV from the DC/DC converter)		Airbag deploys undemandedly or late due to partial deployment in an impact This SG covers functional failures from F.17 - Energy Management	
SG11.11	The Rivian vehicle shall avoid exacerbated injuries to the vehicle occupants due to lack of front passenger airbag disabling in the event of vehicle collision	A	(due to lack of front passenger airbag disabling) (due to undemanded front passenger airbag enabling) (due to loss of LV from the DC/DC converter) (due to Incorrect prioritisation of HV power budget)		This SG covers functional failures from F.17 - Energy Management	
SG11.12	The Rivian vehicle shall avoid exacerbated injuries to the vehicle occupants due to undemanded front passenger airbag enabling in the event of vehicle collision	A	(due to lack of front passenger airbag disabling) (due to undemanded front passenger airbag enabling) (due to excessive LV from the DC/DC converter)		This SG covers functional failures from F.17 - Energy Management	
VEHICLE SECURITY						
SG12.1	Not used				This SG is covered by SG5.06, so functional failure (undemanded immobiliser function enablement) has been transferred to SG5.06, as being mostly done in propulsion.	
SG12.2	Not used					
SG12.3	Not used				This SG has been removed due to steering column lock being removed as a function for the R1 vehicle.	
F.31 - OTA UPDATE						
SG31.1	The Rivian vehicle shall avoid vehicle level hazards due to an undemanded OTA firmware update	D**	(due to undemanded OTA Firmware update)		**Note that the highest ASIL rating for OTA for each feature shall be the highest ASIL rating of that specific feature. For example, if the Wiper function is ASIL A, then this OTA Safety Goal for Wipers should be ASIL A.	
SG31.2	The Rivian vehicle shall avoid vehicle level hazards due to an incorrect/incomplete OTA firmware update	C**	(due to incorrect OTA Firmware update) (due to incomplete OTA Firmware update)		**Note that the highest ASIL rating for OTA for each feature shall be the highest ASIL rating of that specific feature, not to exceed ASIL C. For example, if the Wiper function is ASIL A, then this OTA Safety Goal for Wipers should be ASIL A. Another example, if the Steering function is ASIL D, then this OTA Safety Goal for Steering should be ASIL C.	

GSN Safety Case



Attack-Defence Tree



Appendix G – Ethics Certificate



Certificate of Ethical Approval

Applicant: Luis-Pedro Cobos Yelavives
Project Title: Dependability Assurance for Connected and Automated Vehicles

This is to certify that the above named applicant has completed the Coventry University Ethical Approval process and their project has been confirmed and approved as Low Risk

Date of approval: 21 Oct 2020
Project Reference Number: P112203

Appendix H – Copyright and permission of co-authors on paper content

CONSENT TO PUBLISH and COPYRIGHT TRANSFER

For the mutual benefit and protection of Authors and Publishers, it is necessary that Authors provide formal written Consent to Publish and Transfer of Copyright before publication of the Book. The signed Consent ensures that the publisher has the Author's authorization to publish the Contribution.

Conference: **VEHITS 2021 - 7th International Conference on Vehicle Technology and Intelligent Transport Systems.**

Place/Date: **Online; 28 - 30 April, 2021.**

Book Title: **Proceedings of the 7th International Conference on Vehicle Technology and Intelligent Transport Systems.**

Edited by: **Karsten Berns, Markus Helfert and Oleg Gusikhin.**

Publisher: **SCITEPRESS.**

Paper number: **79.**

Title of the contribution: **Requirements for a Cybersecurity Case Approach for the Assurance of Future Connected and Automated Vehicles.**

Author (name and address):

Luis Pedro Cobos.

United Kingdom.

It is herein agreed that:

The copyright to the contribution identified above is transferred from the Author to the "Science and Technology Publications, Lda" (here forth known as SCITEPRESS).

The copyright transfer covers the exclusive, sole, permanent, world-wide, transferable, sub licensable and unlimited right to reproduce, publish, transmit, archive, lease/lend, sell and distribute the contribution or parts thereof individually or together with other works in any language, revision and version (digital and hard), including reprints, translations, photographic reproductions, microform, audiograms, videograms, electronic form (offline, online), or any other reproductions of similar nature, including publication in the aforementioned book or any other book, as well as, the usage for advertising purposes. SCITEPRESS is also entitled to carry out editorial changes in the contribution with the sole purpose of enhancing the overall organization and form of the contribution. The Author retains the rights to publish the contribution in his/her own web site and thesis, in his/her employer's web site and to publish a substantially revised version (at least 30% new material) elsewhere, as long as it is clearly stated that the contribution was presented at VEHITS 2021, a link to the event web site is made available there and also the presence of the corresponding DOI number. Prior versions of the contribution published on non-commercial pre-print servers like ArXiv/CoRR and HAL can remain on these servers and/or can be updated with Author's accepted version. The final published version (in pdf) cannot be used for this purpose. The Creative Commons license CC BY-NC-ND applies to everyone that wishes to use the published version.

The Author warrants that his/her contribution is original, except for such excerpts from copyrighted works as may be included with the permission of the copyright holder and author thereof, that it contains no libelous statements, and does not infringe on any copyright, trademark, patent, statutory right, or propriety right of others; and that Author will indemnify SCITEPRESS against any costs, expenses or damages for which SCITEPRESS may become liable as a result of any breach of this warranty. The Author signs for and accepts responsibility for releasing this material on behalf of any and all co-authors.

This agreement shall be governed by, and shall be construed in accordance with, the laws of Portugal. The courts of Portugal shall have the exclusive jurisdiction.

In return for these rights:

The publisher agrees to have the identified contribution published, at its own cost and expense, in the event proceedings.

The undersigned hereby gives permission to SCITEPRESS to have the above contribution published.

Date: **04 March, 2021**

Author's Signature:

Luis Pedro Cobos

ASSIGNMENT OF COPYRIGHT

The transfer of copyright from author to the Organizing Committee of the "31st European Safety and Reliability Conference (ESREL2021)" must be clearly stated in writing to enable the Organizers, Editors and Publisher to assure maximum dissemination of the author's work. Therefore, the following assignment of copyright, executed and signed by the author, is required with each manuscript submission. If the article is a "work made for hire" it must be signed by the employer. To the extent transferable, copyright in and to the undersigned Author's Article ("Article") entitled


CYBERSECURITY ASSURANCE CHALLENGES FOR FUTURE CONNECTED AND AUTOMATED VEHICLES

by

Luis Pedro Cobos, Alastair Ruddle and Giedre Sabaliauskaite

submitted to the "31st European Safety and Reliability Conference (ESREL2021)" is hereby assigned to the Organizers for publication. The Article will be published in the form of "Proceedings of the 31st European Safety and Reliability Conference" edited by Bruno Castanier, Marco Cepin, David Bigaud and Christophe Berenguer. In consideration of the acceptance of the Article for publication, I assign to the Organizers, Editors and its publisher "Research Publishing (S) Pte Ltd" whom the Organizers and Editors extending the nonexclusive publishing rights to with full title guarantee all copyright, rights in the nature of copyright and all other intellectual property rights in the Article throughout the world (present and future, and including all renewals, extensions, revivals, restorations and accrued rights of action). Organizers are free to publish the abstracts/papers thro' any medium currently available or made available in future. The Author represents that he/she is the author and proprietor of this Article, that he/she has full power to make this Agreement on behalf of himself/herself and his/her co-authors, and that this Article has not heretofore been published in any form. The Author shall obtain written permission and pay all fees for use of any literary or illustration material for which rights are held by others. The Author agrees to hold the Organizers, Editors and Publisher harmless against any suit, demand, claim or recovery, finally sustained, by reason of any violation of proprietary right or copyright, or any unlawful matter contained in this Article:

Signature



Name of Author(s) Luis Pedro Cobos, Alastair Ruddle and Giedre Sabaliauskaite

Institution or company Horiba-MIRA, Horiba-MIRA and Coventry University

Date April 20, 2021



ASSIGNMENT OF EXCLUSIVE RIGHTS – UNPUBLISHED WORK

This Assignment is effective this 26 day of August, 2021, by and between SAE International, a Pennsylvania not-for-profit corporation having a place of business at 400 Commonwealth Drive, Warrendale, PA 15096-0001 (“SAE”), and

Author(s)/Assignor(s)/Presenter(s): Luis Pedro Cobos

Title of Article/Work: Requirements for the automated generation of attack trees to support automotive cybersecurity assurance

(“Work”). If the Work is a work-made-for-hire pursuant to 17 USC § 101 of the Copyright Act, then such undersigned entity (e.g., employer, consortium, sponsoring entity) shall be deemed the Author for purposes of this Assignment and is the only recognized entity able to assign copyright. All works, image and text, created for an entity as part of a contracted position may be considered third party content. If said content is incorporated in the aforementioned Work, it is the responsibility of the author(s) to certify and carryout the requirements for acquiring republishing permission prior to submitting for assignment, and are required to include the appropriate licensing release documentation with the final manuscript.

Title of Journal: SAE World Congress 2022

Assignor represents, warrants and guarantees that (1) the Work is an original unpublished work; (2) Assignor is the sole and exclusive owner and claimant of all rights, titles and interest in and to the Work, including all copyrights therein; no other party, including an employer or contract provider may claim ownership to the Work’s attributed copyrights, and neither the Work nor copyrights have been assigned, transferred or otherwise encumbered; (3) the Work contains no material which would violate any copyright or other personal or proprietary right of any person or entity if published; (4) the Work is not a work made for the United States Government; and (5) Assignor has the authority to transfer the rights to Assignee and cause this Agreement to be executed as of the date first written above. Assignor further represents, warrants and guarantees to indemnify Assignee in the event a claim is made of copyright ownership for the Work or a portion thereof.

Assignor further represents, warrants and guarantees, to the best of Assignor’s knowledge and ability, that the Work is NOT controlled for export from the United States to any non-U.S. person or any other nation under the International Traffic in Arms Regulations (22 CFR Parts 120–130) or the Export Administration Regulations (15 CFR Parts 730–774) and, accordingly, may be modified, used, copied, distributed or circulated by SAE, in whole or in part, without any export licenses under the foregoing regulations.

Assignor hereby assigns to SAE all rights, titles and interest in and to Assignor's copyright in the Work in the exclusive rights: ((1) to reproduce, and or print, the Work in all media expression now known or hereinafter devised, including use within learning management systems, foreign language translations, digital database storage and delivery, and all other iterations published solely, or in partnership, by SAE International, its imprints, or other licensees throughout the world; (2) to distribute copies of the Work in all media now known or hereinafter devised; and (3) to prepare derivative works based upon the Work including, for example, but not limited to, the right with respect to all or part of the Work to edit, annotate, comment, format/reformat and abstract the Work or incorporate it into a compilation, collection or other work, including any customization prepared. No other exclusive rights in the Work are hereby assigned.

Assignor agrees that it shall not dispute, contest, or aid or assist others in disputing or contesting, either directly or indirectly, SAE's exclusive right, title and interest in the Work and in any and all compilations, collective works and derivative works based on the Work, including copyrights therein or other proprietary rights therein claimed by SAE.

Assignor agrees that, for no additional compensation, Assignor will execute any and all documents that may be necessary to assist SAE to register, perfect and enforce SAE's rights in and to the Work and any and all compilations, customizations, collective works and derivative works based on the Work.

SAE hereby grants Assignor the nonexclusive right to reproduce and publicly distribute the Work in print/film format for one (1) year and in electronic/optical media for five (5) years following six (6) months after first publication by SAE. Any such reproduction or distribution of the Work shall include the SAE copyright notice thereon and shall not be offered for sale or used to imply endorsement by SAE of a service or product. The Assignor may also post an electronic version of the accepted Work to an institutional repository, but not the final typeset Work. Nothing herein shall prohibit Assignor's reproduction and noncommercial distribution of the Work for its own use.

Use by Government Employees or Papers Published Under Government Contract:

This paper was written by a Government (U.S. or otherwise) employee as part of his/her official duties, or the paper was prepared as part of or under a government contract. Author(s) is not the owner of, but is authorized to assign, the copyright in the Work.

This paper was written by a Government (U.S. or otherwise) employee as part of his/her official duties, or the paper was prepared as part of or under a government contract. Author(s) is not the owner of and is not authorized to assign the copyright in the Work.

This paper was prepared as part of or under a government contract. Author(s) is owner of and is authorized to assign the copyright in the Work.

Select one of the options below:

I am authorized to represent my fellow authors of the above-listed paper in assigning copyright. In doing so, we confirm the Work to be original and that no other entity can claim rights to or a lien on any part of Work.

I am authorized to represent myself in assigning copyright, and in doing so, I confirm the Work to be original and that no other entity can claim rights to or a lien on any part of Work. I am NOT



authorized to represent my fellow authors of the above-listed paper. All authors/co-authors will be notified via email to assign copyright.

Author / Company: **Kacper Sowka**
Coventry University

Address: United Kingdom

Signature: KS

Author / Company: **Alastair Ruddle**
Horiba MIRA Ltd.

Address: United Kingdom

Signature: AR

Author / Company: **Paul Wooderson**
Horiba MIRA Ltd.

Address: United Kingdom

Signature: PW

When submitting approved third-party, employer or governmental copyright authorizations to SAE International Intellectual Property and Content Licensing, please include a copy of the licensed material clearly indicating the intended location, including new figure/ table number and caption title, in the new product published by SAE International.

18/08/2022

Kacper Sowka

54 Sidaway Street, Cradley Heath, United Kingdom

To whom it may concern,

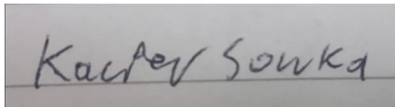
I confirm and give my permission to Luis Pedro Cobos Yelavives of using the text and pictures of his creation on the conference papers I worked with him. The information and data exposed on his thesis are his ideas and the use of such has my consent.

The request is for non-exclusive world rights to use this material in his thesis, in all languages and for all editions and formats, including digital/electronic. These rights will in no way restrict republication of the material in any other form by others authorized.

I therefore agree with the terms as described above to authorize the use of any material on a conference paper I have been a co-author with Mr. Cobos. The signing of this letter confirms that Mr. Cobos already has the copyright from the original publisher of the paper.

If you require any additional information, do not hesitate to contact me at the address and number above.

Sincerely,

A rectangular box containing a handwritten signature in black ink that reads "Kacper Sowka".

sowkak@uni.coventry.ac.uk

17 August 2022

Paul Wooderson
HORIBA MIRA
Watling Street
Nuneaton
Warwickshire
CV10 0TU

To whom it may concern,

I confirm and give my permission to Luis Pedro Cobos Yelavives of using the text and pictures of his creation on the conference papers on which I worked with him. The information and data exposed on his thesis are his ideas and the use of such has my consent.

The request is for non-exclusive world rights to use this material in his thesis, in all languages and for all editions and formats, including digital/electronic. These rights will in no way restrict republication of the material in any other form by others authorized.

I therefore agree with the terms as described above to authorize the use of any material on a conference paper on which I have been a co-author with Mr. Cobos.

If you require any additional information, do not hesitate to contact me at the address and number above.

Sincerely,



Paul Wooderson

Paul.wooderson@horiba-mira.com