AGH

AGH UNIVERSITY OF KRAKOW

FIELD OF SCIENCE ENGINEERING AND TECHNOLOGY

SCIENTIFIC DISCIPLINE AUTOMATION, ELECTRONICS, ELECTRICAL ENGINEERING AND SPACE TECHNOLOGIES

DOCTORAL DISSERTATION

The safety analysis of the in-vehicle control systems with a high degree of automation level

Author: mgr inż. Piotr Piątek

First supervisor:	Paweł Skruch, PhD, DSc
Second supervisor or Auxiliary supervisor:	Szczepan Moskwa, PhD

Completed at: AGH University of Krakow, Faculty of Electrical Engineering, Automatics, Computer Science and Biomedical Engineering

Kraków, 2024

AGH

AKADEMIA GÓRNICZO-HUTNICZA IM. STANISŁAWA STASZICA W KRAKOWIE

DZIEDZINA NAUK INŻYNIERYJNO-TECHNICZNYCH

DYSCYPLINA AUTOMATYKA, ELEKTRONIKA, ELEKTROTECHNIKA
I TECHNOLOGIE KOSMICZNE

ROZPRAWA DOKTORSKA

Systemowa analiza bezpieczeństwa układów sterowania w pojazdach o wysokim stopniu automatyzacji jazdy

Autor: mgr inż. Piotr Piątek

Promotor rozprawy: dr hab. inż. Paweł Skruch prof. AGH
Promotor pomocniczy: dr inż. Szczepan Moskwa

Praca wykonana: Akademia Górniczo- Hutnicza im. Stanisława Staszica w Krakowie,
Wydział Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej

Kraków, 2024

...to my wife for her unwavering support and love...

Abstract

The automotive industry is undergoing a revolutionary transformation with increased automation and data integration, necessitating a paradigm shift in the development of automotive electronic embedded systems. This dissertation addresses the critical need to integrate functional safety and cybersecurity in the design and implementation of highly automated control systems with mixed criticality in vehicles, presenting a holistic approach to solving complex, interdisciplinary, and cross-functional challenges.

Current approaches to analyzing automotive systems often treat safety and cybersecurity as separate domains, leading to increased errors, higher risks, reduced safety confidence, and the emergence of new hazards. This includes remote vehicle takeover, data leaks, vehicle thefts and break-ins, and issues related to service and business development, legal and regulatory compliance. A notable example of the risks involved is the famous "Jeep Hack", where cybersecurity vulnerabilities and insufficient isolation were exploited to remotely control the vehicle, underscoring the critical need for integrated safety and cybersecurity measures.

This dissertation highlights the imperative to analyze these aspects together, proposing a unified methodology that significantly reduces risks and improves system reliability. The integration is grounded in over ten years of industry experience, emphasizing deep technical knowledge in risk analysis and its impact on system design and architectural decisions, which are crucial for product commercialization.

There is a profound interplay between safety and cybersecurity, as both are based on the same fundamental principles. Commonalities such as risk identification, vulnerability analysis, and mitigation implementation exist in both domains. Therefore, a natural progression in the development of advanced systems is to analyze safety and cybersecurity together. Using extensive similarities and generic approaches allows the use of common tools and methodologies, contributing to more effective identification and resolution of potential threats. This coherence provides a unique opportunity to apply a unified approach, fostering greater synergy between domains, minimizing duplication of effort, and accelerating the product development process.

Furthermore, the dissertation underscores the benefits of integrating safety and cybersecurity through Model-Based Systems Engineering (MBSE) and joint engineering trends. The proposed reference organizational model is tailored for automotive Research and Development departments, promoting early collaborative development of safety and cybersecurity requirements. This integration ensures that the development process is both practical and scalable, addressing real-world applicability in industrial settings.

The research introduces the CyberSafety (CySa) process, a novel framework that combines safety and cybersecurity efforts from the earliest stages of product development. Using extensive literature reviews, standard analysis, and industry consultations, the CyberSafety process aims to effectively reduce risks, propose technical solutions, and therefore increase the quality of the system. However, at the same time, optimize resource allocation, reduce time-to-market, and manage maintenance periods and associated risks effectively.

This approach is validated through a newly defined set of Key Performance Indicators (KPI)s as well as a detailed case study of a Highway Pilot (HP) system, which demonstrates a potential reduction in development effort by up to 66.5% and a significant decrease in related risks, thus improving overall quality and security of the product. In addition, a new robust risk scoring methodology, which extends stand-alone Cybersecurity (CySe) and Functional Safety (FuSa), the Weighted Safety Score (WSS) is proposed and evaluated. It takes into account both hazards and threats, with weight factors tailored to various automotive domains. The WSS provides a holistic view of the risk landscape of the system, supporting better informed decision making for risk mitigation and safety improvements.

Furthermore, the proposed solution extends CySe analysis into new domains, removing its traditional deep integration with the Electrical/Electronic (EE) vehicle architecture. Instead, it emphasizes abstracted system functional architecture elements, their interactions, use case data flows, and communication patterns. This abstraction facilitates the identification of risks independently from physical implementations, allowing early detection and mitigation of potential threats before finalizing physical architecture decisions and functional allocations.

The dissertation includes both theoretical and practical dimensions, applying the proposed methods to real active safety systems, specifically the HP, and promoting the innovative use of available toolchains. Through in-depth safety analysis, the research demonstrates a significant reduction in the risk and analysis effort.

The conclusions highlight the success of the CyberSafety process in improving system design decisions and reducing risks. Future work will focus on refining this process with newer tools and methodologies, expanding its applicability beyond the automotive industry, and integrating security patterns into existing cybersecurity standards. Ongoing collaboration with standardization working groups will be essential to keep up with the evolving landscape of autonomous vehicle safety and cybersecurity.

In essence, this dissertation provides a transformative approach to developing safe and secure systems for highly autonomous vehicles, redefining the future of automotive development through innovative risk analysis and comprehensive system integration.

Streszczenie

Przemysł motoryzacyjny przechodzi rewolucyjną transformację, wraz ze wzrostem automatyzacji i integracji danych, co wymaga zmiany paradygmatu w rozwoju elektronicznych systemów wbudowanych w pojazdach. Niniejsza rozprawa podejmuje krytyczną potrzebę integracji bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa w projektowaniu i wdrażaniu wysoko zautomatyzowanych systemów sterowania o mieszanej krytyczności w pojazdach, przedstawiając holistyczne podejście do rozwiązywania złożonych, interdyscyplinarnych i wielofunkcyjnych wyzwań.

Obecne podejścia do analizy systemów motoryzacyjnych często traktują bezpieczeństwo funkcjonalne i cyberbezpieczeństwo jako odrębne dziedziny, co prowadzi do wzrostu błędów, wyższego poziomu ryzyka, mniejszego bezpieczeństwa systemu oraz pojawienia się nowych zagrożeń. Obejmuje to przejęcia pojazdów na odległość, wycieki danych, kradzieże pojazdów i włamania oraz problemy związane z rozwojem usług i biznesu, zgodnością prawną i regulacyjną. Znanym przykładem tych zagrożeń jest słynny atak na Jeep'a, w którym wykorzystano luki w zabezpieczeniach cybernetycznych do zdalnego sterowania pojazdem, co podkreśla krytyczną potrzebę zintegrowanych środków bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa.

Niniejsza rozprawa podkreśla konieczność wspólnej analizy tych aspektów, proponując uwspólnioną metodologię, która znacząco redukuje ryzyka i poprawia niezawodność systemu. Integracja ta opiera się na ponad dziesięciu latach doświadczenia w branży, podkreślając głęboką wiedzę techniczną w zakresie analizy ryzyka oraz jej wpływ na projektowanie systemu i decyzje architektoniczne, które są kluczowe dla komercjalizacji produktu.

Istnieje głęboka interakcja między bezpieczeństwem funkcjonalnym a cyberbezpieczeństwem, ponieważ obie dziedziny opierają się na tych samych fundamentalnych zasadach. Wspólne elementy, takie jak identyfikacja ryzyka, analiza podatności i wdrażanie działań zaradczych, występują zarówno w bezpieczeństwie funkcjonalnym, jak i w cyberbezpieczeństwie. Dlatego naturalnym postępem w rozwoju zaawansowanych systemów jest wspólna analiza bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa. Wykorzystanie licznych podobieństw pozwala na stosowanie wspólnych narzędzi i metodologii, co przyczynia się do bardziej efektywnej identyfikacji i rozwiązywania potencjalnych zagrożeń. Ta spójność między bezpieczeństwem funkcjonalnym a cyberbezpieczeństwem stwarza unikalną okazję do zastosowania zjednoczonego podejścia, sprzyjając większej synergii między dziedzinami, minimalizując powielanie wysiłków i przyspieszając proces rozwoju produktu.

Ponadto, rozprawa podkreśla korzyści płynące z integracji bezpieczeństwa i cyberbezpieczeństwa poprzez inżynierię systemów opartą na modelach (ang. model-based systems engineering) oraz wspólne

trendy inżynierskie. Proponowany model organizacyjny jest dostosowany do działów badawczo-rozwojowych w motoryzacji, promując wczesne, wspólne opracowywanie wymagań dotyczących bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa. Ta integracja zapewnia, że proces rozwoju jest zarówno praktyczny, jak i skalowalny, odpowiadając na rzeczywiste zastosowania w środowiskach przemysłowych.

Badania wprowadzają proces CyberSafety, nowatorskie ramy, które łączą wysiłki w zakresie bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa od najwcześniejszych etapów rozwoju produktu. Wykorzystując obszerne przeglądy literatury, analizy standardów i konsultacje branżowe, proces CyberSafety ma na celu optymalizację alokacji zasobów, skrócenie czasu wprowadzenia na rynek oraz skuteczne zarządzanie okresami utrzymania i związanymi z nimi ryzykami. Podejście to zostało zweryfikowane za pomocą nowo zdefiniowanego zestawu wskaźników efektywności, a także szczegółowego studium przypadku systemu Pilota Autostradowego (ang.Highway Pilot), które wykazało potencjalne zmniejszenie nakładu pracy na rozwój nawet o 66,5% i znaczny spadek powiązanego ryzyka, poprawiając w ten sposób ogólną jakość i bezpieczeństwo produktu. Ponadto zaproponowano i zbadano nową, solidną metodologię oceny ryzyka, która rozszerza samodzielne analizy ryzyk bezpeczeństwa funkcjonalnego oraz cyberbezpieczeństwa tj. Ważony Współczynnik Bezpieczeństwa (ang. Weighted Safety Score (WSS)). Uwzględnia on zarówno zagrożenia, jak i niebezpieczeństwa, ze współczynnikami wagi dostosowanymi do różnych dziedzin motoryzacji. WSS zapewnia całościowy obraz ryzyka związanego z systemem, wspierając podejmowanie bardziej świadomych decyzji w zakresie ograniczania ryzyka i poprawy bezpieczeństwa.

Rozprawa obejmuje zarówno teoretyczne, jak i praktyczne wymiary, stosując proponowane metody do rzeczywistych systemów aktywnego bezpieczeństwa, w szczególności autostradowego wspomagania kierowcy, i promując innowacyjne wykorzystanie dostępnych narzędzi. Poprzez dogłębną analizę bezpieczeństwa, badania wykazują znaczną redukcję ryzyka i nakładu pracy analitycznego.

Wnioski podkreślają sukces procesu CyberSafety w poprawie decyzji projektowych systemów i redukcji ryzyk. Przyszłe prace będą koncentrować się na udoskonalaniu tego procesu za pomocą nowszych narzędzi i metodologii, rozszerzając jego zastosowanie poza branżę motoryzacyjną i integrując wzorce bezpieczeństwa z istniejącymi standardami cyberbezpieczeństwa. Ciągła współpraca z grupami standaryzacyjnymi będzie niezbędna, aby nadążyć za ewoluującym krajobrazem bezpieczeństwa i cyberbezpieczeństwa pojazdów autonomicznych.

W istocie, niniejsza rozprawa dostarcza transformacyjnego podejścia do rozwoju bezpiecznych i zabezpieczonych systemów dla wysoko autonomicznych pojazdów, redefiniując przyszłość rozwoju motoryzacji poprzez innowacyjną analizę ryzyka i kompleksową integrację systemów.

Contents

Acronyms

ADAS Advanced Driver Assistance System

AFR Attack Feasibility Rating

AI Artificial Intelligence

ASIL Automotive Safety Integrity Level

ASPICE Automotive Software Process Improvement and Capability Determination

AUTOSAR Automotive Open System ARchitecture

AV Automated Vehicles

AWI Approved Work Item

BOM Bill of Materials

BPMN Business Process Model and Notation

C-ITS Cooperative Intelligent Transport System

CAL Cybersecurity Assurance Level

CAN Controller Area Network

CICD Continuous integration and continuous delivery

CSMS Cybersecurity Management Systems

CVC Central Vehicle Computer Unit

CVSS Common Vulnerability Scoring System

CySa CyberSafety

CySaIM CyberSafety Incident Monitoring

CySaRA CyberSafety Risk Analysis

CySe Cybersecurity

DCI Design Complexity Index

DCR Design Compliance Rate

DCRR Design Change Request Rate

DDoS Distributed Denial of Service

DFA Dependent Failure Analysis

DIA Development Interface Agreement

DoS Denial-of-Service

DRE Design Review Effectiveness

DSRC Dedicated short-range communications

DTI Diagnostic Test Interval

E-CAD Electronic Computer-Aided Design

E2V Ecosystem-to-Vehicle

ECU Electronic Control Unit

EE Electrical/Electronic

ENISA European Union Agency for Cybersecurity

ERC Effort Reduction Coefficient

ETA Event Tree Analysis

EU European Union

FMEA Failure Mode and Effect Analysis

FMEDA Failure Mode Effect and Diagnostic Analysis

FTA Fault Tree Analysis

FTTI Timing–fault-tolerant Time Interval

FuSa Functional Safety

GPS Global Positioning System

HARA Hazard Analysis and Risk Assessment

HaSI Hazard Safety Indicator

HD High Definition

HIRE Hazard Identification and Risk Evaluation

HMI Human-Machine Interface

HP Highway Pilot

HSI Hardware-to-Software

I2V Infrastructure-to-Vehicle

IDPS Intrusion Detection and Prevention System

IDS Intrusion Detection System

IdsM IDS Manager

IdsR IDS Reporter

IEEE Institute of Electrical and Electronics Engineers

IoT Internet of Things

IPS Intrusion Prevention System

ISO International Organization for Standardization

IT Information Technology

ITF Implementation Task Force

ITS Intelligent Transportation Systems

IV In-Vehicle

KPI Key Performance Indicators

M-CAD Mechanical Computer-Aided Design

M2M Machine to Machine

MaaS Mobility-as-a-Service

MBSE Model-Based Systems Engineering

MSC Mitigation Strategy Completeness

NFC Near-Field Communication

NHTSA National Highway Traffic Safety Administration

NIST National Institute of Standards and Technology

NPD New product development

NTI New Technology Implementation

OBD On-Board Diagnostics

ODD Operational Design Domain

OEM Original Equipment Manufacturers

OT Operational Technology

OTA Over-The-Air Updates

PAS Publicly Available Specification

QoS Quality of Service

RAC Risk Assessment Coverage

RRL Residual Risk Level

S2V Surrounding-to-Vehicle

SAE Society of Automotive Engineers

SDL System Definition Language

SDV Software Defined Vehicle

SE Systems Engineering

SeM Security Event Memory

SeV Security Event

SOTIF Safety of Intended Functionality

SSRC Security and Safety Requirement Coverage

SSRIR Security And Safety Risk Identification Rate

SVA Smart Vehicle Architecture

SysML Systems modeling language

T2V Transportation Networks-to-Vehicle

TAF Targeted Attack Feasibility

TARA Threat Analysis and Risk Assessment

THA Threat and Hazard Analysis Efficiency

ThRS Threat Risk Score

TPM Trusted Platform Module

TS Technical Specification

TSN Time-Sensitive Networking

UML Unified Modeling Language

UNECE United Nations Economic Commission for Europe

V2E Vehicle-to-Ecosystem

V2G Vehicle-to-Grid

V2I Vehicle-to-Infrastructure

V2S Vehicle-to-Surrounding

V2T Vehicle-to-Transportation Networks

V2V Vehicle-to-Vehicle

V2X Vehicle-to-Everything

VDA Verband der Automobilindustrie

WP.29 The UNECE World Forum for Harmonization of Vehicle Regulations

WSS Weighted Safety Score

Chapter 1

Introduction

Amongst all known phenomena, despite its inevitability, change seems to be the least obvious. However, it has a tremendous impact on all aspects of people's lives. Indeed, it is change, which also drives the science in its attempt to solve problems, which non-scholars would not even consider valid. One may ask whether there are rules that drive change.

In "The Laws of Scientific Change" Hakob Baresghyan [1] tries to develop the General Theory of Scientific Change. Baresghyan names all accepted theories and all methods employed as the 'scientific mosaic of the time'. The scientific mosaic is in constant change. The most suitable example given by Hakob is the scientific description of the world, which has rapidly changed during the last 400 years. Up until the 17th century the Aristotelian-medical natural philosophy seemed to be enough. However, on 5 July 1687, it was replaced by Newtonian mechanics, in his famous publication 'Philosophiae naturalis principia mathematica'. Another breakthrough came with Maxwellian electrodynamics equations in 1861 and 1862. Now, one and a half centuries later, it is commonly agreed in the scientific world that general relativity and the Standard Model of quantum physics give the best available description of physical processes.

In the same book, Baresghyan postulates the four laws of scientific change:

- The Zeroth Law – Any given state in the process of scientific change is characterised by mutual compatibility of the elements in the mosaic;
- The First Law - The process is also characterized by a degree of inertia as the mosaic of accepted theories and employed methods normally tends to maintain its state;
- The Second Law - Theories become accepted into the mosaic only when they meet the implicit requirements of the time;
- The Third Law - As for the requirements themselves, they become employed only if they happen to be deductive consequences of the mosaic at the time.

In summarizing, there shall be both a right place and a right time for a scientific change to happen and become approved. One more aspect should be considered as well though, the statistical probability and randomness. Following even the brightest theory, the level of randomness cannot be omitted. Unfortunately, even Albert Einstein was wrong about the probability and did not consider the laws of quantum mechanics as valid. We can find Einstein's opinion on quantum mechanics in his famous quote 'God does not play dice with the universe.'

No one is yet able to tell what fundamental change may happen even in the upcoming 10-20 years, when super-intelligence is available and questions all current knowledge and assumptions. However, we can say with a probability 100%, which is a certainty, that it will happen.

One can argue with chaos theory, the Big Bang Theory, or quantum mechanics, one cannot, however, argue with the fact that the time goes on. Everything that was a nanosecond ago is in the past, it is no longer what it once was, therefore, having changed. With that in mind, humanity is constantly on a growing path, and its dynamic can be expressed with an exponential function, it is always the right place and the right time to come up with new ideas. With the world connected unlike ever before, there is an undeniable opportunity to take another step into a better, developed future, whatever that may be.

Change and development go side by side. Similarly to the expansion of the universe [2], the pace of technological advancement is faster than anyone could imagine. This trend significantly impacts industries, particularly the automotive sector, where we are witnessing a major shift from internal combustion engines to electric motors. In addition, advances in the human-to-car interface, such as autonomous vehicles and enhanced connectivity, are key components of this transformation. As the development of intelligent vehicles progresses, the complexity of their systems continues to increase. A critical challenge for the automotive industry is ensuring the safety and security of autonomous vehicles and their environments under all circumstances.

This mirrors the challenges faced by next-generation industrial systems, part of Industry 4.0, where the convergence of Operational Technology (OT) and Information Technology (IT) demands the integration of safety and cybersecurity to protect critical infrastructures. Similar concerns have been addressed in various sectors, highlighting the importance of effectively managing these interrelated risks to improve system resilience and minimize the need for potentially disastrous recovery strategies. This approach not only safeguards the system but also ensures its continuity under evolving threats and operational conditions [3, 4].

In order to analyze all potential risks for an autonomous vehicle, the ISO 26262:2018 [5] standard is becoming insufficient. It covers only faults resulting from system malfunction, whereas the possible interaction of an autonomous vehicle with the environment goes far beyond this. The new ISO PAS 21448 [6], which defines the paradigm of Safety of Intended Functionality (SOTIF), may increase the level of safety for future intelligent vehicles. However, only in conjunction with cybersecurity can the entire autonomous ecosystem co-exist and, therefore, risk analysis be comprehensive. This observation has already been identified amongs the industry researches [7–12], however in this disertation only a comprehensive solution is proposed on top of already released ISO 21434 standard [13].

Consequently, an integrated analytical approach used for the design and implementation of complex systems should be introduced for the entire life cycle of the system. It shall cover the entire ecosystem of functional safety, safety of the intended functionality, and cybersecurity.

Current approaches often treat safety and cybersecurity in automotive systems as separate domains. This siloed approach leads to increased errors, higher risks, reduced safety confidence, and the emergence of new hazards like remote vehicle takeover, data leaks (e.g., driver information, location data), and vehicle thefts.

The infamous "Jeep Hack" exemplifies this risk, where hackers exploited cybersecurity vulnerabilities to remotely control a vehicle [14]. The risks were not properly identified and there were insufficient isolation measures implemented in vehicle's EE the architecture. Moreover, currently developed ADAS systems are not resistant to safety-critical attacks, targeting control systems. According to the latest experimental findings, context-aware attacks can successfully generate dangers with and 83. 4% success rate, 99. 7% of which occur without prior notice [15]. CySe researchers are finding more and more vulnerabilities in vehicles systems, which may lead to direct safety impact [16, 17].

This underscores the critical need for integrated safety and cybersecurity measures.

Connected vehicles present a wider attack surface due to their increased connectivity [18–20]. Additionally, the databases of known automotive vulnerabilities and attacks are constantly growing [21]. This includes vulnerabilities in vehicle sensors, which are the foundation of data collection for autonomous vehicle operation [22]. Recognizing these risks, leading industry manufacturers are proactively disclosing flaws in their systems to raise awareness and collaborate on comprehensive solutions, as exemplified by recent disclosures from BMW [23].

1.1 Scope of the Thesis

In the midst of what is often referred to as the Fourth Industrial Revolution, characterized by increased automation and enhanced data exchange among machines in manufacturing processes, a notable trend has emerged. This transformative shift is not confined to any particular industry, but rather permeates across sectors, particularly affecting the automotive industry. Alongside advances in propulsion systems, such as vehicle electrification, the automotive industry is dedicated to the development of autonomous driving technologies. These intelligent vehicles represent the next evolutionary step in automotive technology, promising increased safety, efficiency, and convenience.

Regardless of whether the focus is on Advanced Driver Assistance Systems (ADAS) or highly autonomous driving systems, two critical facets consistently underscore their development: Functional Safety (FuSa) and Cybersecurity (CySe). These elements are instrumental in ensuring the safe and secure operation of intelligent vehicles. The entire ecosystem, from individual vehicle components to the overarching system, must adhere to rigorous safety standards. This includes compliance with ISO 26262-1:10:2018 [5] for Functional Safety in Road Vehicles and ISO/PAS 21448 for SOTIF [13], especially crucial when analyzing systems with a high level of autonomy [24, 25].

In today's digital age, another critical concern is cybersecurity, defined under the ISO/SAE 21434 standard [13]. Ensuring the protection of sensitive data and guarding against potential breaches are imperative aspects in the development of connected and autonomous vehicles.

Advanced Driver Assistance System (ADAS) and highly autonomous driving systems now represent the most complex and technologically advanced aspects of modern vehicles. The achievement of the highest levels of safety and performance in these systems requires the collaboration of experts from various disciplines. However, this interdisciplinary approach is still in its infancy, particularly with regard to the integration of FuSa and CySe. Collaboration in the context of safety and security is a relatively new topic, however, emerging quite steadily and at the same time rapidly in recent years, as shown in Figure 1.1.

For Scopus Database filtering, the following queries were used:

- **FS + AUTO** - *(TITLE-ABS-KEY(automotive functional safety) AND PUBYEAR > 1999)*
- **FS + CySe + Auto** - *(TITLE-ABS-KEY(automotive AND cybersecurity AND functional AND safety))*
- **CySe + Auto** - *(TITLE-ABS-KEY(automotive cybersecurity))*

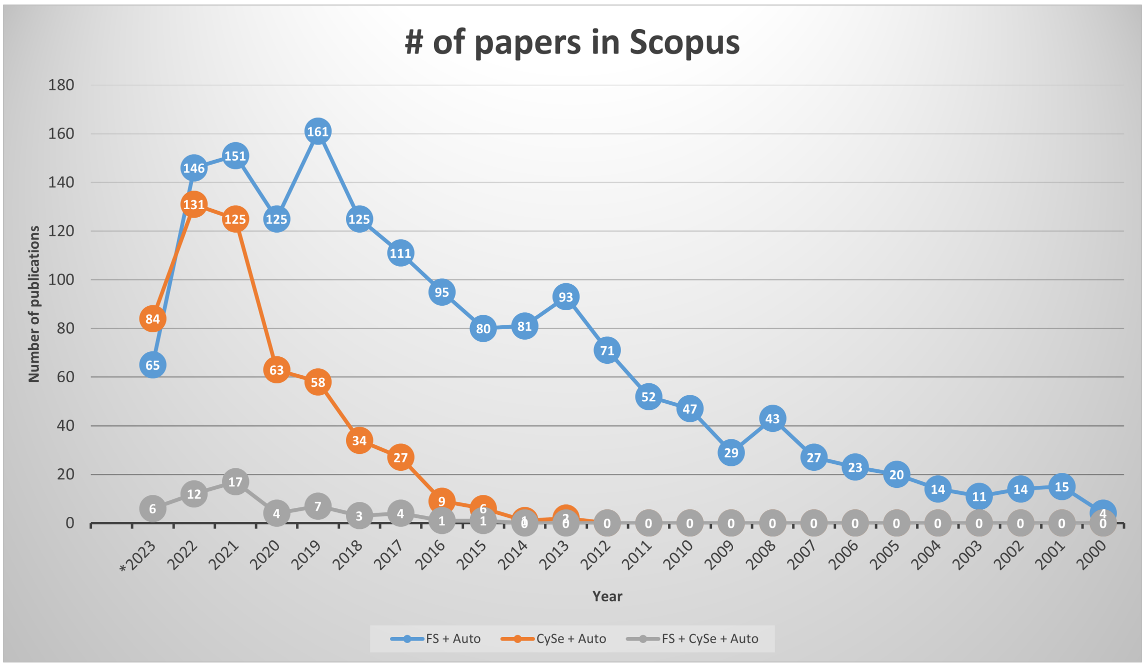


Figure 1.1: Number of papers in Scopus database.(Data as of June 2023.) Source: *https://www.scopus.com/*.

Observing the landscape of publications, it is apparent that the FuSa domain exhibits greater maturity than its counterpart, cybersecurity, within the automotive industry. This maturity is reflected in the larger volume of publications dedicated to FuSa. However, an intriguing trend emerges as we delve into the data: a significant upswing in cybersecurity-related publications coincides with the introduction of the ISO 21434 standard in 2021.

This surge in cybersecurity publications indicates a growing recognition of its importance in the development of modern vehicles. However, it also underscores the relatively nascent stage of integrating cybersecurity into automotive practices. Moreover, it becomes evident that appropriate standards in this realm are still in the process of refinement.

Another notable observation is the paucity of literature that addresses the confluence of FuSa and CySe in the automotive sector. Drawing from a thorough review of more than 150 publications, active participation in over 20 industry-related webinars, and direct discussions during two industry conferences, existing research primarily focuses on the ramifications of FuSa and CySe on the Electronic Control Unit (ECU) that are being designed, there exists a gap in the literature regarding the broader organizational and management aspects influenced by the introduction of new product development processes.

This dissertation highlights the imperative to analyze FuSa and CySe together, proposing a unified methodology that significantly reduces risks and improves the reliability of the system. This integration is grounded in over ten years of industry experience encompassing various development domains. The background of the thesis includes deep technical knowledge in risk analysis and its impact on testing, software development, and systems engineering for diverse automotive embedded systems, including safety-critical components and systems such as charging systems and Advanced Driver Assistance System (ADAS). This comprehensive understanding of the development lifecycle completes the proposed methodology and ensures its practical application in different automotive systems.

Currently, the industry still predominantly treats these concerns as separate entities, which can lead to discrepancies and gaps in analysis. This fragmentation presents risks, ranging from functional failures that could lead to vehicle accidents to cybersecurity vulnerabilities with the potential to cause serious security breaches [25–27].

A holistic perspective is essential to address all phases of the design and production process for highly autonomous systems. The principles of lean management, widely employed in production, also find applicability in the design phase. These principles can streamline processes, eliminate waste, and improve overall system quality. Additionally, adopting Model-Based Systems Engineering (MBSE) principles enables organizations to achieve a more integrated and holistic view of system architecture, leading to enhanced safety and security. MBSE offers a structured approach that employs visual models and simulations to systematically analyze and optimize system design [28–32].

In the future, the imminent introduction of ISO 21434, a vehicle cybersecurity standard, underscores the need for interdisciplinary collaboration. This applies not only to the interaction between functional safety and cybersecurity experts, but also to the realm of Safety of the Intended Functionality in autonomous driving systems. All of these considerations must be harmoniously integrated within the Automotive Software Process Improvement and Capability Determination (ASPICE) framework, a quality model required during the design and production phases in the automotive sector [24, 33].

Beyond establishing methods for interdisciplinary collaboration, there is a need to identify shared work products that can be developed jointly early in the design of complex systems. This approach not only accelerates project timelines but, more crucially, minimizes potential gaps and errors. As a result, safety and security considerations are substantially heightened during the design and production of highly autonomous driving systems.

Several methodologies and techniques can facilitate interdisciplinary collaboration [34–36], even considering the automation technique and Artificial Intelligence (AI) enhancements [27] to bring isolated domains together.

Furthermore, a holistic perspective is essential to address the entire design and production process for highly automatic systems. The principles of lean management, widely employed in production, also find applicability in the design phase. These principles can streamline processes, eliminate waste, and improve overall system quality.

In essence, this research strives to bridge the gap between safety and security in the context of complex system development, particularly in autonomous vehicles, offering a holistic perspective on the design and implementation of these transformative technologies. Through a methodical approach grounded in MBSE principles, this study seeks to propel the automotive industry toward safer, more secure, and highly efficient autonomous driving systems. By integrating Functional Safety and Cybersecurity and SOTIF from the earliest stages of product development, the aim is to contribute to the realization of intelligent vehicles that meet the highest standards of safety, security, and reliability.

FuSa and CySe share fundamental principles like risk identification and vulnerability analysis. A natural progression is to analyze them together. This allows for common tools and methodologies, leading to more effective threat identification and resolution. This coherence provides a unique opportunity for a unified approach, fostering synergy, minimizing duplication of effort, accelerating development, and improving system reliability.

Building trust in vehicles through comprehensive common work products is essential. There is a strong link between being safe and being secure. If the system is not secure, it is probably not safe. However, some mechanical and electrical systems can still work autonomously from software control, and therefore safety and security aspects may differ. Cybersecurity threats evolve more rapidly than safety threats, which emphasizes the need for continuous vigilance [37].

The automatic identification of interactions between safety and security in system models is crucial. With the growing number of safety and security requirements from original equipment manufacturers, more safety and security features are being integrated into automotive systems. These features are often developed independently, potentially leading to missed dependencies between them [27].

In addition, design patterns can play an important role in automating work efforts and enhancing the efficiency of integrating safety and security considerations [38, 39].

In alignment with the rapidly evolving landscape of automotive technology, Aptiv Services Poland recognizes the immense potential within collaborative development processes. The company has made substantial investments in the modeling of system architecture, process optimization, and the adoption of advanced tools. These efforts aim to achieve a dual objective: reducing costs while simultaneously enhancing the quality of products and optimizing resource use.

This dissertation integrates diverse fields encompassing functional safety, cybersecurity, and technical management. It champions a system engineering-oriented approach, designed to enhance system reliability and quality through a novel risk reduction methodology. This holistic perspective ensures the proposed solution meets the ever-evolving demands of the automotive industry.

1.2 Research Hypothesis and Objectives

The dissertation hypothesis is defined as follows:

- **Early collaboration on integrated safety and security throughout the product development lifecycle will yield superior reliability and quality for high-autonomy automotive embedded systems by minimizing risks and ensuring robust performance.**

- **Developing a novel development model that equips companies with comprehensive tools and methodologies for efficiently managing the intricate design of complex, mixed-criticality, high-autonomy automotive embedded systems, while integrating safety and security throughout the**

entire process, will significantly improve system reliability, reduce development time, and enhance overall vehicle safety and security.

This hypothesis is a testable proposition that serves as the cornerstone of the research methodology and guides investigative efforts.

The core objective of this dissertation is to:

- **Formulate a practical and implementable approach to the design and implementation of advanced control systems in highly automated vehicles, aimed at improving system reliability, fostering synergy among development teams, minimizing duplication of effort, and accelerating the overall development;**

- **Propose a reference organizational design model and technical methodology tailored for application within the research and development departments of automotive companies, focusing on advanced control systems in highly automated vehicles, integrating safety and security throughout the development process, and enhancing collaboration and communication within teams.**

The approach proposed in the dissertation is to seamlessly integrate safety and cybersecurity considerations, which is the fundamental hypothesis of this study. The overall objective is to address the critical need for synergy in safety and security in the dynamic automotive landscape, with a strong focus on real-world applicability.

The pragmatic objective goes beyond theoretical considerations and aims to provide a concrete framework for the integration of safety and security in authentic industrial environments. The emphasis is on the practical utility of the proposed framework, particularly in companies involved in the design and development of complex solutions.

Furthermore, the effectiveness of the developed organizational process model is rigorously evaluated using a real-world example, emphasizing the practical applicability of the framework in the design and development of complex solutions within these companies.

The importance of these objectives lies in their potential to increase the safety, security, and improve automotive embedded system system quality. Currently, cybersecurity and safety analyses are often conducted separately, leading to challenges and potential inconsistencies. By integrating safety and security principles from the beginning of product development and implementing the proposed framework in companies specializing in complex active safety solutions, the aim is to contribute to the realization of intelligent vehicles that not only meet the highest safety and security standards, but also exhibit unwavering reliability and effectiveness.

1.3 Structure of the Dissertation

The subsequent chapters of this thesis delve into the methodologies, processes, and findings that contribute to the achievement of these objectives. Chapter 2 provides an extensive review of the literature and current state-of-the-art automotive technologies, setting the stage for research. The research methodology is grounded in a critical analysis of existing analytical methodologies and processes in the domains of safety, cybersecurity, and automotive systems. It focuses on key terminology and identifies errors, defects, and issues associated with current methods, both in the scholarly literature and in industry reports. When referring to the literature, particular emphasis is placed on publications from reputable scientific databases and research libraries, such as Scopus and IEEE Xplore, providing current and validated information. In addition, the examination of industry reports facilitates a thorough understanding of the latest trends, challenges, and innovative solutions in the realms of safety and cybersecurity within the automotive sector. These analyses collectively serve as an objective foundation for the entire dissertation, enabling the proposal of innovative solutions aligned with current industry expectations. The project also explores the development and introduction of a new complex product to the market.

Chapter 3 presents the CyberSafety framework developed. This part focuses on a strategic exploration of risk analysis and process modeling tools, aligning their selection with solutions used throughout the automotive industry to enhance practical applicability. The rationale for tool selection is explicitly tied to their compatibility with Aptiv's practices.

Using Business Process Model and Notation (BPMN) and Systems modeling language (SysML) as modeling languages, this study systematically optimizes and conceptualizes complex design processes to improve the quality and safety of automotive systems. The multifaceted data collection process draws on industry standards, guidelines, and relevant case studies to provide comprehensive insights into safety, security, and systems engineering in the automotive domain. The strategic selection of case studies not only provides a real-world context but also underlines the practical applicability of the findings in actual automotive projects.

Chapter 4 evaluates the proposed design and development framework in the context of active safety systems. In order to validate and refine the proposed organizational process model, an in-depth study of an ADAS function was carried out, specifically the Highway Pilot (HP) system model provided by Ansys Medini. This model, initially a demonstration project, served as a practical reference point to evaluate the applicability and effectiveness of the proposed model. It allowed a detailed analysis of the integration of safety and security considerations within a complex automotive system, demonstrating the need for tools such as Ansys Medini to improve automation, documentation, traceability, and maintenance aspects in the automotive domain. The research used a multifaceted approach including Threat Analysis and Risk Assessment (TARA), Hazard Analysis and Risk Assessment (HARA), Hazard Identification and Risk Evaluation (HIRE), Fault Tree Analysis (FTA), Attack Tree Analysis and MBSE.

Together, these methodologies provided a comprehensive understanding of potential threats, vulnerabilities, and risks, ensuring a holistic approach to risk analysis that considered both the safety and cybersecurity aspects. The Effort Reduction Coefficient was introduced to calculate the reduction in effort following the implementation of the new design framework. The research used specialized software tools such as Bizagi Modeller [40] for process modeling, Ansys Medini [41] for safety and security system analysis, and MS Office Excel for data analysis and charting, highlighting their role in ensuring accuracy and efficiency in the research process. The chosen research design principles, rooted in MBSE principles, aims to seamlessly integrate safety, security, and engineering management aspects within intelligent vehicle development, while maintaining a practical focus to provide actionable insights for the automotive industry. As structured with a review of the literature and evaluation of industry standards, proposed design methodology provides a solid foundation for understanding the field and highlights the importance of these tools in addressing the complexity of the automotive domain.

Finally, Chapter 5 concludes the thesis, summarizing the main contributions and implications of the research and offering considerations for future improvements.

In Annex A, the complete export of the CyberSafety framework from the Bizagi tool can be found, providing an in-depth view of its structure and components. In addition, in Annex B, based on the results of the dissertations, the CyberSafety analysis of the Highway Pilot ADAS feature is presented, offering valuable insights into its safety and cybersecurity aspects.

This research operates within several defined limitations and assumptions. Firstly, the design framework is developed based on industry standards and models language versions available at the time of the research. As newer versions of standards, guidelines, and modeling languages become accessible, they shall be seamlessly integrated into the model to ensure its ongoing relevance. Secondly, Medini Analysis was chosen due to licensing constraints, although ongoing efforts aim to introduce a more versatile system modeling and analysis tool. In addition, the primary focus of model evaluation was the design phase, a key point in project development. This emphasis was necessitated by constraints in time and resources, yet it offers a strategic advantage by allowing a comprehensive system model design and averting significant and costly architectural changes in the future. Furthermore, due to the complex nature of highly automated automotive products, the evaluation was performed on a single system, the HP. This choice was made because it encapsulates various aspects of a cutting-edge ADAS system, including perception, data processing, data fusion, and actuator components, making it an ideal representative of a complex system.

Mostly, since this is a relatively new and trending subject, the process analysis was predominantly taken from the cybersecurity perspective. In addition, not all possible threats and hazards were analyzed for the HP model. Based on the literature review, only highly critical ones were selected to demonstrate the designed framework. It is assumed that the proposed process flow follows an iterative and agile approach, rather than a waterfall model. To address concerns about the confidentiality of customer data, the openly available Highway Pilot system was examined to showcase the model's implementation capabilities. The absence of standardized joint development practices for the analysis of safety and security presented challenges, which were mitigated through direct communication with the tool vendor. The identified issues and proposed enhancements are anticipated to be incorporated into the next tool release. These delineated limitations and assumptions demarcate the scope and application of this research. Although the primary context of the process model is the automotive industry, its adaptability extends to similar domains such as aviation, military, or medical applications.

1.4 Contributions to Scientific Discipline

The increasing complexity of automotive systems, driven by automation and connectivity, has exposed vulnerabilities to cybersecurity threats. This dissertation bridges the gap between safety and cybersecurity by introducing a holistic framework for risk analysis and management in highly automated automotive systems.

This section outlines the key contributions of this work to the discipline, emphasizing novel methodologies and their practical implications.

Pioneering Integration of Cybersecurity and Safety Analysis

By merging Cybersecurity (CySe) and Functional Safety (FuSa) assessments into a unified risk analysis framework, this dissertation offers a comprehensive approach to mitigating accidental failures and malicious attacks. This integrated perspective significantly improves overall road safety by reducing the likelihood of accidents caused by technical malfunctions and cyberattacks. The integration of analyses in these two areas takes into account the functioning of electronic components in automotive systems and software, whose design and operational specifics have so far been analyzed separately in each area. However, the mutual interdependence of threats in these areas suggests that an integrated approach should be adopted.

Illumination of Technical Dependencies and Their Impact on Risk The study underscores the critical role of technical dependencies in the context of a connected vehicle system with a high degree of automation level. By analyzing the potential impact of these dependencies on system CySe and FuSa, including key elements of automotive electronics and software, this research provides valuable information for the design of resilient automotive systems.

Development of a Novel, Flexible, and Quantifiable Risk Analysis Framework

A flexible and scalable risk analysis framework is introduced, tailored to the evolving automotive landscape while adhering to industry standards. The framework enables efficient identification, assessment, and mitigation of risks throughout the product lifecycle. The evaluation of the framework demonstrated a significant reduction in both safety and cybersecurity risks, highlighting its effectiveness in enhancing the reliability and safety of the system.

Emphasis on Early Risk Mitigation and Proactive Safety Culture

The proposed methodology prioritizes early risk identification and mitigation, fostering a proactive safety culture within automotive organizations. By addressing potential vulnerabilities early in the development process, this approach improves product quality and improves overall system resilience.

Promotion of a Systems Engineering Perspective for Enhanced Safety and Security

This research advocates for a systems engineering approach to automotive development, emphasizing the interdependencies of safety and cybersecurity. By treating CySe and FuSa as integral components of the system, this work promotes collaboration among engineering teams and facilitates the development of more secure and reliable vehicles. The proposed approach is complementary to the scope of the scientific discipline of automation, electrical engineering, electronics, and space technologies, which encompasses mutually interconnected areas.

Establishment of Clear Goals and Measurable Outcomes

The dissertation provides a structured approach to defining clear safety and security goals and technical concepts, allowing effective risk management and performance evaluation. By aligning risk mitigation activities with overall system objectives, this work contributes to the development of automotive systems that meet the highest standards of safety and security.

Advancement of Risk Analysis Methodologies

The research introduces novel risk analysis techniques that are tailored to the complexities of highly automated vehicles. By addressing the multidimensional nature of automotive risks, this work provides a foundation for future advances in risk assessment and management.

This dissertation makes significant contributions to the fields of automation, electronics, electrical engineering, and space technologies by addressing the critical interplay between safety and cybersecurity in highly automated mission-critical vehicle systems. The proposed framework provides a foundation for the development of safer, more secure, and reliable systems in the face of increasing complexity and connectivity. In vehicles, where the role of electronics and control elements for mechanical components is growing, autonomous driving will primarily depend on the reliable functioning of electronic systems and software, rather than on the mechanical aspects of vehicle operation. Therefore, ensuring the safety and cybersecurity of these systems is crucial for the future of autonomous transportation.

Chapter 2

State of the Art Review

2.1 New Product Development

In the development of intelligent vehicles, the level of complexity of the system is increasing.The automotive industry faces challenges in terms of the requirements for ensuring the safety and security of autonomous vehicles and their surroundings, under any and all circumstances. Concurrently, Original Equipment Manufacturerss are looking for a way to increase the efficiency and effectiveness of design processes, as well as to shorten the time and decrease the cost of developing new products. Research on the management of large engineering programs (US space programs) has identified the following generic challenges in the management of highly complex programs [42]:

- Reactive program execution;
- A lack of stability, clarity, and completeness of requirements;
- Insufficient alignment and coordination of the extended enterprise;
- A non-optimised value stream throughout the entire enterprise;
- Unclear roles, responsibilities, and accountability;
- Insufficient team skills and unproductive behaviour and culture;
- Insufficient program planning;
- Improper metrics, metric systems, and key performance indicators;
- A lack of proactive management of program uncertainties and risks;
- Poor program acquisition and contracting practices.

New product development (NPD) is usually the most complex process that companies realize. First, this process involves many stakeholders, both internal and external, with different points of view, expectations, and requirements that are addressed to the product and the NPD process itself. NPD processes are usually related to long-term projects: in this case, innovative products with an uncertainty factor due to the products, technologies, and/or standards incorporated into the product. A generic NPD process flow is presented in Figure 2.1.

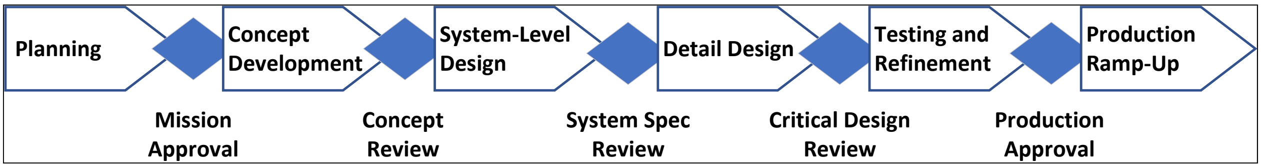


Figure 2.1: Product development process. Source: Based on [43].

In practice, the process alternates between stages and gates; in the literature, this is called the stage-gate approach and was first presented by Robert Cooper [44]. In this process, the concept phase and the system-level design phase are especially critical because, in these phases, designers ensure that the right products will be designed and delivered. In the concept stage, all the requirements related to the designed product must be understood and considered. To increase the effectiveness of NPD processes, companies implement the lean approach, which is well known and widely implemented in production processes. The lean approach developed from the Toyota Production System [45] and was later popularized by American researchers [46]. The first implementations of the lean approach in NPD were conducted in the early 2000s [47–49].

NPD processes should consider the following principles, based on [50]:

- **Identify value:** All the process activities should focus on value generation.
- **Create value stream:** The value defined in the previous step is generated as a result of the process. The opposite of the value is waste. In this step, sources of different types of waste should be identified (presented in Table 2.1) within the processes. This step also consists of the improvement of the process and the outcomes (products) of the process; can be classified as value-added, necessary but non-value-added, or non-value-added (pure waste) activities;
- **Ensure process flow:** Materials and information should constantly flow in the process (stream) without slowdowns, interruptions, delays, or unnecessary stoppages;
- **Establish pull control:** Materials and information are produced at the appropriate time and in the expected quality and amount;
- **Implement perfection:** All activities are performed with the expected quality and perfectly for the first time;
- **Establish rules of respect for people:** For engineering teams from different domains,interpersonal relations that motivate people are crucial. This stage focuses on team-building,trust, and involvement actions.

The first five steps are cyclic. The rules of respect have an impact on all the other steps. Currently, the agile approach is widely implemented, especially for ECU design and development. In general, these two approaches (lean and agile) are similar [52]. Therefore, all stakeholders should be able to make the right decisions based on all the necessary information. This applies not only to technical topics, but also to other

Table 2.1: Type of waste in NDP processes. Based on [51].

Type of Waste	Description/Examples
Overproduction	Creating information that will not be used (e.g., waiting for available resources). Working on unnecessary activities instead of those that are currently needed.
Waiting	Waiting for engineers, information, materials for reviews, decisions, or further actions.
Wrong process	Performing unnecessary activities or tasks. This could also be related to the design of new components instead of using standards/carry-overs.
Transportation	Unnecessary flows of people, information, or materials, e.g., hand-offs.
Motion	Unnecessary actions in the performance of tasks, such as non-productive meeting or project reviews and redundant status reports.
Inventory	Collecting information that is not currently being used. In practice, inventory waste is a result of overproduction.
Correction	All activities related to quality control but not related to quality assurance, as well as reworks.

topics related to the designed product, such as FuSa, SOTIF, or CySe. The main challenges in the planning and concept development stages are the clarification and understanding of all requirements, as well as the creation of the right product concept.

2.2 The "V" Process Model

The "V" model is a widely adopted systems engineering framework, especially for Intelligent Transportation Systems (ITS) [53]. Visually represents the systems engineering process, progressing from system definition on the left side to system verification and validation on the right. Developed in the 1980s, the model has been adapted over time, adding "wings" to illustrate the broader ITS project life cycle, including regional ITS architecture, feasibility studies and concept exploration on the left wing, and operations, maintenance, and retirement on the right wing. The left side focuses on decomposing the system into subsystems and components, aligning requirements at each level. Development follows a series of baselines, ensuring that each phase supports the subsequent one, leading to system implementation and integration at the "V" base and culminating in validation against user needs. Symmetry in the model highlights the interdependence of initial definitions and final validations, with decision points throughout ensuring readiness for each progression step. The framework has been standardized as ISO/IEC 15288 [54] and is followed as a base for the development of automotive systems. Figure 2.2 presents the generic engineering approach from a system development perspective.

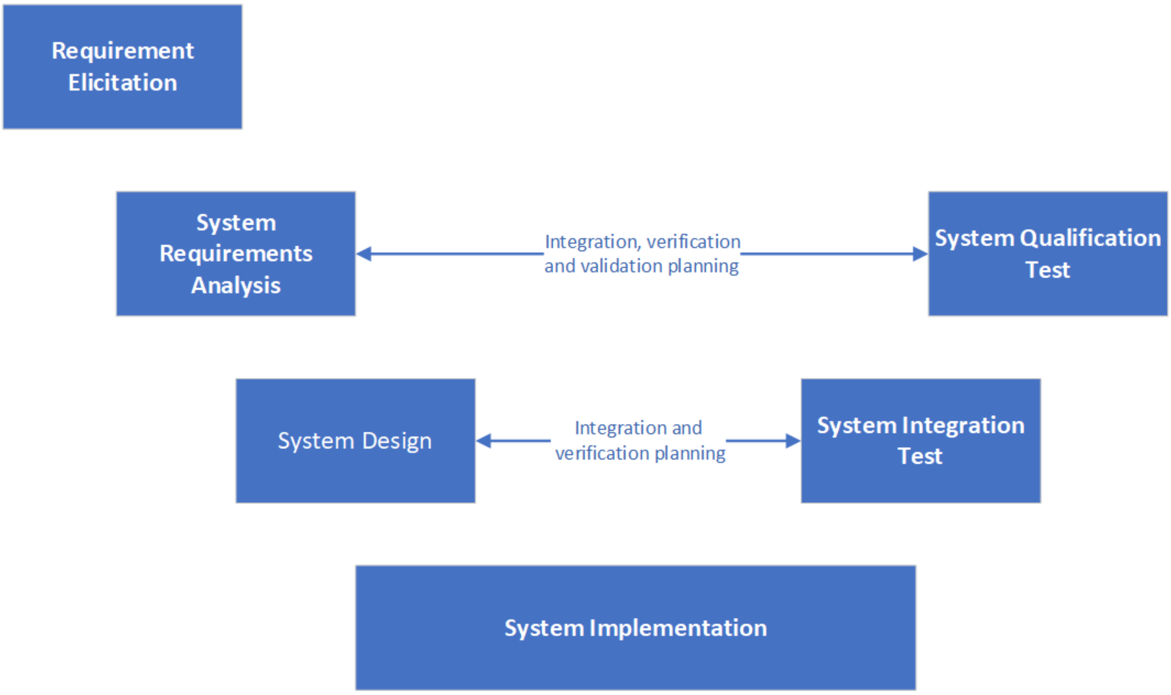

Requirement Elicitation
System Requirements Analysis
Integration, verification and validation planning
System Qualification Test
System Design
Integration and verification planning
System Integration Test
System Implementation

Figure 2.2: Generic V-model from the system development perspective. Source: Based on [55].

2.3 Automotive Standards

The challenges in introducing the new product into the market apply to the automotive industry as well. Currently, to cover all safety related use cases for autonomous vehicles OEMs use the ISO 26262: 2018 [5] standard as an extension to the standard V-model. However,that standard covers only the faults resulting from system malfunctions, whereas the interaction of an autonomous vehicle with an environment goes far beyond this area. The new ISO PAS 21448 [6], which defines the paradigm of Safety of Intended Functionality (SOTIF), increases the level of safety for future intelligent vehicles. However, an entire autonomous ecosystem can coexist only in conjunction with cybersecurity. Finished in 2021, ISO 21434 [13] is initially filling this gap. However, the challenge still remains of how to increase the safety of an electric and autonomous vehicle in the design phase. Therefore, complete integration of the analytical methods used for vehicle design is fundamental. This has a direct impact on the time and effort required for the development of an Electronic Control Unit (ECU) [9]. The identification of a universal vehicle design scheme, as well as the establishment of a way of working among engineers from different fields, such as FuSa and CySe, is challenging [24]. Moreover, the entire design process can be placed in the ASPICE [55] frames [33, 56]. The market demand for environmental friendliness, safety, economic efficiency, and user friendliness requires increasingly complex innovations in shorter intervals. The shorter development cycles and increasing reliability requirements require the improvement of development processes.

Automotive cybersecurity is still a relatively new domain in the industry. It is growing rapidly together with the development of car connectivity. Unfortunately, currently used methods and standards for the development of automotive projects, such as, ISO/IEC/IEEE 15288 Systems and software engineering systems life cycle processes [54], the Functional Safety ISO 26262 series or ISO 21434 for Cybersecurity, are not sufficient to cover threats related to connected and autonomous vehicles in the future. The automotive industry was trying to close this gap by introducing a set of guidelines and best practices related to cybersecurity related to cybersecurity, such as NHTSA's "Cybersecurity Best Practices for Modern Vehicles" [57], Auto-ISAC's "Automotive ISAC Best Practices" [58] and SAE J3061 'Cybersecurity Guidebook for Cyber-Physical Vehicle Systems', as well as localized frameworks such as Japan's 'Approaches for Vehicle Information Security' [59] and the European Union's "ENISA Good Practices for the Security of Smart Cars" [60]. However, in principle, they were received by the automotive industry as suggestions rather than as officially mandated requirements [61].

Undoubtedly, all risks must be taken into account during the early stages of the engineering life-cycle in order to avoid hazardous situations on road, due to the cyberattacks [12].The other aspects, which are unique for cyber-risks in particular, are adaptive and the dynamic of cyber threats. As defense becomes more sophisticated, so do attacks, and the attack response circle widens in unpredictable ways. Therefore, the concept of cyber resilience shall also be introduced into the development cycle [62]. It is part of a risk-based analytical approach and focuses on the ability to prepare for and recover quickly from both known and unknown threats. This concept recognizes the variety of dependencies across the cyber-domain - physical, information, cognitive, and social environments, in which the system exists. The integration of cyber-resilience is one of the answers for rapid evolution, unprecedented nature, and the wide range of cyber threats [62]. This shall allow to prioritize system upgrades (Over-the-Air Updates) and system maintenance.

2.3.1 Automotive Functional Safety

FuSa and reliability have become critical parts of automotive safety applications. Advanced Driver Assistance System (ADAS) are paving the way for future autonomous vehicles. However, the tolerable risk level remains the fundamental challenge for engineering departments during the design of complex systems. To reduce the risk of systematic failures and incidental hardware failures, the ISO 26262 series [5] provides directions for mitigating these risks. It provides an extensive set of requirements and processes for the entire developmental life cycle [5].

Achievement of FuSa can be achieved by the following:

- Tailoring activities for the automotive safety development cycle;
- Determining the automotive-specific integrity level, or Automotive Safety Integrity Level (ASIL);
- Using the ASIL to find which requirements of ISO 26262 should be followed to avoid unreasonable and continuing risks;
- Providing the requirements for FuSa management, design, implementation, verification, validation, and acceptance measures;
- Defining the customer – supplier relationship requirements.

Safety activities are closely connected with common function- and quality-oriented activities and output products. All are addressed and are deeply described in the ISO 26262 series.

FuSa, which is defined in ISO 26262 as ’the absence of unreasonable risk due to hazard caused by malfunctioning behavior of electrical and electronic systems’, brings to product development a change from a quality management system to a safety-oriented culture. The standard demands evidence-based safety. It enforces sticker documentation and around 130 new work packages, which undoubtedly increase the efforts required in the development of each product [63].

The basic chain of safety implications can be represented as follows: Malfunction → Hazard → Risk → Required Risk Reduction.

Malfunctions are classified by the standard into two types:

- Systematic failures - these occur deterministically during the development, manufacturing,or maintenance phases;
- Random failures - incidental hardware failures that occur during a hardware component’s lifetime.

In most cases, systematic failures are caused by an inadequate mechanism in the process. They can be solved by changes in the documentation, manufacturing process,operational procedures, etc. However, random failures are discussed during the design and verification of the Hardware and Software by using safety mechanisms. This enables a product architecture to detect orcorrect malfunctions. This is indicated by assigning an automotive safety integrity level. The concept phase of FuSa is carried out usually by the original equipment manufacturer. The OEM is responsible for assigning a function to a certain system at the vehicle level. The ASIL level and safety goals are also determined there. After these activities, the FuSa requirements are derived. The electronics provider is also involved in the FuSa analysis. Each piece of electronic equipment that is marked as related to safety and will be mounted in the vehicle requires the following [64]:

- Failure Mode Effect and Diagnostic Analysis (FMEDA);
- Timing–fault-tolerant Time Interval (FTTI) and Diagnostic Test Interval (DTI);
- Dependent Failure Analysis (DFA).

In general, FuSa involves the implementation of active methods in order to develop the necessary level of risk mitigation. Furthermore, from a design perspective, Tier 1 suppliers are responsible for the management of safety requirements, the analysis of system failures, and the creation of a technical safety concept. This should be an input for the development team in order to ensure the ASIL level. During project development, all FuSa activities should be verified and managed by a dedicated functional safety manager.

Although safety management networks reduce systematic and random failures and therefore increase safety and quality, they bring additional process overhead. With the increasing level of complexity of autonomous vehicles, FuSa analysis alone cannot provide enough measures to reduce hazardous risks. Other aspects of connected vehicles, such as cybersecurity, must also be considered. Only with a holistic approach to the system can an adequate safety level be ensured.

2.3.2 Automotive Cybersecurity

UNECE Regulation - ECE/TRANS/WP.29/2020/79

Due to the regulatory structure established by the Working Party (WP.29) of the World Forum on Harmonization of Vehicle Regulations within United Nations Economic Commission for Europe (UNECE), innovative vehicle technologies can be introduced to the market. This framework focuses on global vehicle safety development, reduction of environmental pollution and energy consumption, and advancement of anti-theft capabilities [65]. WP.29 established six permanent Working Parties (GRs), which are subsidiary bodies that consider specialized tasks and consist of people with specialized knowledge. One of them is the Automated and Connected Vehicles Working Party (GRVA). GRVA consists of several working groups, one of them being for 'Cybersecurity and (OTA) software updates (CS / OTA)' [66].

The "ECE/TRANS/WP.29/2020/79 Proposal for a new UN regulation on uniform provisions regarding vehicle approval with respect to cyber security and cyber security management systems", which was prepared by the CS/OTA working party, was published on 23 June 2020 [66].

The main areas of interest for this group are Cybersecurity Management Systems (CSMS) and vehicle security. CSMS refers to a systematic risk-based approach that defines organizational processes, responsibilities, and governance to reduce the risks associated with cyber threats to vehicles and protect them from cyberattacks [65]. In this case, vehicle security is the application of a CSMS to a specific type of vehicle. According to the regulation, a vehicle type is defined as one that does not differ in at least one of the following essential ways:

- The OEM's classification of the vehicle type;
- Aspects of the electric/electronic architecture and external interfaces that are critical in terms of cyber security.

The core requirements for a CSMS cover the entire life cycle, from development through production to the post-production phase. CSMS is defined as covering processes for the following [66]:

- Managing cybersecurity;
- Identifying risks of vehicle types;
- Assessing, categorizing, and treating identified risks;
- Confirming and checking if the identified risks are being managed properly;
- Testing the cyber security of a vehicle type;
- Keeping the risk assessment current;
- Monitoring, detecting, and responding to cyberattacks, cyber threats, and vulnerabilities of vehicle types and determining whether the cyber security measures in place are still effective considering recently identified cyber threats and vulnerabilities;

- Providing relevant data for forensic analysis.

Moreover, CSMS must cover the entire supply chain. In summary, the aim is for an OEM to establish a certified cybersecurity management system at the enterprise level. This covers the first discipline of the UNECE: 'Managing vehicle cybersecurity'.

The implementation timeline defined in the requirements of WP.29 is extremely challenging for the entire automotive industry. By 2022, the EU regulation will apply for new vehicle types (EU and Japan), and by 2024 it will apply for the first registrations (EU and Japan).

UNECE requirement paved the way for the industry standardization of cybersecurity, which resulted in the creation of ISO 21434 [13].

Automotive Cybersecurity Standard

Starting in 2016, SAE International, the professional association and standards development organization for engineering professionals, and International Organization for Standardization (ISO), an independent, non-governmental organization composed of representatives of various national standards organizations, decided to work together to issue the industry standard related to automotive cybersecurity.

In the past, both bodies have worked on standards related to automotive safety and security. ISO 26262 [5] set functional safety standards and SAE J3061 [67] set the foundation for cybersecurity standards. ISO and SAE organizations, together with OEMs, ECU suppliers, cybersecurity vendors, governing organizations, and automotive experts from various countries, created a working group to develop a new complete standard for automotive cybersecurity. The ISO/SAE 21434 [13] draft was created focusing on risk management, product development, production, operation, maintenance, decommissioning, process overview and fostering a positive cybersecurity culture in the industry.

ISO/SAE 21434 was specifically developed to provide a high level of safety and security for the ultimate road user / driver. It shall ensure that the risk levels and corresponding cybersecurity measures are set based on the final driver impact. In addition to a standardized cybersecurity framework, the standard defines cybersecurity as an integral part of engineering throughout the entire vehicle life cycle. Starting from the conceptual phase, development, testing and validation, manufacturing, post-production, and decommissioning, it ensures the cybersecurity involvement. Furthermore, the standard requires effective methods for learning, training, and proper communication related to automotive cybersecurity.

The ISO/SAE 21434, explicitly requires from the OEMs the threats and risks analysis throughout a vehicle lifecycle. It shall determine to what extent the road user can be impacted by cyber threats and vulnerabilities in automotive vehicles. The work product is named TARA. The standard defines the way in which the analysis shall be performed and what it consists of.

The document covers, in Annex E, the definition of Cybersecurity Assurance Level (CAL). The need for such a classification was described in [68]. It can be used to provide assurance that the assets of an item or component are adequately protected against the relevant threat scenarios. The CAL does not specify the technical requirements; it shall be used as a guide for cybersecurity engineering, providing a common language for communicating cybersecurity assurance requirements between organizations involved [13].

The ISO/SAE 21434 provides example CALs with their rigors in cybersecurity assurance measures, as summarized in Table 2.2.

A CAL can be determined on the basis of the TARA analysis scenarios. It can be assigned based on the maximum impact and the attack vector of the related threat scenarios. The CAL level shall have an impact on architectural design verification methods, integration verification methods, test case derivation methods, structural coverage metrics at the software unit level, structural coverage at the software architectural level, component testing methods, etc.

Analyzing the structure and content of ISO 21434, it has a tremendous impact on vehicle engineering. Cybersecurity work products are available in each process area; therefore, it requires additional effort on each development step, to be compliant with the ISO 21434 standard. In order to reduce the impact of engineering effort and project timing, more methods should be analyzed to seamlessly incorporate cybersecurity culture into product development.

Table 2.2: Example number of CALs and expected rigor in cybersecurity assurance measures. Based on [13].

Level	Description	Philosophy	Difference from Previous Level
CAL1	Developers or users require a low to moderate level of independently assured cybersecurity	Functionally and structurally tested.	Requiring developer testing, and a vulnerability analysis.
CAL2	Developers or users require a moderate level of independently assured cybersecurity and require a thorough investigation of the item without substantial re-engineering	Methodically tested and checked. It provides assurance through the use of development environment controls.	Procedures that provide moderate confidence that the item will not be tampered with during development.
CAL3	Developers or users require a moderate to high level of independently assured cybersecurity in conventional commodity items and are prepared to incur additional security-specific engineering costs.	Methodically designed, tested, and reviewed (resistance to penetration attackers with an enhanced-basic attack potential).	Requiring more design description, the implementation representation for the security functions, and improved mechanisms and/or procedures that provide confidence that the item will not be tampered with during development
CAL4	Developers or users require the highest-level rigor.	Advanced methodically designed, tested, and reviewed.	Independent tested and reviewed

2.3.3 Automotive Safety of the Intended Functionality

As an outcome of vehicle development, connected and self-driving vehicles are soon expected to replace human drivers. To work flawlessly, a system of linked cooperative Automated Vehicles (AV), which is called the Cooperative Intelligent Transport System (C-ITS), will have to integrate all hazard scenarios. To consider all possibilities, a system risk analysis should include a safety analysis according to ISO 26262 [5], as well as other possible threat scenarios, such as cyber threats. Only by identifying the communication links between various phases of safety and cybersecurity processes can this kind of analysis be prepared. It can include, for example, cyber threats that cause safety losses, or an integrated requirement analysis [69].

However, in order to assess the complete range of risks for systems that rely on sensing the external or internal environment, as well as the hazard behavior caused by the intended functionality or performance limitations of a fault-free system in the ISO 26262 series, ISO/PAS 21448 [6] must be considered.

Examples of limitations given by the standard include the following:

- The function's inability to correctly comprehend the situation and operate safely,which includes functions that employ machine learning algorithms;
- Inadequate function robustness in the face of sensor input variations or varying environmental conditions [6].

The SOTIF applies primarily to emergency intervention systems (e.g., emergency braking systems) and ADAS with automation levels of 1 or 2 according to the SAE standard J3016 [70]. It can also be considered for higher levels of automation systems, although additional measures may be required.

The SOTIF activities are implemented during the design, verification, and validation phases. However, the entire analysis should be followed by an extensive system analysis in order to understand user functions, behaviors, and limitations (ISO / PAS 21448) [71].

For the SOTIF analysis, the relevant hazardous use cases are classified into four areas:

- 1 – known safe scenarios;
- 2 – known unsafe scenarios;
- 3 – unknown unsafe scenarios;
- 4 – unknown safe scenarios.

The primary goal of the standard implementation is to shrink Areas 2 and 3 while expanding Area 1. Area 4 is included only for completeness and is not considered in the analysis, as shown in Figure 2.3. In summary, the analysis tries to identify the unknown and unsafe areas of operation and contain them within an acceptable level of risk. However, it adds another level of processes that should be considered for project development in the standard V-model. To reduce risks and timing of a project, the SOTIF must be evaluated together with cybersecurity and safety measures. To complete the safety ecosystem, vehicle and environmental factors must also be considered, as represented in Table 2.3. This requires interdisciplinary engineering cooperation to include all possible hazardous events. The study should be expanded to define how vehicle and environmental factors can be treated together, which will complete the safety ecosystem of the AV.

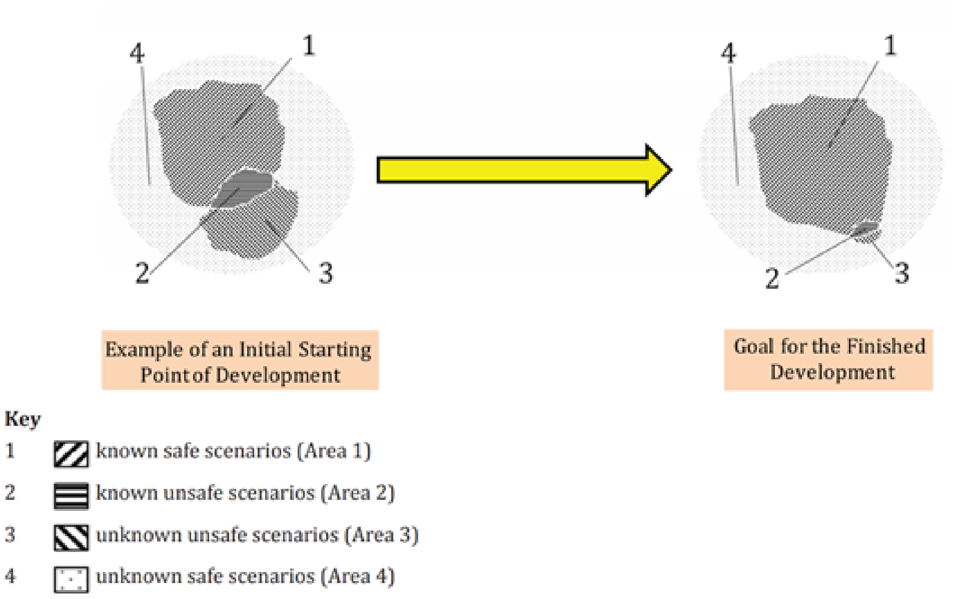

4
1
2
3
4
1
2
3
Example of an Initial Starting Point of Development
Goal for the Finished Development
Key
1 ▨ known safe scenarios (Area 1)
2 ☰ known unsafe scenarios (Area 2)
3 ▧ unknown unsafe scenarios (Area 3)
4 ⬚ unknown safe scenarios (Area 4)

Figure 2.3: Evolution of the scenario categories resulting from the ISO/PAS 21448 activities. Based on [6].

Table 2.3: Hazardous event of AV and required Standards. Based on [6].

Source	Hazardous event	Standard
Vehicle Factor	E/E System failure	ISO 26262 series
	Performance limitations or insufficient situational awareness, with or without reasonably foreseeable misuse	ISO/PAS 21448
	Reasonably foreseeable misuse, incorrect HMI (e.g. user confusion, user overload)	ISO/PAS 21448 ISO 26262 series European statement of principal on design of human-machine interface
	Hazards caused by the system technology	Specific standards
Environmental Factor	Successful attack exploiting vehicle security vulnerabilities	ISO 21434
	Impact from active Infrastructure and/or vehicle to vehicle communication, external devices and cloud services	ISO 20077 series ISO 26262 series ISO 21434
	Impact from car surroundings (other users, “passive” infrastructure, environmental conditions: weather, Electro-Magnetic Interference…)	ISO/PAS 21448 ISO 26262 series

2.3.4 Automotive Standard Development Method

In today's software-driven automotive industry, the quality of code plays a critical role, especially in safety-critical systems where even minor software vulnerabilities can introduce risks leading to accidents, injuries, and fatalities [18, 20–22]. To address these concerns, vehicle manufacturers are increasingly adopting rigorous safety standards and development processes that emphasize risk mitigation, synergy between safety and security teams, and streamlined development to minimize errors and improve overall system reliability. When applying standard development methods, OEMs are focusing on:

- Evaluating the software capability of suppliers;
- Including contractual demands related to software quality;
- Performing supplier software capability assessments both before and during contract performance.

A common development process and monitoring framework, developed by major OEMs and Tier 1 suppliers and currently used throughout the vehicle industry, is Automotive SPICE®. Version 3.1 of the Automotive Software Process Improvement and Capability Determination (ASPICE)®Process Reference and Assessment Model is available and currently used as a Verband der Automobilindustrie (VDA) standard [55]. Although it primarily focuses on the software and system activities of a product, version 3.1 of the standard allows the inclusion of additional engineering disciplines, such as hardware engineering and mechanical engineering, and the corresponding domain-specific processes, depending on the product being developed.

Processes are classified by category in the process reference model and then further divided into process groups based on the types of operations they address. According to the VDA [55], the three process categories are:

- Primary life-cycle processes;
- Organizational life-cycle processes;
- Supporting life-cycle processes.

Each process is described in the form of a purpose statement that includes the unique functional objectives of the process when performed in a specific environment. There is a predefined list of results for each purpose statement, defining the expected results of process performance. In principle, ASPICE®follows the development of a generic V-model-based system, describing all the activities to be performed during system development and their results. The left side of the V-model represents the definition of the project, while the right side focuses on integration and validation.

The current process reference model from version 3.1 of ASPICE®is shown in Figure 2.4.

ISO 21434 standard [13] enhances the ASPICE®framework. The left side of the V-model for CySe includes the following:

- Item definition;

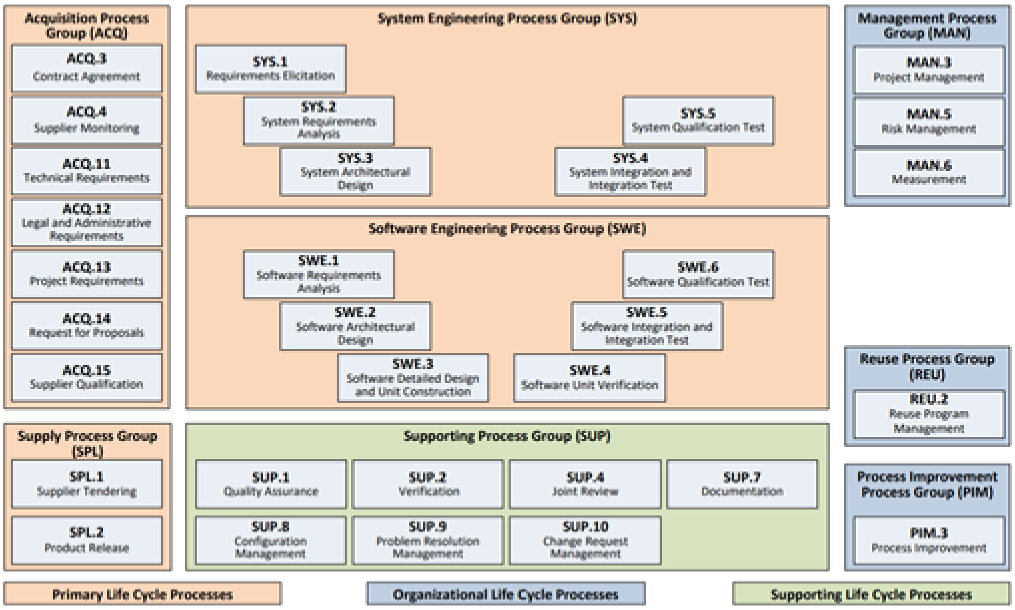

Acquisition Process Group (ACQ)
ACQ.3 Contract Agreement
ACQ.4 Supplier Monitoring
ACQ.11 Technical Requirements
ACQ.12 Legal and Administrative Requirements
ACQ.13 Project Requirements
ACQ.14 Request for Proposals
ACQ.15 Supplier Qualification
System Engineering Process Group (SYS)
SYS.1 Requirements Elicitation
SYS.2 System Requirements Analysis
SYS.3 System Architectural Design
SYS.4 System Integration and Integration Test
SYS.5 System Qualification Test
Software Engineering Process Group (SWE)
SWE.1 Software Requirements Analysis
SWE.2 Software Architectural Design
SWE.3 Software Detailed Design and Unit Construction
SWE.4 Software Unit Verification
SWE.5 Software Integration and Integration Test
SWE.6 Software Qualification Test
Management Process Group (MAN)
MAN.3 Project Management
MAN.5 Risk Management
MAN.6 Measurement
Reuse Process Group (REU)
REU.2 Reuse Program Management
Supply Process Group (SPL)
SPL.1 Supplier Tendering
SPL.2 Product Release
Supporting Process Group (SUP)
SUP.1 Quality Assurance
SUP.2 Verification
SUP.4 Joint Review
SUP.7 Documentation
SUP.8 Configuration Management
SUP.9 Problem Resolution Management
SUP.10 Change Request Management
Process Improvement Process Group (PIM)
PIM.3 Process Improvement
Primary Life Cycle Processes
Organizational Life Cycle Processes
Supporting Life Cycle Processes

Figure 2.4: Automotive SPICE®process reference model - Overview. Based on [72].

- Cybersecurity goals;
- Cybersecurity requirements;
- Cybersecurity concept;
- System Cybersecurity requirements;
- System architectural design;
- Hardware cybersecurity requirements;
- Hardware architectural design;
- Software cybersecurity requirements;
- Software architectural design.

In the same time, the right side of the V-model includes the following:

- Cybersecurity validation,;
- Item integration verification;
- System integration verification;
- Hardware integration verification;
- Software integration verification;

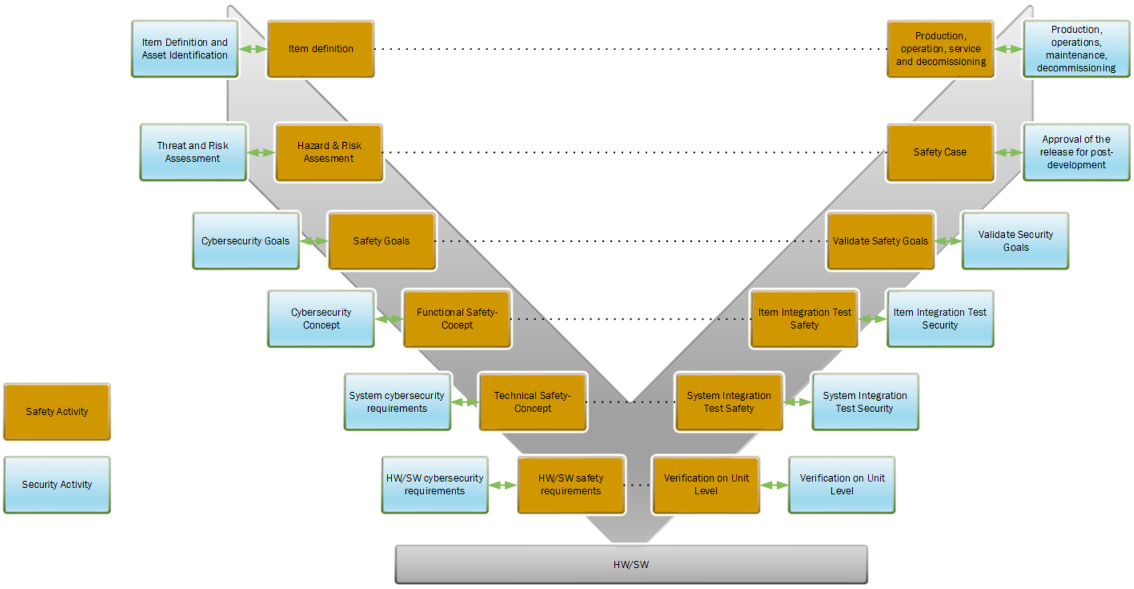

Item Definition and Asset Identification
Item definition
Production, operation, service and decomissioning
Production, operations, maintenance, decommissioning
Threat and Risk Assessment
Hazard & Risk Assesment
Safety Case
Approval of the release for post-development
Cybersecurity Goals
Safety Goals
Validate Safety Goals
Validate Security Goals
Cybersecurity Concept
Functional Safety-Cocept
Item Integration Test Safety
Item Integration Test Security
Safety Activity
Security Activity
System cybersecurity requirements
Technical Safety-Concept
System Integration Test Safety
System Integration Test Security
HW/SW cybersecurity requirements
HW/SW safety requirements
Verification on Unit Level
Verification on Unit Level
HW/SW

Figure 2.5: V-model for Safety and Cybersecurity activities according to the ISO 26262 and ISO/SAE 21434 standards.

Definitely, there is an overlap of the system engineering approach between cybersecurity and safety processes. The processes dependencies are shown in Figure 2.5.

Similarly, ISO / PASS 21448 [6], defines the possible interactions of product development activities with well-established ISO 26262 series processes. The left side of the V-model, responsible for the project definition, shall be covered by:

- Clause 5 - Functional and System Specification;
- Clause 6 - SOTIF related Hazard Identification and Risk Evaluation;
- Clause 7 - Identification and Evaluation of Triggering Events;
- Clause 8 - Functional Modification to reduce SOTIF risks.

The right side of the V-model, responsible for the project test and integration, shall be covered by:

- Clause 9 - Definition of the Verification and Validation Strategy;
- Clause 10 - Verification of the SOTIF: Evaluate Known Scenarios;
- Clause 11 - Validation of the SOTIF: Evaluate Unknown Scenarios;
- Clause 12 - Methodology and Criteria for SOTIF Release.

Taking into account the relationship of all processes, the combined V model for autonomous cyber-physical systems can be proposed, as shown in Figure 2.6. It summarizes well both the interdependencies as well as the challenges of constant verification and validation, which indicates the iteration approach.

In this dissertation a more detailed analysis is performed for all process areas, to identify overlapping processes and define similarities specifically in the design phase.This approach shall manage the risks for the development of new cyber-physical systems in a comprehensive way.

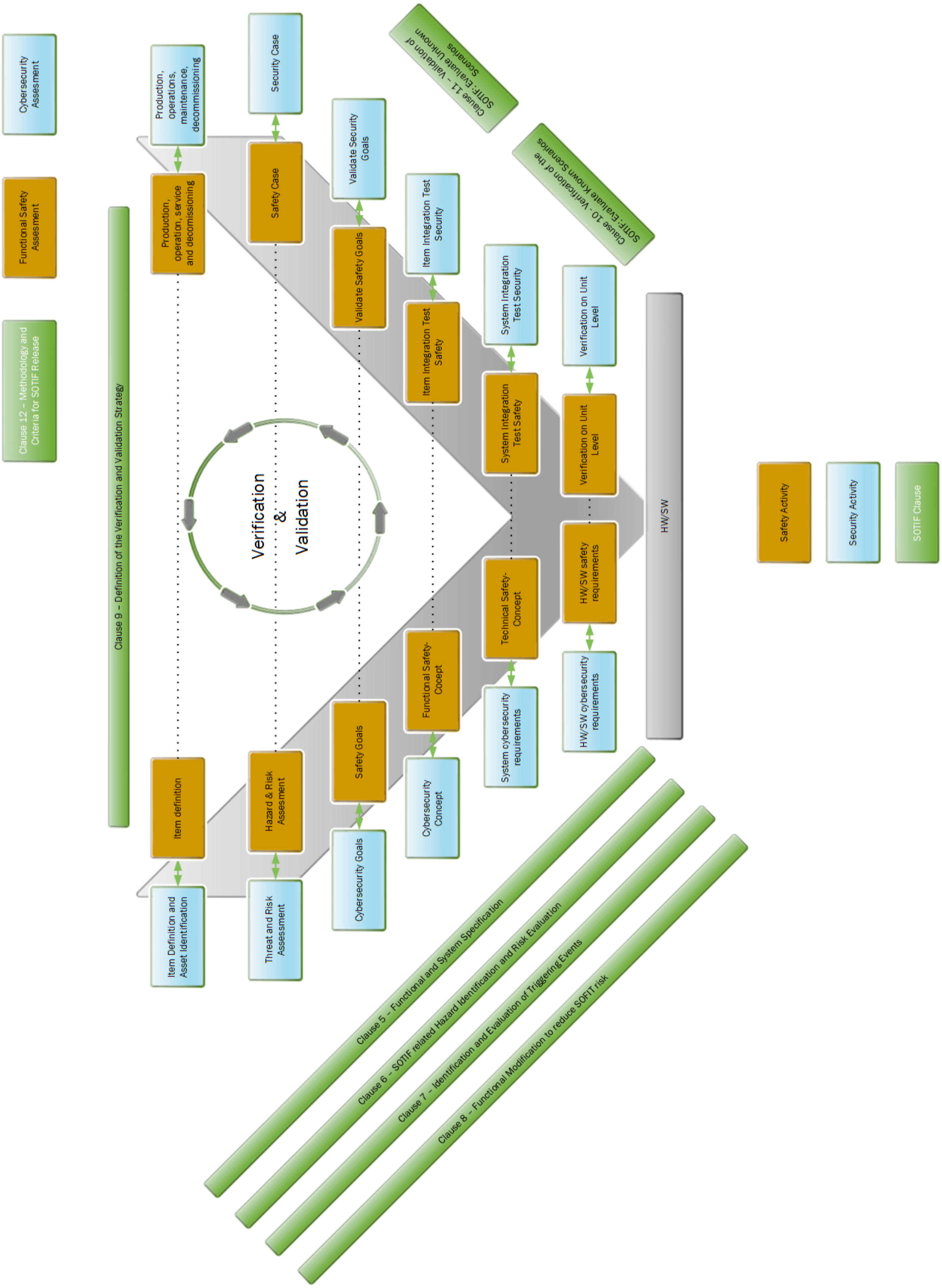

Cybersecurity Assesment
Functional Safety Assesment
Clause 12 – Methodology and Criteria for SOTIF Release
Clause 9 – Definition of the Verification and Validation Strategy
Production, operations, maintenance, decommissioning
Production, operation, service and decomissioning
Security Case
Safety Case
Validate Security Goals
Validate Safety Goals
Clause 11 - Validation of SOTIF: Evaluate Unknown Scenarios
Item Integration Test Security
Item Integration Test Safety
Clause 10 - Verification of the SOTIF: Evaluate Known Scenarios
System Integration Test Security
System Integration Test Safety
Verification on Unit Level
Verification on Unit Level
HW/SW
Verification & Validation
Item definition
Item Definition and Asset Identification
Hazard & Risk Assesment
Threat and Risk Assessment
Safety Goals
Cybersecurity Goals
Functional Safety-Cocept
Cybersecurity Concept
Technical Safety-Concept
System cybersecurity requirements
HW/SW safety requirements
HW/SW cybersecurity requirements
Clause 5 - Functional and System Specification
Clause 6 - SOTIF related Hazard Identification and Risk Evaluation
Clause 7 - Identification and Evaluation of Triggering Events
Clause 8 - Functional Modification to reduce SOFIT risk
Safety Activity
Security Activity
SOTIF Clause

Figure 2.6: Combined V-model for autonomous, cyber-physical systems.

2.3.5 Automotive's Further Standardization

In addition to standardized processes for managing development and the vehicle risks, there is also a need for a standard template, which can be used during the system design, to mitigate known cyber-risks. The widely used concept for, e.g. enterprise systems, networking systems, etc., is the design patterns. Patterns support the understanding of problems and their solutions. Therefore, the given problem can be solved in the most optimized way. The types of patterns for the automotive domain, proposed by [38], are Authorization, Black List, DDoS Redundancy, Firewall, Multifactor authentication, Multilevel Security, Signature IDPS, Symmetric Encryption, Tamper resistance, and Third-Party Validation. The authors are working on the standard way in which the automotive security pattern can be defined. It shall include the name, intent, motivation, properties, applicability, structure, behavior, constraints, consequences, known uses, and related patterns. The choice of pattern shall be taken into account during the Threat Analysis and Risk Assessment process.

In [38] the main focus is on two patterns: Signature-based IDPS and the Blacklist. The Intrusion Detection System Pattern shall provide the mechanism for detecting anomalies in network traffic by using a baseline characteristic of the traffic. However, the blacklist intends to monitor the traffic of potentially malicious addresses in the network. The network traffic shall be blocked in case of the malicious ECU. In this case, the Blacklist is becoming the part of the Intrusion Prevention System (IPS), which complements the Intrusion Detection System (IDS) capabilities.

The AUTOSAR Consortium has already released the first version of the Automotive Intrusion Detection System Design Requirements [73], the Intrusion Detection System Protocol Specification [74], and the Intrusion Detection System Manager [75]. The definition is tailored for both Classic and Adaptive (POSIX) [76] based automotive systems. The list of patterns applicable for the automotive domain and its development shall be further expanded to resolve the requirements included in ISO / SAE 21434. This would complement existing efforts in standardization working groups related to Cybersecurity Assurance Level (CAL) and Targeted Attack Feasibility (TAF) in ISO/SAE 8475 [77], as well as Cybersecurity Verification and Validation in ISO/PAS 8477 and Information Security, Cybersecurity, and Privacy Protection in ISO/IEC 5888 [78].

2.4 Vehicle Architecture Overview

With the transition to autonomous vehicles, the car shall be redefined. It starts with the electric/electric architecture of road vehicles. During the last 50 years, enormous improvements in the complexity and number of Electronic Control Unit (ECU)s can be observed in vehicles [79]. Starting from several ECU at the beginning of the 00s, industry is now reaching the average level of 50. This number is still increasing [79]. Following the trend of vehicle autonomy, Over-The-Air Updates (OTA), connectivity, and electrification, Original Equipment Manufacturers (OEM)s are becoming software companies [80]. However, all newly added technologies must follow strict automotive manufacturing processes, which are not taken into account in the production of IT electronics [81]. In the automotive domain, safety and real-time processing will always remain the main concern.

The cybersecurity approach in embedded systems within the automotive industry places greater emphasis on establishing proper hardware security roots of trust and effective utilization of cryptographic engines for faster cryptographic calculations. This ensures robust protection against potential cyberthreats and unauthorized access to sensitive automotive systems.

Furthermore, it is important to note that in the realm of IT, real-time, safety-critical systems are not prevalent, and timing requirements are not as critical. However, in the automotive industry, real-time responsiveness and safety-critical functionality are paramount. The timing requirements must be meticulously managed to ensure safe vehicle operation and protection of both occupants and pedestrians. Therefore, a key difference between standard IT solutions and those required by the automotive industry lies in the emphasis on safety, market regulations, and standards. Automotive solutions prioritize safety considerations to a much greater extent than typical IT solutions. The critical nature of automotive electronics necessitates a thorough examination of the safety implications for end users and their environments.

Unlike standard IT solutions, automotive electronics undergo rigorous testing processes and adhere to strict development and change management protocols. This encompasses comprehensive documentation, detailed analysis, and meticulous design preparation to ensure that safety standards are not only met, but also maintained throughout the life cycle of the automotive system.

The unique focus of the automotive industry on safety demands a higher level of scrutiny and precision in the design, development, and implementation of solutions compared to the more conventional approach taken in standard IT environments.

Currently, software development is done in parallel with hardware development. In this model, software is an integrated part of a hardware [82]. Even with the OTA update, not all parts of the software can be updated, due to safety and security reasons. Still, a workshop visit is needed, in case of a critical update campaign.

To address the growing demand for vehicle customization while maintaining efficient development, the automotive industry is exploring scalable and modular vehicle architectures. Currently, OEMs maintain multiple architecture variants [81]. This can lead to significant development overheads due to increased complexity. The scalable and modular architectures offer a promising solution [79–82].

The trend in the market is to change the entire thinking of vehicles. Instead of traditional geometric-oriented architectures [82], there shall be a feature-oriented approach. This means an introduction of Service-Oriented Architecture, which is becoming a trend in the IT sector [83] .

2.4.1 Distributed Approach

The current, conventional solution for the Electrical/Electronic (EE) architecture available on the market focuses on adding new functionality to the vehicle by adding the new electronic control unit. This also includes the necessary sensors and actuators [79]. Having this approach, the vehicle architecture is driven by variants, where Bill of Materials (BOM) changes. Thus, there is always a trade-off between functionality and hardware. Figure 2.7 presents the architecture with a single centralized gateway.

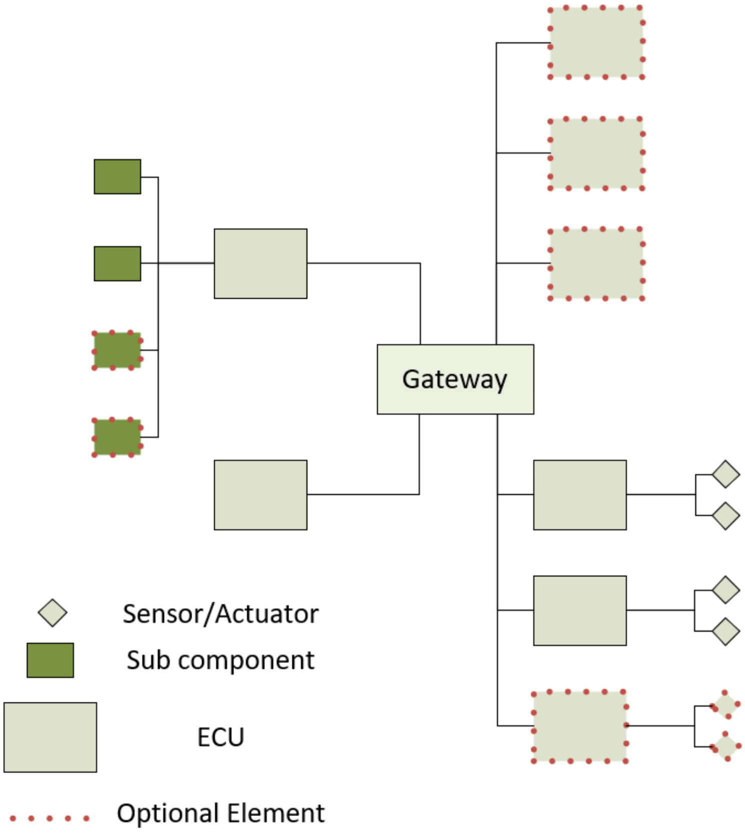


Figure 2.7: Distributed E/E Architecture.

The distributed E/E architecture has its limitations. Some of them are latency, timing, and software update. The bottleneck is the gateway ECU, through which all communication is carried out. With higher communication on the vehicle bus, this architecture becomes insufficient [79]. Therefore, there are suggestions on how to mitigate this risk [80, 83].

2.4.2 Domain Based Approach

One of the existing mitigation plans is to move into the feature base domains and introduce a high-level computation unit per domain. This approach is called Domain-Based Architecture [82]. Due to the domain concentration approach, the level of complexity and the data exchange rate can be reduced. Figure 2.8 presents the view, where functionality is grouped into domain controllers. Also, the scalability of the architecture is better, since the main domain controllers shall remain in all variants. The growth of the function can be achieved by adding more ECUs to the domain. However, it still does not solve the hardware-software dependency and the BOM costs for functionality growth. Even though domain controllers are connected via Quality of Service (QoS) busses, e.g., CAN, FlexRay, or Ethernet, there are still problems with the data latency and timing on the Gateway ECU [79]. Autonomous vehicles require more overlap and redundancy in functions. In this case, the load on the gateway node will still increase. Further improvement shall be introduced to avoid the same.

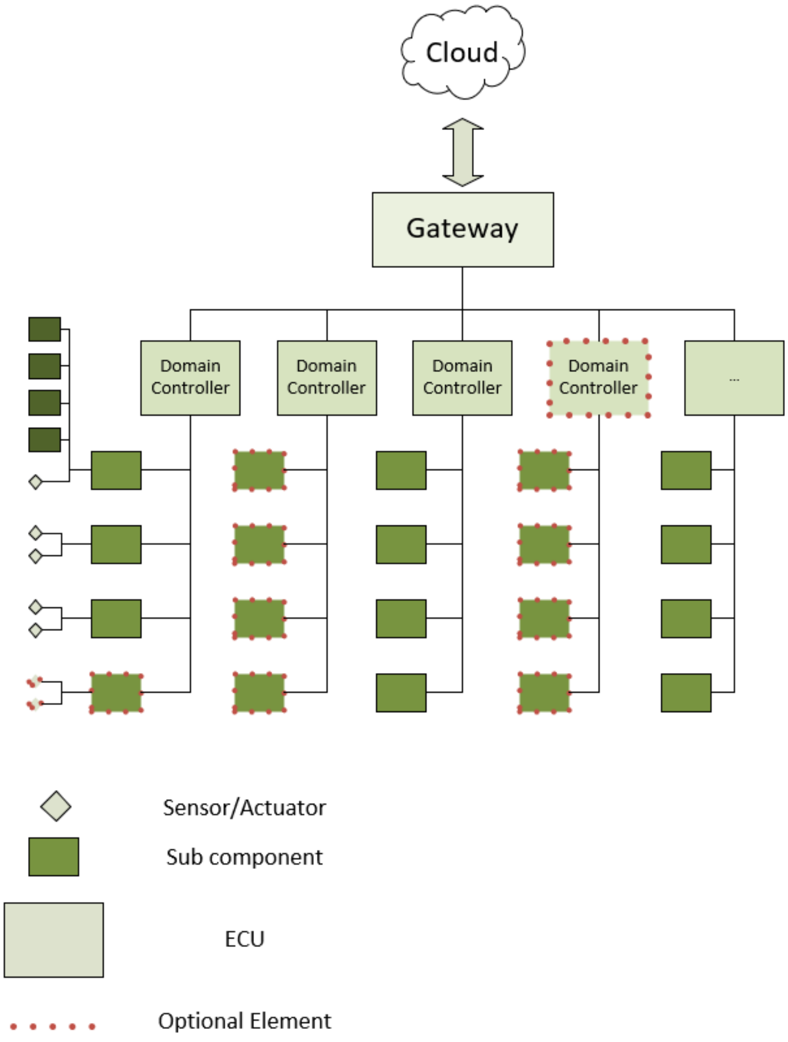


Figure 2.8: Domain Based Approach.

2.4.3 Zone Based Approach

In order to better group the functionalities into a single controller, the zone-based approach is introduced [79]. By definition, it shall incorporate functionalities from a certain zone, e.g., ADAS, Connectivity and Telematics, Infotainment, etc., into a single unit. In order to speed up the processing of data, these operations shall be done in a central entity. In this case, the zone controller provides limited functionalities, including the forwarding task, firewalling, or detection of anomalies. It does not, however, take part in processing of data. Nonetheless, to limit the processing of the data in the Central Sever unit, the basic calculations shall be taken up by the Zone Controller. If needed, e.g. due to the failure, these calculations can be taken by another controller. This approach would add another level of redundancy for safety-critical systems, such as ADAS. The Central Server may behave like a scheduler which manages the tasks and prioritizes them in zones.

As presented in Figure 2.9, there can be several zone controllers in the vehicle. The data is provided by high-quality and fast busses e.g. Ethernet. However, in order to use the Ethernet as a backbone network, the QoS requirement for the data transmission between the server and the peripherals shall be provided. As described in [79], one of the possible solutions may be an introduction of Time-Sensitive Networking (TSN) standards. With the introduction of these standards, the main issues with the Ethernet as a backbone network shall be solved. This includes the Redundancy (IEEE 802.1CB standard), Bandwidth Restrictions (IEEE 802.1 Qci), Dynamic Reconfiguration (IEEE 802.1Qca, IEEE 802.1Qcc), Several timing Domains (IEEE 802.1 AS), Low Latency (IEEE 802.1 Qvb). However, in order to meet the safety requirements of the ISO 26262:2018 standard series, further redundancy of connections should be considered. This is proposed in Figure 2.10.

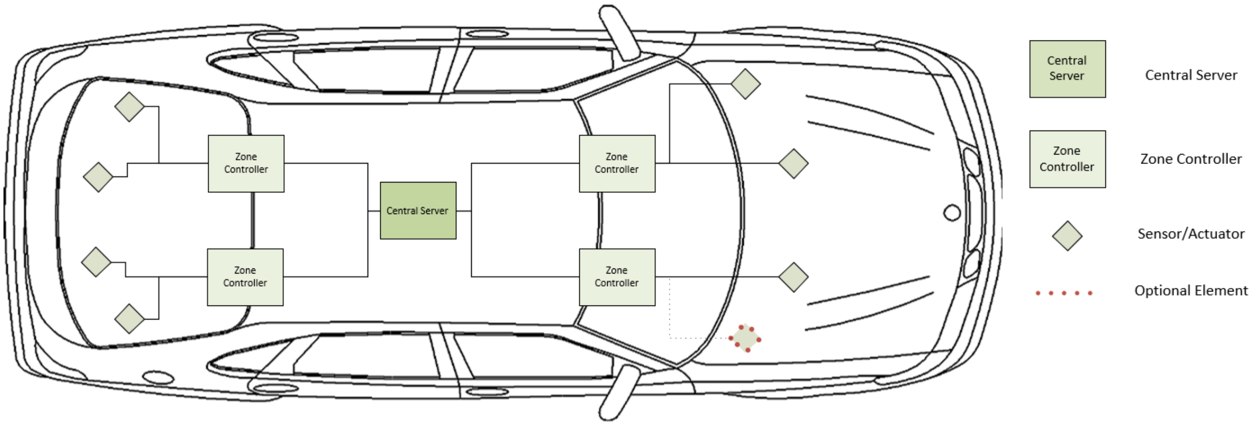


Figure 2.9: Zone Approach.

2.4.4 Centralised Based Approach

Automobile trends are going beyond the zone-based architecture [84]. Since global IT companies are entering the automotive industry, the software-defined and hardware-independent car is the target now. The unified, standardized platform with, e.g., Architecture Framework [80], provides the opportunity for:

- Independent software development;

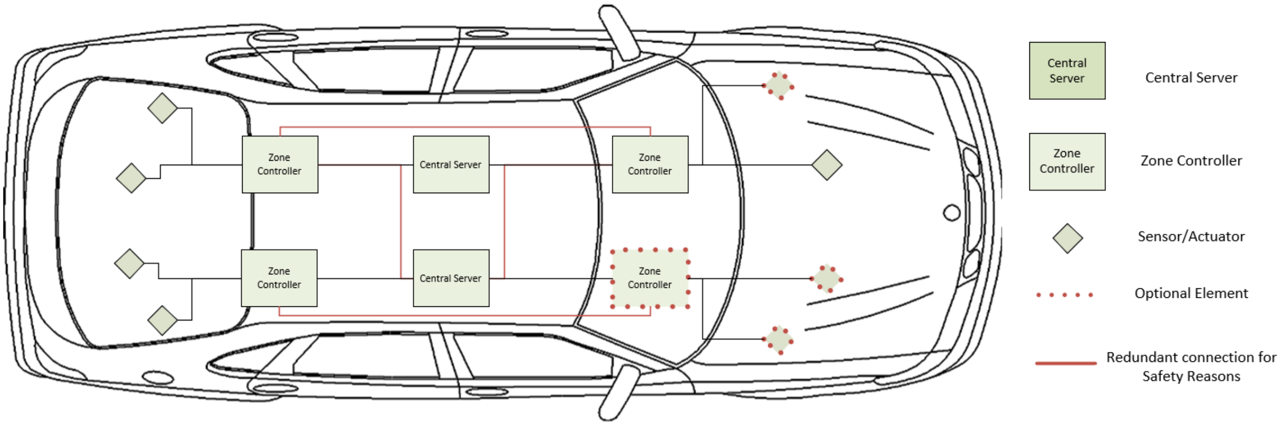


Figure 2.10: Zone Approach with redundancy.

- Full Over the Air update;
- Scalability increase;
- Open application development.

The concept of centralized architecture is presented in Figure 2.11. The possible time frame for this solution to be available on the market is 2025+ [84]. In this case, sensors and actuators can be added as ’plug and play’ devices. This does not require any further development and integration within the Central Vehicle Computer Unit (CVC). The base software is there, and in case of the needed update, the OTA functionality is used. Furthermore, CVC takes on the role of vehicle scheduler and defines the priorities of tasks. The Centralized Architecture exploits emerging technologies, e.g., neural networks, artificial intelligence, and cloud services [80]. The electronics shall follow the trends of performance. It shall also utilize the safety and security mechanisms. Currently, there are studies for more powerful electronics, which can combine functionalities of various ECUs into a secure environment [85]. Some well-positioned semiconductor providers have already begun work on such microprocessors [86].

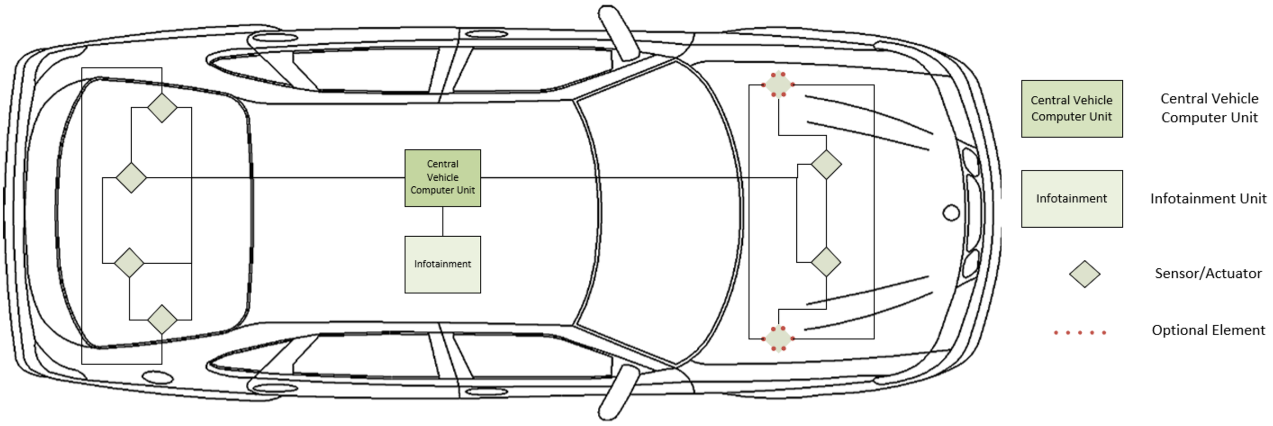

Central Vehicle Computer Unit
Infotainment
Central Vehicle Computer Unit
Central Vehicle Computer Unit
Infotainment
Infotainment Unit
Sensor/Actuator
Optional Element

Figure 2.11: Centralized approach.

However, it cannot be forgotten that the idea of autonomous vehicles goes beyond the boundaries of the car. In order to achieve the next level of development, we need to think of a vehicle as a fleet of connected vehicles. These vehicles shall cooperate not only with each other, but also with an infrastructure. This is defined as Vehicle-to-Everything (V2X) concept [9]. We can think of a car not as defined as 'software', but as defined as 'connectivity'. This introduces the concept of the connected ecosystem which is safe and secure. The high-level idea of such solution is shown in Figure 2.12. This leads to the potential threats which may occur if such a system-of-systems is deployed.

The next step for vehicle architecture development may be the Vehicle Cloud Computing. In this scenario, all major computations are provided by cloud providers as a service. Currently, however, the cloud computing technology has limitations due to the network coverage. However, in the near future it may change with the introduction of new connectivity technologies, such as 5G [87].

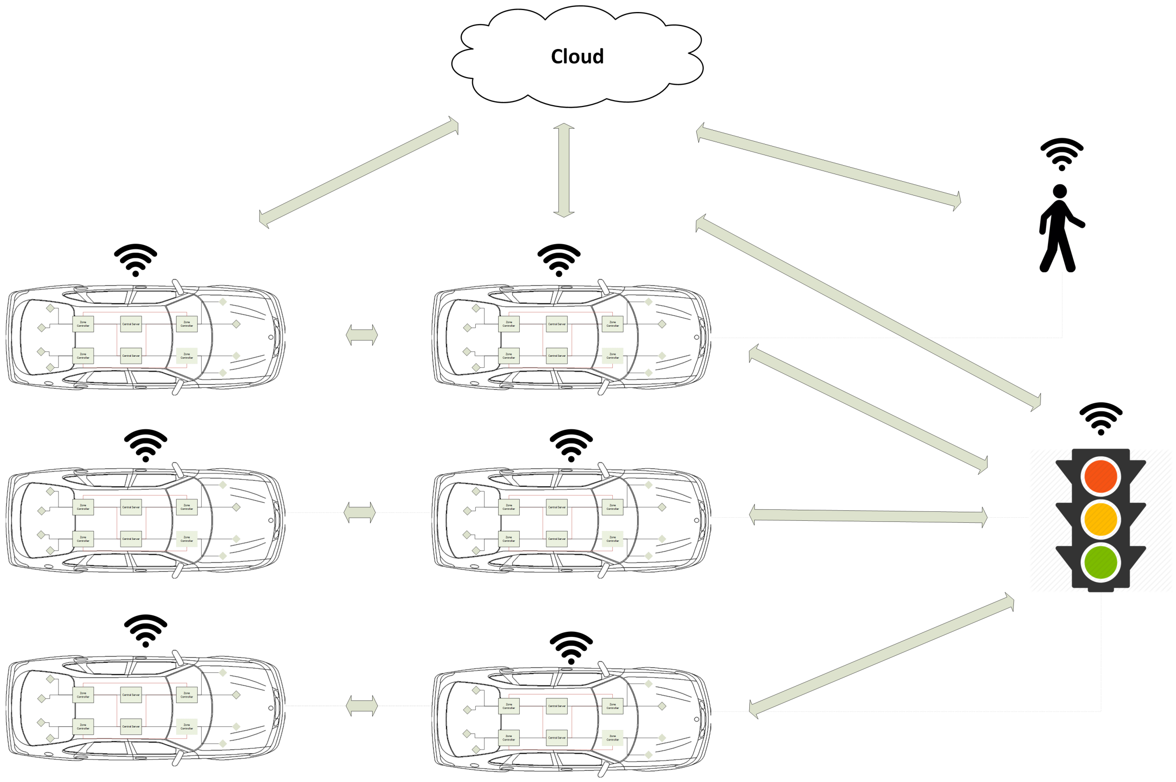


Figure 2.12: Connected ecosystem.

2.5 Vehicle Cybersecurity Landscape

2.5.1 Vehicle Cybersecurity Threats and Challenges

The common, agreed vision of future automotive system-of-systems is that all vehicles shall always be connected. Communication will not only be between a car and an IT back-end system, but it also includes Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Grid (V2G) schemas. The proposed definition of connected vehicle, which takes into account all possible communication mediums, is

V2X [9, 88, 89]. The summary of communication categories can be found in Table 2.4. However, only with the entire ecosystem connected can vehicles be fully autonomous [9].

Table 2.4: Categories of communications in the connected ecosystem. Based on [9].

Acronym	Full Name	Description
IV	In-Vehicle	Communication inside the vehicle, to and from the sensors, status information display, warnings, sound signals, etc., are within a vehicle.
V2V	Vehicle to Vehicle	Two-way communication between vehicles within a limited geographical area. However, one-way communication might be an interim state until all vehicles can interconnect via standard communications protocols.
V2S	Vehicle to Surrounding	Presence of vehicles may be monitored by sensors in surrounding environment.
S2V	Surrounding to Vehicle	Currently one-way visual communications from local sources to drivers. Eventually, likely to see telecommunications from intelligent roadways directly to vehicles.
V2I	Vehicle to Infrastructure	When intelligent roadways are more developed, vehicles will likely communicate with, say, traffic control systems that can manage traffic lights. speed-limit displays, etc.
I2V	Infrastructure to Vehicle	One-way communications to vehicles from sources within several miles. Will likely evolve into two-way communications.
V2E	Vehicle to Ecosystem	Communications from vehicles to external services, such as navigation systems' requested information, e.g., destinations.
E2V	Ecosystem to Vehicle	Communications to vehicles from external global sources, such as GPS.
V2T	Vehicle to Transportation Networks	These one-way and two-way communications apply to systems that monitor and control specific vehicles.
T2V	Transportation Networks to Vehicle	Potential communications to vehicle from intelligent traffic lights, etc.

Acronym	Full Name	Description
S2I	Surroundings to Infrastructure	Initially one-way communications, such as weather information for the immediate area. Eventually two-way communications with information on distant activities.
I2S	Infrastructure to Surroundings	Communications regarding situations that will impact surroundings, such as traffic delays.
I2E	Infrastructure to Ecosystem	Eventual communications where, for example, the infrastructure informs cloud navigation systems of intended actions with respect to traffic control.
E2I	Ecosystem to Infrastructure	Ecosystem-to-Infrastructure Initial communications such as the ecosystem providing local weather information to infrastructure across wide area, such as warnings about impending hurricanes.
V2G	Vehicle to Grid	Two way communication between an electric car and a charging station. Used to manage the energy usage in the electric infrastructure, schedule vehicle charging, share the energy etc. Defined in the ISO 15118 standard series.

Nevertheless, each communication category brings another level of potential cybersecurity threat. According to [9], the main focus of the industry is on in-vehicle systems. The cybersecurity of infrastructure and cloud-based systems is neglected. OEMs see market opportunities only in safety and electrification technologies. However, in order to provide the proper safety level, cybersecurity shall also be taken into account. Therefore, cybersecurity must be embedded in the project life cycle. Moreover, it shall be monitored in-field and considered as decommissioning. To complete the cybersecurity picture, the entire ecosystem will be analyzed for potential threats. Undoubtedly, without universal enforceable standards, this kind of system-of-system cannot be properly protected against cybercrimes [9,68,88–94]. This shall be solved with the UNECE.29 and upcoming ISO 21434 - Road vehicle - Cybersecurity Engineering Standards.

With growing cyberthreats for automotive industry and Threat-as-a-Service possibilities, it is inevitable that the Common Vulnerabilities and Exposure Open Database for car manufacturers shall be created. Unfortunately, still with no success [12].

However, the Upstream Cybersecurity Company was able to prepare the basic report, which attempts to summarize the recently exploited vulnerabilities in the automobile industry [61]. In the Global Automotive Cybersecurity Report prepared by the Upstream, the constant growth of incidents can be observed. The report was created by analyzing more than 600 publicly reported cyber incidents since 2010, 207 of which in 2020 as of November 25th, 2020. The black hats, the criminals who break into a computer network with malicious intent, are responsible for 49.3% of the security bridges. The report also points out the most common attack vectors, which is in line with the thesis available in [9], the IT server infrastructure. The second most common is Keyless entry, and the third are the mobile applications. Server attacks involve a variety of server types, including telematics servers, database servers, web servers, and more. These attacks are of remote and long-range type [61].

The report indicates that all the vehicle industries, OEMs, Tier 1, Tier 2, Fleet Management, Trains, Car Sharing, Car Rental, Car Dealerships, Insurance, Logistics and Delivery Fleets, Autonomous Vehicles, Ride Sharing, Public Transportation, Electric Vehicles, Ride Hailing, Government Fleets/Emergency Services, etc., are equally affected by security attacks. In 2020, for automotive OEMs, Tier1 and Tier2, 33 related Common Vulnerabilities and Exposures (CVE) records were found. However, the impact breakdown between 2010-2020 indicates that data / privacy breaches are the most common – one-third, while car theft is 28. 14% and control car systems is 23.73%. The authors of the report suggest that with the introduction of new cybersecurity requirements defined in the UNECE WP.29 [66] regulations and the ISO/SAE 21434 [13] standard, a critical step in increasing automotive cybersecurity may take place. However, also the impact coming from the deep and dark web cannot be neglected. The new WP.29 regulations, as well as the ISO/SAE 21434 standard, require in-depth threat intelligence; Monitoring the deep and dark web as part of threat intelligence is integral [61]. In order to protect the vehicle industry, all key stakeholders shall accomplish security by design, multilayer security solution (IT and enterprise security), development of effective security operations centers, and shall be compliant with all automotive cybersecurity regulations.

The security concern in the connected automotive world leads to different types of attacks. The high level of vehicle threats can be observed in Figure 2.13. The basic classification of attacks is the one that describes where an attacker is located. In this case, the division would be: an internal threat – as authenticated member of a network, or external – as an intruder into the network. Taking into account the range of an attack, it can be: local – with a limited scope (attack of a single ECU in vehicle), or extended - controls several ECUs in vehicle network. Another division is the purpose of an attack. It can be either malicious, with no personal benefit, or rational, which seeks profit. Looking from the attacker activity, it can be an active attack – the attacker can send the signals, or a passive attack – sniffing the network traffic. The attack may be intended, planned, or unintentional, system internal error.

As described in [94], current vehicle networks have limitations in hardware, timing, autonomy, life cycle, and supplier integration. However, with a change in vehicle architecture, some of them can be solved. Hardware and timing limitation, which mainly includes the available resources, can be solved with an upgrade into the zone-based or centralized architecture. The main, powerful computing unit, available on those architectures, shall take care of e.g. time-consuming cryptographic operations. These operations can be supported with dedicated hardware, which is the Hardware Security Module. It includes hardware accelerators for cryptographic calculations that significantly improve their timing. Another hardware element, which provides the physical level protection, is the Trusted Platform Module (TPM). It can be used, e.g. for storing the private keys for encrypted communication.

The other limitation is the variety of network types used for in-vehicle communication. The primary are LIN, MOST, FlexRay, and CAN. The industry is focusing mainly on CAN/CAN FD and Ethernet as backbone networks [91]. The vulnerabilities of these buses, mentioned in [91], are broadcast transmission, no authentication, no encryption, and an ID-based priority scheme. External communication such as Bluetooth, WiFi, NFC, 4/5G, Smart Charging, DSRC, Diagnostic Communication on OBD also provides the

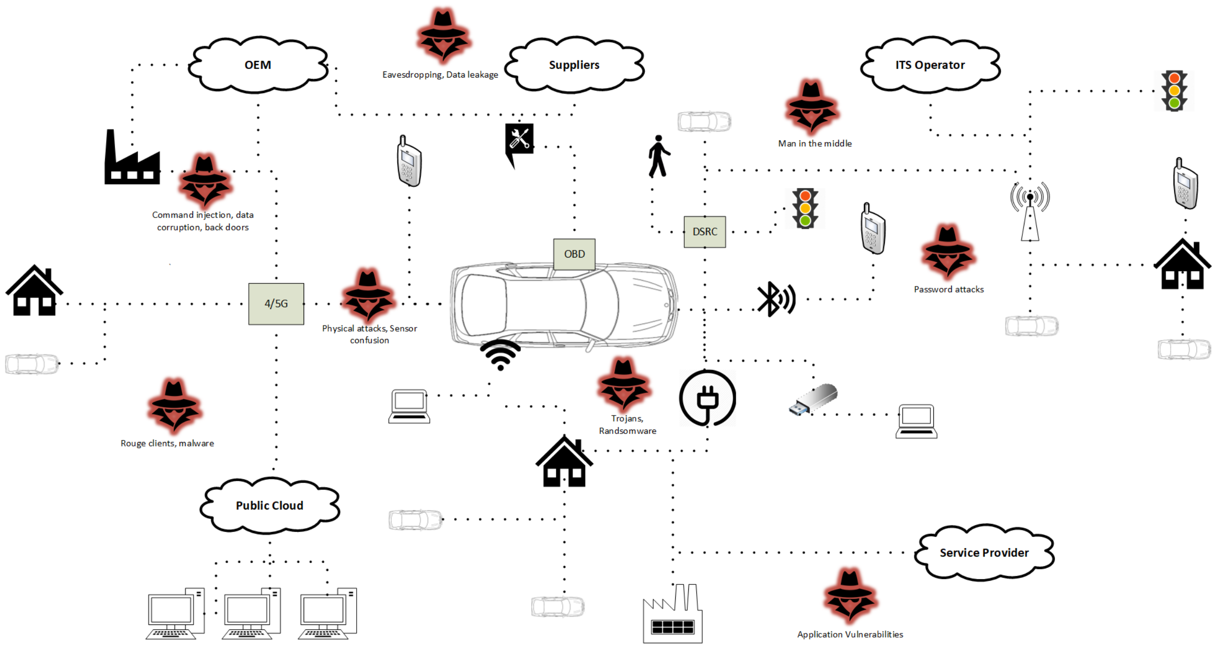


Figure 2.13: Connectivity eco-system and its threats.

attack scenarios. The basic are frame sniffing, frame falsifying, frame injection, reply attacks, DoS. As stated in [90, 91], most of the security principles are identified and ready to be implemented in the future car architectures. The summary is shown in Table 2.5. The possible locations of the security measures in the zone-based approach are shown in Figure 2.14.

Table 2.5: Applying security principles. Based on [91].

	Prevent access	**Detect attack**	**Reduce impact**	**Fix vulnerabilities**
Secure Interface	M2M Authentication & Firewalling	Intrusion Detection System		Secure Updates
Secure Gateway	Firewalling (context aware message filtering)	Intrusion Detection System	Separated Functional Domains	Secure Updates
Secure Network	Secure Messaging	Intrusion Detection System	Message Filtering & Rate Limitation	Secure Updates
Secure Processing	Code/Data Authentication (@start-up)	Code/Data Authentication (@start-up)	Resource Control (Virtualisation)	Secure Updates

Since the Central server is responsible for all calculations and data management, the main security features must be located there. It includes Crypto Primitives storage, Firewall, Key Infrastructure Management, Hypervisor, Data Logging, Intrusion Detection and Prevention System (IDPS), Secure Boot/Flash, Secure Synchronization Time Manager, and Online Remote Update Management. The zone controllers must in-

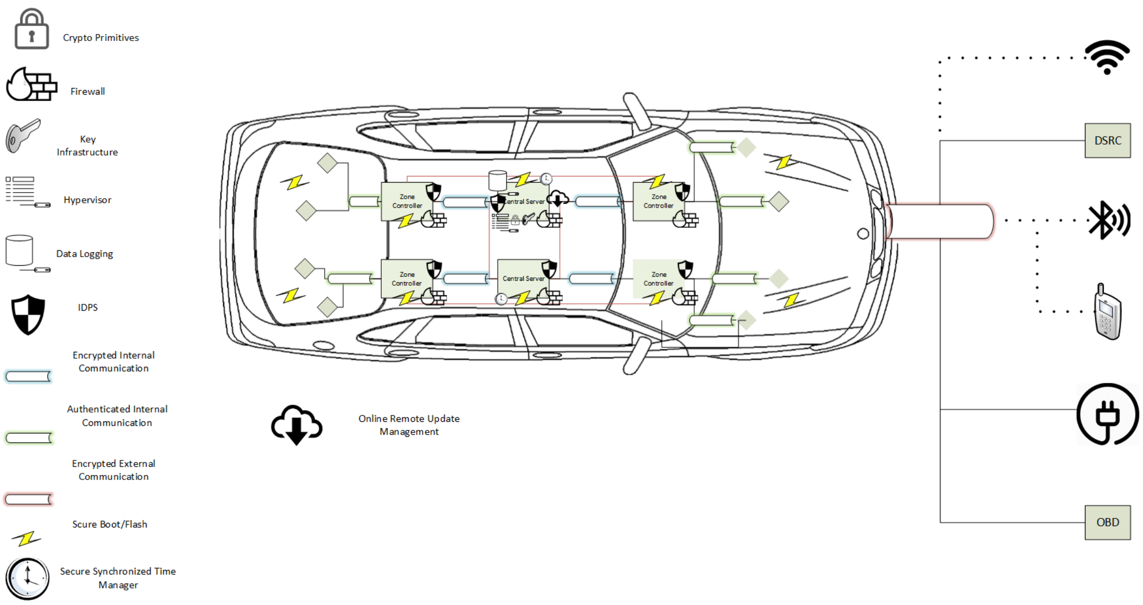


Figure 2.14: Possible security measures location in the zone based approach architecture.

clude the Firewall, since they are responsible for communication within a zone, IDPS instance (the IDPS should be distributed), and Secure Boot/Flashing, to provide the software integrity verification. Moreover, each sensor and actuator must provide its authenticity, following the Secure Boot/Flashing function. All communication must be protected. Since the vehicle is exposed to the external network, each communication protocol (WiFi, DSRC, Bluetooth, Cellular Network, Charging Communication, OBD, etc.) must provide data integrity, confidentiality and availability - and must be encrypted. The in-vehicle backbone network must provide the same level of protection as the external network, as it is responsible for sensitive data transfer. Sensors and actuators must also be taken into account for secure data communication. At least the authenticity of sent data must be ensured in order to avoid reply or injection-type attacks.

The main challenge observed by [90, 91], is to develop an integrated approach, in order to include cybersecurity in the project lifecycle. In must be on both technical and organizational level. In order to avoid any gaps, the measures must be provided at the earliest stage of development. Moreover, there shall be a process that monitors if the product development follows the rules. The overview of an integrated security approach is shown in Figure 2.15.

However, this kind of process should not be detached from existing processes. It must include standards for FuSa, SOTIF, and CySe. Only by providing a holistic approach can gaps during development be avoided.

2.6 Project Management Approaches for Design and Development Process

Agile methods play a crucial role in the development of complex software-based systems. These methods are rooted in a set of principles and practices that prioritize flexibility, collaboration, and iterative development throughout the software development lifecycle. In contrast to traditional linear approaches, agile methods emphasize the ability to adapt to change, involve customers throughout the development process, and continuously improve the software product. Agile teams work in short iterations, delivering functional

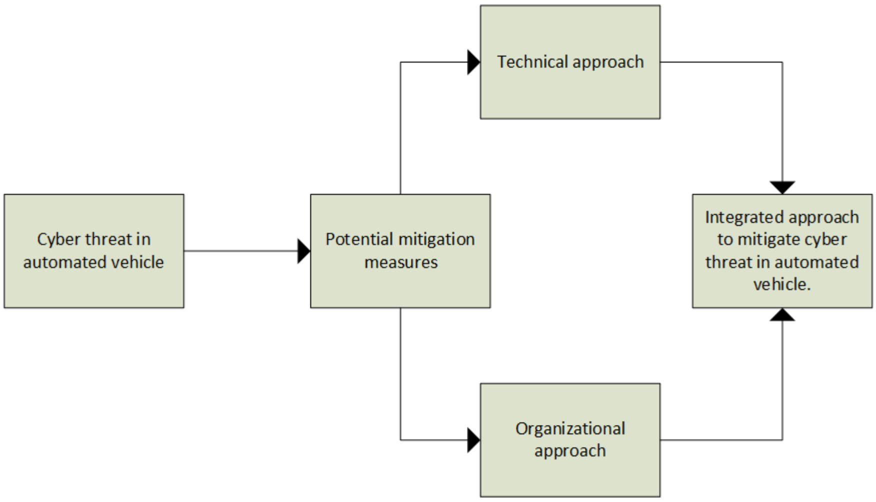

Technical approach
Cyber threat in automated vehicle
Potential mitigation measures
Integrated approach to mitigate cyber threat in automated vehicle.
Organizational approach

Figure 2.15: Integrated security approach for automotive vehicle. Based on [90].

software increments frequently. This iterative approach enables faster feedback cycles and enables teams to respond promptly to evolving requirements. Agile methodologies foster cross-functional teams, promote regular and transparent communication, and maintain a strong focus on providing value to the customer. The ultimate objective of agile methods is to enable organizations to deliver high-quality software products that precisely meet the needs of the customer in a timely and efficient manner [95, 96] .

The adoption of agile practices has become increasingly prevalent in software development due to their flexibility, timely delivery, implementation efficiency, and iterative nature. This trend has expanded to the automotive industry, as it seeks to address challenges such as safety, complexity, user participation, flexibility, and innovation in software development. Traditional approaches in automotive software development struggle to handle these challenges effectively, necessitating the integration of agile methods [97–99].

The automotive industry faces unique challenges in software development, including safety requirements, complexity, and effectively managing change. Traditional approaches, such as the V-model, have been commonly used, but often result in higher costs and risks during the late stages of verification. The fact of the matter is that the traditional approach has evolved into the ’U-Model’, which enlarges existing problems, that is, integration and quality challenges, unmet requirements, poor customer experience, and more delays, rather than solving them, as presented in Figure 2.16. The Agile Manifesto, introduced in 2001, offers an alternative approach that promises earlier product releases, a quick response to changing market needs, user participation, and adaptability to varying requirements [100].

The integration of agile methods into the automotive industry offers a potential solution to the challenges presented by a dynamic market environment. The V-model, a traditional approach, is widely employed, but lacks flexibility. Agile methods, on the other hand, enable incremental development, user participation, and support for late changes. By embracing agile principles, the automotive industry can enhance the efficiency and effectiveness of software development processes.

The transition to agile practices in the automotive industry is not without its challenges. One significant difficulty lies in defining what truly constitutes an agile method. Organizations often seek to increase development speed and reduce time-to-market, but a lack of consensus on agile definitions hinders progress.

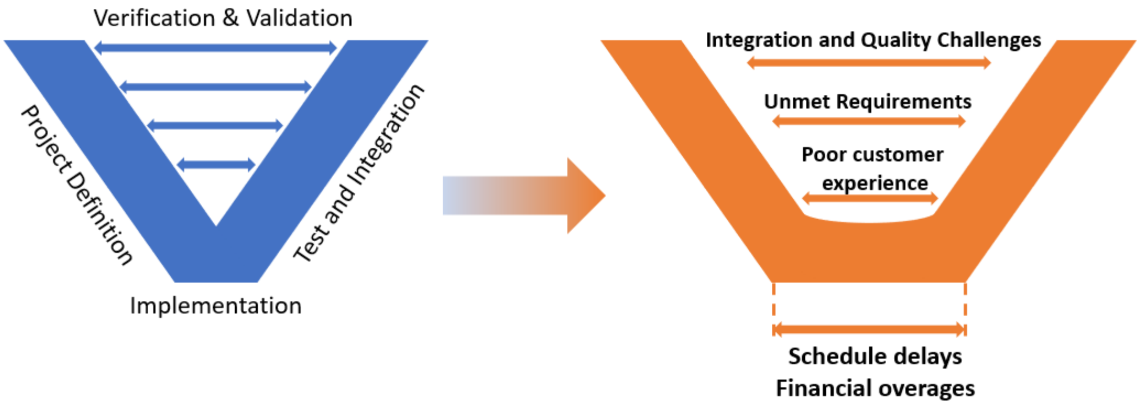


Figure 2.16: Challenge - V-model evolves to "U-Model".

Moreover, scaling agile beyond individual teams poses additional complexities, especially in safety-critical environments and in the coordination of hardware, software, and mechanical components.

Agile methods offer numerous benefits for the development of complex software-intensive systems in the automotive industry. By embracing agile principles, companies can reduce time-to-market, increase flexibility, and rapidly respond to market changes. The ability to deliver working software incrementally allows for continuous improvement and adjustment to evolving requirements. Agile practices also facilitate collaboration, transparency, and effective risk management, improving overall system development efficiency.

In the context of the automotive industry, Figure 2.17 illustrates the integration of Agile methodologies, the V-model, and DevOps practices, showcasing a comprehensive approach to complex system development. The V-Model, represented by the blue "V" shape, delineates the phases of "Project Definition" on the left, "Implementation" at the bottom, and "Test and Integration" on the right. Within the "Project Definition" phase, planning involves setting vehicle specifications and safety requirements, while coding and building encompass developing and compiling embedded software for vehicle control systems. The "Implementation" phase bridges the design and development, ensuring seamless transition to the "Test and Integration" phase. This phase involves rigorous testing, including unit and integration testing, to validate compliance with safety standards, and monitoring post-deployment to ensure real-world performance. The inner loop of the image represents the iterative cycle of DevOps, emphasizing continuous integration and deployment Continuous integration and continuous delivery (CICD), crucial for maintaining up-to-date vehicle systems. Agile methodologies, depicted through iterative cycles within the project phases, facilitate rapid adaptation to changing requirements and continuous customer feedback, essential for integrating new technologies such as ADAS. The overarching arrow emphasizes the critical importance of verification and validation to ensure regulatory compliance and reliability. By combining Agile methods, the V-Model and DevOps practices, automotive companies can achieve a holistic approach to system development, improving efficiency, quality, and customer satisfaction. This integrated approach addresses the challenges of developing complex software-based systems, enabling rapid iteration, thorough testing, and seamless integration of continuous improvements, ultimately leading to safer, more reliable, and innovative automotive solutions.

In conclusion, agile methods, along with the integration of DevOps practices, play a vital role in addressing the challenges associated with complex software-based system development. Agile methods, with their focus on flexibility, collaboration, and iterative development, enable organizations to adapt to changing requirements, involve customers throughout the process, and continuously improve the software product. By working in short iterations and frequently delivering functional software increments, agile teams can gather rapid feedback and respond quickly to evolving needs. However, it is important to note that agile methods alone may not fully address all aspects of system development, especially in environments where hardware and mechanical components are integral. Here, the V-model, a traditional approach, can provide structure and ensure thorough verification and validation. The interaction between agile and the V model can be optimized by embracing DevOps practices, which emphasize seamless integration of development and operations. DevOps enables collaborative and automated processes, ensuring smooth transitions between software development, testing, deployment, and operations. By combining agile, the V-model, and DevOps, organizations can achieve a holistic approach to complex system development, improving efficiency, quality, and customer satisfaction.

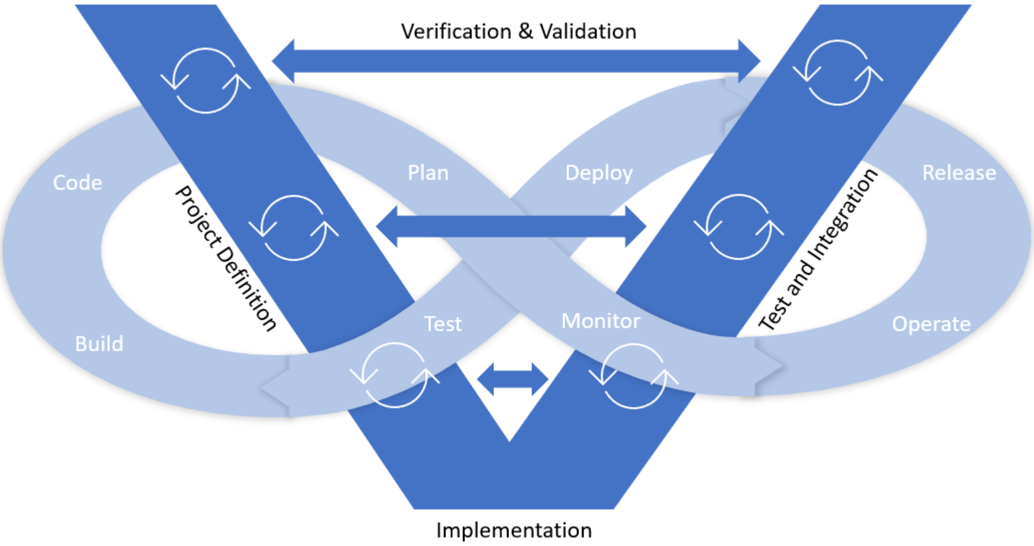


Figure 2.17: New Paradigm: V-Model becomes Agile Engineering + DevOps.

2.7 Systems Engineering Approach

The modern world is constantly evolving, witnessing the development of increasingly complex systems aimed at satisfying diverse stakeholder requirements and market demands. Simultaneously, the expectations for shorter time to market, improved quality, and reduced costs are the key driving factors. Large-scale systems, such as airplanes, trains, ships, spacecraft, satellites, and vehicles, require cross-functional teamwork to achieve their objectives. Embracing innovation involves challenging existing norms, exploring unknown territories, and pushing boundaries. To navigate this complex landscape, engineering teams require a comprehensive set of methodologies and tools.

Fortunately, Systems Engineering (SE) offers a transdisciplinary approach that facilitates the realization of successful systems. SE integrates various disciplines and establishes interfaces between them, as illustrated in Figure 2.18. The primary objective of this approach is to meet the needs of customers, users, and other stakeholders [101].

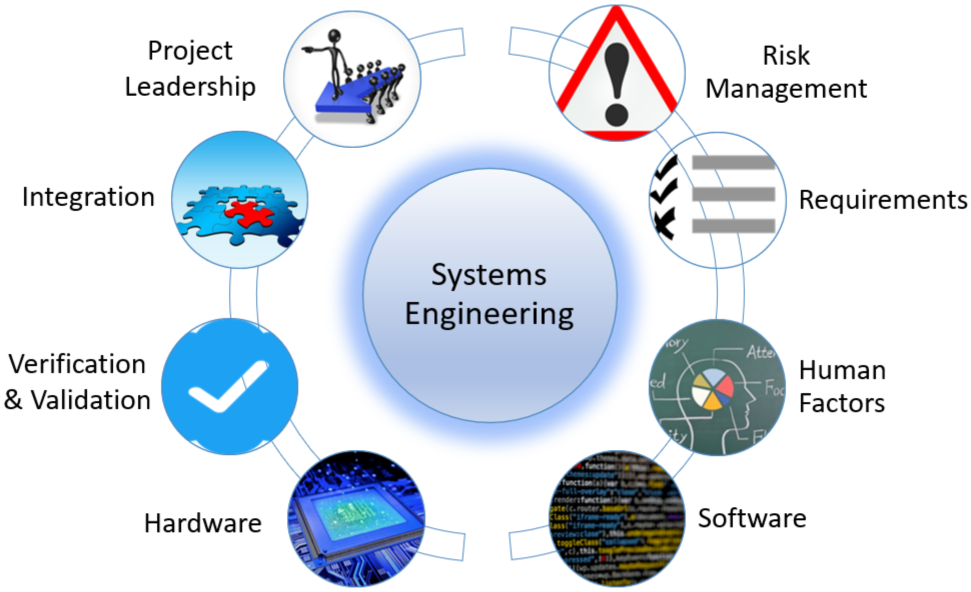


Figure 2.18: Overview of Disciplinary Domains within Systems Engineering.

Key elements of Systems Engineering include [101]:

- Principles and concepts that define a **system** as an interactive combination of system elements working towards a specific objective. Systems interact with their environment, which may include other systems, users, and the natural environment. The elements of the system include hardware, software, firmware, personnel, information, techniques, facilities, services, and other support components;
- The role of a **system engineer**, who plays a crucial role in supporting the transdisciplinary approach. In particular, the systems engineer is responsible for eliciting and translating customer needs into specifications that the system development team can implement;
- A set of **life cycle processes** that the systems engineer employs to realize successful systems. These processes commence early in the conceptual design phase and continue throughout the life cycle of the system, encompassing manufacturing, deployment, usage, and disposal. The systems engineer must analyze, specify, design, and verify the system to ensure that its functional, interface, performance, physical, and other quality aspects, as well as cost, are balanced to meet the requirements of system stakeholders;
- The systems engineer's role in ensuring that all system elements harmoniously integrate to accomplish the overall objectives and ultimately satisfy the needs of customers and other stakeholders who acquire and utilize the system.

To efficiently implement SE into product design, a shift in mindset is required. It is insufficient to view systems as a mere sum of the operations performed by their component functions. Rather, they must be perceived as a functioning whole, embracing the systems' viewpoint. This entails updating the way of thinking about a designed system, starting from the system's perspective within its context, rather than simply decomposing it into its constituent parts. This holistic approach is crucial for the effective application of the SE principles [29].

2.7.1 Systems Modeling

Recognizing the notion that a system encompasses more than the sum of its parts, the International Council of Systems Engineering provides a definition of a system as "a construct or collection of various entities that, when combined, produce outcomes that cannot be achieved by the entities alone" [101]. A system operates within a specific environment and must serve a purpose that justifies the assembly of its elements. However, when it comes to system design activities, the objective is to represent the system in a form that allows for examination, development, verification, and validation. Hence, the definition of a System Model becomes necessary. The System Model enables a comprehensive understanding and analysis of the system, facilitating its design process.

In the realm of engineering design, models play a vital role in bridging the gap between the conceptualization of a design solution and its practical implementation as a real system. These models aim to represent the entities involved in the engineering problem and their interrelationships, while also linking them to the proposed solution or existing mechanism that addresses the problem at hand. The use of such models forms the core of the engineering of model-based systems, allowing a comprehensive and integrated approach to system design [101].

In essence, a model comprises four key elements [101] :

- Language: The model is articulated through a language. The System Definition Language (SDL) is utilized to express and represent the model in a clear manner, facilitating understanding and understanding;
- Structure: A model must possess a well-defined structure. This allows for the capture of system behavior by precisely describing the relationships between the various entities within the system;
- Argumentation: The purpose of the model is to effectively represent the system design, enabling the design team to demonstrate that the system fulfills its intended purposes. The model serves as a means to present a compelling argument supporting the system's capabilities and objectives;
- Presentation: It is not sufficient for the system to be capable of making an argument; there must also be mechanisms in place to showcase and present the argument in an understandable manner. The model should incorporate elements that facilitate effective presentation and communication of the argument.

These elements provide the model with the necessary components to fulfill its purpose of testing the system design solution against the requirements, demonstrating its suitability, and presenting evidence of its suitability to all stakeholders.

Every successful system model has four key characteristics. These encompass [101]:

- Order: A system model exhibits a sense of organization and structure, allowing for clarity and coherence in its representation of the system. It enables a systematic understanding of the system's components and their interactions;
- Demonstrative and Persuasive Power: A model has the ability to illustrate and convey the intended message effectively. It serves as a persuasive tool to communicate ideas, facilitate decision-making, and gain support for the proposed system design;
- Integrity and Consistency: A model demonstrates integrity by accurately capturing the essential elements and relationships within the system. It maintains consistency throughout its representation, ensuring that all aspects align with the defined objectives and requirements;
- Insightful: The model possesses the ability to provide valuable insight into both the problem at hand and its potential solutions. It offers a deeper understanding of the behavior, dynamics, and implications of the system, helping to identify optimal design choices.

These characteristics collectively contribute to the effectiveness and success of a system model, enabling comprehensive analysis, informed decision making, and effective communication among stakeholders [29].

By adopting the system engineering approach and constructing a comprehensive system model, the subsequent phase entails harnessing the capabilities of models to augment and optimize the system engineering process, which is precisely where Model-Based Systems Engineering (MBSE) comes into play.

2.7.2 Model-Based Systems Engineering

MBSE is a comprehensive approach that formalizes system development through the utilization of models. Its broad scope encompasses multiple modeling domains across the system life-cycle, from system of systems to component level. By adopting MBSE, organizations can achieve improvements in quality, productivity, and risk reduction. The approach emphasizes rigor, precision, and effective communication between development teams and stakeholders, while managing the complexities inherent in system engineering.

Figure 2.19 illustrates how Model-Based Systems Engineering (MBSE) with a central System Architectural Model enables seamless integration across various domains, including customer specification, product support, program management, analytical models, verification models, software models, mechanical and electrical models, and manufacturing. This central model acts as a single source of truth, ensuring alignment and coherence among all domains, and facilitates communication and collaboration among different teams, reducing errors, and ensuring that all components work together seamlessly.

MBSE provides a structured approach to systems engineering, which is critical for managing the complexity of modern vehicles that integrate numerous mechanical, electrical and software components. It improves traceability by tracking customer requirements through design, implementation, and testing phases, enhances collaboration between different engineering disciplines, and allows early and continuous verification and validation against requirements, reducing the risk of costly late-stage changes. Additionally, MBSE integrates manufacturing constraints early in the design process, facilitating smoother transitions from design to production, and provides a comprehensive view of the system architecture, helping troubleshoot and maintain the vehicle throughout its life-cycle. Ultimately, MBSE helps automotive companies manage the complexity of modern systems, leading to higher quality, improved efficiency, and greater customer satisfaction.

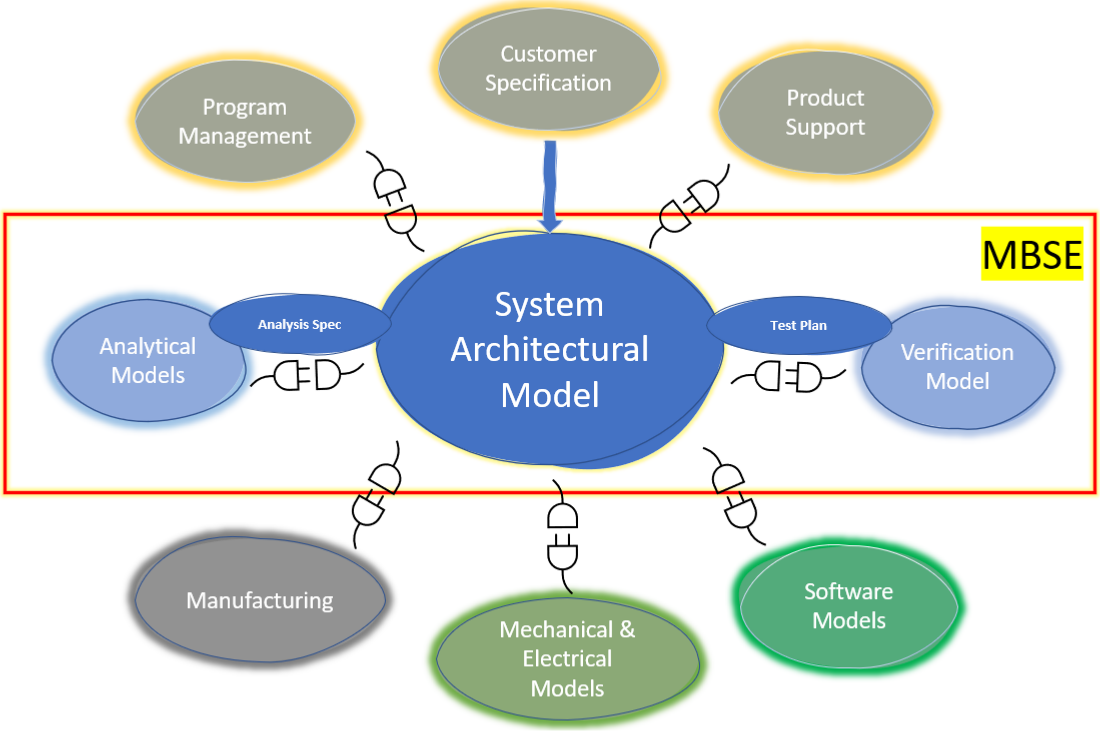


Figure 2.19: The MBSE Integration Across Domains.

In today's era, the focus on Model-Based Engineering goes beyond the use of isolated models. It involves changing the authority record from traditional documents to digital models, including Mechanical Computer-Aided Design (M-CAD),Electronic Computer-Aided Design (E-CAD), SysML, and UML, all managed in a data-rich environment. This transition enables engineering teams to better understand the impacts of design changes, effectively communicate design intent, and analyze system designs before physical realization.

One of the key benefits of MBSE is the ability to achieve a deeper understanding of systems through integrated analytics linked to a model-centric technical baseline. Data-centric specifications enable automation and optimization, allowing system engineers to focus on value-added tasks and maintain a balanced approach. Successful implementation of a model-based approach requires appropriate scoping of the problem, determining the desired outcomes, required fidelity, and success criteria.

MBSE also extends beyond the creation of specifications and interface control documents. It leverages a Systems Architecture Model as a central hub for data integration and transformation throughout the product lifecycle. This facilitates the ability to link analysis to the systems model, providing valuable insight for architectural and system-level decision making.

The industry's push toward Model-Based Engineering primarily focuses on integrating data through models. By bringing together diverse, yet interconnected models within an architecture-centric environment, organizations can achieve unprecedented levels of system understanding. This integrated end-to-end modeling environment empowers engineers to comprehend all factors that could impact a design and resolve them efficiently.

In general, Model-Based Systems Engineering has emerged as a powerful approach to managing and engineering complex systems. It shifts the paradigm away from document-centric methods and harnesses the power of models for various purposes, including requirement specification, design, trade-offs, architecture, verification, validation, simulations, and support. By serving as an "insurance policy" against engineering errors and reducing the costs of failure, MBSE enables organizations to achieve more efficient and successful system development and support phases.

Systems engineering, system modeling, and the MBSE approach play crucial roles in achieving comprehensive system design and facilitating cybersecurity and safety analysis.

Systems engineering encompasses a transdisciplinary approach, combining various disciplines and establishing interfaces between them. It focuses on understanding and addressing stakeholder requirements, ensuring that the systems meet their needs. System modeling, a key element of systems engineering, involves creating formal and visual representations of system elements, relationships, and behavior. These models provide a holistic view of the system and help in analysis, design, and communication.

MBSE takes system modeling a step further by making models central to the entire system engineering process. Using the power of models to capture and represent the requirements, design, and behavior of the system is leveraged. This approach enhances collaboration, improves system understanding, and supports decision making throughout the system lifecycle.

When applied in a comprehensive system design, MBSE enables a systematic approach to addressing cybersecurity and safety. By integrating cybersecurity and safety considerations into the system model, potential risks and vulnerabilities can be identified and mitigated early in the design process. The use of models facilitates analysis and verification, ensuring that cybersecurity and safety requirements are met, leading to more robust and secure system designs.

The challenges associated with adopting an MBSE approach to cybersecurity and functional safety include issues such as integrating concepts and tools, adapting tool chains to existing processes, and error-prone transitions between models. Competitive pressures in the embedded systems market, coupled with time constraints, raise concerns about delivering high quality systems and ensuring safety in the automotive industry. In addition, the evolution of IoT technologies introduces new cyber security challenges that require specific measures for successful implementation of MBSE in these critical domains. The implementation of MBSE requires substantial organizational adjustments within research and development departments. MBSE emphasizes designing through a digital toolchain, the effective utilization of which requires additional training and qualifications. However, access to such training programs remains limited.

Due to the ongoing development of MBSE, there exists a lack of standardized approaches for its implementation, which can be attributed to both the lack of experience and the high barrier to entry. In addition, another significant challenge arises from the high dependence on internal organizational conditions and the specific types of products being designed.

In summary, systems engineering, system modeling, and the MBSE approach provide a framework for comprehensive system design. By incorporating cybersecurity and safety analysis within this framework, potential risks can be proactively addressed, leading to more resilient and secure systems.

2.8 Integrating Program Management Methods for Complex System Design

The automotive industry is witnessing an increase in complexity due to the introduction of connectivity and autonomous features. This presents new challenges in concept development, integration, and risk management. To address these issues, the Lean Process has emerged as an effective approach to effectively combine all engineering methods under the same umbrella. In this section, we will explore the key elements of the Lean Process, its relevance in complex systems design, and its interaction with Agile, Systems Engineering, and DevOps methods.

2.8.1 Key Elements of the Lean Process

The Lean Process is rooted in the principles of streamlining work processes, increasing quality, and reducing waste. Objectives are to eliminate various types of waste, such as waiting, transportation, inventory, motion, overproduction, excessive processing, defects, and waste of human talent. These wastes can also be observed in engineering processes, including information overload, inventory of information, unnecessary movement of information and people, waiting, rework / defects, and over-processing [102]. The summary of engineering waste is shown in Table 2.6.

The Lean Process is guided by several fundamental principles. First, it emphasizes value creation, ensuring that all activities generate value for the customer. Second, it focuses on mapping the value stream, which involves identifying and eliminating waste sources within processes to improve their efficiency and quality. Third, the Lean Process promotes the flow of information and materials, aiming to ensure a constant flow without unnecessary stops or delays. Fourth, it advocates for a pull-based approach, where information is produced in the appropriate quantity and quality in response to client requirements. Fifth, the Lean Process encourages continuous improvement and perfection of activities to meet customer expectations. Finally, it emphasizes respect for people, promoting teamwork, trust, and participation in the work performed [102, 103].

Table 2.6: Types of waste in engineering processes. Based on [103].

Types of Waste	Examples
Overproduction of information	• producing more than needed by next process • redundant tasks, unneeded tasks • sending a volume when a single number was requested • work on an incorrect release • lack of reuse of expertise
Inventory of information	• keeping more information than needed • excessive time intervals between reviews • poor configuration management and complicated retrieval • poor 5S's (sort, set in order, shine, standardize, sustain) in office or databases
Unnecessary movement of information	• hand-offs • excessive information distribution • disjoined facilities, lack of collocation
Unnecessary movement of people	• unnecessary movement during task execution • people having more to move to gain or access information • manual intervention to compensate for the lack of process
Waiting	• waiting for information or decisions • information or decisions waiting for people to act • large queues throughout the review cycle • long approval sequences • unnecessary serial effort
Rework, defects	• unstable requirements • complex uncoordinated task that takes so much time to execute that it is obsolete when finished and has to be redone • incomplete, ambiguous, or inaccurate information • inspection to catch defects
Over-processing	• refinements beyond what is needed • point design used too early, causing massive iterations • uncontrolled iteration • lack of standardisation • data conversions • use of excessively complex software monuments for no apparent reason

2.8.2 Relevance in Complex Systems Design

In the context of complex system design, the Lean Process offers significant benefits. It enables the quantification of interdependencies between software components, allowing for the prediction of a feasible configuration space and the effects of tuning parameters on overall performance. By defining requirements that enable later tuning, the Lean Process reduces the risk of delays during integration. Facilitates the compatibility between individual components and optimizes the design of e.g. autonomous driving functions or other complex systems, resulting in a more efficient and practical development process.

The Lean Process does not operate in isolation but interacts with other methodologies, including Agile, Systems Engineering, and DevOps. Agile methodologies focus on iterative and incremental development, promoting flexibility and responsiveness to changing requirements. The Lean Process complements Agile by providing a structured framework for optimizing processes, identifying waste, and ensuring continuous improvement.

SE plays a vital role in complex system development by ensuring that customer and stakeholder needs are met throughout the system's life cycle. The Lean Process can be integrated into Systems Engineering practices to streamline processes, reduce errors, and enhance the overall efficiency of system development.

DevOps emphasizes collaboration and integration between development and operations teams. The Lean Process aligns well with DevOps principles by eliminating waste, improving flow, and promoting a culture of continuous improvement. It helps optimize software development and deployment processes within the DevOps framework, enabling faster delivery, higher quality, and better customer satisfaction.

The Lean Process offers a systematic approach to address the challenges posed by complex systems design in the automotive industry and other domains. By focusing on value creation, waste reduction, and continuous improvement, it enhances the efficiency, quality, and predictability of development processes. When integrated with Agile, Systems Engineering, and DevOps methods, the Lean Process synergistically contributes to the successful delivery of complex systems, meeting customer needs, and achieving program objectives.

As illustrated in Figure 2.20, in the modern engineering ecosystem, the successful development and delivery of complex systems are based on the constant interaction between people, processes, and products. The central diagram is divided into three interrelated sections: People, Process, and Product, each representing a critical aspect of system development. This dynamic environment operates through a continuous feedback loop, where insights and lessons learned from each stage of the development process inform and shape subsequent iterations. Among these core triads are various methodologies and approaches, Agile, MBSE, Lean, DevOps, and Systems Engineering, that improve the efficiency and effectiveness of the development process.

The segment "People" emphasizes the importance of collaboration and communication within teams. Agile methodologies support this by fostering an iterative collaborative environment in which team members and stakeholders work closely together to adapt to changing requirements. The "Process" segment focuses on the workflows and practices that guide development, with Lean principles aiming to streamline processes and minimize waste, and DevOps ensuring seamless integration and continuous delivery. The "Product" segment represents the end result of these efforts, encompassing the physical and software components of the system, and is influenced by MBSE and Systems Engineering to ensure thorough planning, analysis, and validation.

These methodologies provide frameworks and tools that enable teams to collaborate effectively, streamline processes, and deliver real solutions that meet the evolving needs of end users. Agile facilitates rapid iteration and responsiveness, MBSE integrates models to define and document system architecture, Lean focuses on efficiency, DevOps emphasizes continuous integration and deployment, and Systems Engineering ensures a structured approach to meeting system requirements and managing complexity.

By embracing these complementary approaches and leveraging the synergies between them, engineering programs can navigate the complexities of modern system development and achieve successful results. This holistic approach ensures that all aspects of development are considered, from initial requirements through to final delivery, and that feedback from each phase is used to continuously improve both the product and the process.

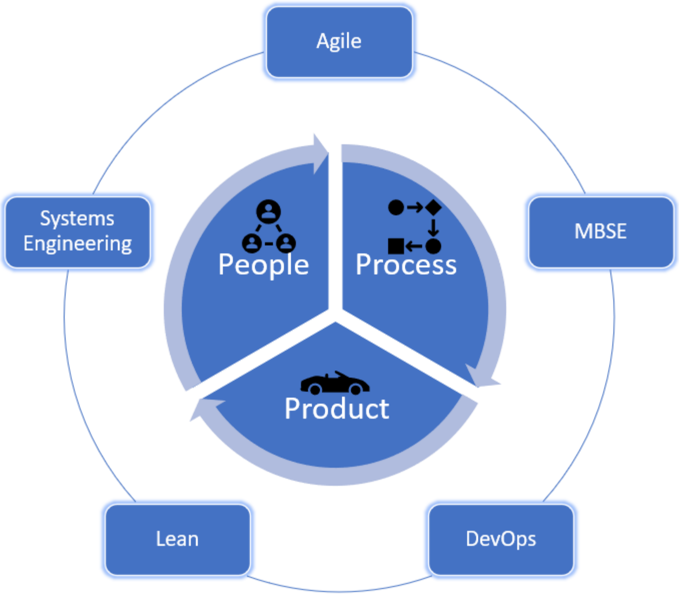


Figure 2.20: The Modern Engineering Ecosystem.

2.9 Automotive Industry Insides

Aptiv, a prominent automotive supplier, has positioned itself as a leader in creating a safer, greener, and more connected automotive environment. This section explores Aptiv's three main pillars – safety, zero emissions, and connectivity – and how the company is driving innovation to shape the future of mobility.

Safety

Aptiv prioritizes safety with a commitment to achieving zero fatalities, zero injuries, and zero accidents. The company leads the industry in advanced safety technology, offering scalable solutions in various vehicle sizes and markets. By focusing on active safety components, Aptiv contributes to a future where vehicles can deliver unprecedented levels of safety, comfort, convenience, and communication to both drivers and passengers.

Zero Emissions

Aptiv is actively contributing to vehicle electrification, thus reducing CO2 emissions and improving fuel economy. The company embraces sustainability initiatives to minimize emissions, waste, and water consumption in all regions of operation. By pursuing a green agenda, Aptiv aligns itself with the global movement toward a more environmentally friendly automotive industry.

Connectivity

Recognizing consumer expectations for seamless connectivity in vehicles, Aptiv focuses on creating software solutions that enable easy communication between vehicles, passengers, and the surrounding environment. As vehicles evolve to sense and respond to their surroundings, Aptiv's connectivity solutions play a pivotal role in shaping a future where cars become an integral part of the interconnected digital ecosystem.

Data Connectivity and Smart Vehicle Architecture

Aptiv acknowledges the increasing demand for data connectivity in vehicles and emphasizes the role of Smart Vehicle Architecture (SVA™). Serving as both the "brain" and the "nervous system" of vehicles, SVA™ ensures robust data connectivity, enabling the integration of safety features, reducing vehicle weight, and fostering innovation. Automotive Ethernet, mini-coaxial cable, and PCI Express are identified as promising technologies to build vehicles that meet evolving standards [104].

Over-the-Air (OTA) Software Updates

Aptiv recognizes the transformative power of OTA updates, enabling vehicles to evolve continuously by receiving software and firmware updates securely. This approach not only facilitates the development of software-defined vehicles, but also opens up possibilities for innovative services, features, and business models, ensuring that vehicles remain up-to-date and competitive throughout their life cycle [105].

Software-Defined Vehicles and Continuous Improvement

Aptiv emphasizes the strength of software-defined vehicles, highlighting their ability to continuously improve. Unlike traditional hardware, software-defined vehicles can evolve throughout their lifecycle, offering users the latest features and improvements through OTA updates. Aptiv's Smart Vehicle Architecture™ lays the foundation for future enhancements, combining flexible hardware designs and advanced software solutions [106] [107].

Cybersecurity Management in Software-Defined Vehicles

As software-defined vehicles become prevalent, Aptiv underscores the critical importance of robust cybersecurity management. The company advocates for the integration of security at every layer of software development, leveraging continuous security testing, compliance audits, and collaboration within industry organizations such as Auto-ISAC to address shared cybersecurity challenges [108].

Addressing Future Safety Challenges

Aptiv's innovative approach to the automotive industry includes a commitment to safety, sustainability, and connectivity. Through Smart Vehicle Architecture™, OTA updates, and a focus on cybersecurity, Aptiv is actively shaping the future of mobility, creating a roadmap for software-defined vehicles that prioritize safety, adaptability, and a differentiated user experience.

Addressing current state-of-the-art processes and development challenges is a key aspect of this dissertation, in line with Aptiv's commitment to safety, sustainability, and connectivity. Despite progress in the automotive industry, safety and cybersecurity often exist in silos, with limited areas of collaboration officially stated in existing processes. As an active member of working groups, I have observed efforts to address these issues, but the predominant focus has been on maintaining separate processes rather than establishing a unified safety framework that incorporates both safety and security aspects. This perspective has even influenced Aptiv in the choice of analysis software platform, where the more flexible and modern approach to cybersecurity has taken precedence over functional safety compliance.

The aim is to take a holistic and comprehensive approach to the safety problem, highlighting the commonalities between safety and cybersecurity processes in the V-model. I advocate a paradigm shift that promotes close collaboration and treats safety as a unified concept without differentiating between functional safety and cybersecurity. This approach leads to more accurate architecture, comprehensive analysis, and detailed, comprehensive requirements. Ultimately, it contributes to improved product quality, reduced risk, and faster time-to-market delivery.

One notable commonality identified is the need for an Intrusion Detection System (IDS), a market requirement that serves both safety and security measures. At Aptiv, we are actively working with industry leaders in cybersecurity to implement a comprehensive IDS solution across platforms. This system goes beyond traditional security measures to help make vehicles more resilient to a wide range of threats. Although the automotive industry may not prioritize such systems, Aptiv's proactive engagement with cybersecurity leaders reflects commitment to delivering innovative and comprehensive solutions that meet the evolving needs of the market and ensure the safety and security of platforms.

Chapter 3

New Framework for Electronic Control Modules Design Processes

The automotive sector is up against a new type of adversary. In addition to fighting against air pollution, fumes, and global warming, another unseen and intangible ingredient is filling in the gaps in this intricate jigsaw. Cybersecurity has risen to prominence as a result of Industry 4.0 and the increase in system connectivity. With continual communication, the vehicle is also extremely vulnerable to both internal and external attacks. Although the total number of vehicles in Europe and the United States may decrease slightly by 2030 [109], the industry's worldwide profit will be much higher. The driving force is Mobility-as-a-Service (MaaS)and a different ownership model for vehicle sharing [110]. Automotive risks are on the rise, with a particular emphasis on Original Equipment Manufacturers (OEM)s' IT infrastructure and car communication systems. Moreover, between 2010 and 2022, 79.6% of cyberattacks were carried out remotely. During this time period, one third of cyberattacks targeted data / privacy breaches, 28% vehicle theft / break-ins, 24% vehicle control systems and 20% service / business interruption. Fraud, Car System Manipulation, Location Tracking, and Policy violations accounted for 13% of the overall attack effect [61].

3.1 Combined Method for Autonomous Cyber-Physical Systems Development

3.1.1 Introduction - Analysis Coordination

The CyberSafety process model (proposed naming convention), which adheres to the system engineering paradigm for system development, captures the core activities included in the industry V-model approach while also attempting to target cross-dependencies between core automotive domains i.e. CySe, FuSa, and SOTIF. However, it does not cover the supporting processes that are required by ASPICE [72]. It is proposed to develop a holistic engineering design approach for cyber-, safety-critical systems within the automotive industry. The primary goal is to define the interfaces between engineering activities, which aids in the early stages of product development in organizing and holistically analyzing the design problem. The proposed CyberSafety process description will not focus on in-depth process analysis for ISO 26262:2018, ISO

21434:2021, and ISO 21448:2019 independently. It reveals dependencies and connection points to cover all necessary aspects inside a single engineering design cycle. Appendix A contains a comprehensive explanation of each designated activity, including its objectives, work deliverable, and role definition. A high-level overview of the CyberSafety framework is depicted in Figure 3.1. The next chapter takes a thorough dive into the process flow.

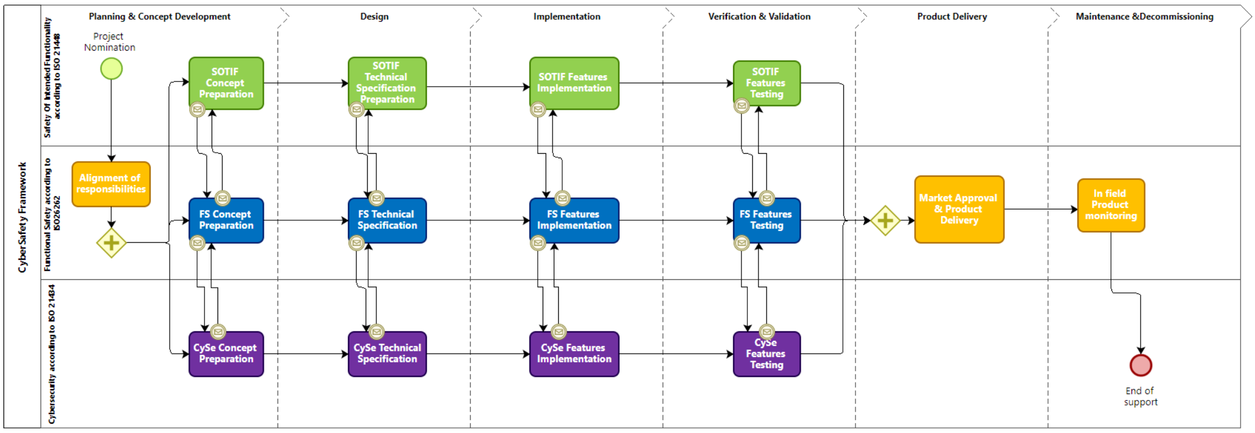

CyberSafety Framework
Safety Of Intended Functionality according to ISO 21448
Functional Safety according to ISO26262
Cybersecurity according to ISO 21434
Planning & Concept Development
Design
Implementation
Verification & Validation
Product Delivery
Maintenance &Decommissioning
Project Nomination
Alignment of responsibilities
SOTIF Concept Preparation
FS Concept Preparation
CySe Concept Preparation
SOTIF Technical Specification Preparation
FS Technical Specification
CySe Technical Specification
SOTIF Features Implementation
FS Features Implementation
CySe Features Implementation
SOTIF Features Testing
FS Features Testing
CySe Features Testing
Market Approval & Product Delivery
In field Product monitoring
End of support

Figure 3.1: A high level view of CyberSafety Framework. Color coding: Green - SOTIF, Blue - FuSa, Purple - CySe, Yellow - Common.

The purpose of the CyberSafety framework is to provide a holistic picture of the entire product development process, with a primary focus on the design phase. The remaining phases of the process are explained from a general standpoint, providing basic principles and, therefore, allowing for comprehensive strategy, implementation, verification, and validation details.

Due to its ease of use and widespread adoption by business analysts in all industries, Business Process Modeling and Notation 2.0 [111] is chosen to model the process. In essence, Business Process Management provides a systematic approach to managing organizational processes. It includes strategies, rules, technologies, and best practices to streamline workflows and constantly improve efficiency.It is a sequence of interrelated operations that engage several people and resources to create a valued output for a client. These procedures can use both internal and external systems, data, and resources. They might be carried out inside a single company or through a partnership with others. Business processes are the basic functions that enable a company to run, rather than individual activities. They have a direct influence on an organization's prospective income and expense structure by impacting its financial statements. Due to their crucial function, corporate processes must be protected against dangers such as fraud [112].

Bizagi Modeler [40], a desktop program, is used to create a process model. It supports version control, Business Process Model and Notation (BPMN) model validation, model simulation, and publication of high-quality documentation in formats such as Word, PDF, Web, and Wiki. Bizagi Modeler provides various enhancements to view a process model in different aspects and define connections and flows as well. The following flow objects and connecting objects are leveraged in the model (with all of the variations available in the BPMN 2.0 standard notation) and shown in Figure 3.2 i.e. Activities, Events, Gateways, Data, Artifacts, Swimlanes, and Connectors.

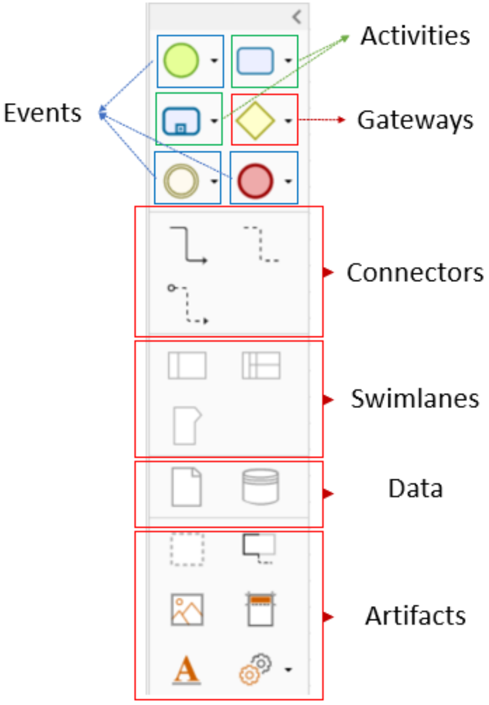


Figure 3.2: Basic objects available in BPMN 2.0, based on Bizagi Modeler [40].

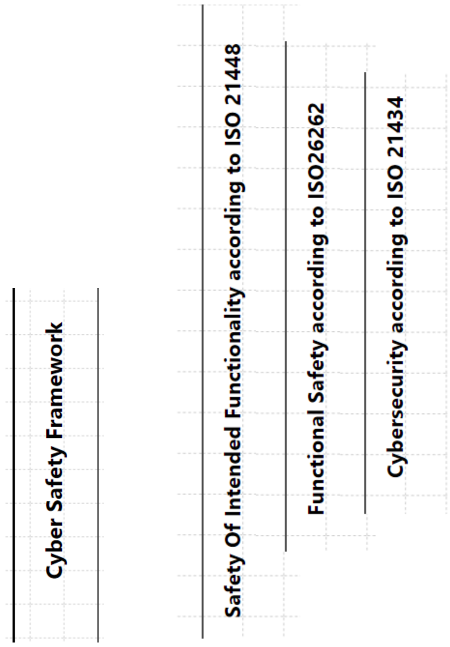
The CyberSafety Framework is included as a foundation in the single Pool (Figure 3.3a), with three Lines (Figure 3.3b), as depicted in Figure 3.3:

- Safety of Intended Functionality according to ISO 21488;
- Functional Safety according to ISO 26262;
- Cybersecurity according to ISO 21434.

Since the Lines are self-contained, only one line may be deployed within the scope of the project. Nevertheless, depending on the complexity of the present project and future expectations, installing the full process architecture may be necessary. Tailoring may be acceptable for either legacy systems or very basic sensors and actuators without advanced logic. However, tailoring actions must be properly evaluated and a proper rationale presented.

The CyberSafety process model is divided into concept, design, implementation, and verification and validation milestones, according to the most recent V-shaped design approach. Each Milestone is described in separate sections. It is shown in Figure 3.4 and is defined as follows:

- Project Preparation;
- Concept;
- Design;
- Implementation;


Cyber Safety Framework
Safety Of Intended Functionality according to ISO 21448
Functional Safety according to ISO26262
Cybersecurity according to ISO 21434

(a) CySa Pool.

(b) CySa Lanes.

Figure 3.3: CyberSafety model Pool and Lanes definition.

- Verification;
- Validation;
- Release Maintenance;
- Decommissioning.

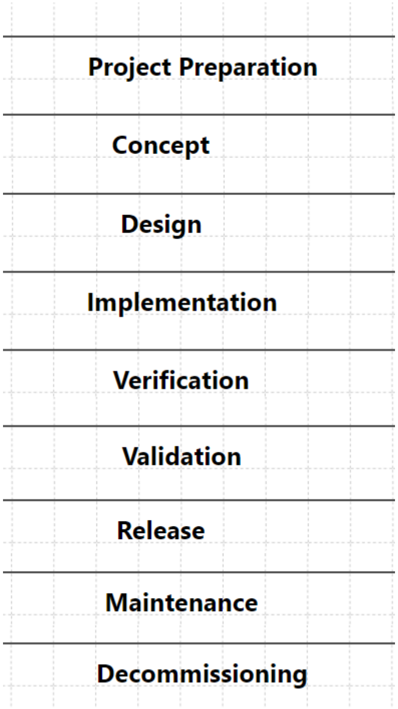
Each CyberSafety Framework Line includes all engineering operations needed by the associated standard. Then, for each Activity Box, a thorough explanation is provided, which contains the Activity Name, Description, and project resource roles such as Performer, Accountable, Consulted, and Informed. The example is shown in Figure 3.5. The activity may be tied to a process that is explained in depth. BPMN also allows you to connect numerous events to an activity in order to better portray the data flow. Message, Timer, Error, Compensate, Conditional, Signal, Multiple, Parallel, Multiple, Escalation are all examples of these. The branching and merging idea of Gateways is utilized for alternate flows.

The CyberSafety process describes the model resources necessary for process execution, as each process needs different roles and responsibilities, as shown in Figure 3.6, such as, e.g.:

- Role - CyberSafety Manager
- Description - CyberSafety Manager is responsible for coordination of Safety and Cybersecurity activities in project.

It is saved in the Bizagi Modeler database, along with a description of the position.

Sub-process concept is presented for the framework's complicated actions.Its graphical representation includes a 'plus' sign at the bottom-central part of the box. It is used to analyze risks and track incidences.



Project Preparation

Concept

Design

Implementation

Verification

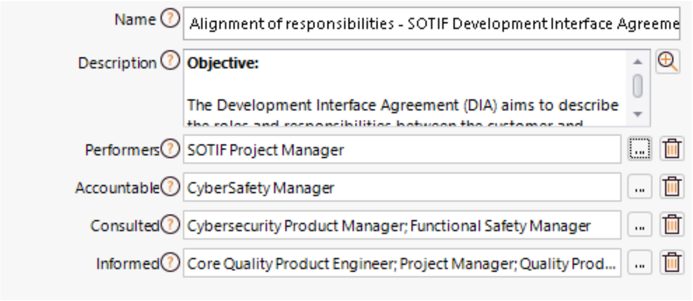
Validation

Release

Maintenance

Decommissioning

Figure 3.4: CyberSafety Framework Milestones.



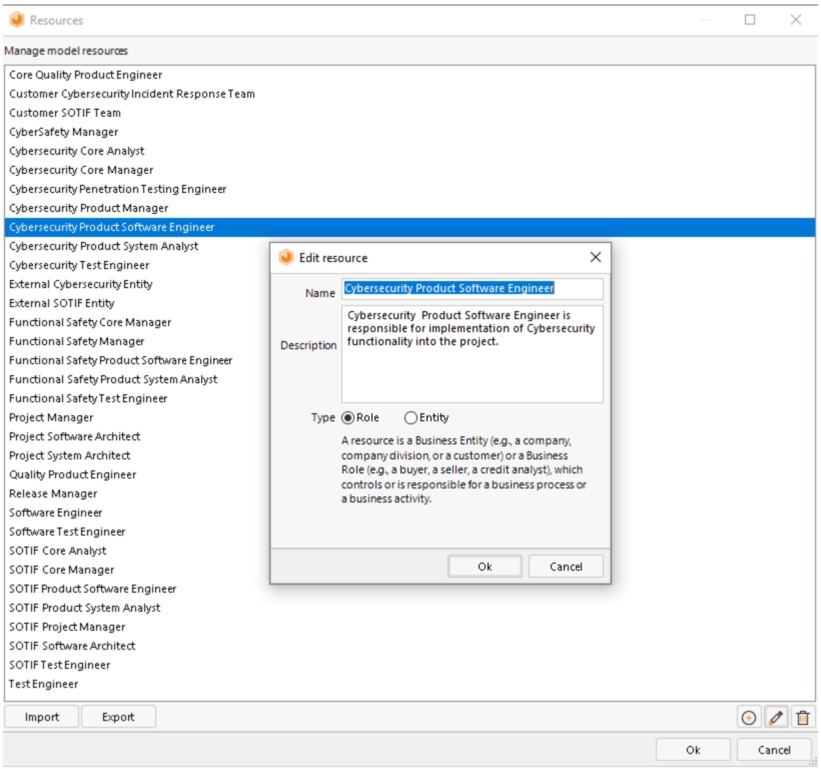
Name	Alignment of responsibilities - SOTIF Development Interface Agreeme
Description	**Objective:** The Development Interface Agreement (DIA) aims to describe the roles and responsibilities between the customer and
Performers	SOTIF Project Manager
Accountable	CyberSafety Manager
Consulted	Cybersecurity Product Manager; Functional Safety Manager
Informed	Core Quality Product Engineer; Project Manager; Quality Prod...

Figure 3.5: CyberSafety Framework Activity Box properties - example.

The example sub-processes are shown in Figure 3.7. Each of the aforementioned tasks has an embedded process that details the additional dependencies.

The color convention is adopted to identify the activities inside Lines. Green for SOTIF, blue for FuSa, and purple for CySe. The example is visible in Figure 3.7.

The CyberSafety framework is not a waterfall approach by definition. A valid result requires multiple iterations on both the large and small scales, as already indicated in Figure 2.6. The ultimate goal is to complete the System Model, which covers all elements of safety and security. The CyberSafety definition is used for actions that are shared by FuSa, CySe, and SOTIF. The activity blocks include the objectives and work products.



Manage model resources

Core Quality Product Engineer
Customer Cybersecurity Incident Response Team
Customer SOTIF Team
CyberSafety Manager
Cybersecurity Core Analyst
Cybersecurity Core Manager
Cybersecurity Penetration Testing Engineer
Cybersecurity Product Manager
Cybersecurity Product Software Engineer
Cybersecurity Product System Analyst
Cybersecurity Test Engineer
External Cybersecurity Entity
External SOTIF Entity
Functional Safety Core Manager
Functional Safety Manager
Functional Safety Product Software Engineer
Functional Safety Product System Analyst
Functional Safety Test Engineer
Project Manager
Project Software Architect
Project System Architect
Quality Product Engineer
Release Manager
Software Engineer
Software Test Engineer
SOTIF Core Analyst
SOTIF Core Manager
SOTIF Product Software Engineer
SOTIF Product System Analyst
SOTIF Project Manager
SOTIF Software Architect
SOTIF Test Engineer
Test Engineer

Name: Cybersecurity Product Software Engineer

Description: Cybersecurity Product Software Engineer is responsible for implementation of Cybersecurity functionality into the project.

Type: ● Role ○ Entity

A resource is a Business Entity (e.g., a company, company division, or a customer) or a Business Role (e.g., a buyer, a seller, a credit analyst), which controls or is responsible for a business process or a business activity.

Figure 3.6: CyberSafety Framework Roles description - example.

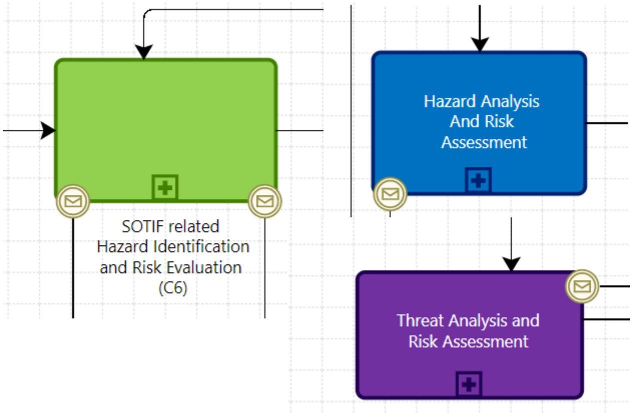


Figure 3.7: CyberSafety framework SubProcess - examples. Color coding: Green - SOTIF, Blue - FuSa, Purple - CySe.

3.1.2 Project Preparation Phase

Before starting any engineering activity, after a Project Nomination Trigger Point there is a project preparation phase to establish project milestones, estimate resources, etc. Figure 3.8. Another critical difficulty is defining the scope, roles, and responsibilities of the project. It is commonly referred to as a "Project Responsibility Assignment Matrix" preparation. To be more specific, the ISO standards express the requirement for developing the Development Interface Agreement, also known as the DIA for Functional Safety (according to ISO 26262: 2018), and the Cybersecurity Interface Agreement (according to ISO 21434:2021).

SOTIF standard itself does not address this section, yet in order to cover all safety issues, it should be additionally evaluated for FuSa DIA.

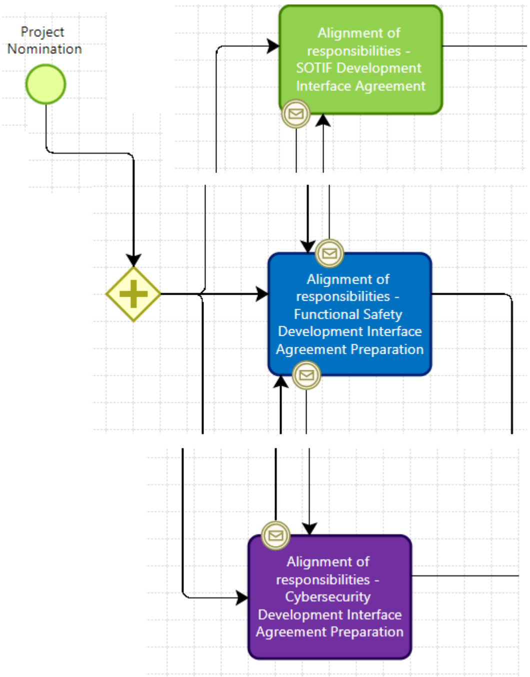

Project Nomination
Alignment of responsibilities - SOTIF Development Interface Agreement
Alignment of responsibilities - Functional Safety Development Interface Agreement Preparation
Alignment of responsibilities - Cybersecurity Development Interface Agreement Preparation

Figure 3.8: CyberSafety Framework - Project Initialisation and Responsibility Assignment preparation, including Project Nomination "Trigger Point", A Parallel Gateway, and Activity boxes from FuSa, CySe and SOTIF, which follow the colour convention.Color coding: Green - SOTIF, Blue - FuSa, Purple - CySe.

As a result, comprehensive Work Product planning is created based on the "Alignment of responsibilities" activity outlined in each Line within the CyberSafety process. The trigger event for which the process start is shown in Figure 3.8. A Parallel Gateway indicates that interface agreements can be utilized concurrently. The key part is communicating information about the responsibilities in order to better estimate the work required and to have a better understanding of the overall scope of the project. This can be managed by an additional identified role in the CyberSafety framework, named CyberSafety Manager. This function is primarily responsible for overseeing the safety and security operations of a project. Spending extra time on this work package is extremely beneficial, as clearly defined roles and responsibilities ease subsequent project processes. The information exchange in the process diagram is represented with Message Event, which is cross-referenced between lines.

3.1.3 Concept Phase

The concept phase is concerned with the vehicle's functionality, use cases, and related stakeholders. It combines business requirements with vehicle manufacturer specifications, market regulations, and standards. The described example design flow is depicted in Figure 3.9. Based on the supplied data, the first iteration of the system architecture may be created as a starting point for additional research. It is depicted in the process model with the System Model Preparation activity block, as visible in Figure 3.10.

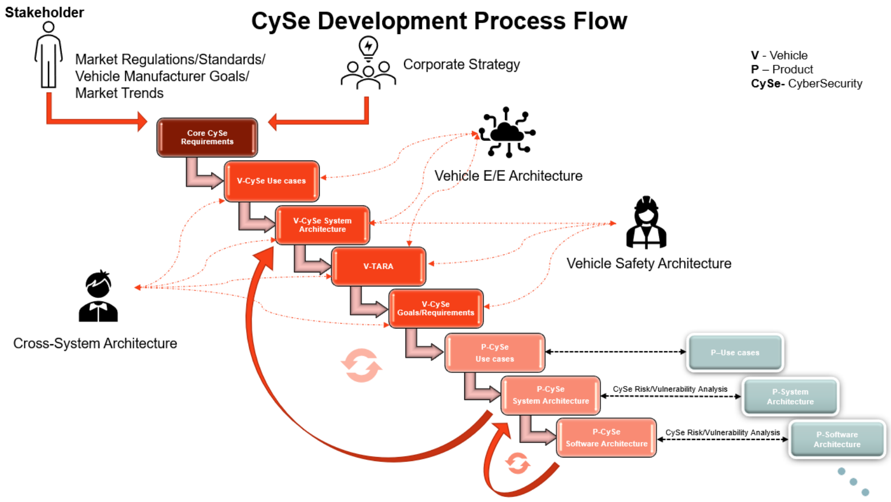

Stakeholder
CySe Development Process Flow
Market Regulations/Standards/
Vehicle Manufacturer Goals/
Market Trends
Corporate Strategy
V - Vehicle
P – Product
CySe- CyberSecurity
Core CySe Requirements
V-CySe Use cases
Vehicle E/E Architecture
V-CySe System Architecture
V-TARA
Vehicle Safety Architecture
V-CySe Goals/Requirements
Cross-System Architecture
P-CySe Use cases
P–Use cases
P-CySe System Architecture
CySe Risk/Vulnerability Analysis
P-System Architecture
P-CySe Software Architecture
CySe Risk/Vulnerability Analysis
P-Software Architecture

Figure 3.9: Example design work flow for CySe activities.

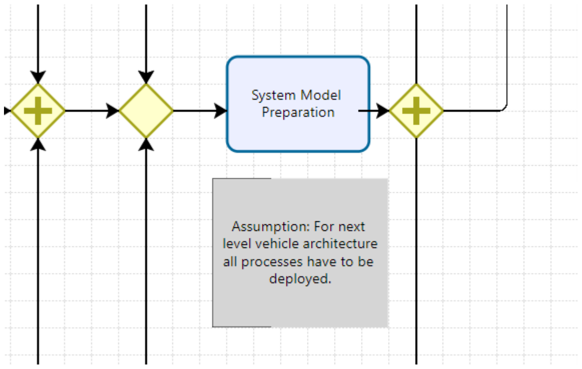

System Model Preparation
Assumption: For next level vehicle architecture all processes have to be deployed.

Figure 3.10: CyberSafety Framework - System Model Preparation.

After gathering the necessary data, the next step is to create an Item Definition, which is needed by both ISO 26262 and ISO 21434. In general, an Item is a component or combination of components that implements a function or part of a function at the vehicle level. The boundaries, interfaces, and environmental circumstances of an item should be well described. It should include all the information required by ISO 26262 Hazard Analysis and Risk Assessment (HARA), ISO 21434 TARA, and ISO 21448 HIRE.

Item Definition should be tackled jointly for both CySe and FuSa operations for the CyberSafety framework analysis, since autonomous features in connected vehicles can be accessible remotely by definition. As a result, there is a strong inclination to prioritize CySe activities above FuSa measures, which is summarized in Figure 3.11. Because once a function is compromised by malicious activity, safety is also jeopardized.

SOTIF does not expressly need an Item Definition, but it is an essential aspect of the safety analysis process. As a result, it is reasonable to assume that FuSa and SOTIF are, in theory, working on the same item.

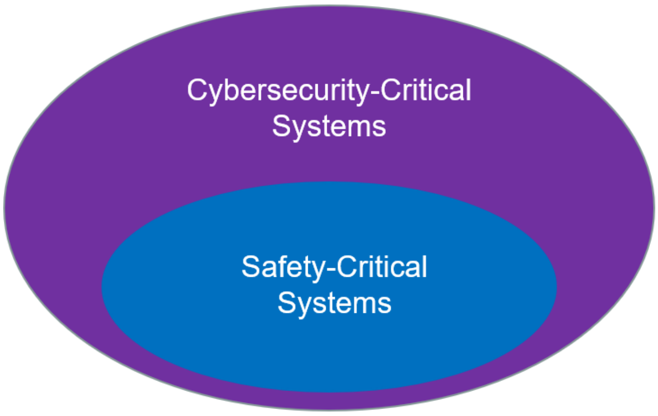


Figure 3.11: Relationship between Cybersecurity-Critical and Safety-Critical Systems based on [67].

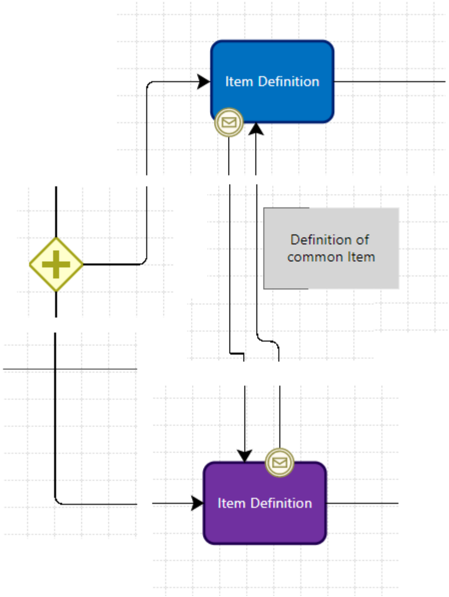


Figure 3.12: CyberSafety Framework Common Item Definition. Color coding: Blue - FuSa, Purple - CySe, Yellow - Common

The Item Definition decencies are signalled in the CyberSafety framework via a connected event to the Item Definition activity, as shown in Figure 3.12. The CyberSafety Manager is in charge of coordinating actions. By jointly defining an Item, with its:

- boundaries - the item boundary distinguishes the item from its operational environment;
- internal/external interfaces - the description of the item boundary can include interfaces with other items internal to the vehicle and/or with EE systems external to the vehicle;

- sub components - a specialized part of a larger system that performs a specific function, interacts with other components, and has defined dependencies and interfaces;
- operating environment - combination of hardware, software, and infrastructure that supports the execution and functioning of an item;
- stakeholders/actor - an individual, group, or organization that has an interest in or is affected by the outcome of an item;
- use-cases - a detailed description of how a system or application will be used by an actor to achieve a specific goal or complete a task.;
- limitations - item contraints e.g. related to performance, quality;
- operating modes and states - different conditions or configurations in which an item can function, each defined by specific behaviors, capabilities, and performance characteristics;
- sensors/actuator capabilities - specific functions and performance characteristics of sensors and actuators, including their ability to detect physical conditions or changes (sensors) and to influence or control physical processes (actuators) within an item;
- dependencies with other items - the relationships and reliance between components or systems, where the functionality or performance of one item is contingent on the presence, state, or output of another;

work can move forward with risk, threats and hazard analysis. The assumption is that "Item definition" for both CySe and FuSa may be started concurrently owing to available resources, project time, etc., however, synchronization is required.

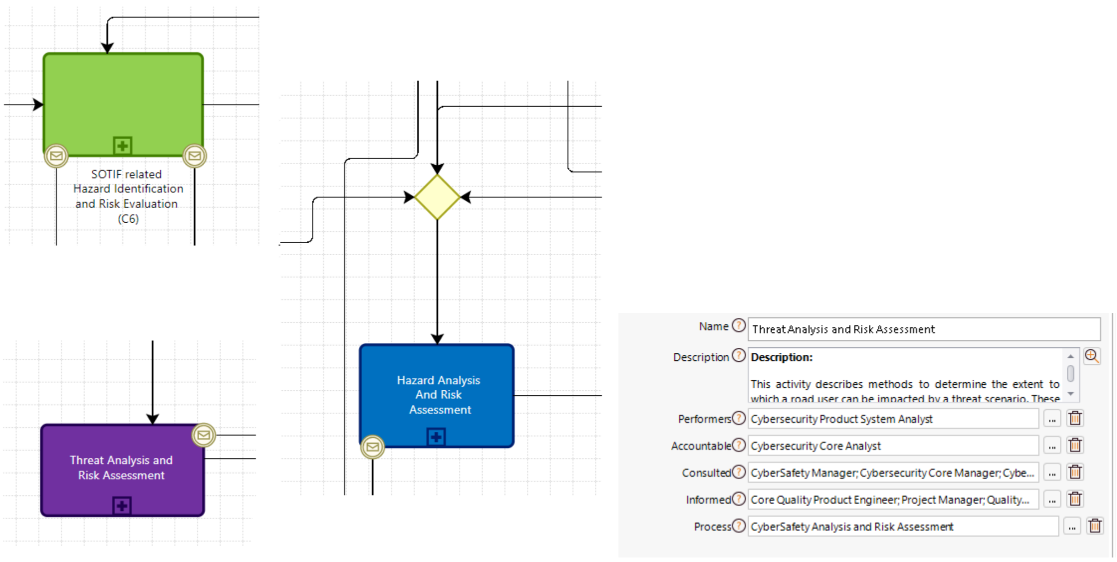
CyberSafety Analysis and Risk Assessment

A core aspect of the left side of V-model development is concept phase analysis over an Item. At this point, all system hazards and threats should be recognized, prioritized, and mitigated. The results of these operations are high-level objectives known as goals, which the system must finally accomplish in order to meet consumer expectations and, of course, market regulations.

With respect to the FuSa, CySe, and SOTIF standards, there are specific state-of-the-art frameworks that must be followed during the concept analysis. Hazard Analysis and Risk Assessment is the term used for functional safety analysis. It is expanded to Hazard Identification and Risk Evaluation when the SOTIF element is added. In terms of CySe, it is known as Threat Analysis and Risk Assessment.

Due to universally acknowledged interfaces between these analyses, there is currently a belief within the industry to merge them into a unified framework. However, there are still highly distinguishing aspects that define TARA, HARA, and HIRE that cannot be neglected [24, 56, 113–116].

In this situation, there is a great need to create a common analytical flow that can meet all industry standards while also performing a holistic risk analysis throughout a system. This is especially important when considering modern connectivity automotive systems that are exposed to the outside world. If a vulnerability on such systems is exploited, the system's safety is jeopardized and may result in a hazard.


SOTIF related Hazard Identification and Risk Evaluation (C6)
Hazard Analysis And Risk Assessment
Threat Analysis and Risk Assessment
Description
Performers
Accountable
Consulted
Informed
Process
...

Name: Threat Analysis and Risk Assessment

Description: **Description:**

This activity describes methods to determine the extent to which a road user can be impacted by a threat scenario. These

Performers: Cybersecurity Product System Analyst

Accountable: Cybersecurity Core Analyst

Consulted: CyberSafety Manager; Cybersecurity Core Manager; Cybe...

Informed: Core Quality Product Engineer; Project Manager; Quality...

Process: CyberSafety Analysis and Risk Assessment

(a) CyberSafety Framework, HARA, HIRE, TARA connections. Color coding: Green - SOTIF, Blue - FuSa, Purple - CySe, Yellow - Common.

(b) CyberSafety Framework - TARA, example roles assignment.

Figure 3.13: CyberSafety Framework - analysis coordination.

Taking all aspects into account, the CyberSafety Framework includes activity boxes for Hazard Analysis and Risk Assessment, Hazard Identification and Risk Evaluation, and Threat Analysis and Risk Assessment within its concept milestone, as shown in Figure 3.13a. It is determined that there is a correlation between these boxes by inserting a message trigger between them. Each relevant activity diagram contains specific information from an applicable standard that identifies what is needed to perform the analysis. In addition, roles and responsibilities are specified as shown in Figure 3.13b.

Analysis-related action boxes are linked to a single sub-process known as CyberSafety Analysis and Risk Assessment. The CyberSafety Analysis and Risk Assessment subprocess is divided into three lines, representing actions of related standards, similar to the CyberSafety framework, as shown in Figure 3.14.

An item definition begins with CyberSafety Risk Analysis (CySaRA) (proposed nomenclature to be used). The FuSa's Situation Analysis and Hazard Identification, CySe's Asset Identification, and SOTIF's Situation Analysis and Risk Identification operations can then be launched in concurrently, as depicted in Figures 3.15 and Figure 3.16.

The first strong correlation in the combined CyberSafety Risk Analysis (CySaRA) analysis is between Situation Analysis and Hazard Identification, which is expanded with Situation Analysis and Hazard Identification, and Asset Identification and related Threat Scenario Identification, as visible in Figure 3.15 and Figure 3.16.

The Asset Identification activity is undertaken first from the viewpoint of CySe. An asset is a valuable object that must be secured in order to avoid a damage scenario, which is a negative consequence involving a car or a vehicle function that impacts a road user. All damaged situations listed in the TARA section

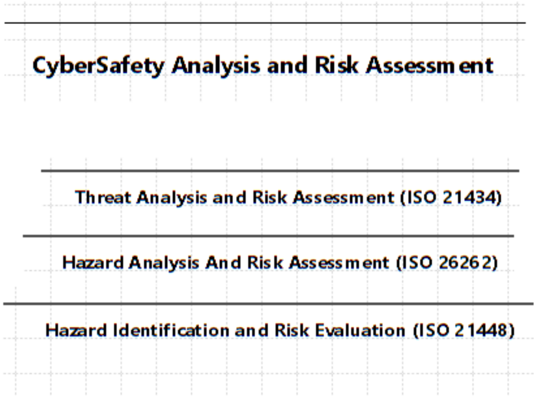

CyberSafety Analysis and Risk Assessment
Threat Analysis and Risk Assessment (ISO 21434)
Hazard Analysis And Risk Assessment (ISO 26262)
Hazard Identification and Risk Evaluation (ISO 21448)

Figure 3.14: CyberSafety Analysis and Risk Assessment, Pool and Lines definition.

must be considered during Situation Analysis and Hazard Identification and Situation Analysis and Hazard Identification.

SOTIF Hazard Scenarios and SOTIF Hazardous Events should be included in FuSa's Situation Analysis and Hazard Identification. Similarly, Hazardous Events and Hazardous Scenarios derived from FuSa analysis must be fed into Situation Analysis and Hazard Identification. The main aim of this connection is to broaden the area of safety analysis to performance limitations of intended functionality and hazards of unintended behavior, rather than focusing just on systematic error incidence, as FuSa always does. As a possible Damage Scenario, the FuSa and SOTIF Hazard Scenarios should be further investigated in the CySe section, as shown in Figure 3.15 and Figure 3.16.

Following the CySe flow, the next stage is Threat Scenario Identification, which is a possible source of compromise of one or more assets' cybersecurity attributes in order to execute a damage scenario. A threat scenario that has been discovered is a relevant input to both Situation Analysis and Hazard Identification, and Situation Analysis and Hazard Identification as a result of the intended functionality, which is visible in Figure 3.15 and Figure 3.16.

All detected threat scenarios should be analyzed from a safety point of view so that further prospective safety measures can be implemented to reduce a risk. Using this approach, FuSa and SOTIF Hazardous Events should be assessed as possible threat scenarios that can be mitigated subsequently by implementing CySe procedures, as shown in Figure 3.17.

With this first link established, the FuSa, CySe, and SOTIF analysis becomes more comprehensive, encompassing all aspects of end-user safety, including external factors (such as an attacker activity), internal malfunctions related to system, hardware, or software design, as well as aspects of intended function safety, taking into account potential misuse and performance limitations.

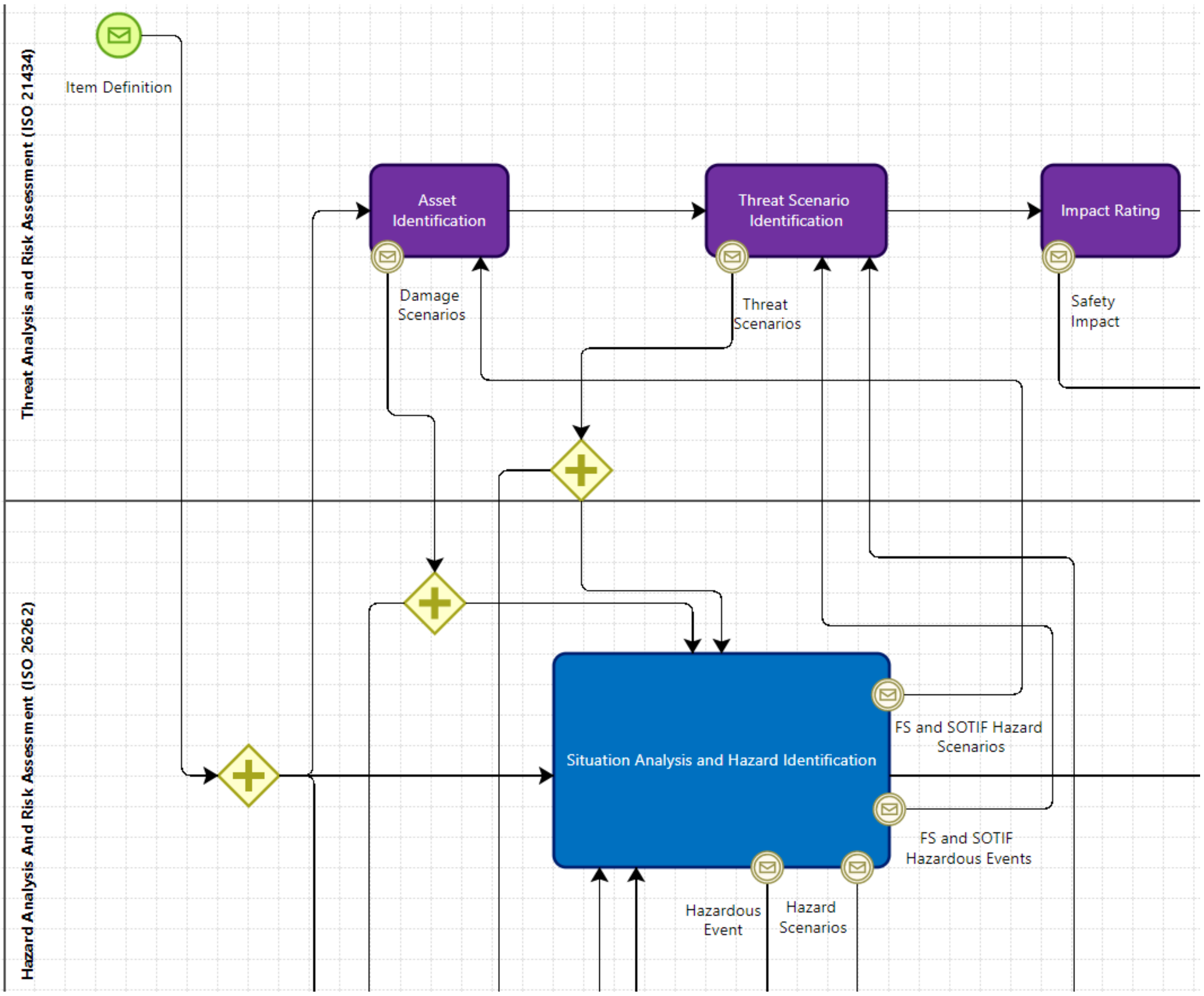

Threat Analysis and Risk Assessment (ISO 21434)
Item Definition
Asset Identification
Damage Scenarios
Threat Scenario Identification
Threat Scenarios
Impact Rating
Safety Impact
Hazard Analysis And Risk Assessment (ISO 26262)
Situation Analysis and Hazard Identification
FS and SOTIF Hazard Scenarios
FS and SOTIF Hazardous Events
Hazardous Event
Hazard Scenarios

Figure 3.15: CyberSafety TARA and HARA dependencies. Color coding: Blue - FuSa, Purple - CySe.

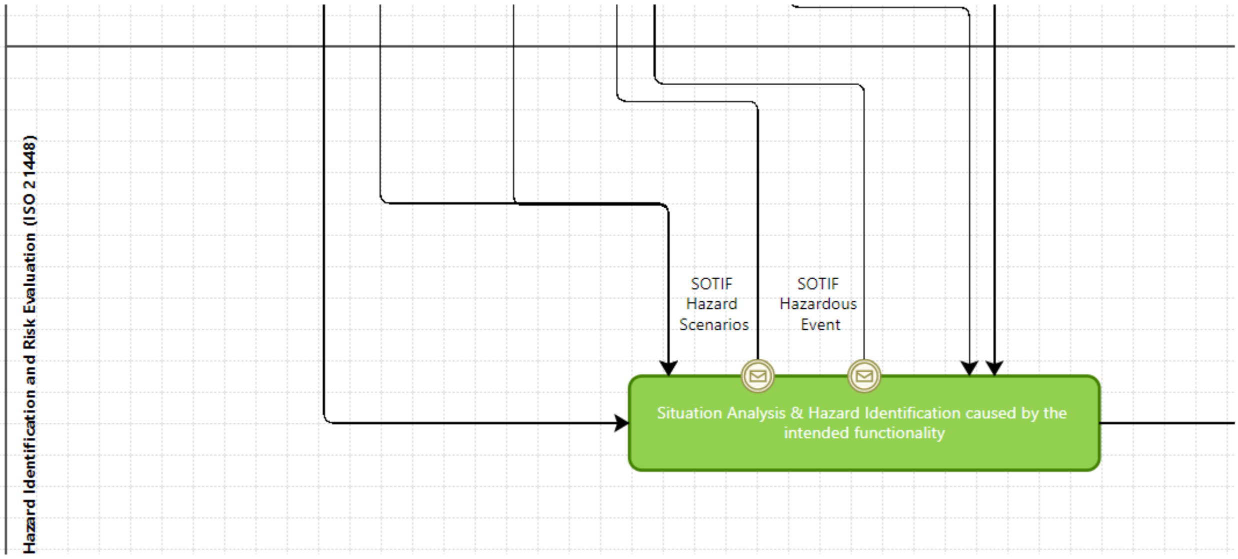

Hazard Identification and Risk Evaluation (ISO 21448)
SOTIF Hazard Scenarios
SOTIF Hazardous Event
Situation Analysis & Hazard Identification caused by the intended functionality

Figure 3.16: CyberSafety HARA and HIRE dependencies. Color coding: Green - SOTIF.

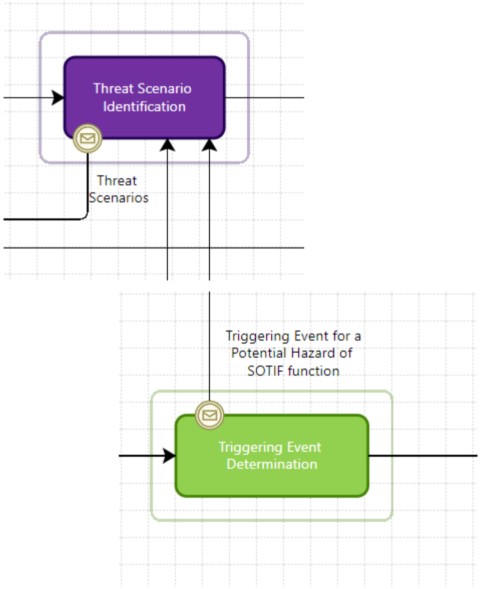

Threat Scenario Identification
Threat Scenarios
Triggering Event for a Potential Hazard of SOTIF function
Triggering Event Determination

Figure 3.17: CyberSafety TARA and SOTIF dependencies.Color coding: Green - SOTIF,Purple - CySe.

After identifying all potential damage scenarios, threat scenarios, and related hazard scenarios and events, the next step is to classify them. FuSa and SOTIF use for this purpose a similar strategy, utilizing the one proposed in ISO 26262, as presented in Figure 3.18. In this case, all identified hazardous events shall be classified with the following classes [5]:

- Severity class (S0-S3) in accordance with ISO 26262-3, which indicates the severity of potential harm;
- Exposure class (E0-E4) in accordance with ISO 26262-3, which indicates the probability of exposure of each operational situation;
- Controllability class (C0-C4) in accordance with ISO 26262-3, which indicates the controllability of each hazardous event, by the driver or the persons involved in the operational situation.

In this situation, FuSa and SOTIF perform a complementary analysis for hazard classification, which can be performed at the same time, as depicted in Figure 3.19.

CySe analysis provides information for hazardous event classification. To begin with, the CySe impact assessment takes into account factors such as safety, financial, operational, and privacy. For each impact category, the impact rating of a damage scenario must be one of the following [5]:

- Severe;
- Major;
- Moderate;
- Negligible.

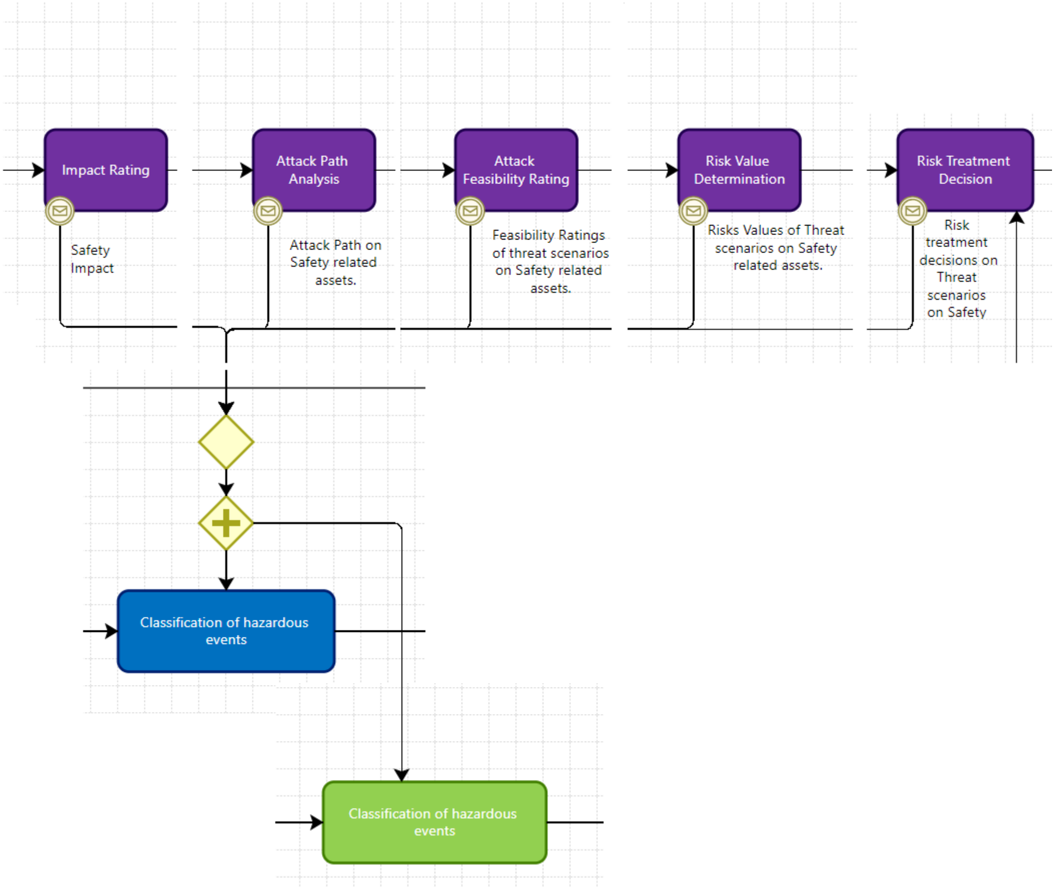

Impact Rating
Safety Impact
Attack Path Analysis
Attack Path on Safety related assets.
Attack Feasibility Rating
Feasibility Ratings of threat scenarios on Safety related assets.
Risk Value Determination
Risks Values of Threat scenarios on Safety related assets.
Risk Treatment Decision
Risk treatment decisions on Threat scenarios on Safety
Classification of hazardous events
Classification of hazardous events

Figure 3.18: CyberSafety Analysis Hazard classification and TARA dependencies. Color coding: Green - SOTIF, Blue - FuSa, Purple - CySe.

ISO 21434:2021 itself redirects to ISO 26262:2018 for a safety impact determination. Hence, if the safety impact is identified, it should be further evaluated during the classification of hazards for FuSa and SOTIF and may have a direct impact on ASIL determination, if identified CySe Safety level is severe.

Next, after identifying the CySe threat scenario, each of them must be examined to find attack paths. This may involve both internal and external interfaces as well as a variety of other alternatives. If an attack path through a safety-related asset is discovered during this activity, it should be reported to the safety team and reviewed during categorization.

Although all potential attack vectors can be recognized, not all are equally likely to occur. As a result, during the attack feasibility rating activity, an analysis is performed to determine how likely a certain assault is. ISO 21434:2021 specifies numerous rating methodologies, including the attack feasibility rating, the attack potential-based approach, CVSS, and the attack vector-based approach. The technique is determined by business policy or analysts. As a consequence, information is provided that indicates if a certain attack feasibility is high, medium, or low (depending on the chosen analysis strategy). If the attack feasibility of a safety-related asset is considered high or medium, it should be reported to the safety team and examined during classification.

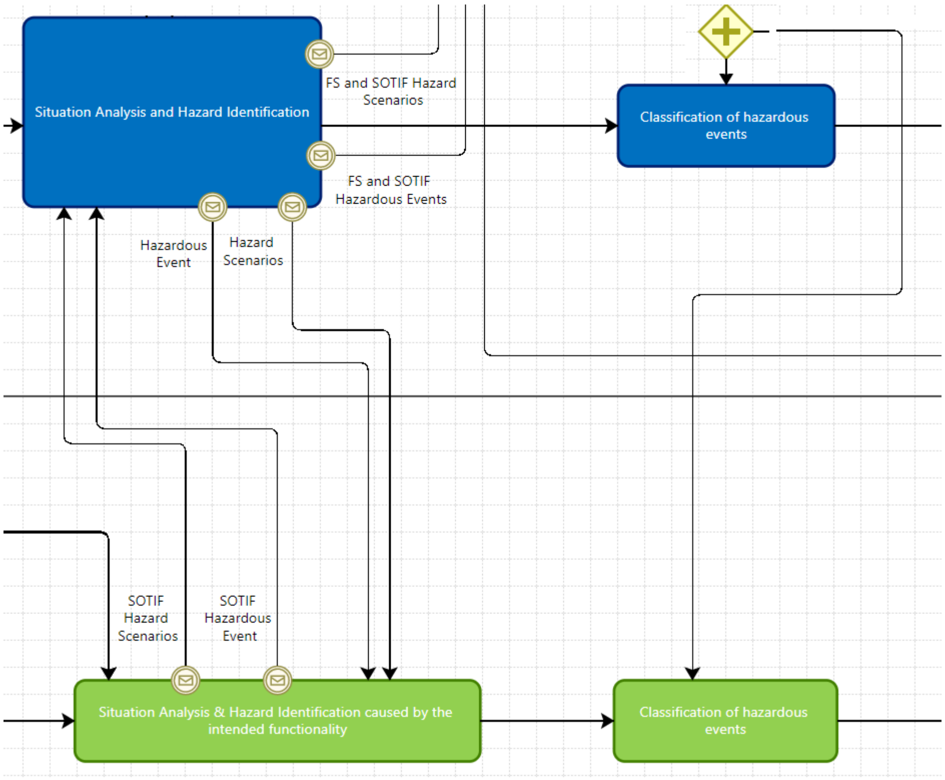

Situation Analysis and Hazard Identification
FS and SOTIF Hazard Scenarios
Classification of hazardous events
FS and SOTIF Hazardous Events
Hazardous Event
Hazard Scenarios
SOTIF Hazard Scenarios
SOTIF Hazardous Event
Situation Analysis & Hazard Identification caused by the intended functionality
Classification of hazardous events

Figure 3.19: CyberSafety Analysis Hazard classification for FuSa and SOTIF. Color coding: Green - SOTIF, Blue - FuSa.

Moving forward, even if a threat is rated as low, its influence on the system may be rated as high. Hence, the risk value evaluation is conducted in the following phase for the CySe. The risk value for each threat scenario is defined by the effect of the associated damage scenarios and the attack capability of the related attack channels. The risk value of a threat scenario must be between 1 and 5, with 1 being the lowest danger. If the risk value of the threat scenario on the safety-related asset is considered as high (i.e., more than 3), it should be reported to the safety team and examined during classification, as indicated in Figure 3.20.

The Risk Treatment Decision is the final stage in the TARA process. For each threat scenario, one or more of the following risk treatment alternatives must be identified, taking into account the risk value [13]:

- Avoiding the risk;
- Reducing the risk;
- Sharing the risk;
- Retaining the risk.

The risk treatment decision on Threat Scenarios on Safety-related assets should be reported to the safety team and examined during classification.

In parallel activity for FuSa, the ASIL level is determined according to ISO 26262-3 following the classification of hazardous events. There are four ASILs defined: ASIL A, ASIL B, ASIL C, and ASIL D, with ASIL A being the lowest and ASIL D the highest. Because information on the safety classification of an Item or an item's component may influence risk treatment decisions, a message event is added to the CySaRA process model. Moreover, the ASIL level has influence on the modification of certain functions of the SOTIF to defend against specific scenarios and hazard events, as visible in Figure 3.20.

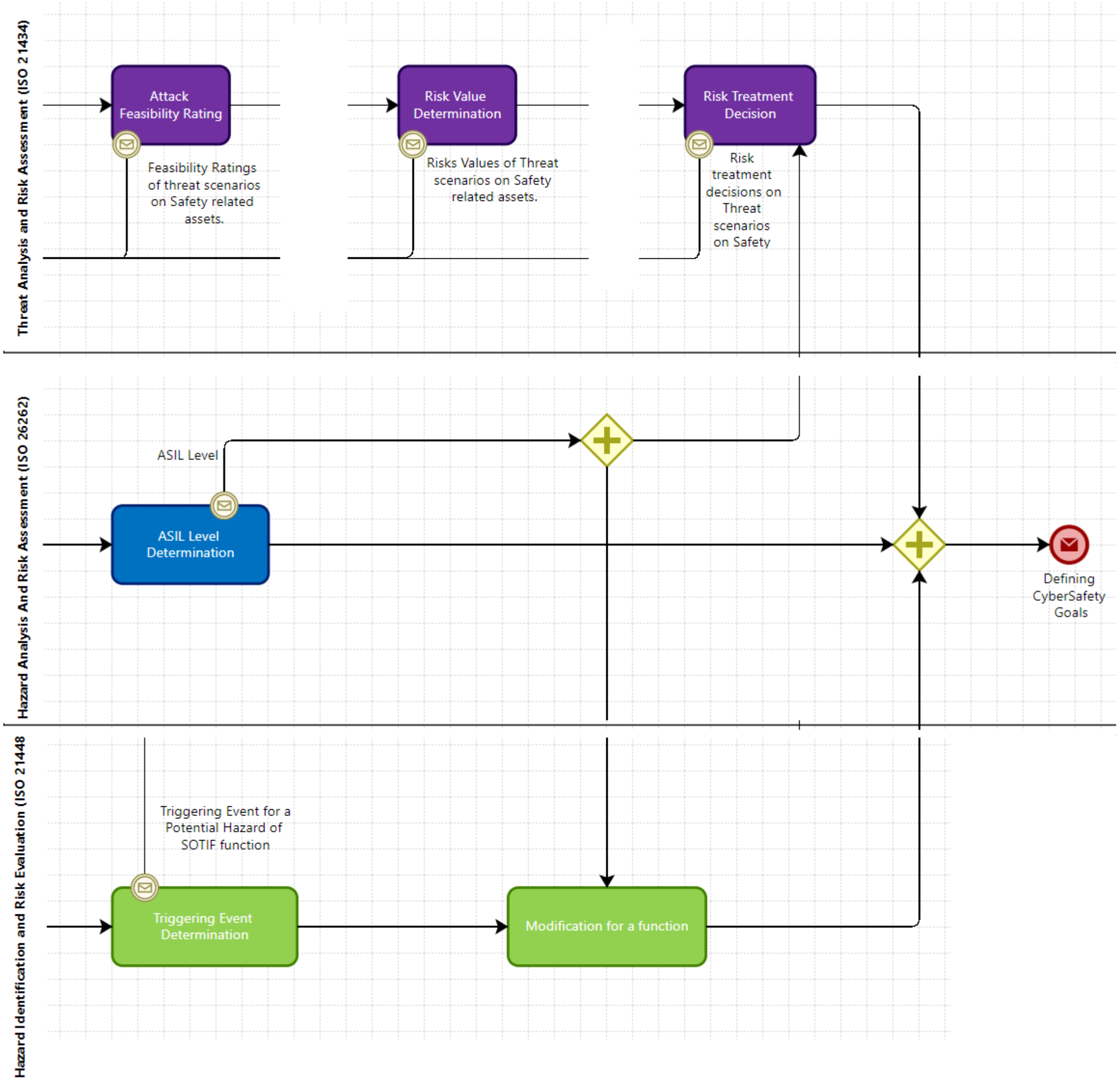

Threat Analysis and Risk Assessment (ISO 21434)
Attack Feasibility Rating
Feasibility Ratings of threat scenarios on Safety related assets.
Risk Value Determination
Risks Values of Threat scenarios on Safety related assets.
Risk Treatment Decision
Risk treatment decisions on Threat scenarios on Safety
Hazard Analysis And Risk Assessment (ISO 26262)
ASIL Level
ASIL Level Determination
Defining CyberSafety Goals
Hazard Identification and Risk Evaluation (ISO 21448
Triggering Event for a Potential Hazard of SOTIF function
Triggering Event Determination
Modification for a function

Figure 3.20: CyberSafety analysis ASIL level determination interfaces between from FuSa to SOTIF and CySe. Color coding: Green - SOTIF, Blue - FuSa, Purple - CySe.

At this point, the testing strategy for FuSa, CySe, and SOTIF should be established, then refined throughout the development life cycle and applied at the Verification and Validation milestones.

CyberSafety Goals

The CyberSafety Manager must ultimately coordinate all analytic activity, and common CyberSafety goals must be created.

Following ISO standards [5, 6, 13], CyberSafety goals:

- Shall be defined for each hazardous event with an ASIL reviewed in the HARA and HIRE;
- Shall be determined for each threat scenario evaluated in the TARA;
- Shall be stated in line with ISO 26262:2018 Clause 6 and ISO 21434:2021;
- Shall be verified to confirm completeness, consistency with respect to the risk treatment decisions.

3.1.4 Design Phase

CyberSafety Concept

After defining the CyberSafety goals and high-level concept requirements, the next stage is to break them down into more technical specifics and, as a result, come up with engineering solutions at the design level. Defining the CyberSafety concept falls between the Concept and Design phases. It is featured in the Design Milestone for the CyberSafety framework because it defines a more specific architectural perspective than the goals themselves, as presented in Figure 3.21.

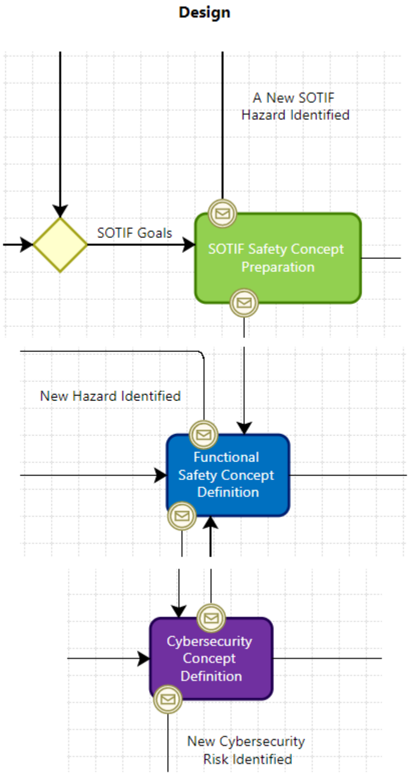

Design
A New SOTIF Hazard Identified
SOTIF Goals
SOTIF Safety Concept Preparation
New Hazard Identified
Functional Safety Concept Definition
Cybersecurity Concept Definition
New Cybersecurity Risk Identified

Figure 3.21: CyberSafety Framework, Design Milestone, Concept Preparation. Color coding: Green - SOTIF, Blue - FuSa, Purple - CySe.

The main common objectives of a solution concept definition, following FuSa, CySe, SOTIF standards are [5, 6, 13]:

- to specify the item's functioning or reduced functional behavior in line with its objectives coming from TARA, HARA, and HIRE;
- to define the restrictions for appropriate and timely detection and management of relevant problems in line with its CyberSafety objectives including intrusion detection and prevention mechanisms;
- to provide item-level strategies or procedures to achieve specified fault tolerance or properly mitigate the consequences of relevant defects and threats by the item, the driver, or external measures;

- to define a rollback protection to prevent downgrading the device to an older version of its software that is outdated due to security concerns;
- to define logging strategy for forensic analysis;
- to allocate FuSa, CySe, SOTIF requirements to the system model architecture design or external actors;
- to verify the solution concept and specify the validation criteria.

Following industry best practices for a solution concept:

- The CyberSafety requirements shall be derived from each CyberSafety goal;
- At least one CyberSafety requirement shall be derived from CyberSafety goal;
- CyberSafety requirement shall be written to comply with ISO26262:2018 and ISO21434:2021 standards.

If a new Hazard or Threat is detected during the CyberSafety Concept activity, the discovery should be addressed in TARA, HARA, and HIRE processes and re-analyzed. A message event from a concept definition to TARA or HARA is noted in the process diagram. If a new Hazard is discovered, it is proposed that it should also be considered for the HIRE analysis.

Various approaches may be used for this activity to better examine the risks and hazards of suggested conceptual solutions. An alternative is to develop a CyberSafety Failure Mode and Effect Analysis (FMEA), which investigates not only hazards due to failure of safety mechanisms, but also the impact of a lack/malfunction of cybersecurity controls.

The link between the Functional Safety Concept and the Cybersecurity Concept is denoted by a bidirectional messaging event between both activities.

For connected and autonomous cars, creating a unified CyberSafety concept that encompasses all types of risk assessment provides a comprehensive perspective of a built system. A suitable System Architecture Model Refinement is enabled by starting with a common Item Definition, common CyberSafety Goals, and a thorough end concept. However, the common notion should be developed only for functions that are considered significant in both safety and cybersecurity.

CyberSafety Technical Concept

As per the process flow, the next action within the given milestone is Technical Concept preparation. It should include additional technical information about an engineering solution. Similarly to the CyberSafety Concept, a shared CyberSafety Technical Concept should be established for functions that are related to both safety and cybersecurity, as presented in Figure 3.22.

The CyberSafety Technical Concept integrates the CyberSafety criteria with the applicable system architectural design, as well as the reasons why the system architectural design model is suitable for achieving CyberSafety standards. The defined requirements describe the technical implementation of CyberSafety standards while accounting for CySe, FuSa, and SOTIF dependencies.

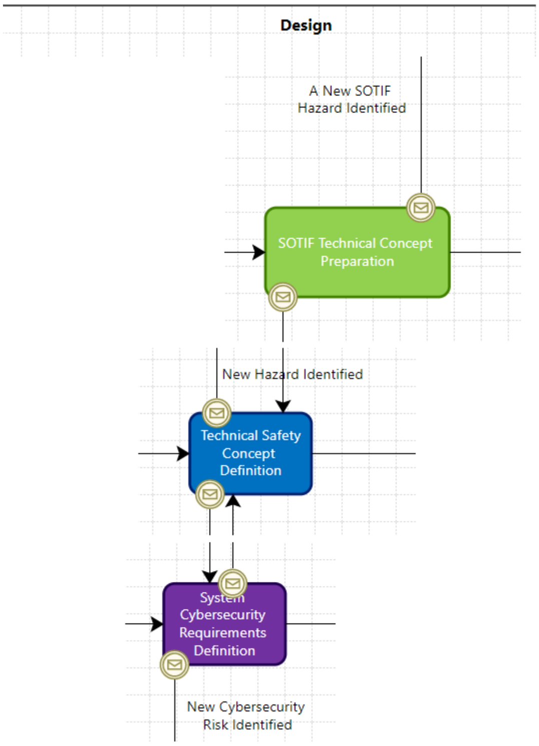

Design
A New SOTIF Hazard Identified
SOTIF Technical Concept Preparation
New Hazard Identified
Technical Safety Concept Definition
System Cybersecurity Requirements Definition
New Cybersecurity Risk Identified

Figure 3.22: CyberSafety Framework, Design Milestone, Technical Concept Preparation. Color coding: Green - SOTIF, Blue - FuSa, Purple - CySe.

A System Architectural Model is a system-level solution that is chosen and implemented by a technical system. It is intended to meet both CyberSafety and non-CyberSafety criteria. The System Architectural Model can be improved once the CyberSafety Technical Concept has been specified. If a new hazard or threat scenario is discovered when developing the CyberSafety Technical Concept, TARA, HARA, and HIRE should be revised to deal with the new potential risks. A Message Event is used to signify this in the CyberSafety framework.

The premise is that the CyberSafety Concept is defined collaboratively by CySe, FuSa, and SOTIF and is overseen by the CyberSafety Manager. With the participation of all stakeholders, appropriate CyberSafety measures may be created to address both hazards and threats.

Addressing the ISO standards and industry best practices CyberSafety Technical Concept:

- Shall be defined in accordance to CyberSafety Concept and System Architectural Design model of an Item and consider:
  - functional and performance limitations of Item and its elements;
  - external interfaces;
  - system reconfigurability;
  - vulnerability management;
  - cybersecurity controls coming from CyberSafety Concept;
  - safety mechanisms coming from CyberSafety Concept;

  - compliance to market regulations and requirements.

- All trigger points for implementing CyberSafety measures for incidents and hazards must be defined;
- CyberSafety an non-CyberSafety requirements shall not contradict;
- Shall define CyberSafety mechanisms of detecting and mitigating the CyberSafety threats and failures in accordance to market regulations and standards including:
  - The CyberSafety mechanism concerned with the detection, indication and control of threats and system failures;
  - The CyberSafety mechanisms concerned with the detection, indication, and management of threats as well as failures in other external components that interact with the system;
  - The CyberSafety mechanisms that support the system to achieve or maintain the item's CyberSafety state;
  - The CyberSafety mechanisms to define and implement the warning and degradation strategy;
  - The CyberSafety mechanisms responsible for defining and implementing the warning and degradation strategy.
- Shall provide measure to control the random hardware failures and threats during operation;
- Shall define the hardware and software CyberSafety measures allocation;
- Shall define the Hardware-to-Software (HSI) interface;
- Shall define the requirements for production, operation and decommissioning focusing on CyberSafety measures.

CyberSafety Mechanisms

The following should be described for each CyberSafety mechanism that allows an item to achieve or maintain a CyberSafety state:

- Interstate transition;
- Threat and fault handling time interval with respect to the timing requirement;
- The emergency operation tolerance time interval;
- Mechanisms how to prevent faults and threats to be latent;
- Multiple-point failures diagnostic strategy;
- CyberSafety mechanisms shall be in line with Automotive Safety Integrity Level (ASIL) and Cybersecurity Assurance Level (CAL) level assigned during analysis.

To meet cybersecurity requirements, it is possible to use safety measures; nevertheless, a suitable justification and analysis should be provided. In general, CyberSafety mechanisms should address criteria from both domains. Therefore, prior to developing the CyberSafety Technical Concept, there should be a specified catalog of proven CyberSafety Mechanisms that are consistent with industry standards. Following that, an appropriate, proven technique can be chosen to meet CyberSafety goals and concept criteria.

System Architectural Design Specification and the CyberSafety Technical Concept

The System Architectural Design Model, together with use-cases, static and dynamic diagrams, serves as the foundation for CyberSafety requirements and concepts. As a result, consistency should be maintained while developing CyberSafety requirements, since when the CyberSafety Technical Concept is finalized, all needs must be included in the System Architectural Design Model. This shall allow to :

- verify the System Architectural Design model;
- address the technical capability of the intended hardware and software elements with regard to the achievements of CyberSafety;
- perform the verification during system integration.

The internal and external interfaces of CyberSafety-related elements shall be defined such that other elements shall not have adverse CyberSafety-related effects on the CyberSafety-related elements.

CyberSafety Analysis and Avoidance of Threats and Failures

CyberSafety analysis on the System Architectural Design Model must be undertaken in line with ISO standards to give proof for the system design's suitability to offer the stated CyberSafety related functions and characteristics in relation to the CAL and ASIL. In addition, it should identify failures and possible risks, as well as the consequences of these flaws. Additionally, this activity must discover or confirm CyberSafety-related features and interfaces, as well as assist with the design specification and validate the performance of CyberSafety mechanisms.

Identified internal or external causes of threats or failures shall be eliminated, or their effects mitigated, where necessary, to comply with the CyberSafety goals or requirements. Where possible, well-trusted system design principles should be implemented to limit the possibility of systematic failures and recognized threats. This might involve reusing well-known concepts, design features, systems to detect and control threats and failures, and standardized interfaces. An appropriateness study of trusted design patterns must be carried out and recorded. To limit the likelihood of failures and threats, the design of the system must adhere to the core principles of modularity, graduality, and simplicity.

Measures for Control the Random Hardware Failures and Threats during operation

To meet the ISO standard criteria, methods must be in place to detect, control, or mitigate random hardware failures in the architecture of the system. Furthermore, procedures must be put in place to detect and mitigate threats posed by malicious activity that may affect safety measures. This set of requirements is applied to systems that have been identified as CyberSafety relevant prior to system definition.

CyberSafety Measures Allocation to Hardware and Software

CyberSafety Technical requirements must be assigned to components of the system architectural design, hardware, or software as the implementing technology. All allocation and partitioning choices must adhere to the system architectural design and CyberSafety analysis.

Hardware to Software Interface (HSI) Specification

HSI must define how hardware and software interact in accordance with the CyberSafety Technical Concept. It must include the specification of hardware components controlled by software, as well as hardware resources that facilitate the safe and secure execution of the software. To establish a chain of trust and a trusted execution environment, a secure element within the system that meets the technical specifications must be identified. The HSI specification shall include:

- the required hardware device operating modes, the relevant configuration options, including debug port protection;
- hardware components that maintain element independence or facilitate software partitioning, also inside a secure element;
- exclusive and shared usage of hardware resources for safety-critical features;
- exclusive and shared usage of hardware resources for cybersecurity-critical features;
- definition of interface to a secure element;
- the timing constraints derived from the CyberSafety Technical concept.

Furthermore, HSI must incorporate essential hardware diagnostic and error detection capabilities, as well as employ the suitable software, including the secure element.

Production, Operation, Service and Decommissioning

CyberSafety Technical concept shall address the requirement for production, operation, service, and decommissioning, identified during the system architectural design. These shall include:

- generation and provisioning of security artefacts during production;
- management of the debug ports protection;
- measures required to achieve, maintain or restore the CyberSafety-related functions and properties of the item and its elements during production, service or decommissioning;
- Remote Data Acquisition strategy (Field Monitoring), including Over-The Air Software/Firmware Update;
- the CyberSafety-related special characteristics;
- the requirements that ensure proper identification of systems or element, including open source software libraries;
- the verification measures for production for software and hardware elements;
- the service requirements including diagnostic data and service note, including managing the field returns;
- measures for decommissioning, including erasure of sensitive data, lack of software update support.

Verification

The requirements of the CyberSafety Technical Concept, as with all other CyberSafety work products, must be validated in line with ISO standards to offer proof for its accuracy, completeness, and consistency with regard to the stated boundary conditions of the system. The System Architectural Design model, HIS specification, and the specifications for manufacturing, operation, maintenance, and decommissioning, as well as the CyberSafety Technical Concept, must be validated in line with ISO standards, providing proof that all objectives are met, i.e.:

- all requirements are appropriate and sufficient to meet the CyberSafety requirements;
- consistency between the System Architectural Design Model the CyberSafety Technical Concept is proven;
- prior development stages ensure the validity and conformity with the System Architectural Design Model.

3.1.5 Implementation Phase

The logical engineering work flow progresses from concept through implementation, when a tangible work output is produced. This phase includes not just software solutions, but also mechanical and electrical designs. With the Systems Architecture Model specified, these operations may be carried out separately and concurrently. Undoubtedly, there must be areas of contact between them. On a business level, this is controlled by the project manager. From the standpoint of CyberSafety, the critical responsibility is again allocated to the CyberSafety Manager to ensure that all associated competences take into consideration the CyberSafety criteria, as shown in Figure 3.23.

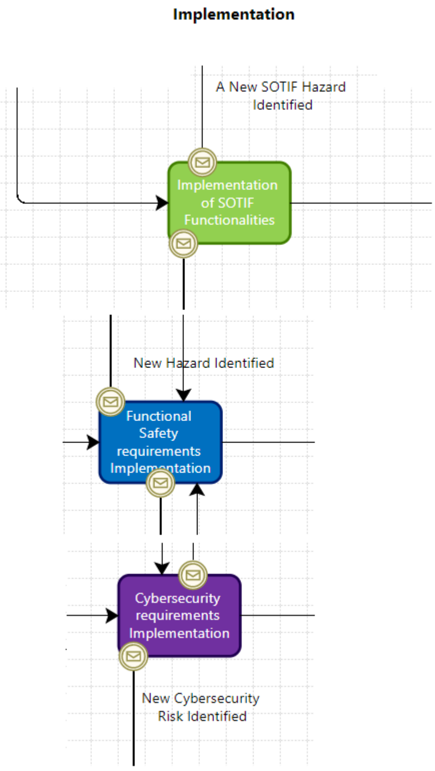

Implementation
A New SOTIF Hazard Identified
Implementation of SOTIF Functionalities
New Hazard Identified
Functional Safety requirements Implementation
Cybersecurity requirements Implementation
New Cybersecurity Risk Identified

Figure 3.23: CyberSafety Framework, Implementation Milestone. Color coding: Green - SOTIF, Blue - FuSa, Purple - CySe.

Since the major automotive paradigm is now connected to software capabilities and the so-called Software Defined Vehicle (SDV), this section provides a generic overview of software implementation technique to fulfill the CyberSafety requirements.

After the CyberSafety Technical Concept has been created, the responsibility of the Software Architect is to prepare a Software Architecture Solution that adheres to the CyberSafety objectives and employs the most recent and reliable CyberSafety design solutions. Further comprehensive software unit design and implementation may be controlled on the basis of this.

As a result, one of the primary goals of the software implementation phase is to create a software unit design that is in accordance with the software architecture solution, design criteria and assigned software requirements and that supports the implementation and verification of the software unit as specified.

The design and implementation of software units should be capable of meeting software requirements, in accordance with the architectural design of software and the Hardware-to-Software (HSI) specification. In order to reduce the introduction of faults and weaknesses, trusted design and implementation principles should be applied. In addition to that, generic notation, such as consistency, comprehensibility, maintainability, and verifiability, must be addressed. The software design itself must specify the functional behavior in sufficient detail for implementation. In order to achieve the standard properties of correct order of execution, consistency within software units, correctness of data flow within and between software units, simplicity, readability, and comprehensibility, robustness, suitability for software modification, and verifiability of the source code must also be followed.

As stated in the CyberSafety framework with the message event, if a hazard or threat is detected during implementation, it should be notified to the architects and CyberSafety analysis (including TARA, HARA, and HIRE) should be revisited and new requirements and concepts provided and evaluated. In order to coordinate CyberSafety operations, the CyberSafety Manager should be informed about the implementation plan.

CySe, FuSa, and SOTIF implementation may be handled by a single development team with shared responsibilities using agile approaches.

3.1.6 Verification Phase

Once a product of implementation has been created, the procedure moves on to the following step, which is to check the outcome. The V-model begins to migrate to the 'right-side' at this point, as visible in Figure 3.24.

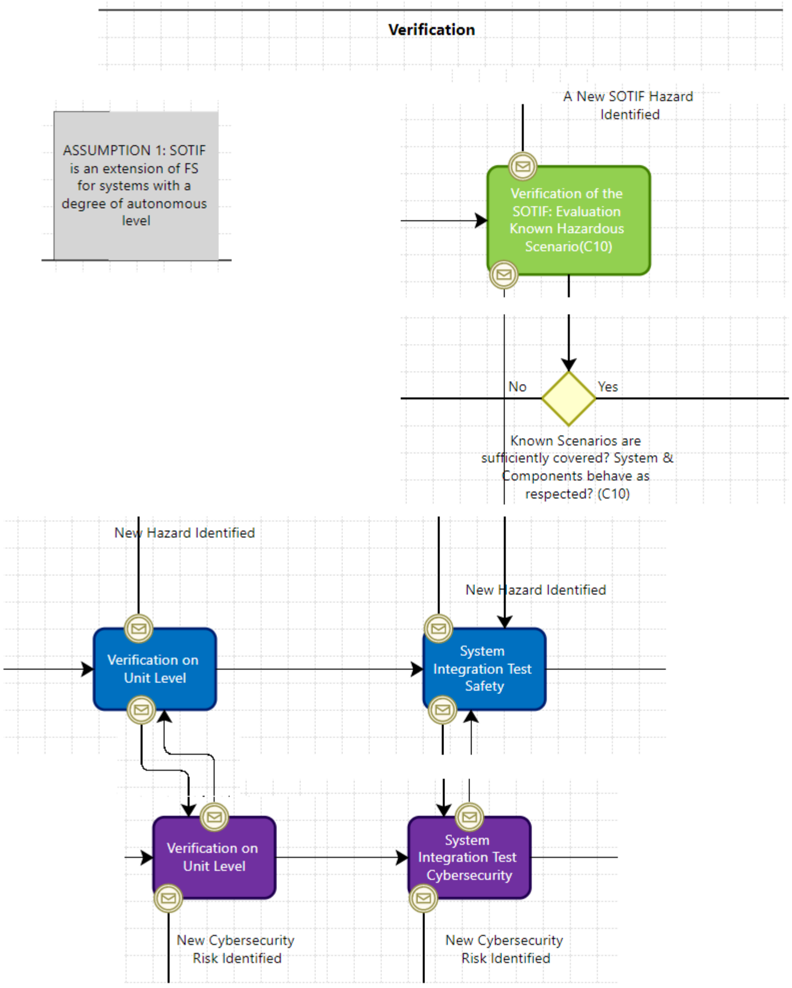

Verification
ASSUMPTION 1: SOTIF is an extension of FS for systems with a degree of autonomous level
A New SOTIF Hazard Identified
Verification of the SOTIF: Evaluation Known Hazardous Scenario(C10)
No
Yes
Known Scenarios are sufficiently covered? System & Components behave as respected? (C10)
New Hazard Identified
New Hazard Identified
Verification on Unit Level
System Integration Test Safety
Verification on Unit Level
System Integration Test Cybersecurity
New Cybersecurity Risk Identified
New Cybersecurity Risk Identified

Figure 3.24: CyberSafety Framework, Verification Milestone. Color coding: Green - SOTIF, Blue - FuSa, Purple - CySe.

The verification activity process is formed to assess whether a planned and developed item, such as a software component, hardware component, mechanical component, etc., is created in accordance with the given specifications. As a result, testing at the unit and system integration levels is performed throughout this activity. It is specified in the CyberSafety framework with two activity blocks for each line, namely "Verification on Unit Level" and "System Integration Test." As stated in the CyberSafety framework with the message event, if a hazard or threat is detected during verification, it should be notified to the architects and CyberSafety analysis (including TARA, HARA, and HIRE) should be revisited and new requirements and concepts provided and evaluated. In order to coordinate CyberSafety operations, the CyberSafety Manager should be informed about the verification plan.

The main objective of verification on the unit level is to provide evidence that a unit design satisfies the allocated requirements and is suitable for implementation. Furthermore, it must ensure that any CyberSafety measures emerging from the analysis are appropriately implemented. Following that, it should be obvious that there are no undesirable functions or qualities related to CyberSafety. Various testing methodologies, such as dynamic and static analysis, fuzzing, binary analysis, etc., might be explored for this purpose.

System integration tests are primarily used to validate the CyberSafety Technical Concept and HIS requirements. In the first place, the strategy for integrating the system parts, as well as clear testing goals, must be defined. The other target is to ensure that the CyberSafety measures, derived from the system architecture level CyberSafety analysis, are appropriately implemented. Furthermore, it provides proof that the integrated system parts meet their CyberSafety requirements as defined by the architectural design model of the system.

The evaluation should also focus on correct functional performance, accuracy, and timing of CyberSafety mechanisms for known hazardous scenarios and its triggering events. Further, on consistence and correct implementation of interfaces and robustness.

In order to establish complete verification scenarios and goals, information on verification strategy should be shared across CySe, FuSa, and SOTIF. This should result in improved test coverage, reduced redundancy, and increased test quality. In the CyberSafety framework, it is signaled via a messaging event between these actions. During this exercise, the CyberSafety Manager should maintain team synchronization.

3.1.7 Validation Phase

The next phase on the right side of the V-model is validation. It is the process of determining whether the final product satisfied the genuine needs and expectations of the stakeholders, as represented in Figure 3.25.

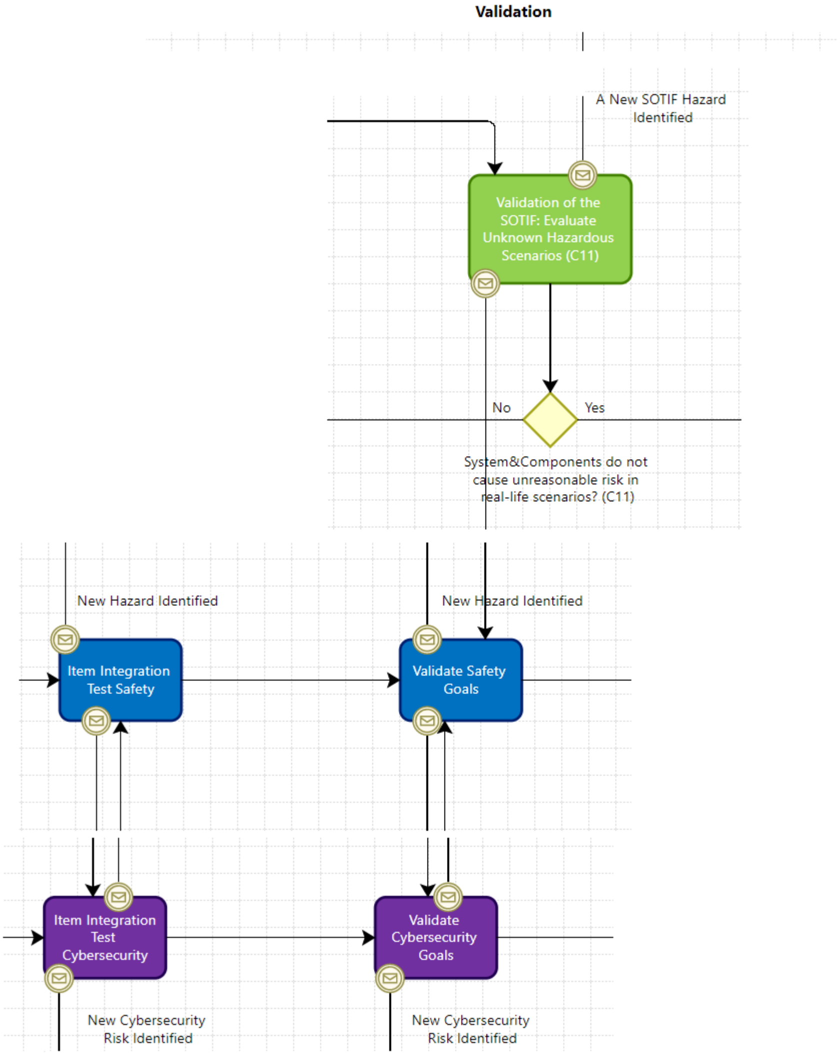

Validation
A New SOTIF Hazard Identified
Validation of the SOTIF: Evaluate Unknown Hazardous Scenarios (C11)
No
Yes
System&Components do not cause unreasonable risk in real-life scenarios? (C11)
New Hazard Identified
Item Integration Test Safety
New Hazard Identified
Validate Safety Goals
Item Integration Test Cybersecurity
Validate Cybersecurity Goals
New Cybersecurity Risk Identified
New Cybersecurity Risk Identified

Figure 3.25: CyberSafety framework, Validation Milestone. Color coding: Green - SOTIF, Blue - FuSa, Purple - CySe.

The validation of the CyberSafety concept criteria and CyberSafety goals is now being carried out using the CyberSafety process model. It is divided into two primary activities, the Item Integration Test and the Validate Goals for each line. As stated in the CyberSafety framework with the message event, if a hazard or threat is detected during validation, it should be notified to the architects and CyberSafety analysis (including TARA, HARA, and HIRE) should be revisited and new requirements and concepts provided and evaluated. In order to coordinate CyberSafety operations, the CyberSafety Manager should be informed about the validation plan.

The primary purpose of Item Integration is to offer proof that each system element interacts appropriately, meets CyberSafety Concept requirements, and provides an acceptable level of confidence that unintended or malicious activity that could violate the CyberSafety objectives is absent. To confirm the CyberSafety Goals, the Item should be incorporated into the vehicle, and a vehicle integration test should be performed. At this stage, the item's interface specification with the in-vehicle as well as the out-vehicle communication network and the in-vehicle power supply network must be verified.

Moving on to Goals Validation, it should provide proof that an Item, when incorporated into the vehicle, achieves the CyberSafety goals. This exercise also validates that the CyberSafety concept and the CyberSafety Technical Concept are acceptable to achieve CyberSafety for an item in this circumstance. Validation of CyberSafety objectives should take place in a representative context, i.e., on the vehicle level testing environment, taking into account vehicle types and variants. However, a definition of CyberSafety validation methods should be created first.

The attainment of CyberSafety for the item when incorporated into the vehicle must be validated in terms of controllability, performance of external measurements, and effectiveness of other technologies' parts. The following set of methods can be applied for validation of CyberSafety:

- Repeatable tests with specified test procedures, test cases, and pass/fail criteria;
- Analysis of architecture design;
- Long term tests;
- Stress tests;
- Operational use cases, under real-life conditions;
- Reviews;
- Vehicle fleet testing.

All validation results must be evaluated to provide evidence that the implemented CyberSafety goals for the item are met.

In order to establish complete validation scenarios and goals, information on validation strategy should be shared across CySe, FuSa, and SOTIF. This result is a greater test coverage, better test quality, and evaluation of real-world test situations. In the CyberSafety framework, it is signalled via a messaging event between these actions. During this evaluation, the CyberSafety Manager maintains team synchronization.

3.1.8 Release Phase

There is a Release milestone further inside the CyberSafety framework. It covers the general notion of releasing work items, such as software, hardware, and mechanical. This milestone can be broken down into substeps, such as developing a process conformance proof and performing a process assessment, what is shown in Figure 3.26.

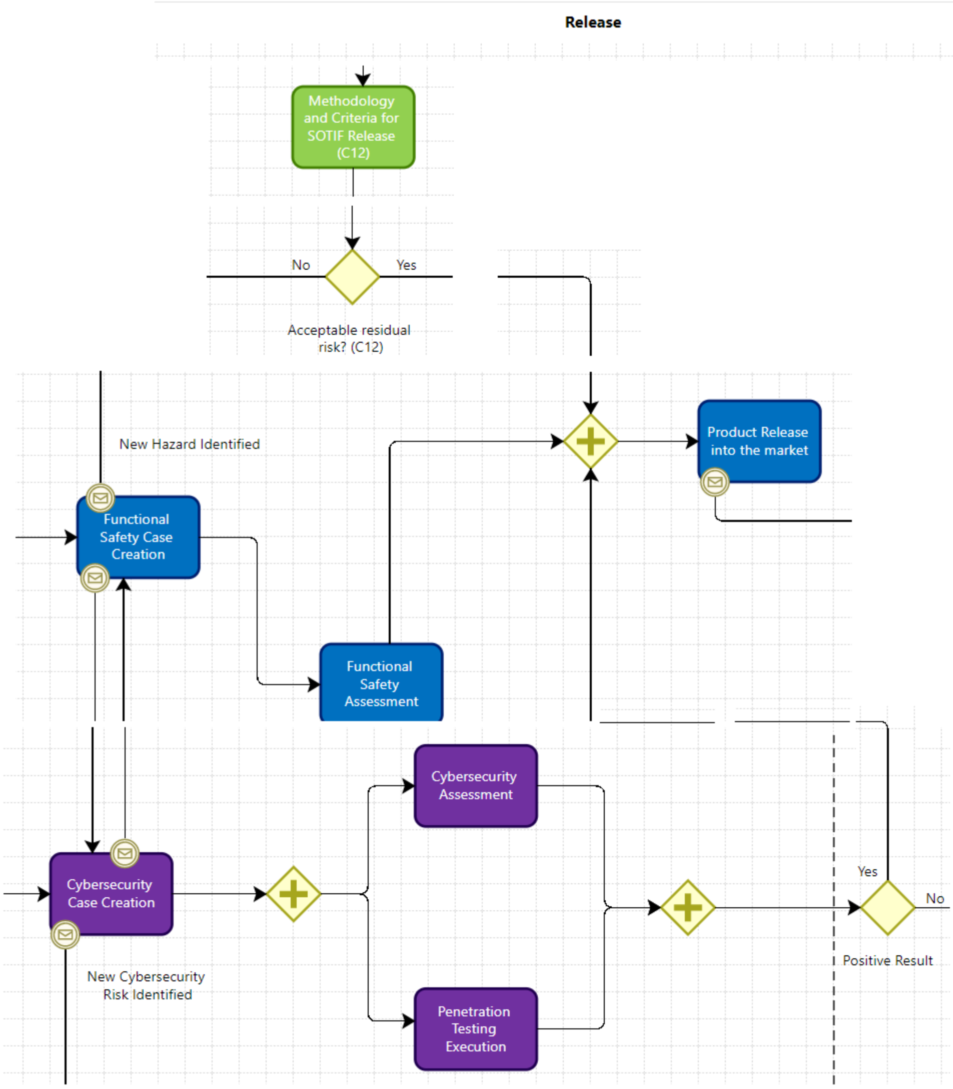

Release
Methodology and Criteria for SOTIF Release (C12)
No
Yes
Acceptable residual risk? (C12)
New Hazard Identified
Product Release into the market
Functional Safety Case Creation
Functional Safety Assessment
Cybersecurity Assessment
Cybersecurity Case Creation
Yes
No
Positive Result
New Cybersecurity Risk Identified
Penetration Testing Execution

Figure 3.26: CyberSafety framework, Release Milestone. Color coding: Green - SOTIF, Blue - FuSa, Purple - CySe.

The ISO standard word for proof of conformity is The Case. Depending on the scope, it can then be divided into two parts: safety and cybersecurity. CyberSafety Case must be produced for the CyberSafety framework, which combines the elements FuSa, SOTIF, and CySe. In addition, it has to be developed in accordance with the CyberSafety plan. The development of the CyberSafety Case can already be initiated at the beginning of development and finalized during the release phase. In the case of dispersed development, the item's CyberSafety Case might be a mix of the customer's and the suppliers' safety cases, which reference evidence from the work products provided by the respective parties. Further, it should also cover the requirements for post-development activities.

As proposed in the CyberSafety framework with the message event, if a hazard or threat is detected during the creation of the CyberSafety Case, it should be notified to the architects and the CyberSafety analysis (including TARA, HARA, and HIRE) should be revisited and new requirements and concepts should be provided and evaluated. In order to coordinate CyberSafety operations, the CyberSafety Manager should be informed about the CyberSafety plan creation.

Before the product is officially released on the market, it must be evaluated in accordance with ISO 26262:2018 and ISO 21434:2021. This action must demonstrate that all of the work items needed by the standards are available. Because the CyberSafety framework incorporates identified common features, once the procedure is completed, both assessments should be completed. Once the assessment is completed, the assessor should produce a report indicating the level of conformity and, if applicable, any deficiencies discovered. If there is a need for improvement, the development team is required to create a remediation plan, carry out it, and present the improvements to an assessor in an acceptable time frame.

Penetration tests must be performed concurrently with assessment operations from a cybersecurity point of view. It is a different method of addressing a system, network, or online application to identify cybersecurity vulnerabilities that an attacker may exploit. It can be carried out by an independent team or a third-party company. Depending on the policy, the findings of the Penetration tests may or may not be completely published.

3.1.9 Maintenance Phase

Post-Development Activities - Incident Management Process

By 2025, all new cars delivered will be linked, implying not just the ability to leverage the Internet or geolocation services, but also the adoption of the Vehicle-to-Everything (V2X) paradigm [60]. In order to achieve it, so called "software defined vehicle" concept is becoming widely spread throughout industry. The implementation of this idea is achievable primarily through the redefining of vehicle EE architecture, in which the Ethernet bus replaces the CAN bus as the backbone network, as well as the development of microprocessors with high virtualization and isolation capabilities [117, 118]. All of these factors, regrettably, do not reduce cybersecurity threats for connected vehicles, but rather the opposite [60, 91, 119]. The philosophy of security by design may not be adequate to avoid zero-day exploits throughout the vehicle's life cycle. As a result, to ensure the safety of the product, it should be monitored after it reaches the end user. CyberSafety can only be maintained by responding quickly to discovered flaws. For this, a comprehensive maintenance monitoring technique should be established, particularly for systems where driver assistance systems play a major role, and it should be present before autonomous or automated vehicles reach the L3, according to the SAE level of autonomy [70].

All of these difficulties are currently addressed by industry norms and standards. Furthermore, the requirement for cybersecurity incident management is included in UNECE R155 CSMS [66]. Furthermore, standards ISO21434 [13], SAE J3061 [67], and VDA [120] already give certain principles for the establishment and operation of the incident management process. They are all based on their predecessor, NIST.SP800-61r2 [121], where all basic components are defined, as shown in Figure 3.27.

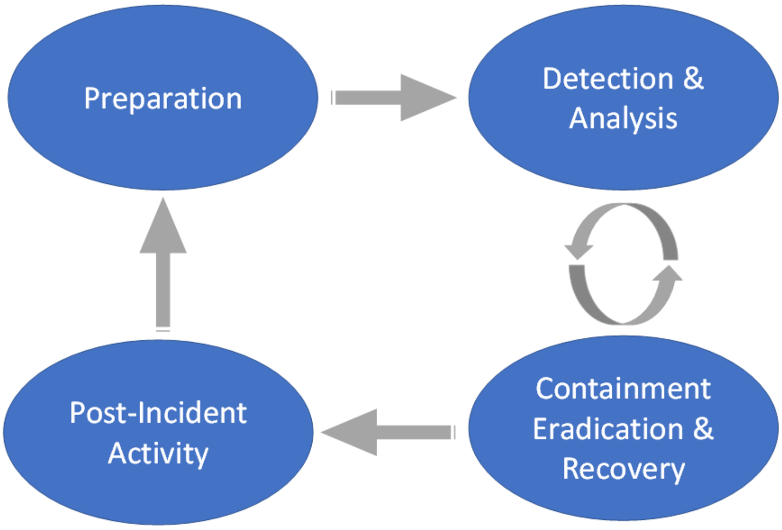


Figure 3.27: Incident Response Life Cycle [121].

The comparison of mentioned guidelines is summarised in Table 3.1. However, in order to complete this picture, cybersecurity threats are not the only ones to be concerned about. Since the vehicle's first concern is the safety of its passengers, it should also be closely monitored, with a significant emphasis on the SOTIF [6] and Functional Safety [5] systems, e.g. object detection systems [122]. Only then we would be able to maintain a vehicle's CyberSafety for a longer period of time, which is defined by UNECE regulation for minimum 10 years ofter end of production [65] .

Table 3.1: Comparison of Incident Monitoring Guidelines for the Automotive Industry.

Guideline Name	Main Scope
NIST SP 800-61 Rev2 Computer Security Incident Handling Guideline	• Incident response policy and plan creation. • Procedures for performing incident handling and reporting. • Guidelines for communication with third parties regarding incidents. • Team structure and staffing model. • Relationship and lines establishment between incident response team and other groups. • Incident Response Team Services definition. • Staffing and training.
SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems	• Covers all points mentioned by NIST for Incident Response. • Expands the recommendations for incident analysis with automotive specific use cases i.e., public safety concerns, financial loses (Vehicle theft, Warranty, Loss of sales etc.), loss of privacy, unauthorized vehicle tracking, loss of function or denial of service.
United Nations Regulation No 155	• Defines a Cybersecurity Management Systems (CSMS) requirements, which shall cover processes used to monitor, detect and respond to cyberattack. • The vehicle manufacturer is obliged to report at least once a year, or more frequently if relevant, to the Approval Authority or the Technical Service the outcome of their monitoring activities.
Quality Management in Automotive Cybersecurity Management System – VDA	• A quality guideline, which defines a list of check points, which has to be fulfilled to prove CSMS. • It defines a criterion for Incident Response process certification.

In addition to current standards and recommendations, the International Organization for Standardization is developing its own Guidelines for Auditing Cybersecurity Engineering, namely ISO/PAS 5112 [123], which will encompass Incident Monitoring operations. Furthermore, it is proposed to standardize areas of cross-process interaction (safety, cybersecurity). The Safety for Automated Driving Systems is in the early stages of development, and a Technical Specification ISO/AWI TS 5083 [124] is in the works.

The CyberSafety Incident Monitoring (CySaIM) process model displays all the tasks that must be completed in order to achieve cross-functional in-field monitoring. It may be scaled to fit a wide range of automotive goods. The high-level picture of the model is shown in Figure 3.28.

A single pool was created in the CyberSafety model to emphasize the close association between cybersecurity and safety. It was termed "Joint Incident Monitoring Activities ISO 21434/ISO21448."

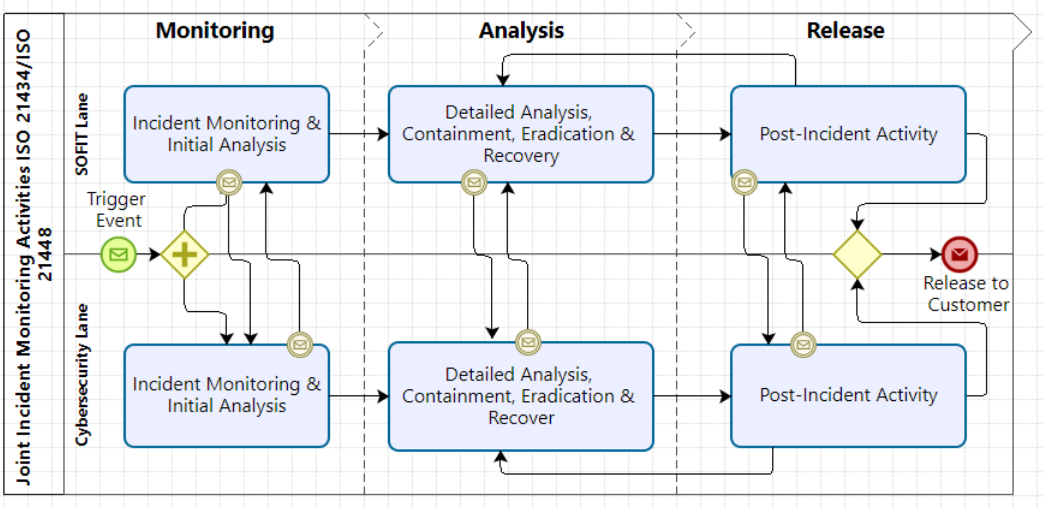
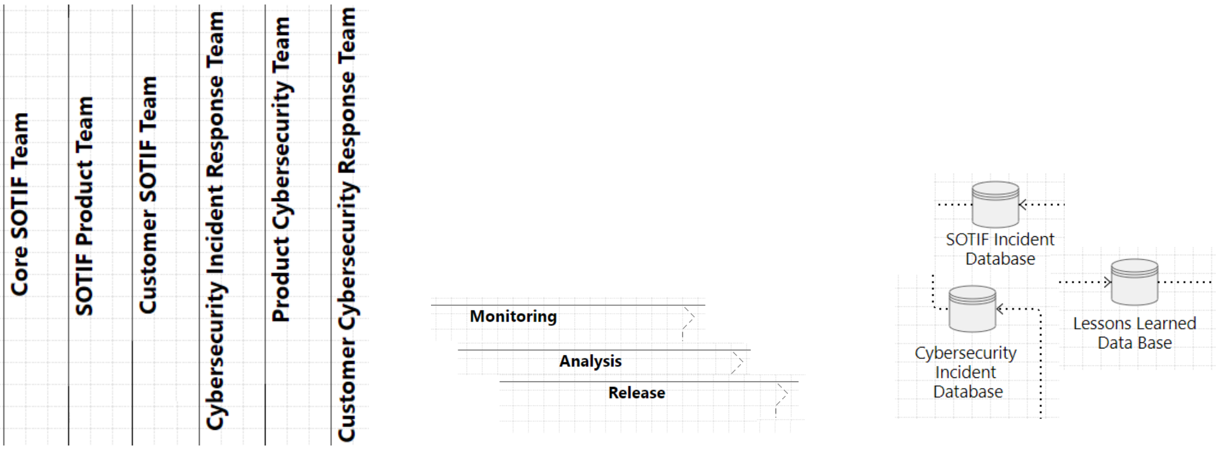

Joint Incident Monitoring Activities ISO 21434/ISO 21448
Monitoring
Analysis
Release
SOFIT Lane
Cybersecurity Lane
Incident Monitoring & Initial Analysis
Detailed Analysis, Containment, Eradication & Recovery
Post-Incident Activity
Trigger Event
Release to Customer
Incident Monitoring & Initial Analysis
Detailed Analysis, Containment, Eradication & Recover
Post-Incident Activity

Figure 3.28: Overview of the CySaIM Process Model.


Core SOTIF Team
SOTIF Product Team
Customer SOTIF Team
Cybersecurity Incident Response Team
Product Cybersecurity Team
Customer Cybersecurity Response Team
Monitoring
Analysis
Release
SOTIF Incident Database
Lessons Learned Data Base
Cybersecurity Incident Database

(a) Definition of CySaIM lanes in Bizagi Modeler.

(b) Definition of CySaIM milestones in Bizagi Modeler.

(c) Definition of CySaIM data stores in Bizagi Modeler.

Figure 3.29: Elements of CyberSafety Incident Monitoring Process Model Framework used in Bizagi Modeler.

BPMN introduces the Lane idea to describe and differentiate process aspects such as roles and departments. Six lanes were drawn in this model Figure 3.29a to represent the various entities involved in the process . The model includes the following teams: the Core SOTIF Team, the SOTIF Product Team, the Customer SOTIF Team, the Cybersecurity Incident Response Team, the Product Cybersecurity Team, and the Customer Cybersecurity Team. The elements of each lane are distinguished by various colors.

Furthermore, the Milestones are used by BPMN to subdivide the Process. In order to comply with all guidelines, three Milestones are specified in this model: Monitoring, Analysis, and Release. The Monitoring Milestone is followed by a Release Milestone phase, as summarized in Figure 3.29b and Figure 3.30.

The incidents that were recorded in this model, as well as the lessons learned, must be saved. The Data Store offers ways for activities to retrieve or change stored information, and it will survive beyond the scope

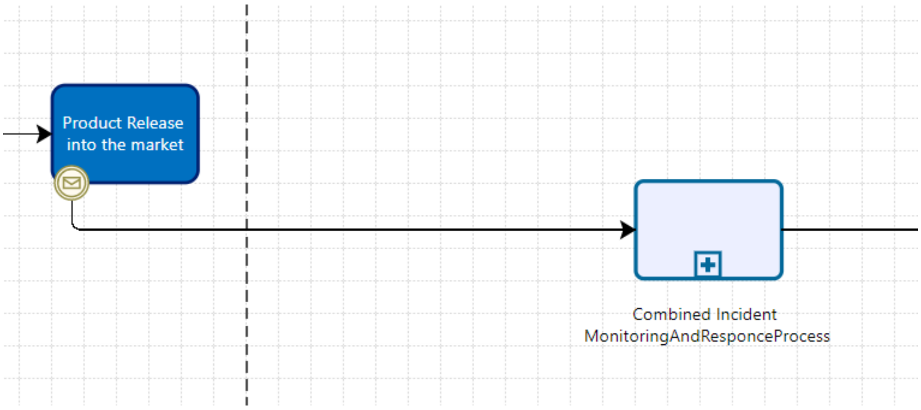

Product Release into the market
Combined Incident MonitoringAndResponceProcess

Figure 3.30: Snapshot of model's Release and Maintenance milestones. Color coding: Blue - FuSa.

of the Process. Three Databases are included in the CyberSafety model to store incidents found and lessons learned, as shown in Figure 3.29c.

A trigger event is required for each model. The major trigger event in this scenario is a notification from the Product Team regarding a product release. When the process starts, SOTIF and the Cybersecurity Incidents team begin monitoring activities. The incident notice might come from a variety of sources. The model distinguishes between internal and external sources. Internal events are initiated by the Monitoring Teams once they found an issue, whereas external events are initiated by third parties such as an independent market monitoring organization, market regulator, university, foundation, etc. Finally, the customer's team may be a notifier of issues. All of the triggering events are related in the Model, which implies that if any of them are available, both SOTIF and the Cybersecurity Incidents team begin Initial Assessment and Risk Evaluation operations, as shown in Figure 3.31.

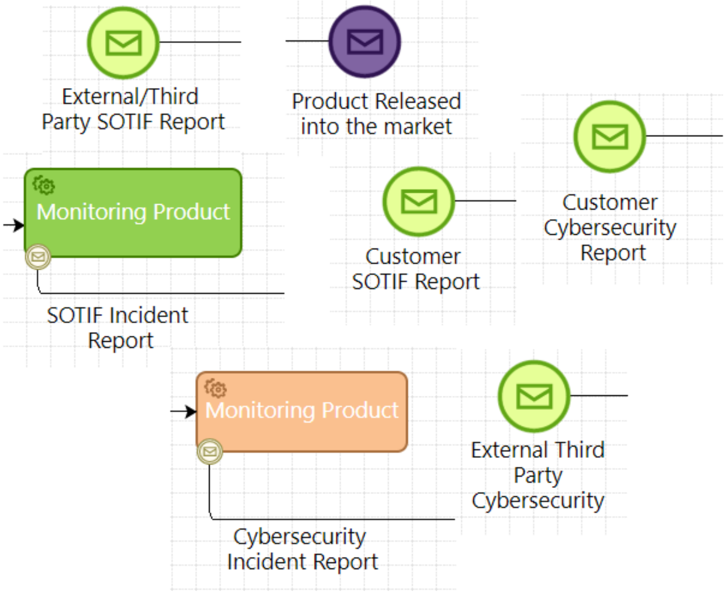
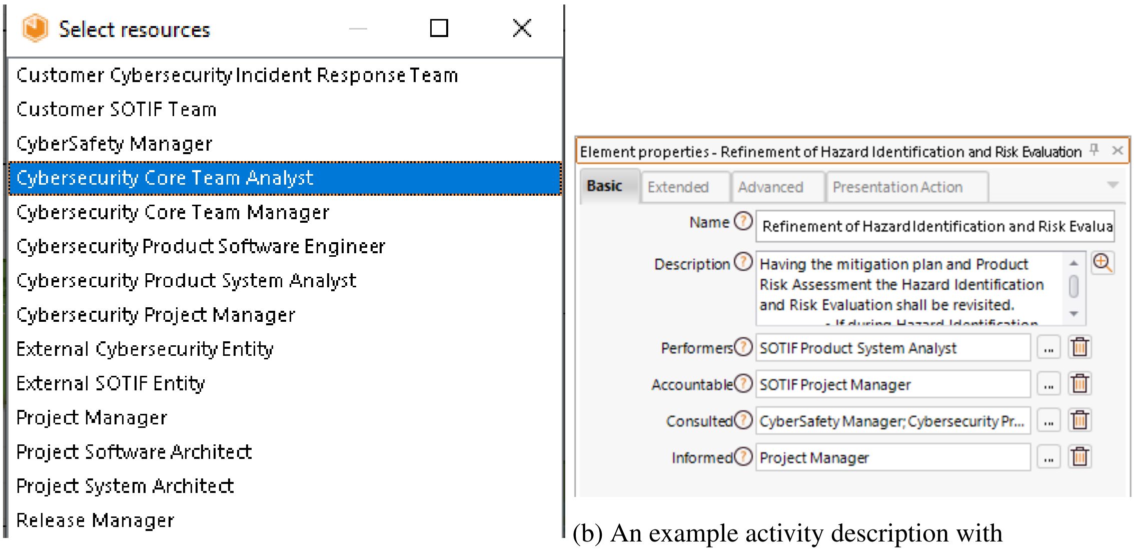

External/Third Party SOTIF Report
Product Released into the market
Customer Cybersecurity Report
Monitoring Product
Customer SOTIF Report
SOTIF Incident Report
Monitoring Product
External Third Party Cybersecurity
Cybersecurity Incident Report

Figure 3.31: Snapshot of model's trigger events. Color coding: Green - Core SOTIF Team, Purple - SOTIF Product Team, Orange - CySe Incident Response Team.



Select resources

Customer Cybersecurity Incident Response Team
Customer SOTIF Team
CyberSafety Manager
Cybersecurity Core Team Analyst
Cybersecurity Core Team Manager
Cybersecurity Product Software Engineer
Cybersecurity Product System Analyst
Cybersecurity Project Manager
External Cybersecurity Entity
External SOTIF Entity
Project Manager
Project Software Architect
Project System Architect
Release Manager

(a) Definition of model's resources.

Element properties - Refinement of Hazard Identification and Risk Evaluation

Name: Refinement of Hazard Identification and Risk Evalua

Description: Having the mitigation plan and Product Risk Assessment the Hazard Identification and Risk Evaluation shall be revisited.
- If during Hazard Identification

Performers: SOTIF Product System Analyst

Accountable: SOTIF Project Manager

Consulted: CyberSafety Manager; Cybersecurity Pr...

Informed: Project Manager

(b) An example activity description with a role assignment.

Figure 3.32: CyberSafety model resources and roles assignment.

BPMN notation requires a resource definition that will take part in activity actions. Internal and external resources described in the CyberSafety Model are depicted in Figure 3.32a. The process introduces the notion of a CyberSafety Manager, who is in charge of synchronizing cybersecurity and safety actions throughout the process lifecycle. Each action requires the designation of a role, as stated in Figure 3.32b. A specified resource may participate in an activity as a primary performer, responsible, consultant, or just receive information about the final results.

In addition to synchronizing the trigger events, the key challenge of the process was to capture activity link points between SOTIF and cybersecurity. The primary focus was on the Analysis milestone and activities that are shared by both regions, including Initial Assessment and Risk Evaluation, Root Cause Analysis and Recovery Scenarios. For the Core SOTIF Team Lane, a cybersecurity message can be triggered as an input for Cybersecurity Initial Assessment during analysis at each state.

Initial Assessment and Risk Assessment, a SOTIF Core Team Analyst may determine a SOTIF incident to be cybersecurity related and notify the Cybersecurity Incident Response Team, as presented in Figure 3.33. Furthermore, a Cybersecurity Vulnerability may be discovered during Root Cause Analysis and should be immediately disclosed to the cybersecurity team. Finally, during the Recovery Scenario Creation process, a requirement for a new cybersecurity control may be established. This should also send a notification to the cybersecurity team. All of these initiatives must be discussed with the CyberSafety Manager.

In addition, the Cybersecurity Incident Response Team may also generate an input for SOTIF analysis, as shown in Figure 3.34. Following the completion of an event's Initial Assessment and Risk Evaluation, the Cybersecurity Team may find safety-related implications, which should be immediately notified to the Core SOTIF Team. Later in the Root Cause Analysis process, the Cybersecurity Team may discover a vulnerability impacting SOTIF Safety Mechanisms, which should also be disclosed. If a new SOTIF Trigger is detected, the Recovery Scenario might be a source of an additional trigger for the SOTIF team. To avoid false positives, the connecting points must be reviewed with a CyberSafety Manager.

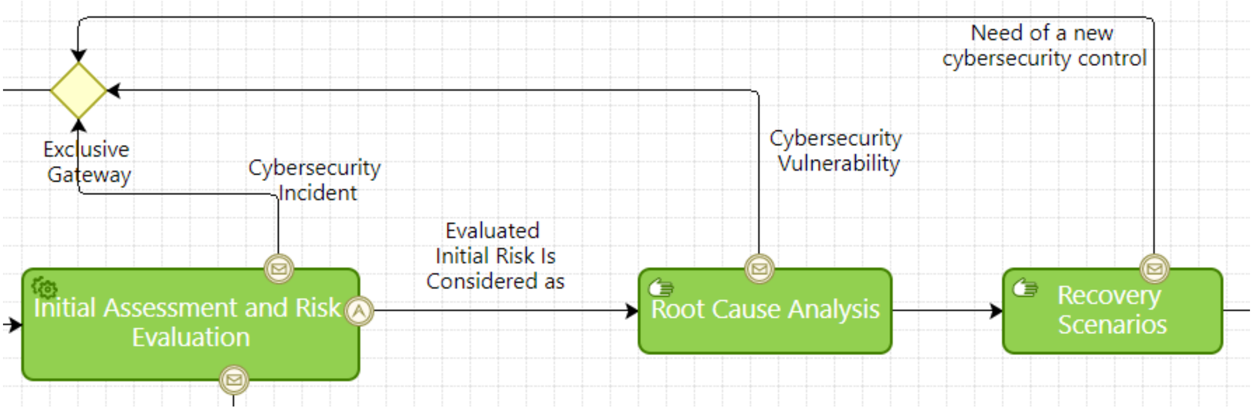

Need of a new cybersecurity control
Exclusive Gateway
Cybersecurity Incident
Cybersecurity Vulnerability
Evaluated Initial Risk Is Considered as
Initial Assessment and Risk Evaluation
Root Cause Analysis
Recovery Scenarios

Figure 3.33: Snapshot of the model's synchronization points between SOTIF and cybersecurity activities during the Analysis Milestone. Color coding: Green - Core SOTIF Team.

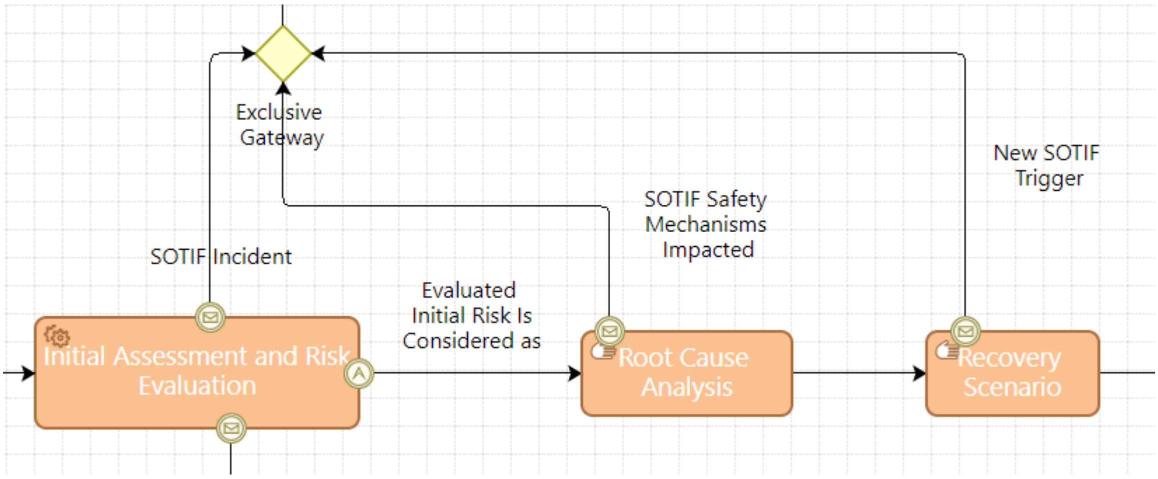

Exclusive Gateway
New SOTIF Trigger
SOTIF Safety Mechanisms Impacted
SOTIF Incident
Evaluated Initial Risk Is Considered as
Initial Assessment and Risk Evaluation
Root Cause Analysis
Recovery Scenario

Figure 3.34: Snapshot of the model's synchronization points between cybersecurity and SOTIF activities during Analysis Milestone. Color coding: Orange - CySe Incident Response Team.

The synchronization points go from the Analysis Lane to the Release Lane. The CyberSafety model defines the refinement actions after the mitigation (SOTIF), or remediation plan (cybersecurity) is developed. If a new SOTIF Trigger Event is discovered during the refinement of Hazard Identification and Risk Evaluation (HIRE), it should be treated as an extra Threat Scenario in TARA (Threat Analysis and Risk Assessment) analysis. Similarly, if a new SOTIF risk is discovered during TARA refining, it should be taken into account in Hazard Identification and Risk Evaluation, as presented in Figure 3.35. In this situation, a CyberSafety Manager must be familiar with both processes in order to adequately identify the dependencies. The process instance is terminated after the release operations are completed and a software upgrade is determined as necessary. Occurring events can be processed in parallel.

The Incident Monitoring is a continuous process and lasts for a particular product until the decommissioning period defined by a car producer. Table 3.2 verifies whether the proposed model follows the VDA CSMS guidelines. A process can only be approved if all questions receive a "Yes" answer. If any other responses are given, such as "No" or "Partially," the points must be revisited, and the evaluated part corrected to ensure full applicability.

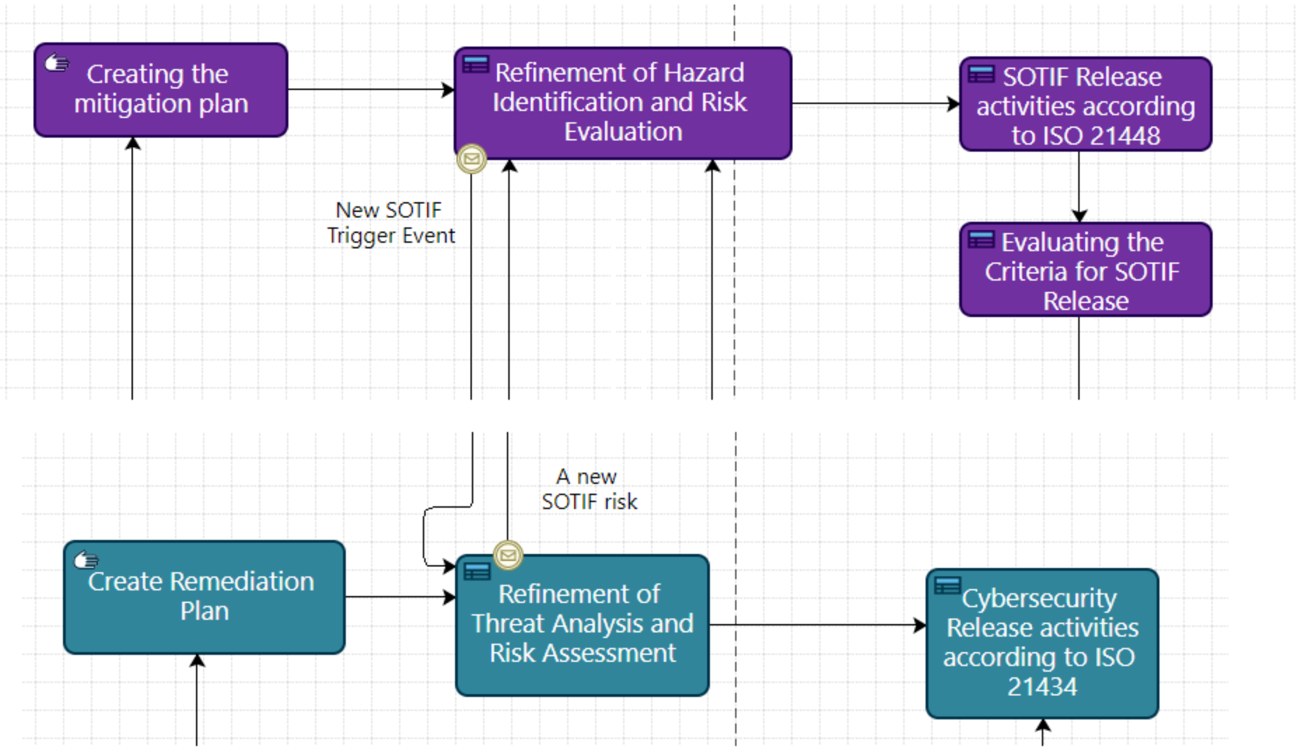

Creating the mitigation plan
Refinement of Hazard Identification and Risk Evaluation
SOTIF Release activities according to ISO 21448
Evaluating the Criteria for SOTIF Release
New SOTIF Trigger Event
A new SOTIF risk
Create Remediation Plan
Refinement of Threat Analysis and Risk Assessment
Cybersecurity Release activities according to ISO 21434

Figure 3.35: Snapshot of the model's synchronization points between HIRE and TARA during refinement activities. Color coding: Purple - SOTIF Product Team, Dark Green - Product CySe Team.

The amount of cybersecurity issues is increasing as Intelligent Cyber-connected Vehicles emerge. In the case of the automobile sector, it may have an influence not only on intellectual property and financial losses but also, and most importantly, on people's safety. Timing is critical; a zero-day exploit may result in a number of casualties before a mitigation strategy is devised and a remedy is released. An unanswered question is how to determine if the vehicle should continue to run when a high threat is recognized. Is it legal for the OEM to turn off the car for the sake of the user's safety? We may soon be forced to confront these uncomfortable issues. An indecent response procedure, by definition, reduces the likelihood of a vulnerability being exploited. The time element is considerably more crucial in a very formal automotive environment.

The suggested CyberSafety Incident Monitoring Process gives a response in a variety of domains, particularly in the collaboration of safety and cybersecurity teams, and outlines action and resources to carry out these actions. It also takes into account future industry regulations for automotive cybersecurity. Both cybersecurity and safety specialists are in great demand in the automotive business. However, these are not distinct things. Cybersecurity procedures must be in place to demonstrate safety. Other approaches, such as MBSE (Model Based System Engineering), can be investigated further to assist in the creation of a complex system design, which can save design time and boost system quality.

The proposed Incident Handling Process Model provides a ready solution for automotive entrepreneurs to meet the market criteria imposed by the new rules. It outlines roles, actions, and interactions to save time and effort during incident response monitoring, analysis, and release processes. The contact between cybersecurity and SOTIF safety specialists throughout the entire procedure is the crucial recognized point. As a connection between the cybersecurity and safety domains, the need for a CyberSafety Manager is

Table 3.2: VDA Cybersecurity CSMS Questionnaire for CyberSafety Incident Response Process.

Question	Minimum Requirements relevant for evaluation
Q7.1 Is a process established to search for cybersecurity information?	Yes. The process has been developed, and roles and duties have been specified. To obtain information, several parties monitor internal and external sources.
Q7.2 Is a process established to detect cybersecurity events?	Yes. There are defined events that will set off the subsequent actions.
Q7.3 Is a process established to assess cybersecurity events and analyze vulnerabilities?	Yes. Dedicated actions are established with analytical tasks such as Initial Assessment, Risk Evaluation, and Root Cause Analysis.
Q7.4 Is a process established to address the identified vulnerabilities?	Yes. On several levels, detected vulnerabilities are addressed based on analysis to the client. Mutual communication channels have been created.
Q7.5 Is a process established to respond to cybersecurity incidents?	Yes. Activities are described for a Root Cause Analysis, a Recovery Scenario, and the formulation of a Remediation/Mitigation strategy. The Core Team monitors progress. The time limits must be agreed upon with the customer.
Q7.6 Is a process established to validate the effectiveness and appropriateness of the response?	Yes. The CyberSafety Model has Core teams that are in charge of monitoring and tracking activities.
Q8.1 Is a process established to provide the relevant data for analysing attempted or successful cyberattacks?	Yes. Reports are made available for internal and external customer review by both the Core and Product teams.

established. The CySe Process Model was shown to be effective when tested against the VDA questionnaire questions for Incident Response Process. Finally, the Incident Handling Process for CyberSafety System Design should reduce the amount of time and effort necessary for process implementation while preventing the introduction of common or acknowledged flaws. Because collaboration zones are carefully specified, they should also improve overall quality.

3.1.10 Decommissioning Phase

Each market product has its own life cycle. The automotive industry is still in the process of implementing a decommissioning plan, particularly in terms of software and communication capabilities. Similarly to the IT sector, patches will not be provided and software will not be maintained after a certain period of time. As a result, using such a vehicle can be dangerous to the person and the environment. This raises a number of possible legal issues that are not addressed in this debate.

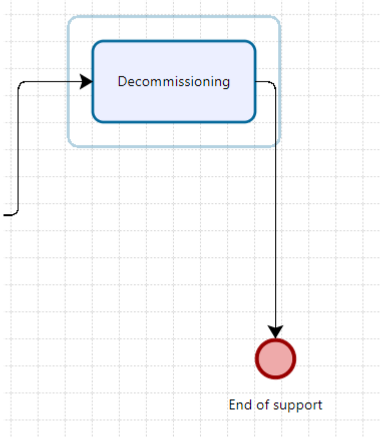


Figure 3.36: CyberSafety framework, decommissioning activity.

In the CyberSafety framework, decommissioning has its own milestone and activity, as presented in Figure 3.36. Its main purpose is to safely remove a product from the market and to identify the people responsible for achieving decommissioning. As a result, the organization should assign someone to be in charge of completing the decommissioning and providing the decommissioning proof in accordance with all applicable standards and requirements. It involves evaluating all data storage, intellectual property, and cybersecurity artifacts. Physical destruction is a popular method for erasing stored data. It is often regarded as the most secure and permanent method of data eradication. However, because even a small fragment of a disk might contain data, this must be done to a verifiable degree. Grinding, shredding, incineration, the use of corrosive chemicals, or the application of extremely high voltage are examples of common processes.

3.1.11 Summary

Thanks to the CyberSafety development framework developed, a wide range of common work products have been identified. These work products serve as invaluable repositories of summarized information for each phase of the project. In doing so, they provide a consolidated reference point for all stakeholders involved in the project. This holistic approach not only enhances efficiency and communication, but also ensures that essential insights are captured and retained throughout the development process. Tables 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9 provide an entire summary of common work-products per each project phase.

Table 3.3: Summary of Common Work Products for CyberSafety framework for **Concept Phase**.

ISO 21448:2019	**ISO 26262:2018**	**ISO 21434:2021**	**CyberSafety (CySa)**
Use Case Specification Operational Scenarios HIRE Report Safety Goals Assumptions and Limitations	Item Definition Concept of Operations HARA Safety Goals System Requirements System Architecture Hardware and Software Requirement Safety Requirements	Item Definition Use Case Specification TARA Security Goals Hazardous Events Security Requirements	CySa Item Definition CySa Concept of Operation CySa Use Case Specification CySa Risk Analysis CySa Risk Analysis Report CySa Assumptions and Limitation CySa Goals CySa System Architecture CySa Concept Requirement

Table 3.4: Summary of Common Work Products for CyberSafety framework for **Design Phase**.

ISO 21448:2019	ISO 26262:2018	ISO 21434:2021	CyberSafety (CySa)
Technical Safety Concept	Techical Safety Concept Hardware Architecture	Technical Security Concept	CySa Technical Concept
System Design Specification	Software Architecture	System Design Specification	System Design Specification
Hardware Design Specification	Communication Architecture	Hardware Design Specification	Hardware Design Specification
Software Design Specification	Hardware Safety Manual	Software Design Specification	Software Design Specification
Safety Requirements Verification Matrix	Software Safety Manual	Security Requirements Verification Matrix	CySa Requirements Verification Matrix
Safety Analysis Report	Safety Case Safety Analysis Report	Security Analysis Report	CySa Analysis Report

Table 3.5: Summary of Common Work Products for CyberSafety framework for **Implementation Phase**.

ISO 21448:2019	**ISO 26262:2018**	**ISO 21434:2021**	**CyberSafety (CySa)**
	Hardware Development Plan		CySa Product Development Plan
	Software Development Plan		CySa Hardware and Software Integration Plan
Product Development Plan	Hardware Verification Plan	Product Development Plan	CySa Hardware Verification Plan
Hardware and Software Integration Plan	Software Verification Plan	Hardware and Software Integration Plan	CySa Software Verification Plan
Hardware and Software Safety Integration Plan	Software Verification Plan	Hardware and Software Security Integration Plan	CySa Hardware Manual
Test Specification	Hardware Safety Manual	Test Specification	CySa Software Manual
Test Report	Software Safety Manual	Test Report	CySa Analysis Report
	Safety Analysis Report		CySa Test Specification
	Test Specification Test Report		CySa Test Report

Table 3.6: Summary of Common Work Products for CyberSafety framework for **Verification Phase**.

ISO 21448:2019	ISO 26262:2018	ISO 21434:2021	CyberSafety (CySa)
Safety Requirements Verification Report Hardware Verification Report Software Verification Report Traceability Report	Technical Safety Verification Report Hardware Integration Verification Report Software Integration Verification Report Safety Case Safety Analysis Report Traceability Report	Technical Security Verification Report Hardware Verification Report Software Verification Report Security Requirements Verification Report Traceability Report	CySa Techical Verification Report CySa Hardware and Software Integration Verification Plan CySa Requirements Verification Report CySa Traceability Report CySa Case CySa Analysis Report

Table 3.7: Summary of Common Work Products for CyberSafety framework for **Validation Phase**.

ISO 21448:2019	ISO 26262:2018	ISO 21434:2021	CyberSafety (CySa)
Safety Validation Plan Test Specification Test Report	System Integration Validation Plan Technical Safety Validation Plan Safety Validation Report	Technical Security Validation Plan Security Validation Plan Test Report Safety Validation Report	CySa System Validation Plan CySa Test Specification CySa Test Report CySa Validation Report

Table 3.8: Summary of Common Work Products for CyberSafety framework for **Production Phase**.

ISO 21448:2019	**ISO 26262:2018**	**ISO 21434:2021**	**CyberSafety (CySa)**
			Production Plan
Production Plan	Production and Operation Plan	Production Plan	Manufacturing Process Plan
Quality Management Plan	Quality Management Plan	Quality Management Plan	Quality Management Plan
Quality Assurance Plan	Quality Assurance Plan	Quality Assurance Plan	Quality Assurance Plan
Manufacturing Process Plan	Production Release Verification	Manufacturing Process Plan	Production Release Verification
	Production Release Approval		Production Release Approval

Table 3.9: Summary of Common Work Products for CyberSafety framework for **Operation Phase**.

ISO 21448:2019	**ISO 26262:2018**	**ISO 21434:2021**	**CyberSafety (CySa)**
Maintenance Plan	Service Life Plan	Maintenance Plan	CySa Incident Monitoring and Response Plan
Configuration Management Plan	Field Monitoring Plan	Configuration Management Plan	Maintenance Plan
Field Failure Analysis Report	Field Failure Analysis Report	Field Failure Analysis Report	Configuration Management Plan
Feedback of Experience Report	Feedback of Experience Report		

3.2 Implementation of the CyberSafety Process in Organizations

Introducing a new process into an organization is a multi-dimensional initiative that requires a thorough understanding of the organization itself, its external environment, and the potential impact of the forthcoming changes. The driving forces behind this initiative are varied and include the organization's need to adapt to a rapidly changing business landscape, improve internal operational efficiency, and support informed strategic decision making. However, the implementation of new processes and technologies often represents a significant change in the way an organization operates, raising concerns and uncertainties that can affect its workforce.

A key approach in this context is New Technology Implementation (NTI), a dynamic process that involves the application of knowledge, tools, materials, and techniques to develop innovative solutions to existing challenges [125]. The NTI framework is the subject of ongoing scrutiny and refinement by various scholars as they seek to develop a more comprehensive industry strategy for effective change management. In essence, the introduction of new processes follows a sequence of fundamental stages, beginning with the initial stage, progressing through the adoption phases, and culminating in full implementation. These phases involve activities at various levels of the organization and begin with the recognition of a need or opportunity for change. As organizations embark on the adoption of new technologies, they seek to transform, improve, or extend their existing workflows and operations.

The introduction of a new process or technology depends on various aspects. In addition to understanding and supporting top management, it depends on organizational culture. Furthermore, change management strategy should be introduced that addresses resistance to change and supports employees in the transition. It must also be evaluated to determine whether the new process will impact customers and whether it will meet their needs. The customer has to be well informed about the change and the impact on them. Undoubtedly, the new process should position the company in an advantage over competitors, which gives potential for a better review. However, it all depends on organization size, where a large organization works with certain inertia, and all new processes require lots of approval, trainings, adjusting to different cultures and market regulations. Definitely smaller players, can adopt changes faster. However, on the other hand, larger organizations may have more resources and are forced by the market regulators to adopt. The business environment and industry are also important. Certain industries are not so much driven by regulations, safety, and industry standards etc. so can adopt and change no so rapidly.

The successful implementation of a new process or technology depends on several critical factors [102]. Among the most influential is the unwavering support and understanding of top management. Organizational culture plays a key role in this process as it can facilitate or prevent the adoption of change. Developing an effective change management strategy is essential to address and overcome resistance to change and to support employees through the transition.

It is equally important to carefully assess the impact of the new process on customers. It is imperative that the new process aligns with the needs and expectations of the customer. Transparent and timely communication with customers is essential to ensure that they are well informed about the upcoming changes and their potential impact. In addition, the new process should enhance the organization's competitive advantage, ultimately leading to improved revenues. However, these aspects often depend on the size of the organization. Large organizations typically exhibit a certain degree of inertia in adopting new processes due to the need for extensive approvals, training, and adaptation to different internal cultures and external market regulations. Smaller players, on the other hand, tend to be more agile in adopting change. It is worth noting, however, that larger organizations often have greater resources and may be forced to adapt by stringent regulatory requirements.

The broader business environment and the dynamics of the industry are also key factors. Certain industries are highly regulated, with an emphasis on safety, security, and adherence to industry standards, which can sometimes slow the adoption of new processes. In contrast, industries that are less regulated may have greater flexibility to embrace change at a faster pace.

Introducing the CyberSafety framework into an automotive organization requires a systematic approach based on a number of key steps and considerations. The framework is ideally suited to organizations with well-established processes that provide a solid foundation for its implementation. A proposed summary of the steps for the introduction of the CySa process framework is illustrated in Figure 3.37.

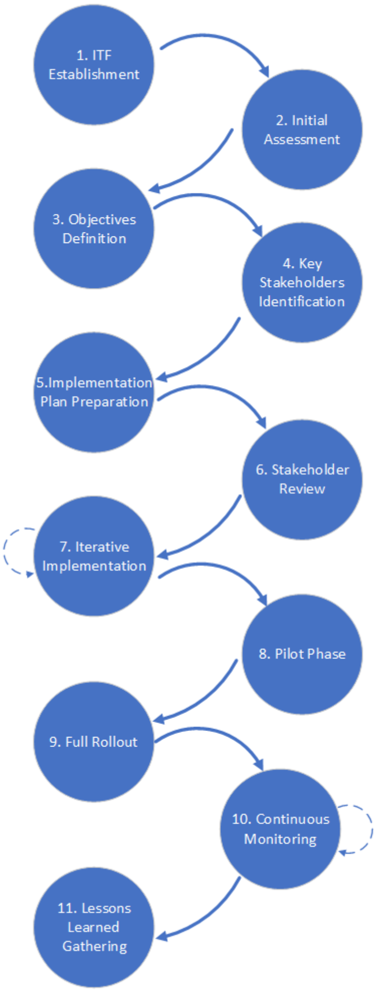

1. ITF Establishment
2. Initial Assessment
3. Objectives Definition
4. Key Stakeholders Identification
5.Implementation Plan Preparation
6. Stakeholder Review
7. Iterative Implementation
8. Pilot Phase
9. Full Rollout
10. Continuous Monitoring
11. Lessons Learned Gathering

Figure 3.37: CyberSafety framework, process introduction proposal.

To begin this path, the first step is to establish an Implementation Task Force (ITF) that is responsible for overseeing the implementation of the framework and regularly reporting progress to senior management. The ITF's first task is to conduct a thorough assessment of existing processes, workflows, roles, and interface structures. The results of this assessment must be carefully documented, with a strong focus on identifying areas for improvement and refinement.

This is followed by a critical phase to define the precise objectives of the new process. This involves explicitly stating the issues that the framework is intended to address and describing the desired outcomes.

A fundamental aspect of this implementation is the identification of key stakeholders - individuals and teams within the organization who will be directly affected by the framework. Each of these entities should nominate a representative responsible for providing valuable feedback and ensuring seamless transfer of information. With these basic elements in place, the ITF proceeds to develop a detailed implementation plan. This plan should include workflows, delineation of responsibilities, a well-defined timeline, allocation of necessary resources, an outline of training activities, and adaptation of the CySa framework to the organization's specific operational landscape. Once formulated, this comprehensive plan is presented to top management for approval.

Implementation is iterative, with the ITF continually adapting the CySa framework to the evolving needs of the organization and regularly reporting progress to top management. A critical element of this phase is to conduct stakeholder reviews and initiate a pilot phase in a controlled environment. This pilot phase is critical for gathering valuable feedback, addressing emerging issues, and making the necessary adjustments to optimize the effectiveness of the framework.

Following a successful pilot phase, the full rollout is initiated, affecting the entire organization. Throughout this expansive roll-out, constant monitoring of process performance, ongoing collection of feedback, and proactive resolution of emerging challenges are essential.

An integral part of this implementation is the establishment of mechanisms to collect ongoing feedback from employees and stakeholders. These mechanisms promote a culture of continuous improvement, allowing iterative enhancements and alignment with industry best practice and technological innovation.

It is also imperative to cultivate a culture of adaptability within the organization, preparing it for future challenges and updates. Accepting change as a constant within the organization is critical to long-term success.

Finally, at the end of the implementation and launch phase, a comprehensive lessons-learned session is convened to gain insights for future projects, ensuring that the wealth of experience gained is used for continuous improvement. Thorough documentation of the entire implementation process is essential to capture the journey in its entirety.

Chapter 4

Proposed Model for an Active Safety System Design Evaluation

4.1 Case Study on Advanced Driver Assistance System

Advanced Driver Assistance System (ADAS) are now an integral part of automotive systems in a constantly evolving market. These systems, which rely on data from various sensors such as radar, cameras, lidars, and GNSS, significantly enhance road safety and reduce the number of accidents. They achieve this by providing functionalities like lane keeping, adaptive cruise control, collision avoidance, highway pilot and automated parking.

However, as vehicles become more connected, they are increasingly exposed to potential cyber threats. Ensuring the cybersecurity resilience of these systems is crucial to protect them from external malicious adversaries. Traditional risk analysis for ADAS has primarily focused on safety concerns, neglecting the cybersecurity perspective. This oversight, lack of sufficient risk analysis and therefore pure design have led to severe hazard consequences, as evidenced by incidents such as the Jeep Cherokee hack [14], Tesla Model 3 collision (with the Autopilot function on) with a parked police car [126], and other documented vulnerabilities in automotive systems related to sensor limitations [127] or safety features deployment [128].

This research introduces a novel solution by integrating safety and cybersecurity processes during all product development phases, focusing on a unified risk analysis framework. By addressing all aspects of risk scenarios, this approach not only mitigates potential safety hazards, but also improves the overall resilience of the system against cyber attacks. The comprehensive integration of these two critical areas ensures that systems with a high degree of autonomy level i.e. ADAS can provide a higher quality and more secure service, ultimately leading to safer and more reliable automotive systems.

Moreover, the proposed solution advances CySe analysis into new territories, where it is no longer deeply intertwined with the EE vehicle architecture. Instead, it focuses on abstracted system functional architecture elements, their interactions, use case data flows, and communication. This abstraction allows for the identification of risks independently from the physical solutions, enabling early risk identification and mitigation before decisions regarding physical architecture and functional allocation are made.

The innovative combination of safety and cybersecurity considerations allows for a more thorough identification and reduction of risks, offering a significant improvement over traditional methods. This integrated approach is essential for the development of next-generation ADAS that are robust against accidental failures and intentional malicious threats.

In principal, model evaluation is an essential component of the process development cycle. It serves to verify that the proposed framework contributes to the enhancement of product design.

In this case study, several basic assumptions were made in order to provide a structured and realistic assessment of the implementation of the model within an organization. Firstly, we assume that the organization under consideration is medium to large in size. This size is important because it brings its own complexities and challenges in adapting to new processes and technologies.

Secondly, we assume that the organization has a comprehensive and stable development lifecycle that includes quality, safety, and security processes. This existing framework not only ensures that the organization operates efficiently, but also serves as a robust foundation for the incorporation of the CySa process framework.

In addition, a critical requirement is that there is unwavering support from top management. This support is crucial, as it paves the way for the successful implementation of new processes. It includes not only the approval of necessary changes but also the allocation of essential resources and tools.

It also requires that all necessary resources and tools are readily available. This includes human resources, budget allocations, and the necessary technology infrastructure. The availability of these resources is critical to the effective execution of the implementation plan.

Finally, for this particular case study, it is assumed that the initial system architecture is already in place. Having a foundational system architecture in place is a strategic advantage as it allows the CySa process framework to be seamlessly aligned with the existing infrastructure.

These assumptions provide a comprehensive background for evaluating the implementation of the CySa process framework within a medium to large organization. They create a scenario that is well prepared to efficiently integrate new processes and technologies, making the assessment more effective and relevant.

The CyberSafety process framework was assessed through validation of its effectiveness using the Highway Pilot (HP) function. HP is a level 3 vehicle automation function that operates in an integrated manner by controlling speed (including braking to a standstill and accelerating again) and steering when engaged. It is subject to specific operational parameters, such as motorway driving without intersections or opposing traffic and with guard rails to separate traffic, up to a maximum speed of 120 km/h. While the vehicle is in motion, the driver may engage in secondary tasks, but must be able to promptly regain control within several seconds when prompted by the system.

As HP significantly affects the driver and the surrounding environment, it is critical to consider cybersecurity along with the Safety of Intended Functionality (SOTIF) analysis given the increasing integration of vehicles with other systems and the Internet of Things (IoT).

Various technologies are available to facilitate the analysis of product safety and cybersecurity. The current trend towards more complex projects and increased regulatory demands has resulted in a growing need for automation and tool-based support for conducting such analyses.

To analyze the HP function, Ansys Medini tools was selected as proven analysis support in the automotive industry. Ansys Medini is a software tool used in the vehicle domain for complex systems safety analysis and risk assessment [41]. It helps engineers identify and analyze potential hazards and failures in the design of automotive components, such as Electronic Control Unit (ECU), sensors, and software systems. Ansys Medini provides a comprehensive set of safety analysis techniques, such as Failure Mode and Effect Analysis (FMEA), Fault Tree Analysis (FTA), and Event Tree Analysis (ETA), which allow engineers to identify potential risks and failure modes in the early stages of the design process.

Using Ansys Medini, automotive engineers can ensure that their designs meet the required safety standards and regulations, which is critical to ensuring the reliability and safety of automotive components and systems. In addition to furnishing a safety analysis framework, Medini offers a means of scrutinizing systems according to ISO 21434 standards. The tool is useful in identifying potential vulnerabilities and cybersecurity threats inherent in a vehicle's software systems, and boasts a broad array of cybersecurity analysis techniques such as Attack Path Analysis and Attack Tree Analysis. Employing Ansys Medini, automotive engineers are well equipped to tackle cybersecurity challenges mandated by ISO 21434, and to ensure that their designs conform to the standard while offering optimal security.

The safety and cybersecurity analysis approaches incorporated within the Medini tool are presently considered distinct endeavors with no shared activities or dependencies available. Nevertheless, by applying both methodologies within the same workspace during the analysis of, for example, the HP function, it becomes possible to visually represent how a CyberSafety joint analysis may be conducted, thereby demonstrating its effectiveness and comprehensiveness.

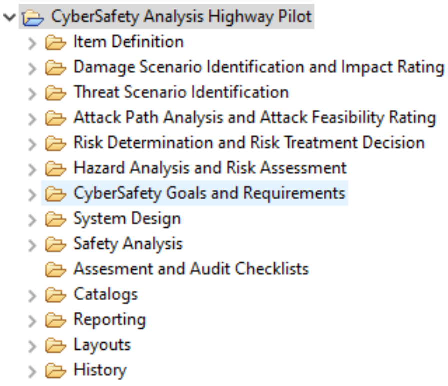
Ansys provides various template projects that give an overview of the tools' capabilities. It was decided to utilize the Highway Pilot Safety analysis and enrich it with the cybersecurity part. This can be a common approach for analysis systems with a high degree of automation.

The CyberSafety framework was evaluated using Ansys Mednini for the HP highway pilot function, focusing on the design phases of V-model with a closer look into the HARA and TARA dependencies, resulting in common CyberSafety Goals and requirements. Potential security measures can also be applied in a system design model.

The Asnsys Medini project "CyberSafety Analysis Highway Pilot.mprx' file, as well as data export, are available in Annex B of the dissertation.

With a combination of cybersecurity and functional safety process steps, a CyberSafety analysis model is proposed in Medini, as shown in Figure 4.1.

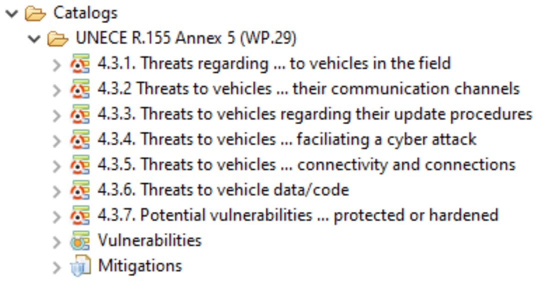
The analysis structure consists of a common Item definition on which CyberSafety analysis is conducted. Then there are packages that indicate the steps taken in the TARA and HARA analyses, that is, for TARA: Damage Scenario Identification and Impact Rating, Threat Scenario Identification, Attack Path Analysis and Attack Feasibility Rating, Risk Determination and Risk Treatment Decision and for HARA: Hazard Analysis and Risk Assessment. There is a separate package for CyberSafety Goals and Requirements. Although the majority of System Design and Safety Analysis's operations are related to safety, it is possible to identify linkages with cybersecurity. The ability to create custom packages and collections is important for adding, for example, UNR155 Annex5 Threats, Vulnerabilities, and Mitigations, as depicted in Figure 4.2.



CyberSafety Analysis Highway Pilot
- Item Definition
- Damage Scenario Identification and Impact Rating
- Threat Scenario Identification
- Attack Path Analysis and Attack Feasibility Rating
- Risk Determination and Risk Treatment Decision
- Hazard Analysis and Risk Assessment
- CyberSafety Goals and Requirements
- System Design
- Safety Analysis
- Assesment and Audit Checklists
- Catalogs
- Reporting
- Layouts
- History

Figure 4.1: Medini Analyze - CyberSafety Model Browser.

This provides the opportunity to establish a library of recognized threats, controls, and attacks that may be used in subsequent system analyzes.



Catalogs
- UNECE R.155 Annex 5 (WP.29)
  - 4.3.1. Threats regarding ... to vehicles in the field
  - 4.3.2 Threats to vehicles ... their communication channels
  - 4.3.3. Threats to vehicles regarding their update procedures
  - 4.3.4. Threats to vehicles ... faciliating a cyber attack
  - 4.3.5. Threats to vehicles ... connectivity and connections
  - 4.3.6. Threats to vehicle data/code
  - 4.3.7. Potential vulnerabilities ... protected or hardened
  - Vulnerabilities
  - Mitigations

Figure 4.2: Medini Analyze - UNR155 Catalog.

For the HP Cyber Safety analysis, a common Item definition is considered. Medini gives the possibility of following a model-based approach for system definition. Therefore, as a base for analysis, Item Architecture and Item Functions diagrams are provided. The item architecture consists of the Highway Pilot Core Function, which collects inputs from sensors such as Perception Subsystem, Ego Motion Sensing, HD Roadmap and Self Localization and Human-Machine Interface (HMI) elements (Steering Wheel, Pedal, Selectors). It gives an output to PowerTrain Control, Brake Control, Steering Control, Outside Signaling and HMI Elements, i.e., Indicators, Warning, as illustrated in Figure 4.3.

Item Function Diagram provides a picture of how the HP system operates at the Vehicle level and its dependencies, whereas Item Architecture concentrates on system components and their dependencies. For the clarity purposes, e.g. cybersecurity related functions can be marked in a different color, as shown in Figure 4.4.

The common view of Item definition gives a possibility of defining Cybersecurity Assets and their losses. This is achieved by checking the "Asset" option. Once selected on a certain diagram element (it can be a function, port, activity, connection type, etc.), a decision is made as to what cybersecurity property should be considered. As an example, the HP object list from the Perception System was marked as an asset with the protection of the following cybersecurity properties:

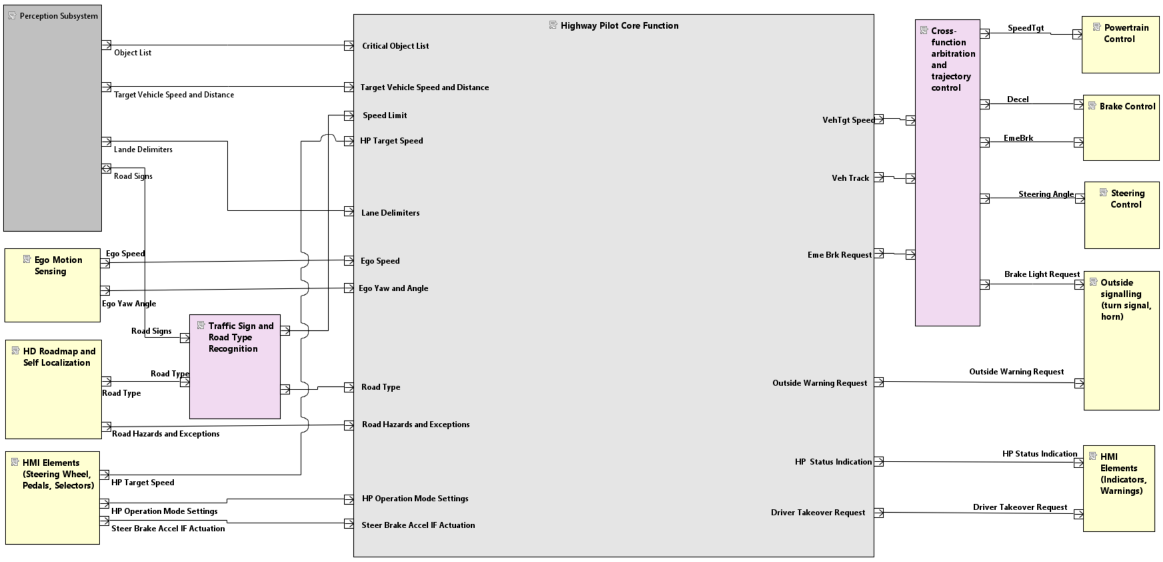


Figure 4.3: CyberSafety Analysis HP - Item Architecture.

- Integrity;
- Availability;
- Authenticity;
- Confidentiality;
- Authorization;
- Non-Repudiation.

Based on this assignment, the tool creates an appropriate cybersecurity losses, which can be visible in the Model Browser for further evaluation, what can be observed in Figure 4.5.

Damage Scenario Definition (for CySe) and Hazards Definition for FuSa, as depiceted in Figure 4.6, are the following shared activities and potential intersections that can be evaluated together. With the help of the tool, it is possible to visually display the relationships between defined Damage Scenarios and Hazards Scenarios. A list of hazards has been produced with an appropriate description for the HP function.

Damage Scenarios, as visible in Figure 4.7, may also be established, linked to cybersecurity property losses, and assessed for their impact on safety, finances, operations, and privacy. For an HP function evaluation, similar collection of Damage Scenarios was prepared with a correlation to Hazards.

The Damage Scenarios were derived from Hazards, giving an indication that intended manipulation of certain signals may lead to a hazard, as well as by analyzing purely the loss of certain cybersecurity property loss on a HP function behavior. In this case, a naming convention linkage has been created, what is summaried in Table 4.1.

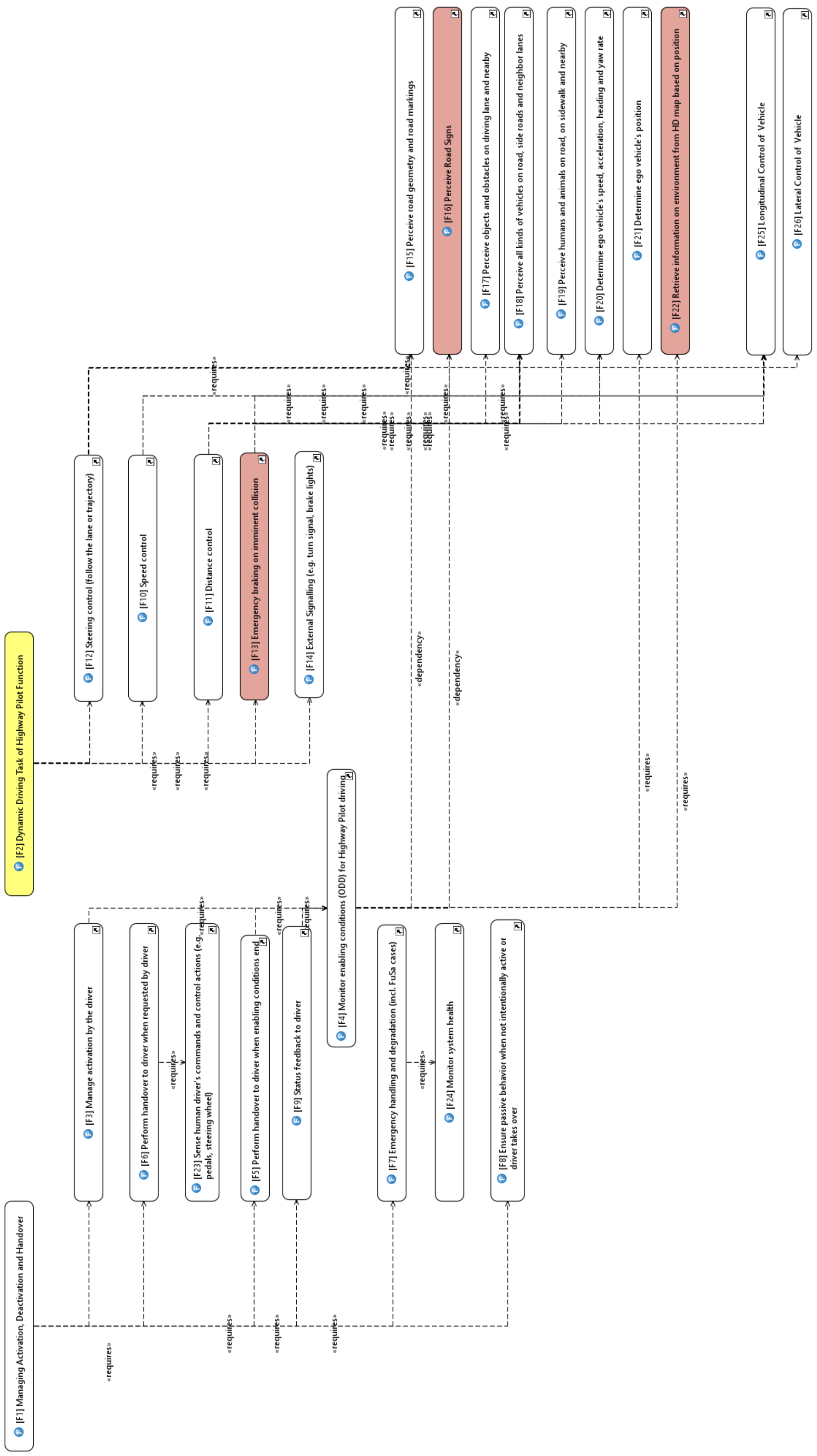
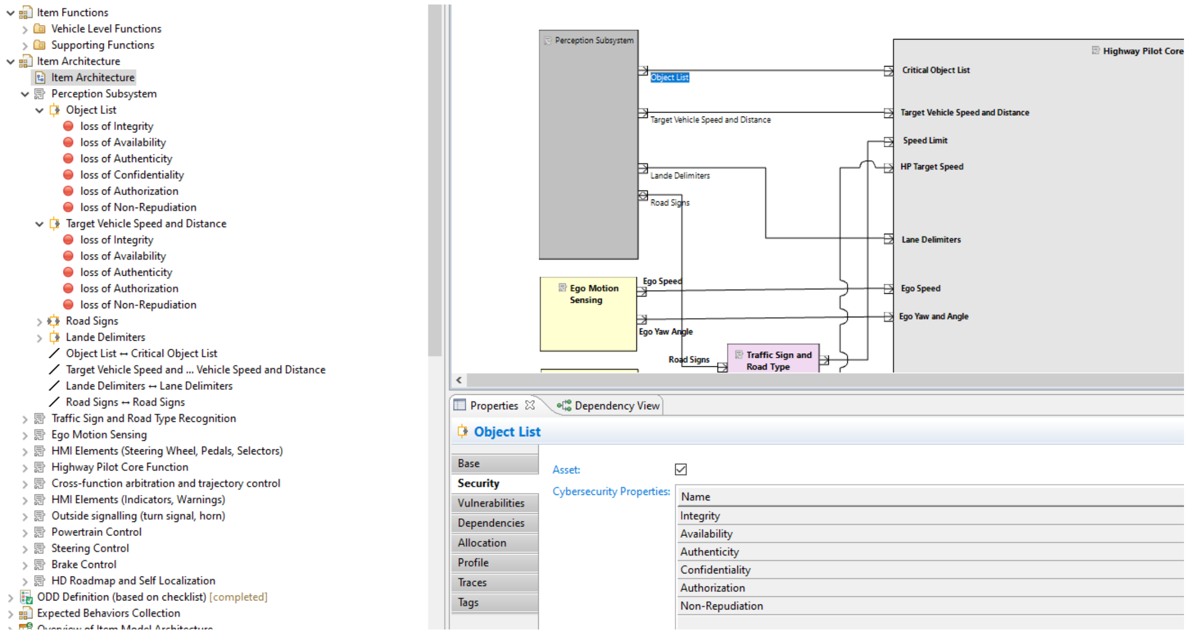

[F1] Managing Activation, Deactivation and Handover
[F2] Dynamic Driving Task of Highway Pilot Function
[F3] Manage activation by the driver
[F6] Perform handover to driver when requested by driver
[F23] Sense human driver's commands and control actions (e.g. pedals, steering wheel)
[F5] Perform handover to driver when enabling conditions end
[F9] Status feedback to driver
[F4] Monitor enabling conditions (ODD) for Highway Pilot driving
[F7] Emergency handling and degradation (incl. FuSa cases)
[F24] Monitor system health
[F8] Ensure passive behavior when not intentionally active or driver takes over
[F12] Steering control (follow the lane or trajectory)
[F10] Speed control
[F11] Distance control
[F13] Emergency braking on imminent collision
[F14] External Signalling (e.g. turn signal, brake lights)
[F15] Perceive road geometry and road markings
[F16] Perceive Road Signs
[F17] Perceive objects and obstacles on driving lane and nearby
[F18] Perceive all kinds of vehicles on road, side roads and neighbor lanes
[F19] Perceive humans and animals on road, on sidewalk and nearby
[F20] Determine ego vehicle's speed, acceleration, heading and yaw rate
[F21] Determine ego vehicle's position
[F22] Retrieve information on environment from HD map based on position
[F25] Longitudinal Control of Vehicle
[F26] Lateral Control of Vehicle
«requires»
«dependency»

Figure 4.4: CyberSafety Analysis HP - Item Functions. Cybersecurity Relevant functions marked in red.



- Item Functions
  - Vehicle Level Functions
  - Supporting Functions
- Item Architecture
  - Item Architecture
  - Perception Subsystem
    - Object List
      - loss of Integrity
      - loss of Availability
      - loss of Authenticity
      - loss of Confidentiality
      - loss of Authorization
      - loss of Non-Repudiation
    - Target Vehicle Speed and Distance
      - loss of Integrity
      - loss of Availability
      - loss of Authenticity
      - loss of Authorization
      - loss of Non-Repudiation
    - Road Signs
    - Lande Delimiters
    - Object List ↔ Critical Object List
    - Target Vehicle Speed and ... Vehicle Speed and Distance
    - Lande Delimiters ↔ Lane Delimiters
    - Road Signs ↔ Road Signs
  - Traffic Sign and Road Type Recognition
  - Ego Motion Sensing
  - HMI Elements (Steering Wheel, Pedals, Selectors)
  - Highway Pilot Core Function
  - Cross-function arbitration and trajectory control
  - HMI Elements (Indicators, Warnings)
  - Outside signalling (turn signal, horn)
  - Powertrain Control
  - Steering Control
  - Brake Control
  - HD Roadmap and Self Localization
- ODD Definition (based on checklist) [completed]
- Expected Behaviors Collection

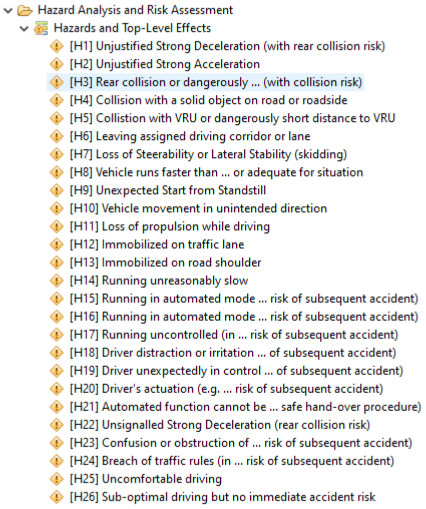
Object List

Asset: ☑

Cybersecurity Properties:

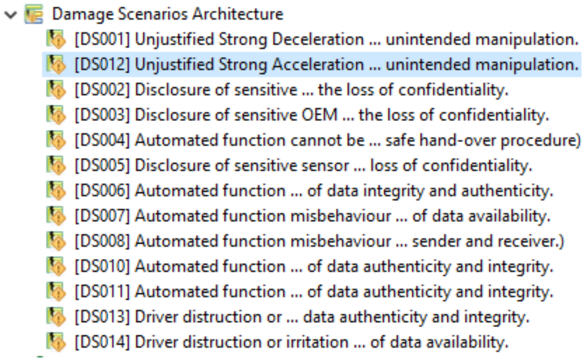
Name
Integrity
Availability
Authenticity
Confidentiality
Authorization
Non-Repudiation

Figure 4.5: CyberSafety Analysis HP - CySe assets and losses assignment.



- Hazard Analysis and Risk Assessment
  - Hazards and Top-Level Effects
    - [H1] Unjustified Strong Deceleration (with rear collision risk)
    - [H2] Unjustified Strong Acceleration
    - [H3] Rear collision or dangerously ... (with collision risk)
    - [H4] Collision with a solid object on road or roadside
    - [H5] Collision with VRU or dangerously short distance to VRU
    - [H6] Leaving assigned driving corridor or lane
    - [H7] Loss of Steerability or Lateral Stability (skidding)
    - [H8] Vehicle runs faster than ... or adequate for situation
    - [H9] Unexpected Start from Standstill
    - [H10] Vehicle movement in unintended direction
    - [H11] Loss of propulsion while driving
    - [H12] Immobilized on traffic lane
    - [H13] Immobilized on road shoulder
    - [H14] Running unreasonably slow
    - [H15] Running in automated mode ... risk of subsequent accident)
    - [H16] Running in automated mode ... risk of subsequent accident)
    - [H17] Running uncontrolled (in ... risk of subsequent accident)
    - [H18] Driver distraction or irritation ... of subsequent accident)
    - [H19] Driver unexpectedly in control ... of subsequent accident)
    - [H20] Driver's actuation (e.g. ... risk of subsequent accident)
    - [H21] Automated function cannot be ... safe hand-over procedure)
    - [H22] Unsignalled Strong Deceleration (rear collision risk)
    - [H23] Confusion or obstruction of ... risk of subsequent accident)
    - [H24] Breach of traffic rules (in ... risk of subsequent accident)
    - [H25] Uncomfortable driving
    - [H26] Sub-optimal driving but no immediate accident risk

Figure 4.6: CyberSafety Analysis HP - Hazard Collection.



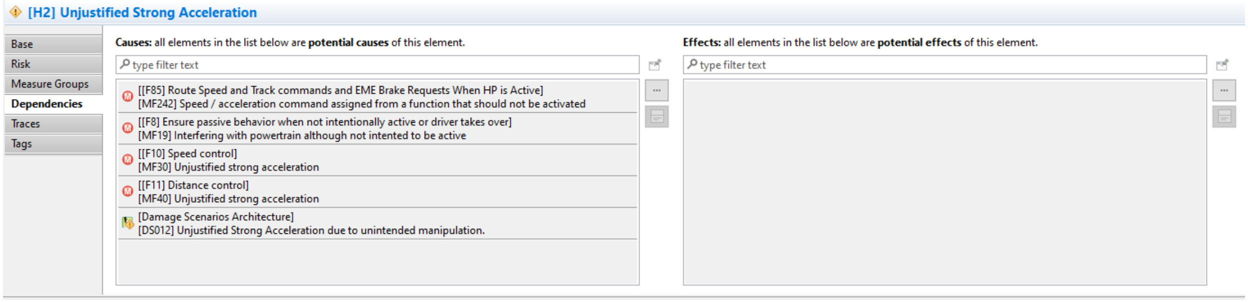
- Damage Scenarios Architecture
  - [DS001] Unjustified Strong Deceleration ... unintended manipulation.
  - [DS012] Unjustified Strong Acceleration ... unintended manipulation.
  - [DS002] Disclosure of sensitive ... the loss of confidentiality.
  - [DS003] Disclosure of sensitive OEM ... the loss of confidentiality.
  - [DS004] Automated function cannot be ... safe hand-over procedure)
  - [DS005] Disclosure of sensitive sensor ... loss of confidentiality.
  - [DS006] Automated function ... of data integrity and authenticity.
  - [DS007] Automated function misbehaviour ... of data availability.
  - [DS008] Automated function misbehaviour ... sender and receiver.)
  - [DS010] Automated function ... of data authenticity and integrity.
  - [DS011] Automated function ... of data authenticity and integrity.
  - [DS013] Driver distruction or ... data authenticity and integrity.
  - [DS014] Driver distruction or irritation ... of data availability.

Figure 4.7: CyberSafety Analysis HP - Damage collection.

Table 4.1: HP CyberSafety Analysis - Hazard vs Damage Scenario.

Hazard Scenario	Damage Scenario
Unjustified Strong Deceleration (With rear collision))	Unjustified Strong Deceleration due to data unintended manipulation.
Unjustified Strong Acceleration	Unjustified Strong Acceleration due to unintended manipulation.
Driver distraction or irritation (in worst case risk of subsequent accident)	Driver distraction or irritation due to malicious activity resulting from the loss of data authenticity and integrity. Driver distraction or irritation due to malicious activity resulting from the loss of data availability.

At the same time, by using the drag-and-drop option and "Show Cause/Effect Net" view, the Hazard/-Damage Scenario correlation can be shown in a "Cause/Effect" convention. In the considered example, Damage Scenario "Unjustified Strong Deceleration due to data unintended manipulation" has an impact on (Causes) Hazard "Unjustified Strong Deceleration (with rear collision)", as visible in Figure 4.8.



Causes: all elements in the list below are **potential causes** of this element.

[[F85] Route Speed and Track commands and EME Brake Requests When HP is Active]
[MF242] Speed / acceleration command assigned from a function that should not be activated

[[F8] Ensure passive behavior when not intentionally active or driver takes over]
[MF19] Interfering with powertrain although not intented to be active

[[F10] Speed control]
[MF30] Unjustified strong acceleration

[[F11] Distance control]
[MF40] Unjustified strong acceleration

[Damage Scenarios Architecture]
[DS012] Unjustified Strong Acceleration due to unintended manipulation.

Effects: all elements in the list below are **potential effects** of this element.

Figure 4.8: CyberSafety Analysis HP - Hazard-Damage scenario relation.

By defining the Cybersecurity Losses, tool automatically derives Threat Scenarios based on the STRIDE threat model. The full extract of defined cybersecurity losses can be seen in Annex B - Threat_Scenarios.xlsx file. This is also visible in the "Show Cause/Effect Net" option. With this overview available early in the development cycle, analysts can identify and mitigate risks early in the development process. This can lead to more reliable and safer products. For example, if a hazard is identified in a particular scenario, the designer can implement safety measures or design changes to prevent the hazard from occurring or mitigate its effects, what can be seen in Figure 4.9.

Each damage scenario that has been described within a collection is evaluated in light of the effects it will have on the system under analysis in terms of safety, finances, operations, and privacy. This is another point where CySe and FuSa connect. The Safety Impact can be linked and used to determine the ASIL level. Various discussions are taking place in the industry about how to determine the ASIL level based on the ISO 21434 Safety Impact Rating. The complete list of defined threats scenarios for HP is available in Annex B - Threat_Scenarios.xlsx.

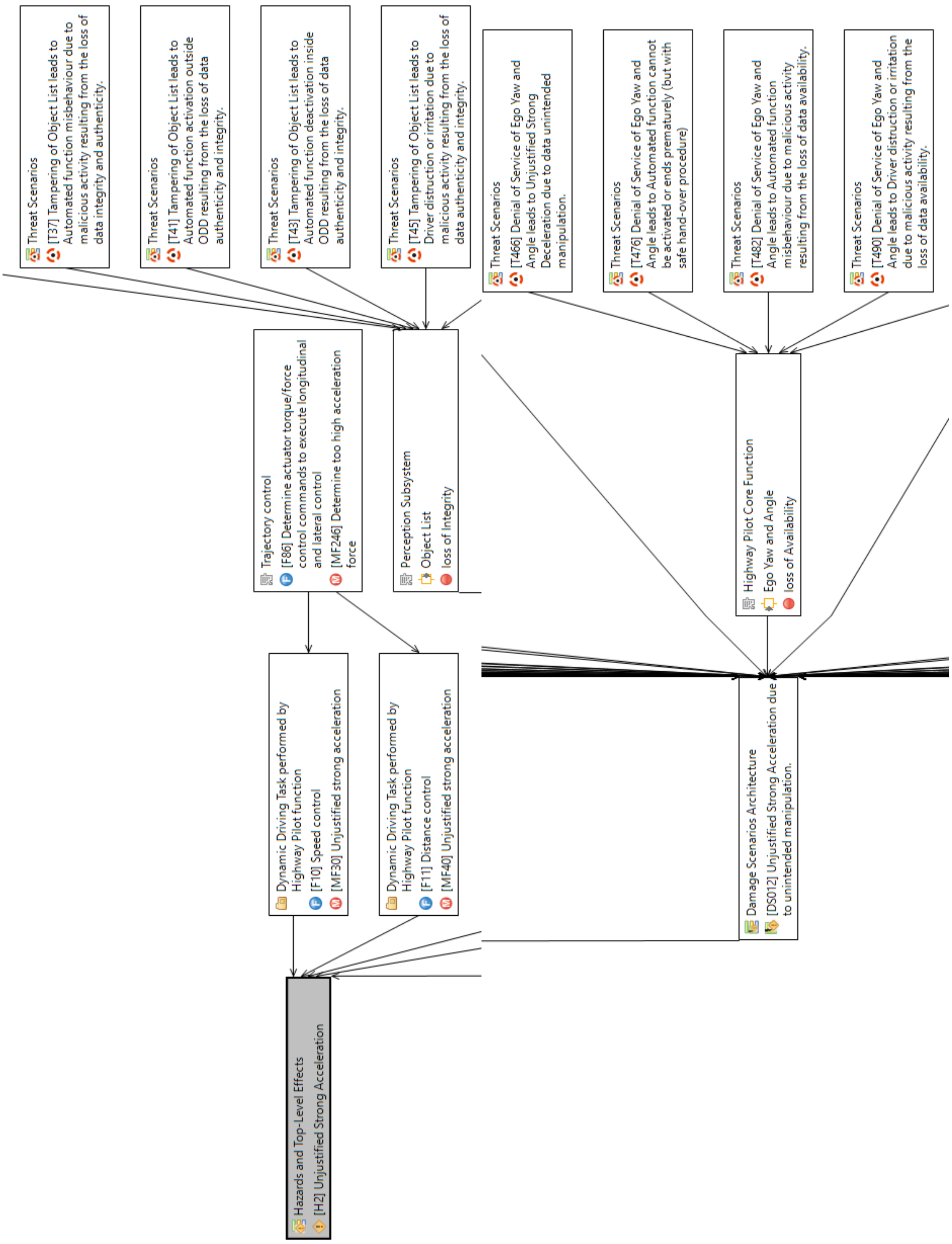

Threat Scenarios
[T37] Tampering of Object List leads to Automated function misbehaviour due to malicious activity resulting from the loss of data integrity and authenticity.
Threat Scenarios
[T41] Tampering of Object List leads to Automated function activation outside ODD resulting from the loss of data authenticity and integrity.
Threat Scenarios
[T43] Tampering of Object List leads to Automated function deactivation inside ODD resulting from the loss of data authenticity and integrity.
Threat Scenarios
[T45] Tampering of Object List leads to Driver distruction or irritation due to malicious activity resulting from the loss of data authenticity and integrity.
Threat Scenarios
[T466] Denial of Service of Ego Yaw and Angle leads to Unjustified Strong Deceleration due to data unintended manipulation.
Threat Scenarios
[T476] Denial of Service of Ego Yaw and Angle leads to Automated function cannot be activated or ends prematurely (but with safe hand-over procedure)
Threat Scenarios
[T482] Denial of Service of Ego Yaw and Angle leads to Automated function misbehaviour due to malicious activity resulting from the loss of data availability.
Threat Scenarios
[T490] Denial of Service of Ego Yaw and Angle leads to Driver distruction or irritation due to malicious activity resulting from the loss of data availability.
Trajectory control
[F86] Determine actuator torque/force control commands to execute longitudinal and lateral control
[MF246] Determine too high acceleration force
Perception Subsystem
Object List
loss of Integrity
Highway Pilot Core Function
Ego Yaw and Angle
loss of Availability
Dynamic Driving Task performed by Highway Pilot function
[F10] Speed control
[MF30] Unjustified strong acceleration
Dynamic Driving Task performed by Highway Pilot function
[F11] Distance control
[MF40] Unjustified strong acceleration
Damage Scenarios Architecture
[DS012] Unjustified Strong Acceleration due to unintended manipulation.
Hazards and Top-Level Effects
[H2] Unjustified Strong Acceleration

Figure 4.9: CyberSafety analysis Hazard-Damage Scenario Cause/Effect Net view.

In the HP example the following threats were labeled:

- “Unjustified Strong Deceleration due to data unintended manipulation”;
- “Disclosure of sensitive OEM information without the OEM’s consent resulting from the loss of confidentiality”;
- “Automated function misbehavior due to malicious activity resulting from the loss of data integrity and authenticity”;
- “Automated function misbehavior due to malicious activity resulting from the loss of data availability”;
- “Automated function misbehavior due to malicious activity resulting from the loss of non-repudiation property. (Proof of delivery is not provided to the sender and receiver.)”;
- “Automated function activation outside ODD resulting from the loss of data authenticity and integrity”;
- “Unjustified Strong Acceleration due to unintended manipulation.”.

were labeled with the Safety impact as "Severe," indicating a higher priority for further investigation above other lower level Safety impacts. The "Impact Justification" for each Damage Scenario is provided and can be seen in Figure 4.10.

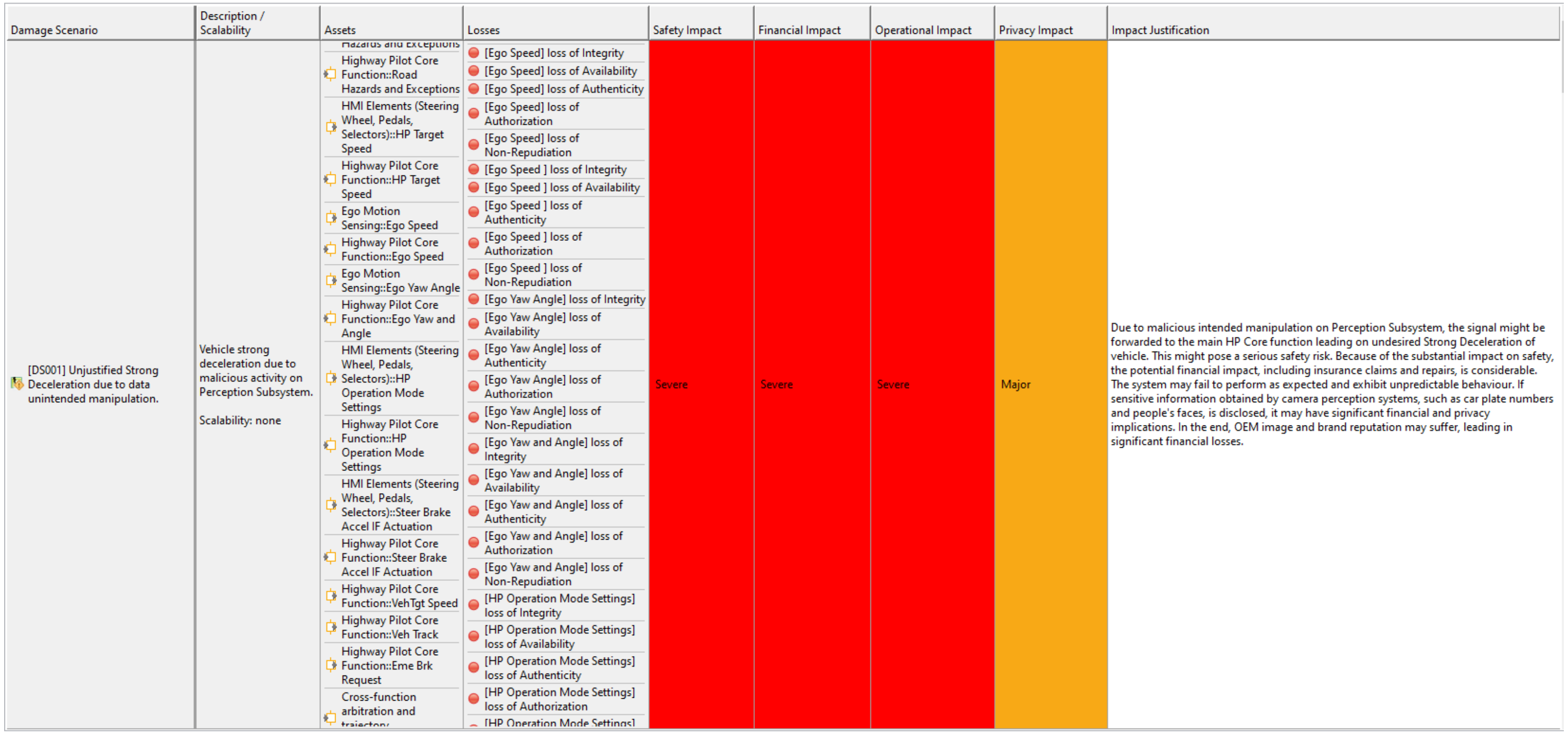
From the standpoint of CySe, having Damage Scenarios defined and rated, as well as Threat Scenarios created, leads to the most difficult activity, "Attack Path Analysis" and "Attack Feasibility Rating". Based on their experience, the analysts develop potential attack scenarios and analyze them in accordance with the ISO 21434 standard, resulting in the determination of the "Attack Feasibility Rating." ISO 21434 recommends three approaches to attack analysis, namely:

- Attack Potential-based Approach;
- CVSS-based Approach;
- Attack-Vector-based Approach.

The "Attack Potential-based Approach" and "Attack-Vector-based Approach" according to ISO 21434 Annex G were used for the HP model analysis to assess the Attack in terms of an attacker’s knowledge and necessary resources, as well as providing a context of attack complexity and privileges required.

Attack Potential-based Approach relies on five core parameters:

- Elapsed time;
- Specialist Expertise;
- Knowledge of the item or component;



Damage Scenario	Description / Scalability	Assets	Losses	Safety Impact	Financial Impact	Operational Impact	Privacy Impact	Impact Justification
[DS001] Unjustified Strong Deceleration due to data unintended manipulation.	Vehicle strong deceleration due to malicious activity on Perception Subsystem. Scalability: none	Hazards and Exceptions Highway Pilot Core Function::Road Hazards and Exceptions HMI Elements (Steering Wheel, Pedals, Selectors)::HP Target Speed Highway Pilot Core Function::HP Target Speed Ego Motion Sensing::Ego Speed Highway Pilot Core Function::Ego Speed Ego Motion Sensing::Ego Yaw Angle Highway Pilot Core Function::Ego Yaw and Angle HMI Elements (Steering Wheel, Pedals, Selectors)::HP Operation Mode Settings Highway Pilot Core Function::HP Operation Mode Settings HMI Elements (Steering Wheel, Pedals, Selectors)::Steer Brake Accel IF Actuation Highway Pilot Core Function::Steer Brake Accel IF Actuation Highway Pilot Core Function::VehTgt Speed Highway Pilot Core Function::Veh Track Highway Pilot Core Function::Eme Brk Request Cross-function arbitration and trajectory	● [Ego Speed] loss of Integrity ● [Ego Speed] loss of Availability ● [Ego Speed] loss of Authenticity ● [Ego Speed] loss of Authorization ● [Ego Speed] loss of Non-Repudiation ● [Ego Speed] loss of Integrity ● [Ego Speed] loss of Availability ● [Ego Speed] loss of Authenticity ● [Ego Speed] loss of Authorization ● [Ego Speed] loss of Non-Repudiation ● [Ego Yaw Angle] loss of Integrity ● [Ego Yaw Angle] loss of Availability ● [Ego Yaw Angle] loss of Authenticity ● [Ego Yaw Angle] loss of Authorization ● [Ego Yaw Angle] loss of Non-Repudiation ● [Ego Yaw and Angle] loss of Integrity ● [Ego Yaw and Angle] loss of Availability ● [Ego Yaw and Angle] loss of Authenticity ● [Ego Yaw and Angle] loss of Authorization ● [Ego Yaw and Angle] loss of Non-Repudiation ● [HP Operation Mode Settings] loss of Integrity ● [HP Operation Mode Settings] loss of Availability ● [HP Operation Mode Settings] loss of Authenticity ● [HP Operation Mode Settings] loss of Authorization ● [HP Operation Mode Settings]	Severe	Severe	Severe	Major	Due to malicious intended manipulation on Perception Subsystem, the signal might be forwarded to the main HP Core function leading on undesired Strong Deceleration of vehicle. This might pose a serious safety risk. Because of the substantial impact on safety, the potential financial impact, including insurance claims and repairs, is considerable. The system may fail to perform as expected and exhibit unpredictable behaviour. If sensitive information obtained by camera perception systems, such as car plate numbers and people's faces, is disclosed, it may have significant financial and privacy implications. In the end, OEM image and brand reputation may suffer, leading in significant financial losses.

Figure 4.10: CyberSafety Analysis HP - Damage scenario Impact Rating.

- Window of opportunity;
- Equipment.

Whereas Attack-Vector-based Approach takes into account the following:

- Attack Vector;
- Attack Complexity;
- Privileges required;
- User Interaction.

Ansys Medini, based on ISO 21434 Annex G calculates the Attack Feasibility rating, taking into account selected analysis method. For the defined Attacks for HP, following Attacks were considered with a “High” feasibility rating:

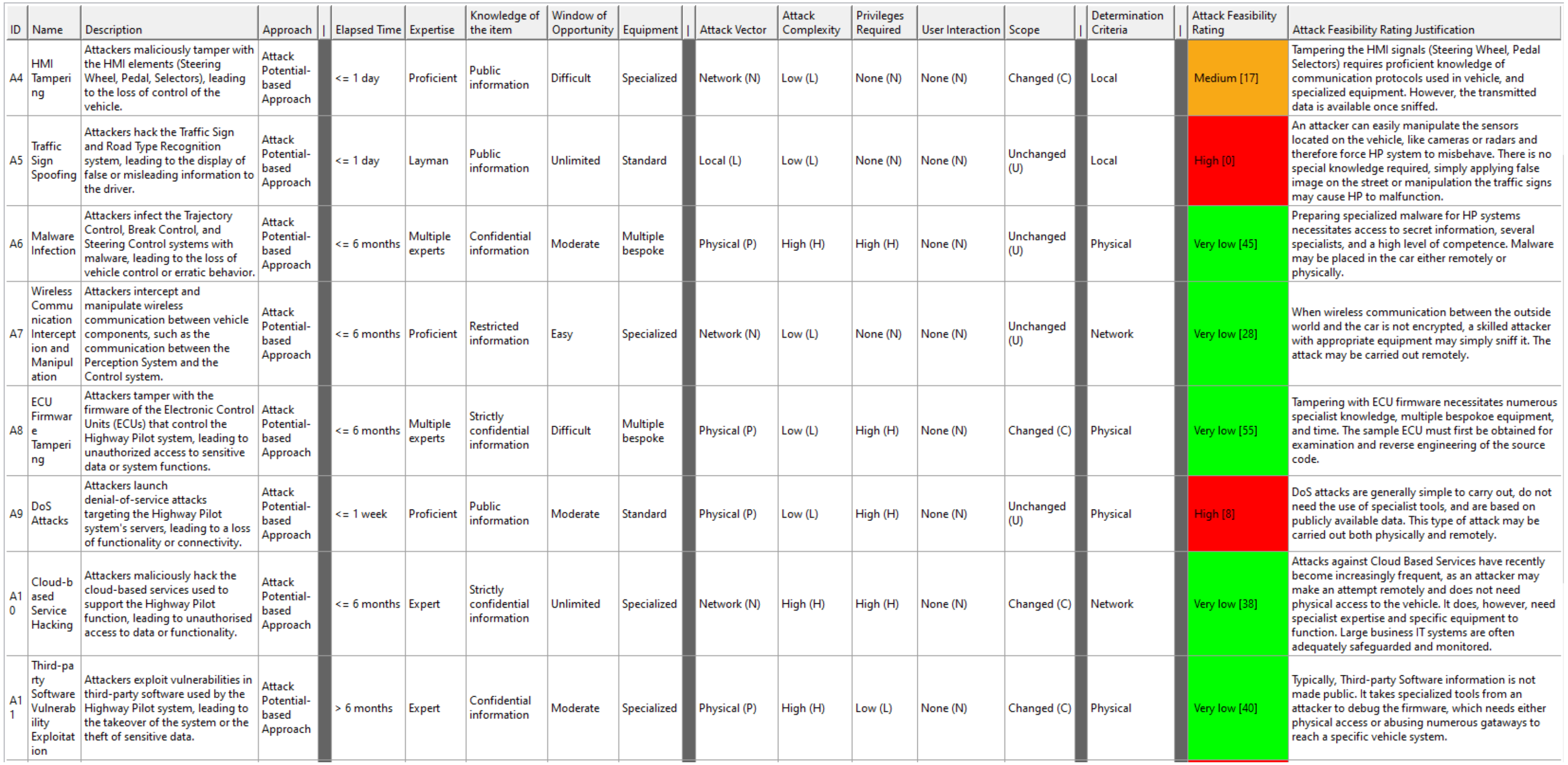
- GPS Spoofing of Jamming;
- Traffic Sign Spoofing;
- DoS Attack;
- Phishing and Social Engineering Attacks;
- Physical Attacks.

For each attack the “Attack Feasibility Rating Justification” was given, what can be observed in Figure 4.11. The complete list of attacks is available in the Annex B - Attack_Paths.xlsx.

To restrict the scope of the study, the next stage was to create Attack Trees on these attacks, which leads to significant Threats for the most critical Damage Scenario from a safety standpoint. As a result, the following threats were chosen:

- T1 - Tampering of Object List leads to Unjustified Strong Deceleration due to data unintended manipulation; Figure 4.12.
- T2 - Denial of Service of Object List leads to Unjustified Strong Deceleration due to data unintended manipulation; Figure 4.15.
- T846 - Denial of Service of EmeBrk leads to Unjustified Strong Deceleration due to data unintended manipulation; Figure 4.16.

The concept of a Transfer Gate, which is present in Medini, was used to more clearly represent the Attack Path. It provides the ability to reuse a certain Attack Branch in other Attack Branches or Attack Paths, as shown in Figure 4.13 and Figure 4.14.



ID	Name	Description	Approach	Elapsed Time	Expertise	Knowledge of the item	Window of Opportunity	Equipment	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Determination Criteria	Attack Feasibility Rating	Attack Feasibility Rating Justification
A4	HMI Tampering	Attackers maliciously tamper with the HMI elements (Steering Wheel, Pedal, Selectors), leading to the loss of control of the vehicle.	Attack Potential-based Approach	<= 1 day	Proficient	Public information	Difficult	Specialized	Network (N)	Low (L)	None (N)	None (N)	Changed (C)	Local	Medium [17]	Tampering the HMI signals (Steering Wheel, Pedal Selectors) requires proficient knowledge of communication protocols used in vehicle, and specialized equipment. However, the transmitted data is available once sniffed.
A5	Traffic Sign Spoofing	Attackers hack the Traffic Sign and Road Type Recognition system, leading to the display of false or misleading information to the driver.	Attack Potential-based Approach	<= 1 day	Layman	Public information	Unlimited	Standard	Local (L)	Low (L)	None (N)	None (N)	Unchanged (U)	Local	High [0]	An attacker can easily manipulate the sensors located on the vehicle, like cameras or radars and therefore force HP system to misbehave. There is no special knowledge required, simply applying false image on the street or manipulation the traffic signs may cause HP to malfunction.
A6	Malware Infection	Attackers infect the Trajectory Control, Break Control, and Steering Control systems with malware, leading to the loss of vehicle control or erratic behavior.	Attack Potential-based Approach	<= 6 months	Multiple experts	Confidential information	Moderate	Multiple bespoke	Physical (P)	High (H)	High (H)	None (N)	Unchanged (U)	Physical	Very low [45]	Preparing specialized malware for HP systems necessitates access to secret information, several specialists, and a high level of competence. Malware may be placed in the car either remotely or physically.
A7	Wireless Communication Interception and Manipulation	Attackers intercept and manipulate wireless communication between vehicle components, such as the communication between the Perception System and the Control system.	Attack Potential-based Approach	<= 6 months	Proficient	Restricted information	Easy	Specialized	Network (N)	Low (L)	None (N)	None (N)	Unchanged (U)	Network	Very low [28]	When wireless communication between the outside world and the car is not encrypted, a skilled attacker with appropriate equipment may simply sniff it. The attack may be carried out remotely.
A8	ECU Firmware Tampering	Attackers tamper with the firmware of the Electronic Control Units (ECUs) that control the Highway Pilot system, leading to unauthorized access to sensitive data or system functions.	Attack Potential-based Approach	<= 6 months	Multiple experts	Strictly confidential information	Difficult	Multiple bespoke	Physical (P)	Low (L)	High (H)	None (N)	Changed (C)	Physical	Very low [55]	Tampering with ECU firmware necessitates numerous specialist knowledge, multiple bespokoe equipment, and time. The sample ECU must first be obtained for examination and reverse engineering of the source code.
A9	DoS Attacks	Attackers launch denial-of-service attacks targeting the Highway Pilot system's servers, leading to a loss of functionality or connectivity.	Attack Potential-based Approach	<= 1 week	Proficient	Public information	Moderate	Standard	Physical (P)	Low (L)	High (H)	None (N)	Unchanged (U)	Physical	High [8]	DoS attacks are generally simple to carry out, do not need the use of specialist tools, and are based on publicly available data. This type of attack may be carried out both physically and remotely.
A10	Cloud-based Service Hacking	Attackers maliciously hack the cloud-based services used to support the Highway Pilot function, leading to unauthorised access to data or functionality.	Attack Potential-based Approach	<= 6 months	Expert	Strictly confidential information	Unlimited	Specialized	Network (N)	High (H)	High (H)	None (N)	Changed (C)	Network	Very low [38]	Attacks against Cloud Based Services have recently become increasingly frequent, as an attacker may make an attempt remotely and does not need physical access to the vehicle. It does, however, need specialist expertise and specific equipment to function. Large business IT systems are often adequately safeguarded and monitored.
A11	Third-party Software Vulnerability Exploitation	Attackers exploit vulnerabilities in third-party software used by the Highway Pilot system, leading to the takeover of the system or the theft of sensitive data.	Attack Potential-based Approach	> 6 months	Expert	Confidential information	Moderate	Specialized	Physical (P)	High (H)	Low (L)	None (N)	Changed (C)	Physical	Very low [40]	Typically, Third-party Software information is not made public. It takes specialized tools from an attacker to debug the firmware, which needs either physical access or abusing numerous gataways to reach a specific vehicle system.

Figure 4.11: CyberSafety Analysis HP - Attack Feasibility Rating.

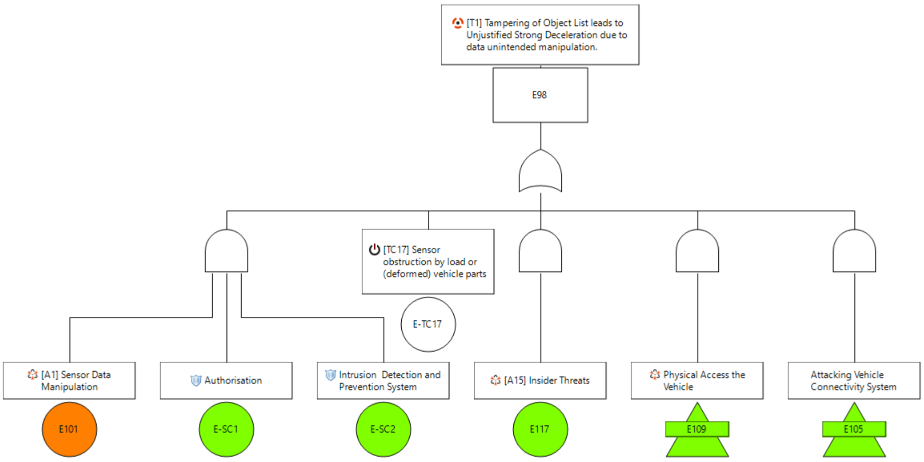

[T1] Tampering of Object List leads to Unjustified Strong Deceleration due to data unintended manipulation.
E98
[TC17] Sensor obstruction by load or (deformed) vehicle parts
E-TC17
[A1] Sensor Data Manipulation
E101
Authorisation
E-SC1
Intrusion Detection and Prevention System
E-SC2
[A15] Insider Threats
E117
Physical Access the Vehicle
E109
Attacking Vehicle Connectivity System
E105

Figure 4.12: CyberSafety Analysis HP - Tampering of Object List Attack Tree.

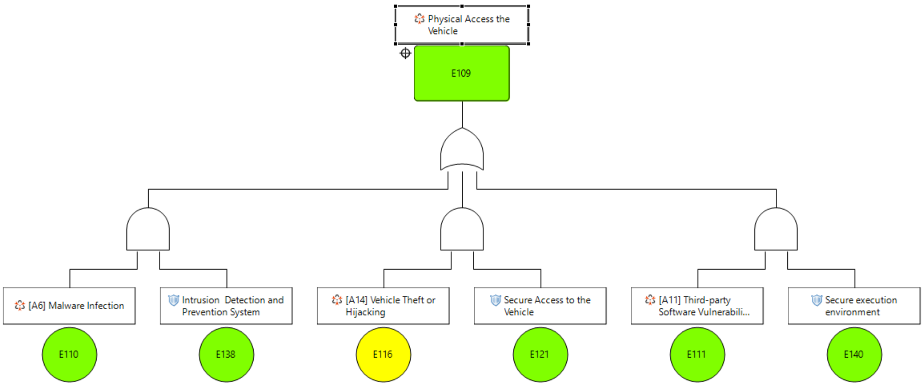

Physical Access the Vehicle
E109
[A6] Malware Infection
E110
Intrusion Detection and Prevention System
E138
[A14] Vehicle Theft or Hijacking
E116
Secure Access to the Vehicle
E121
[A11] Third-party Software Vulnerabili...
E111
Secure execution environment
E140

Figure 4.13: CyberSafety Analysis HP - Tampering of Object List Attack Tree - Physical Access Event.

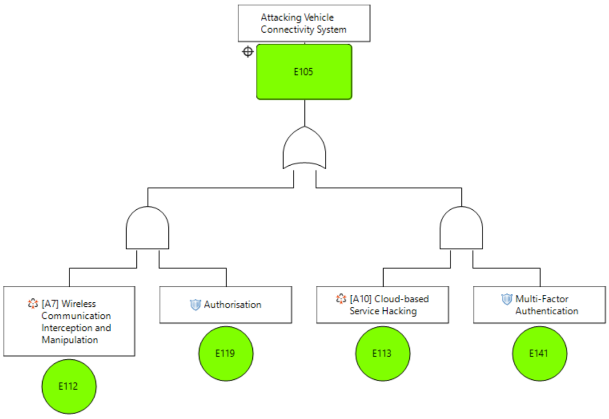

Attacking Vehicle Connectivity System
E105
[A7] Wireless Communication Interception and Manipulation
E112
Authorisation
E119
[A10] Cloud-based Service Hacking
E113
Multi-Factor Authentication
E141

Figure 4.14: CyberSafety Analysis HP - Tampering of Object List Attack Tree - Vehicle Connectivity System Attack Event.

Using Ansys Medini's Attack Tree concept, it is possible to visually depict the relationships between CySe Attack and Safety malfunction or SOTIF trigger. As an example, SOTIF trigger "[TC17] Sensor obstruction by load or (deformed) vehicle parts", may be one of the various triggers considered for CySe

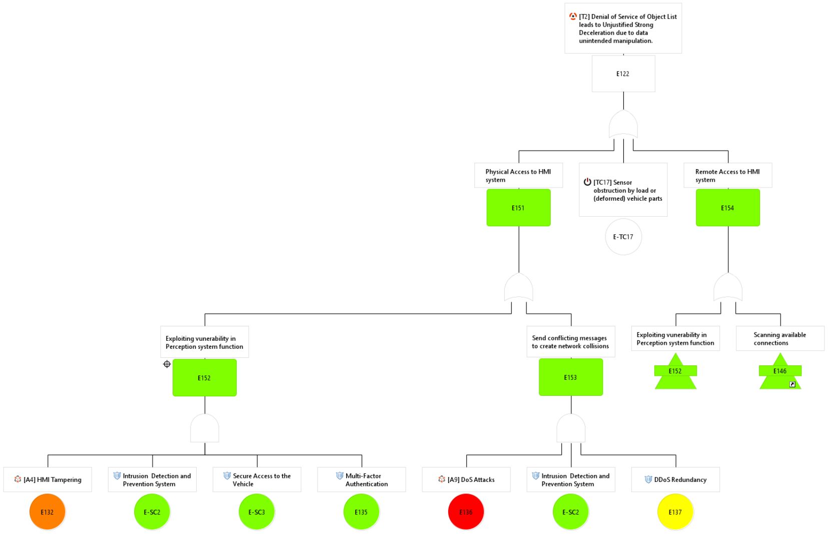

[T2] Denial of Service of Object List leads to Unjustified Strong Deceleration due to data unintended manipulation.
E122
Physical Access to HMI system
E151
[TC17] Sensor obstruction by load or (deformed) vehicle parts
E-TC17
Remote Access to HMI system
E154
Exploiting vunerability in Perception system function
E152
Send conflicting messages to create network collisions
E153
Exploiting vunerability in Perception system function
E152
Scanning available connections
E146
[A4] HMI Tampering
E132
Intrusion Detection and Prevention System
E-SC2
Secure Access to the Vehicle
E-SC3
Multi-Factor Authentication
E135
[A9] DoS Attacks
E136
Intrusion Detection and Prevention System
E-SC2
DDoS Redundancy
E137

Figure 4.15: CyberSafety Analysis HP - Denial of Service of Object List Attack Tree.

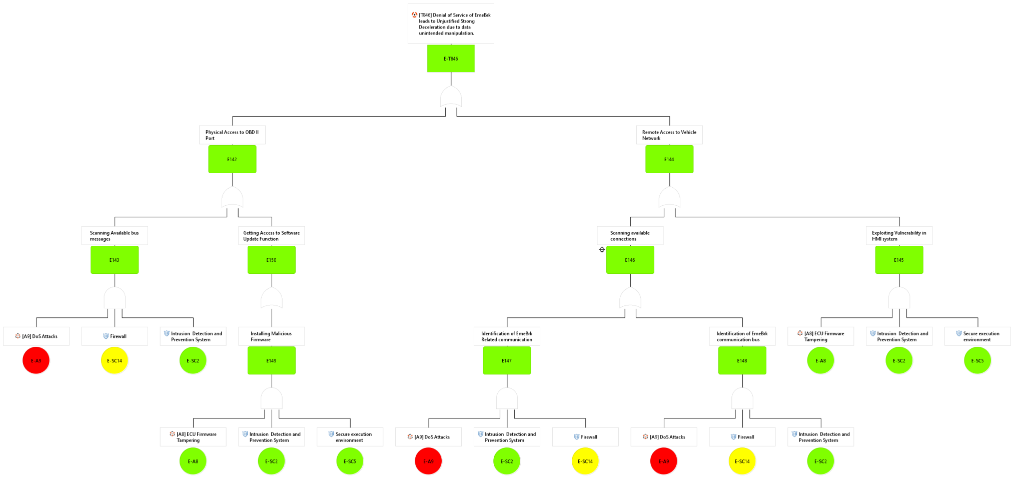

[T846] Denial of Service of EmeBrk leads to Unjustified Strong Deceleration due to data unintended manipulation.
E-T846
Physical Access to OBD II Port
E142
Remote Access to Vehicle Network
E144
Scanning Available bus messages
E143
Getting Access to Software Update Function
E150
Scanning available connections
E146
Exploiting Vulnerability in HMI system
E145
[A9] DoS Attacks
E-A9
Firewall
E-SC14
Intrusion Detection and Prevention System
E-SC2
Installing Malicious Firmware
E149
Identification of EmeBrk Related communication
E147
Identification of EmeBrk communication bus
E148
[A8] ECU Firmware Tampering
E-A8
Intrusion Detection and Prevention System
E-SC2
Secure execution environment
E-SC5
[A8] ECU Firmware Tampering
E-A8
Intrusion Detection and Prevention System
E-SC2
Secure execution environment
E-SC5
[A9] DoS Attacks
E-A9
Intrusion Detection and Prevention System
E-SC2
Firewall
E-SC14
[A9] DoS Attacks
E-A9
Firewall
E-SC14
Intrusion Detection and Prevention System
E-SC2

Figure 4.16: CyberSafety Analysis HP - Denial of Service of EmeBrk Attack Tree.

[T1] Tampering of the Object List leads to Unjustified Strong Deceleration due to unintended data manipulation", as observed in Figure 4.12. Similarly, the relationship between safety malfunction, Safety Goal and Cybersecurity Threat can be captured utilizing the in build "Trace" option during Fault Tree Analysis (FTA) analysis. In the HP example, Unjustified breaking by HP, can be caused not only by defined system malfunction such as :

- Wrong positioning or classification;
- Brake decision made although no dangerous object reported;
- Strong braking although not commanded;
- Detection of non-existing object.

But also defined CySe events are considered, e.g.:

- Sensor Data Manipulation;
- ECU Firmware Tampering;
- Physical Access the Vehicle;
- Attacking Vehicle Connectivity System.

This provides a holistic perspective of the potential effects on safety and cybersecurity from many aspects, leading to the formulation of clearer and more comprehensive goals and requirements for an evaluated system, as shown in Figure 4.17.

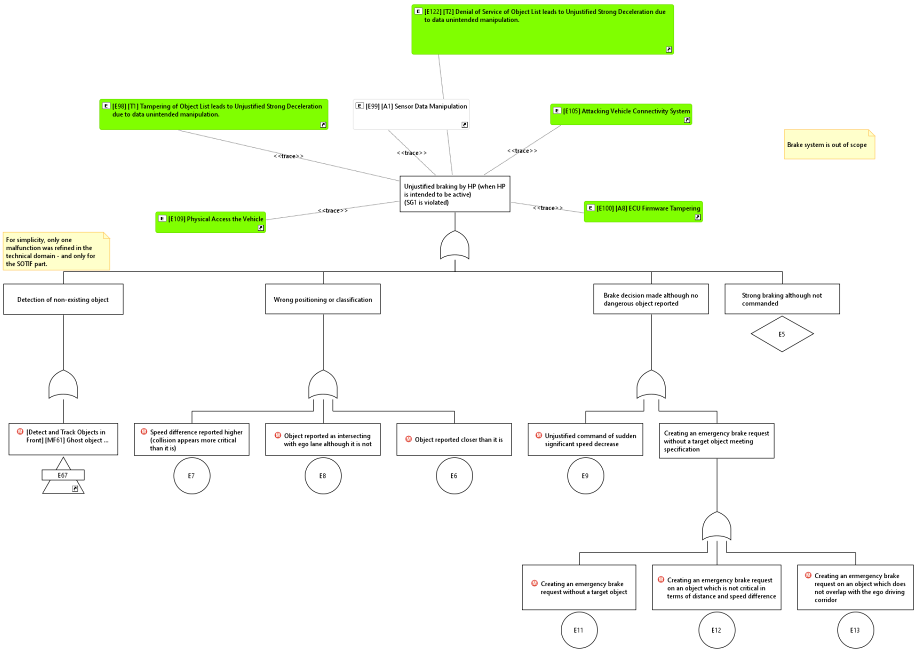
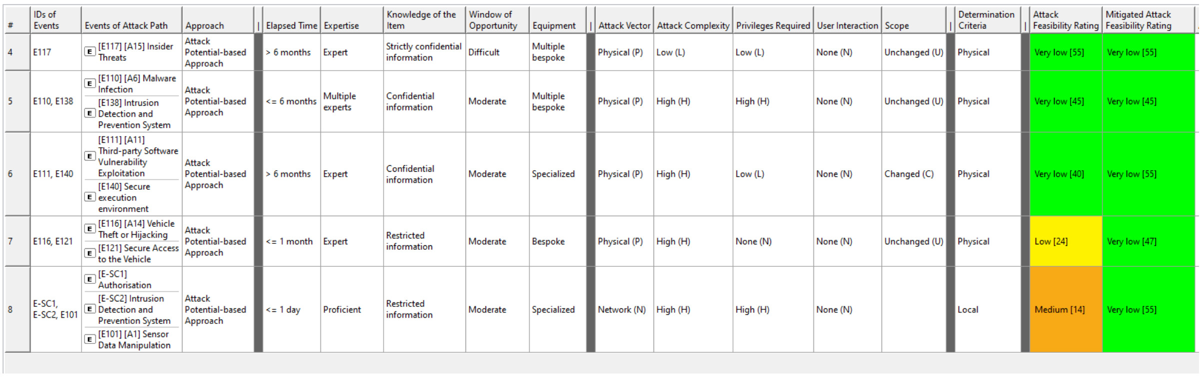

E [E122] [T2] Denial of Service of Object List leads to Unjustified Strong Deceleration due to data unintended manipulation.
E [E98] [T1] Tampering of Object List leads to Unjustified Strong Deceleration due to data unintended manipulation.
E [E99] [A1] Sensor Data Manipulation
E [E105] Attacking Vehicle Connectivity System
Brake system is out of scope
<<trace>>
<<trace>>
<<trace>>
<<trace>>
<<trace>>
Unjustified braking by HP (when HP is intended to be active) (SG1 is violated)
E [E109] Physical Access the Vehicle
E [E100] [A8] ECU Firmware Tampering
For simplicity, only one malfunction was refined in the technical domain - and only for the SOTIF part.
Detection of non-existing object
Wrong positioning or classification
Brake decision made although no dangerous object reported
Strong braking although not commanded
E5
[Detect and Track Objects in Front] [MF61] Ghost object ...
E67
Speed difference reported higher (collision appears more critical than it is)
E7
Object reported as intersecting with ego lane although it is not
E8
Object reported closer than it is
E6
Unjustified command of sudden significant speed decrease
E9
Creating an emergency brake request without a target object meeting specification
Creating an emergency brake request without a target object
E11
Creating an emergency brake request on an object which is not critical in terms of distance and speed difference
E12
Creating an ermergency brake request on an object which does not overlap with the ego driving corridor
E13

Figure 4.17: CyberSafety Analysis HP - FTA for [SG1] - CyberSafety Analysis Highway Pilot.

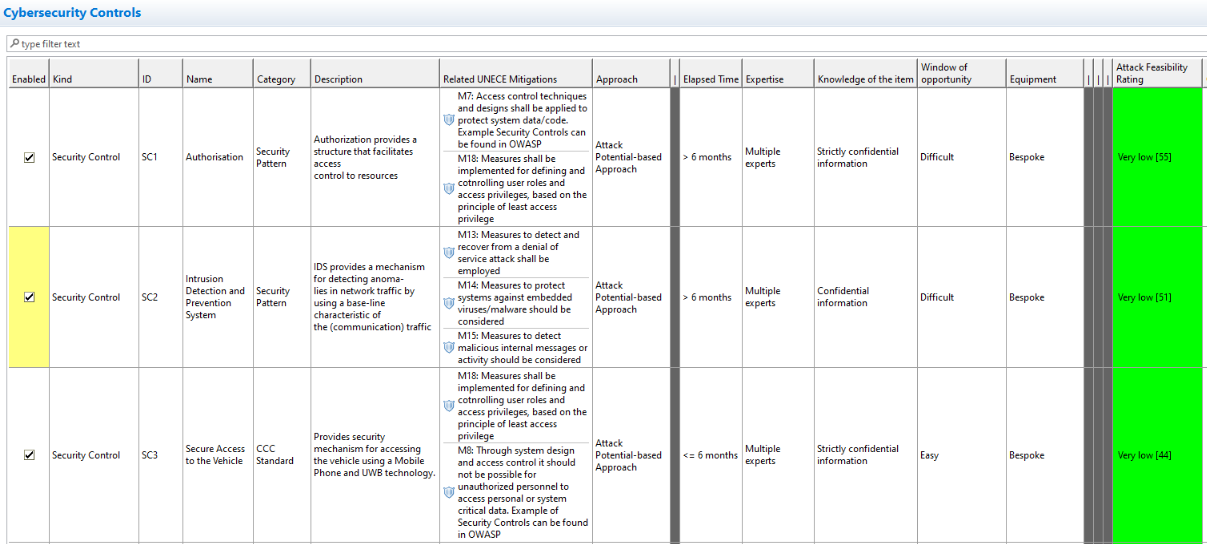
Ansys Medini allows computing and assessing each event in the attack path, which is depicted in Figure 4.18 independently, and record how a risk might be minimized by adopting the right mitigation technique in the form of Cybersecurity Control.



#	IDs of Events	Events of Attack Path	Approach	Elapsed Time	Expertise	Knowledge of the Item	Window of Opportunity	Equipment	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Determination Criteria	Attack Feasibility Rating	Mitigated Attack Feasibility Rating
4	E117	E [E117] [A15] Insider Threats	Attack Potential-based Approach	> 6 months	Expert	Strictly confidential information	Difficult	Multiple bespoke	Physical (P)	Low (L)	Low (L)	None (N)	Unchanged (U)	Physical	Very low [55]	Very low [55]
5	E110, E138	E [E110] [A6] Malware Infection E [E138] Intrusion Detection and Prevention System	Attack Potential-based Approach	<= 6 months	Multiple experts	Confidential information	Moderate	Multiple bespoke	Physical (P)	High (H)	High (H)	None (N)	Unchanged (U)	Physical	Very low [45]	Very low [45]
6	E111, E140	E [E111] [A11] Third-party Software Vulnerability Exploitation E [E140] Secure execution environment	Attack Potential-based Approach	> 6 months	Expert	Confidential information	Moderate	Specialized	Physical (P)	High (H)	Low (L)	None (N)	Changed (C)	Physical	Very low [40]	Very low [55]
7	E116, E121	E [E116] [A14] Vehicle Theft or Hijacking E [E121] Secure Access to the Vehicle	Attack Potential-based Approach	<= 1 month	Expert	Restricted information	Moderate	Bespoke	Physical (P)	High (H)	None (N)	None (N)	Unchanged (U)	Physical	Low [24]	Very low [47]
8	E-SC1, E-SC2, E101	E [E-SC1] Authorisation E [E-SC2] Intrusion Detection and Prevention System E [E101] [A1] Sensor Data Manipulation	Attack Potential-based Approach	<= 1 day	Proficient	Restricted information	Moderate	Specialized	Network (N)	High (H)	High (H)	None (N)		Local	Medium [14]	Very low [55]

Figure 4.18: CyberSafety Analysis HP - Attack Feasibility Rating and Mitigation.

For the HP example, Cybersecurity Controls have been created based on Security Patterns as defined by [38] and [129]. The complete list of HP Cybersecurity Controls can be found in Annex B - Cybersecurity_Controls.xlsx. Using the Attack Potential-based Approach, each Cybersecurity Control was evaluated in terms of its mitigation potential. It is also feasible to co-relate implemented Security Controls with UNECE Mitigations at this stage, what is presented in Figure 4.19.


Cybersecurity Controls

type filter text

Enabled	Kind	ID	Name	Category	Description	Related UNECE Mitigations	Approach	Elapsed Time	Expertise	Knowledge of the item	Window of opportunity	Equipment	Attack Feasibility Rating
☑	Security Control	SC1	Authorisation	Security Pattern	Authorization provides a structure that facilitates access control to resources	M7: Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP M18: Measures shall be implemented for defining and cotnrolling user roles and access privileges, based on the principle of least access privilege	Attack Potential-based Approach	> 6 months	Multiple experts	Strictly confidential information	Difficult	Bespoke	Very low [55]
☑	Security Control	SC2	Intrusion Detection and Prevention System	Security Pattern	IDS provides a mechanism for detecting anomalies in network traffic by using a base-line characteristic of the (communication) traffic	M13: Measures to detect and recover from a denial of service attack shall be employed M14: Measures to protect systems against embedded viruses/malware should be considered M15: Measures to detect malicious internal messages or activity should be considered	Attack Potential-based Approach	> 6 months	Multiple experts	Confidential information	Difficult	Bespoke	Very low [51]
☑	Security Control	SC3	Secure Access to the Vehicle	CCC Standard	Provides security mechanism for accessing the vehicle using a Mobile Phone and UWB technology.	M18: Measures shall be implemented for defining and cotnrolling user roles and access privileges, based on the principle of least access privilege M8: Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Example of Security Controls can be found in OWASP	Attack Potential-based Approach	<= 6 months	Multiple experts	Strictly confidential information	Easy	Bespoke	Very low [44]

Figure 4.19: CyberSafety Analysis HP - Cybersecurity Controls Rating.

By applying certain Cybersecurity Control, the CySe risk is mitigated, which is indicated by a color convention on the Attack Tree Diagrams. As an example, Figure 4.16 represents the Attack Tree with enabled IDS as a Cybersecurity Control, while Figure 4.20 shows the Attack Tree when IDS as a Cybersecurity Control is disabled.

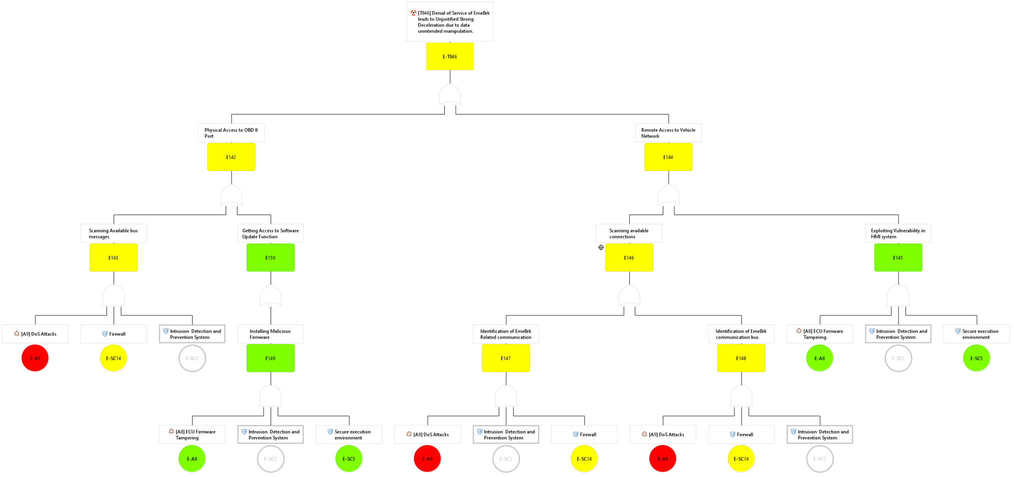
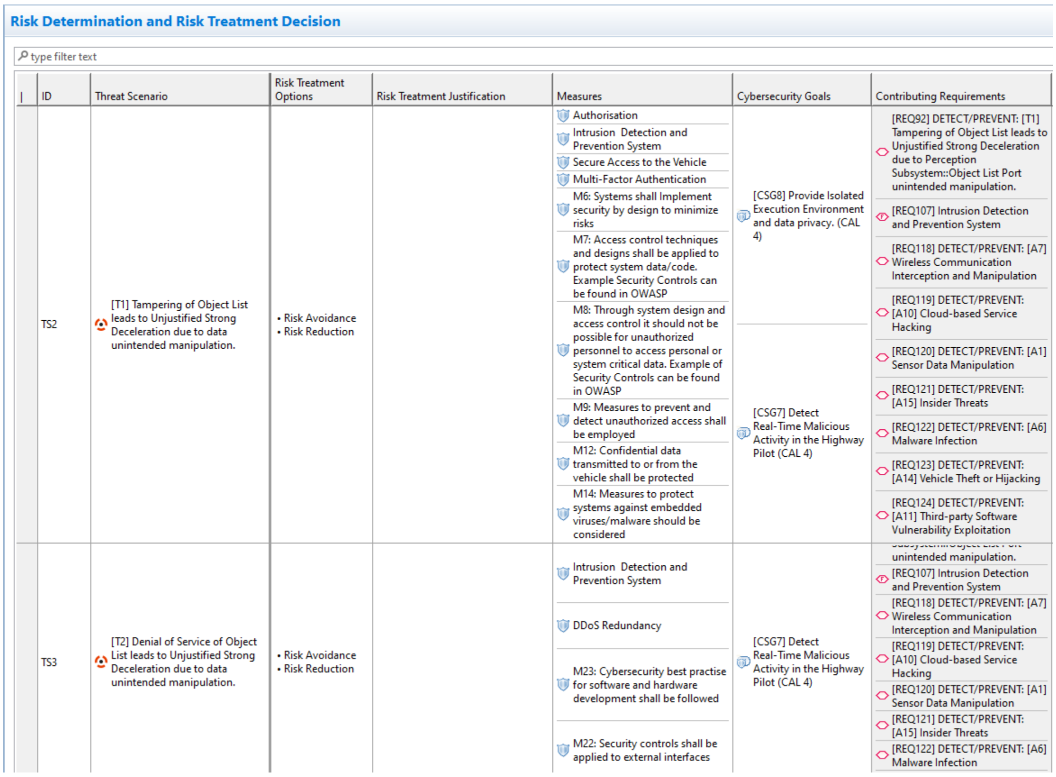

[T846] Denial of Service of EmeBrk leads to Unjustified Strong Deceleration due to data unintended manipulation.
E-T846
Physical Access to OBD II Port
E142
Remote Access to Vehicle Network
E144
Scanning Available bus messages
E143
Getting Access to Software Update Function
E150
Scanning available connections
E146
Exploiting Vulnerability in HMI system
E145
[A9] DoS Attacks
E-A9
Firewall
E-SC14
Intrusion Detection and Prevention System
E-SC2
Installing Malicious Firmware
E149
Identification of EmeBrk Related communication
E147
Identification of EmeBrk communication bus
E148
[A8] ECU Firmware Tampering
E-A8
Intrusion Detection and Prevention System
E-SC2
Secure execution environment
E-SC5
[A8] ECU Firmware Tampering
E-A8
Intrusion Detection and Prevention System
E-SC2
Secure execution environment
E-SC5
[A9] DoS Attacks
E-A9
Intrusion Detection and Prevention System
E-SC2
Firewall
E-SC14
[A9] DoS Attacks
E-A9
Firewall
E-SC14
Intrusion Detection and Prevention System
E-SC2

Figure 4.20: CyberSafety Analysis HP - Denial of Service of EmeBrk Attack Tree - IDS Disabled.

The Risk Determination and Risk Treatment Decision page contains the summary of the performed analysis, as well as a formal Risk Treatment Decision. The evaluated threats are available in Annex B: Risk_Determination_Risk_Treatment_Decision.xlsx Here, analysts decide on a strategy for dealing with a certain threat, such as risk avoidance, risk reduction, risk acceptance, or risk sharing. The tool also allows to set Measures and Cybersecurity Goals to minimize certain threats. Once requirements are created, the requirements that contribute to the Cybersecurity Goals are also visible here, as shown in Figure 4.21.



Risk Determination and Risk Treatment Decision

type filter text

|	ID	Threat Scenario	Risk Treatment Options	Risk Treatment Justification	Measures	Cybersecurity Goals	Contributing Requirements
	TS2	[T1] Tampering of Object List leads to Unjustified Strong Deceleration due to data unintended manipulation.	• Risk Avoidance • Risk Reduction		Authorisation Intrusion Detection and Prevention System Secure Access to the Vehicle Multi-Factor Authentication M6: Systems shall Implement security by design to minimize risks M7: Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP M8: Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Example of Security Controls can be found in OWASP M9: Measures to prevent and detect unauthorized access shall be employed M12: Confidential data transmitted to or from the vehicle shall be protected M14: Measures to protect systems against embedded viruses/malware should be considered	[CSG8] Provide Isolated Execution Environment and data privacy. (CAL 4) [CSG7] Detect Real-Time Malicious Activity in the Highway Pilot (CAL 4)	[REQ92] DETECT/PREVENT: [T1] Tampering of Object List leads to Unjustified Strong Deceleration due to Perception Subsystem::Object List Port unintended manipulation. [REQ107] Intrusion Detection and Prevention System [REQ118] DETECT/PREVENT: [A7] Wireless Communication Interception and Manipulation [REQ119] DETECT/PREVENT: [A10] Cloud-based Service Hacking [REQ120] DETECT/PREVENT: [A1] Sensor Data Manipulation [REQ121] DETECT/PREVENT: [A15] Insider Threats [REQ122] DETECT/PREVENT: [A6] Malware Infection [REQ123] DETECT/PREVENT: [A14] Vehicle Theft or Hijacking [REQ124] DETECT/PREVENT: [A11] Third-party Software Vulnerability Exploitation
	TS3	[T2] Denial of Service of Object List leads to Unjustified Strong Deceleration due to data unintended manipulation.	• Risk Avoidance • Risk Reduction		Intrusion Detection and Prevention System DDoS Redundancy M23: Cybersecurity best practise for software and hardware development shall be followed M22: Security controls shall be applied to external interfaces	[CSG7] Detect Real-Time Malicious Activity in the Highway Pilot (CAL 4)	unintended manipulation. [REQ107] Intrusion Detection and Prevention System [REQ118] DETECT/PREVENT: [A7] Wireless Communication Interception and Manipulation [REQ119] DETECT/PREVENT: [A10] Cloud-based Service Hacking [REQ120] DETECT/PREVENT: [A1] Sensor Data Manipulation [REQ121] DETECT/PREVENT: [A15] Insider Threats [REQ122] DETECT/PREVENT: [A6] Malware Infection

Figure 4.21: CyberSafety Analysis HP - Risk Determination and Risk Treatment Decision.

CyberSafety goals can be created when the TARA and HARA analyses are completed and the touching points are considered. In addition to the previously specified Safety Goals, the following CyberSafety Goals have been established and summarized in Table 4.2.

All system goals can be represented graphically as a diagram with dependencies between them. "[CSG 7] Detect Real_Time Malicious Activity in the HP" is indicated as a critical Goal for HP system evaluation needs due to UNR155 Regulation requirements and strong dependency with other stated Goals Figure 4.22.

The diagramming option enables to define each CyberSafety Goal's prerequisites and track their dependencies. The Annex B CySaGoals_Requirements.Reqif file contains all the defined requirements for the HP system. ReqIf It is a file format for exchanging requirements and the metadata that goes with them in XML. It also outlines a method for partners to communicate the status of requirements.

Table 4.2: HP CyberSafety Analysis - CyberSafety Goals Definition.

ID	CyberSafety Goal	Description
CSG7	Detect Real-Time Malicious Activity in the Highway Pilot.	A HP L3 vehicle function must be able to detect and respond to threats in real-time. This requires a system that can quickly analyze sensor data, identify potential hazards, and take appropriate action to avoid or mitigate them.
CSG8	Provide Isolated Execution Environment and data privacy.	As with any connected device, the L3 vehicle function must be designed to protect user data and prevent unauthorized access. This involves implementing robust encryption protocols, firewalls, and other security measures to prevent hacking and data breaches.
CSG9	Prevent Highway Pilot Function Modification.	A HP function must be designed with tamper -proof measures that prevent unauthorized access and manipulations of the system. This includes secure boot processes, encrypted communications, and other security measures that ensure the integrity of the system.
CSG10	Limit Access to External Diagnostic Interface.	External interfaces can be potential points of attack for hackers and malicious actors who may attempt to gain unauthorized access to the vehicle's systems and compromise its safety and security. By limiting access to these interfaces, the vehicle can reduce the risk of unauthorized access and mitigate potential security threats.
CSG11	Safe transition to manual driving.	When HP L3 function is disengaged and the driver takes control of the vehicle, the transition should be seamless and safe. The system shall provide clear and timely instructions to the driver, and ensure that the vehicle is in a safe condition to be driven manually.

ID	CyberSafety Goal	Description
CSG12	Provide CyberSafe Over-the-Air function update.	A HP L3 vehicle function must collect and transmit data about the vehicle's operation to enable advanced features like predictive maintenance and performance optimization. However, this data must be collected in a privacy-preserving manner, with appropriate anonymization and deidentification measures to protect the privacy of the vehicle occupants.
CSG13	Provide privacy-preserving data collection.	When HP L3 function is disengaged and the driver takes control of the vehicle, the transition should be seamless and safe. The system shall provide clear and timely instructions to the driver, and ensure that the vehicle is in a safe condition to be driven manually.

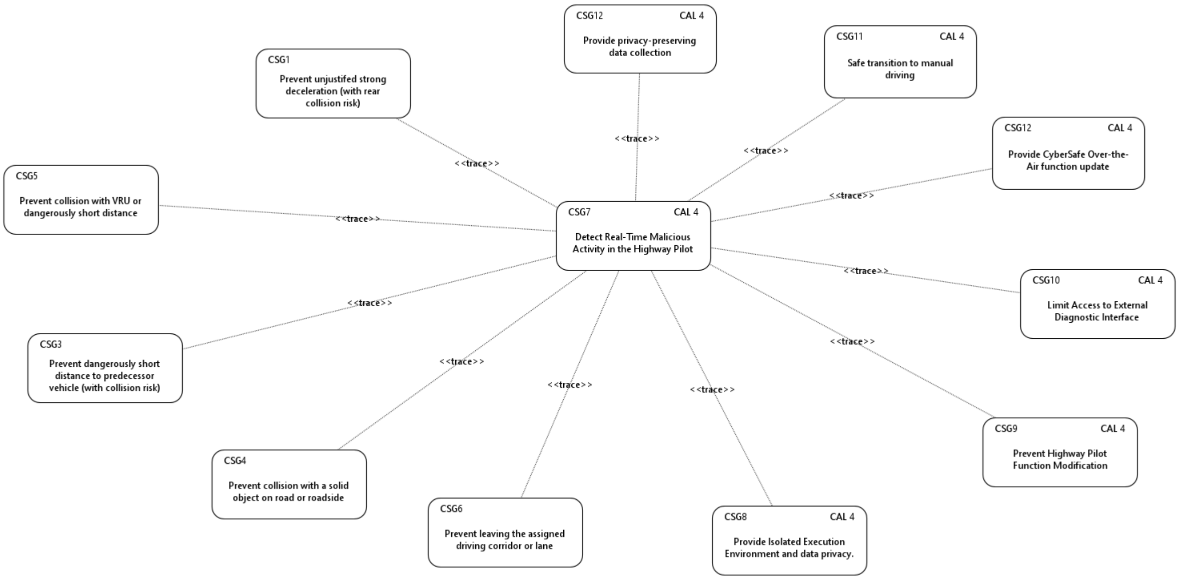

CSG12 CAL 4
Provide privacy-preserving data collection
CSG1
Prevent unjustifed strong deceleration (with rear collision risk)
CSG11 CAL 4
Safe transition to manual driving
<<trace>>
<<trace>>
<<trace>>
CSG12 CAL 4
Provide CyberSafe Over-the-Air function update
CSG5
Prevent collision with VRU or dangerously short distance
<<trace>>
<<trace>>
CSG7 CAL 4
Detect Real-Time Malicious Activity in the Highway Pilot
<<trace>>
CSG10 CAL 4
Limit Access to External Diagnostic Interface
<<trace>>
CSG3
Prevent dangerously short distance to predecessor vehicle (with collision risk)
<<trace>>
<<trace>>
<<trace>>
<<trace>>
CSG9 CAL 4
Prevent Highway Pilot Function Modification
CSG4
Prevent collision with a solid object on road or roadside
CSG6
Prevent leaving the assigned driving corridor or lane
CSG8 CAL 4
Provide Isolated Execution Environment and data privacy.

Figure 4.22: CyberSafety Analysis HP - CyberSafety Goals.

As an example of further correlation between FuSa and CySe, dependency on "[CSG1] Prevent unjustified strong deceleration (with rear collision risk)" requirements is shown in Figure 4.23. For the clarity purposes, CySe related requirements are marked in gray. In this particular example, in order to satisfy CSG1 Goal, DETECTING/PREVENTING of following requirements, which are derived from possible attacks, shall be considered:

- REQ98 – ECU Firmware Tampering;
- REQ99 – Third-party Software Vulnerability Exploitation;
- REQ101 - Cloud-based Service Hacking;
- REQ96 – Malware Infection.

The associated attack is visible in the requirement name in brackets e.g. [A10].

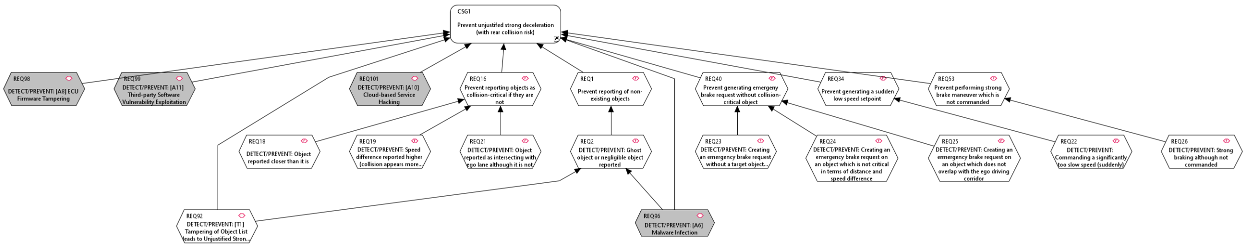

CSG1
Prevent unjustifed strong deceleration (with rear collision risk)
REQ98
DETECT/PREVENT: [A8] ECU Firmware Tampering
REQ99
DETECT/PREVENT: [A11] Third-party Software Vulnerability Exploitation
REQ101
DETECT/PREVENT: [A10] Cloud-based Service Hacking
REQ16
Prevent reporting objects as collision-critical if they are not
REQ1
Prevent reporting of non-existing objects
REQ40
Prevent generating emergeny brake request without collision-critical object
REQ34
Prevent generating a sudden low speed setpoint
REQ53
Prevent performing strong brake maneuver which is not commanded
REQ18
DETECT/PREVENT: Object reported closer than it is
REQ19
DETECT/PREVENT: Speed difference reported higher (collision appears more...
REQ21
DETECT/PREVENT: Object reported as intersecting with ego lane although it is not
REQ2
DETECT/PREVENT: Ghost object or negligible object reported
REQ23
DETECT/PREVENT: Creating an emergency brake request without a target object...
REQ24
DETECT/PREVENT: Creating an emergency brake request on an object which is not critical in terms of distance and speed difference
REQ25
DETECT/PREVENT: Creating an ermergency brake request on an object which does not overlap with the ego driving corridor
REQ22
DETECT/PREVENT: Commanding a significantly too slow speed (suddenly)
REQ26
DETECT/PREVENT: Strong braking although not commanded
REQ92
DETECT/PREVENT: [T1] Tampering of Object List leads to Unjustified Stron...
REQ96
DETECT/PREVENT: [A6] Malware Infection

Figure 4.23: CyberSafety Analysis HP - Requirement Diagram for CSG1.

More specific requirements have been derived and presented in the requirement diagram, since the Intrusion Detection and Prevention System (IDPS) pattern has been considered the most important cybersecurity control with dependencies on safety. Each requirement is given an adequate description. With this definition, part of the CyberSafety Functional Concept is covered, as shown in Figure 4.24 and Figure 4.25.

The HP System Architecture Model in Medini was enhanced with IDPS system components and their relationships with Functional Safety elements according to the AUTOSAR Foundation Distributed IDPS concept [73]. In order to identify anomalies known as Security Event (SeV), the IDS Security Sensor element, illustrated as a blue box, should be placed in each logical component. This Security Events can be locally stored in the system for further analysis and forensic purposes by Security Event Memory (SeM),orange box. In the same time, SE can be further analyzed and qualified by IDS Manager (IdsM), represented by the black box. Finally, all Qualified Security Events can be sent by IDS Reporter (IdsR), represented by the dark purple box, to the back-end system, where using more advanced methods, including Machine Learning, an intrusion can be determined and a mitigation strategy planned, as visible in Figure 4.26.

Ansys Medini may be used to develop the CyberSafety Technical Concept for the HP system, which must satisfy all analyses and requirements. Since the HP system needs to meet the requirements for isolation, physical security, secure boot software protection, and encryption, a new element, called Secure Element, is suggested. It is a specialized chip designed to run a small number of applications and store encrypted and private data. It is secure by design from unauthorized access. It is used to carry out cryptographic operations in an isolated environment and contributes to the chain of trust. Each computing domain should have this

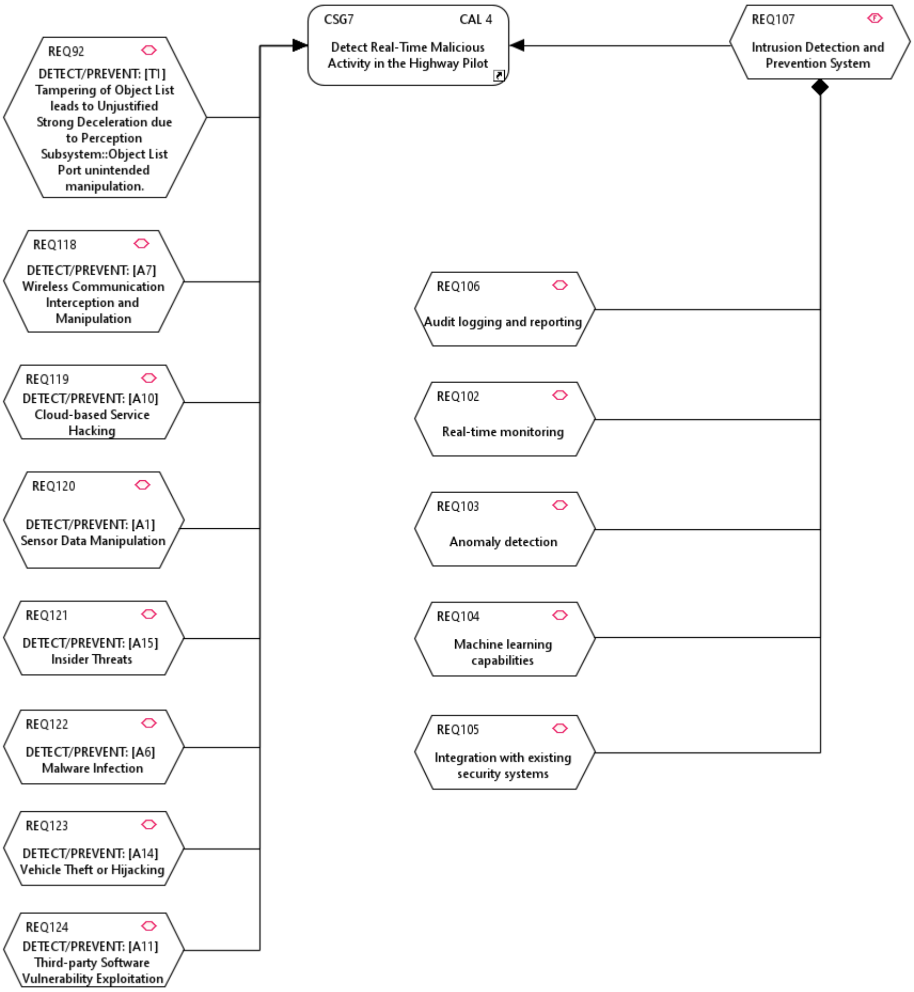
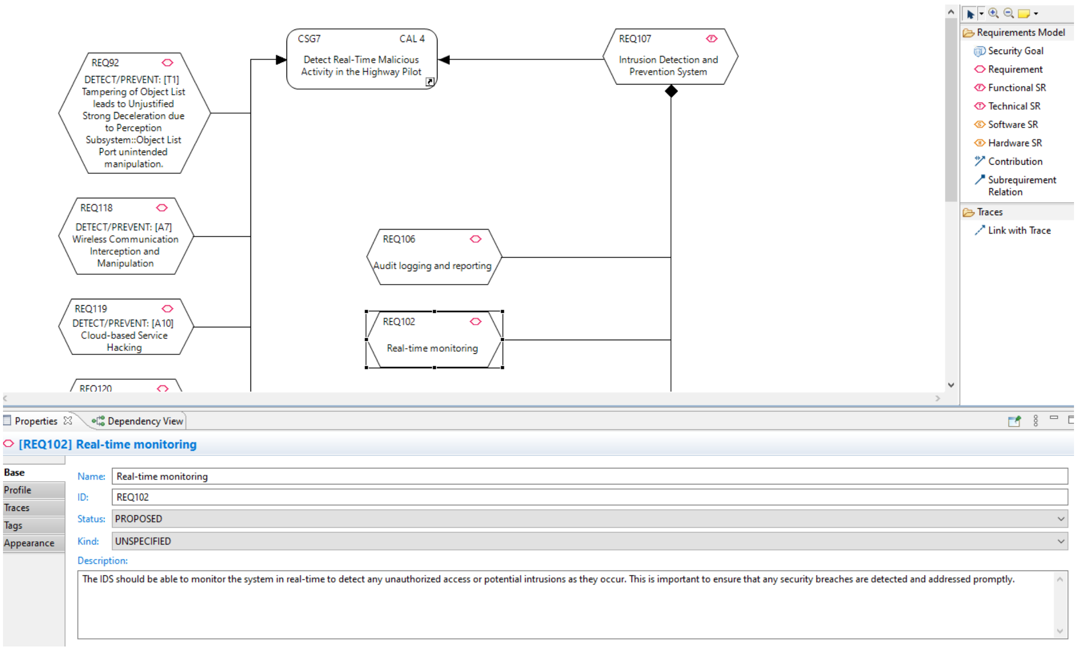

CSG7
CAL 4
Detect Real-Time Malicious Activity in the Highway Pilot
REQ107
Intrusion Detection and Prevention System
REQ92
DETECT/PREVENT: [T1] Tampering of Object List leads to Unjustified Strong Deceleration due to Perception Subsystem::Object List Port unintended manipulation.
REQ118
DETECT/PREVENT: [A7] Wireless Communication Interception and Manipulation
REQ119
DETECT/PREVENT: [A10] Cloud-based Service Hacking
REQ120
DETECT/PREVENT: [A1] Sensor Data Manipulation
REQ121
DETECT/PREVENT: [A15] Insider Threats
REQ122
DETECT/PREVENT: [A6] Malware Infection
REQ123
DETECT/PREVENT: [A14] Vehicle Theft or Hijacking
REQ124
DETECT/PREVENT: [A11] Third-party Software Vulnerability Exploitation
REQ106
Audit logging and reporting
REQ102
Real-time monitoring
REQ103
Anomaly detection
REQ104
Machine learning capabilities
REQ105
Integration with existing security systems

Figure 4.24: CyberSafety Analysis HP - Requirement Diagram for CSG7.

secure element, which in the case of HP would be the "Perception Soc" and "Operations Microcontroller", which can be seen in Figure 4.27.

In the context of system analysis, the CyberSafety framework represents a significant development by integrating key elements from CySe, FuSa, and SOTIF. Using the powerful Asnsys Medini tool, common activities were investigated and successfully implemented in the Highway Pilot system example. The analysis process encompassed the product development cycle, starting from the Item Definition phase and culminating in the Technical Concept phase. To fully validate the CyberSafety V-model components, including implementation, verification, and validation, additional tools may need to be explored. Nevertheless, the ultimate objective should be to identify a single tool capable of creating, implementing, verifying, and validating models, thus supporting the model-based system engineering paradigm. Adopting the CyberSafety approach is essential for conducting comprehensive and meticulous analyses in light of the increasing complexity of modern systems.

In summary, the CyberSafety framework represents a major advance in system analysis by drawing on the best practices of CySe, FuSa, and SOTIF. Using the Asnsys Medini tool, common activities in the example of the Highway Pilot system were successfully identified, and the product development cycle from


REQ92
DETECT/PREVENT: [T1] Tampering of Object List leads to Unjustified Strong Deceleration due to Perception Subsystem::Object List Port unintended manipulation.
REQ118
DETECT/PREVENT: [A7] Wireless Communication Interception and Manipulation
REQ119
DETECT/PREVENT: [A10] Cloud-based Service Hacking
REQ120
CSG7
CAL 4
Detect Real-Time Malicious Activity in the Highway Pilot
REQ107
Intrusion Detection and Prevention System
REQ106
Audit logging and reporting
REQ102
Real-time monitoring
Requirements Model
Security Goal
Requirement
Functional SR
Technical SR
Software SR
Hardware SR
Contribution
Subrequirement Relation
Traces
Link with Trace
Properties
Dependency View
Base
Profile
Traces
Tags
Appearance

[REQ102] Real-time monitoring

Name: Real-time monitoring

ID: REQ102

Status: PROPOSED

Kind: UNSPECIFIED

Description:

The IDS should be able to monitor the system in real-time to detect any unauthorized access or potential intrusions as they occur. This is important to ensure that any security breaches are detected and addressed promptly.

Figure 4.25: CyberSafety Analysis HP - Requirement Description for CSG9.

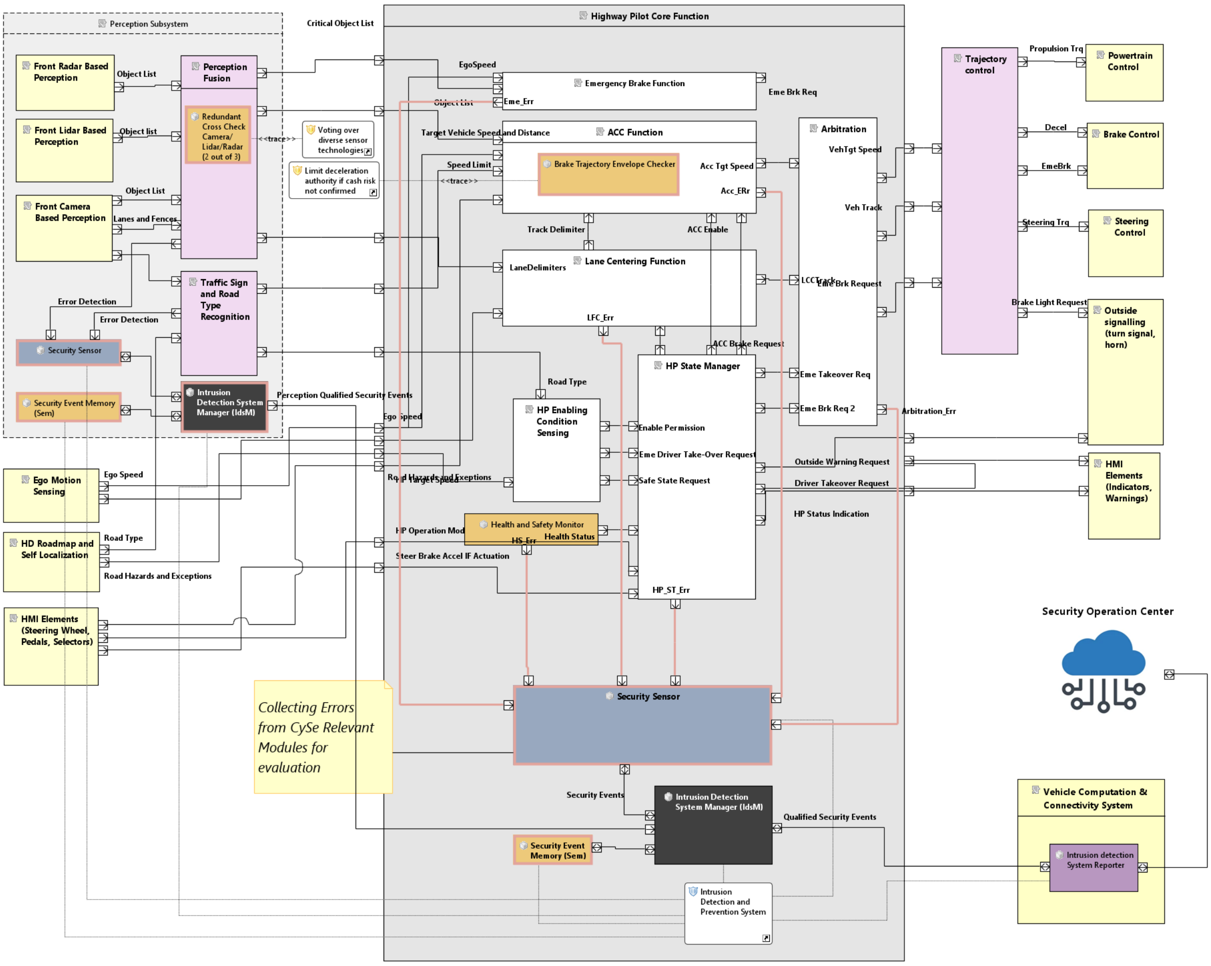

Perception Subsystem
Front Radar Based Perception
Object List
Front Lidar Based Perception
Object list
Front Camera Based Perception
Object List
Lanes and Fences
Perception Fusion
Redundant Cross Check Camera/ Lidar/Radar (2 out of 3)
<<trace>>
Voting over diverse sensor technologies
Limit deceleration authority if cash risk not confirmed
<<trace>>
Traffic Sign and Road Type Recognition
Error Detection
Error Detection
Security Sensor
Security Event Memory (Sem)
Intrusion Detection System Manager (IdsM)
Perception Qualified Security Events
Critical Object List
Highway Pilot Core Function
EgoSpeed
Emergency Brake Function
Object List
Eme_Err
Eme Brk Req
Target Vehicle Speed and Distance
ACC Function
Speed Limit
Brake Trajectory Envelope Checker
Acc Tgt Speed
Acc_ERr
Track Delimiter
ACC Enable
LaneDelimiters
Lane Centering Function
LFC_Err
ACC Brake Request
Arbitration
VehTgt Speed
Veh Track
LCCTrack
Eme Brk Request
Eme Takeover Req
Eme Brk Req 2
Arbitration_Err
Trajectory control
Propulsion Trq
Powertrain Control
Decel
EmeBrk
Brake Control
Steering Trq
Steering Control
Brake Light Request
Outside signalling (turn signal, horn)
HMI Elements (Indicators, Warnings)
Road Type
HP State Manager
HP Enabling Condition Sensing
Ego Speed
Enable Permission
Eme Driver Take-Over Request
Safe State Request
Outside Warning Request
Driver Takeover Request
HP Status Indication
Road Hazards and Exeptions
HP Target Speed
HP Operation Mod
Health and Safety Monitor
HS_Err
Health Status
Steer Brake Accel IF Actuation
HP_ST_Err
Ego Motion Sensing
Ego Speed
HD Roadmap and Self Localization
Road Type
Road Hazards and Exceptions
HMI Elements (Steering Wheel, Pedals, Selectors)
Collecting Errors from CySe Relevant Modules for evaluation
Security Sensor
Security Events
Intrusion Detection System Manager (IdsM)
Qualified Security Events
Security Event Memory (Sem)
Intrusion Detection and Prevention System
Security Operation Center
Vehicle Computation & Connectivity System
Intrusion detection System Reporter

Figure 4.26: CyberSafety Analysis HP - Safety and Security Mechanisms.

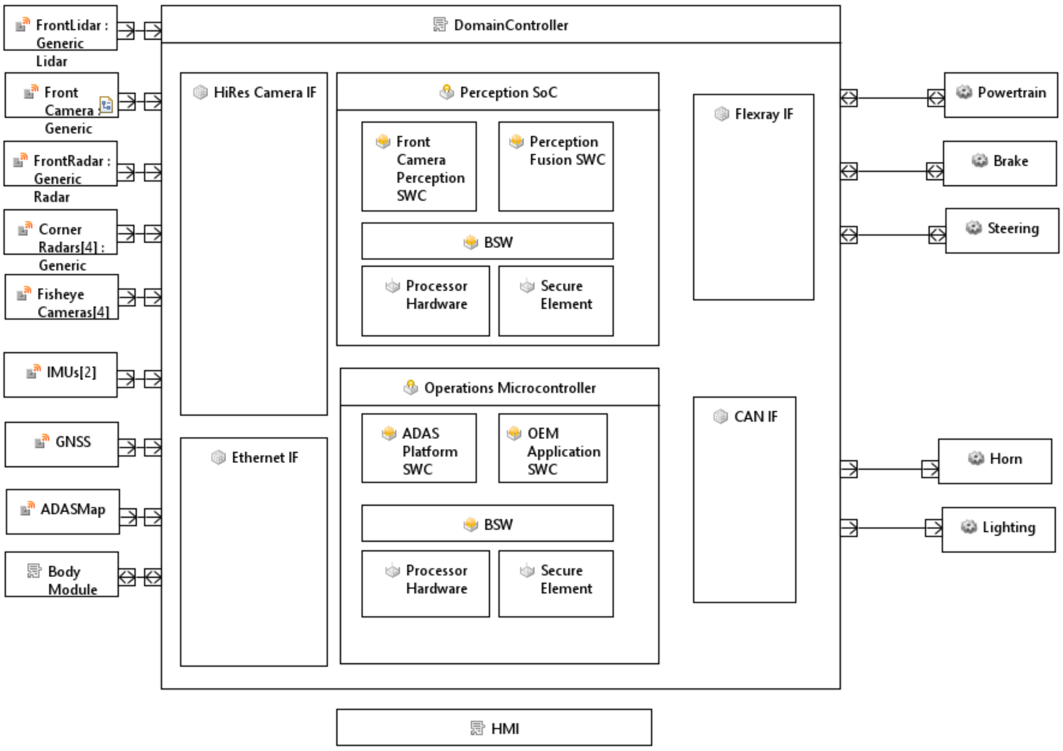


Figure 4.27: CyberSafety Analysis HP - CyberSafety Technical Concept.

Item Definition to Technical Concept was examined. Further exploration of various tools may be required to fully validate the components of the CyberSafety V-model, but the ultimate aim is to identify a single tool capable of handling all aspects of model creation, implementation, verification, and validation. Only by adopting the CyberSafety approach can we perform thorough and comprehensive analyzes of increasingly complex systems.

4.2 Interpreting Highway Pilot Case Study Metrics

The CyberSafety analysis performed using Ansys Medini during the design phase of the V-model provides valuable insights that support the notion of a joint analysis approach, as shown in Figure 4.28. The results of this analysis demonstrate its efficacy in delivering comprehensive results, optimizing overall efforts, and mitigating CyberSafety risks.

In this study, the main emphasis was on the synergistic integration of Threat and Risk Assessment (TARA) and Hazard and Risk Assessment (HARA) activities, complemented by the application of the SOTIF study. The objective was to ensure a comprehensive assessment of the safety and security aspects in a unified manner.

Upon the identification of a shared system Item, comprising 12 fundamental elements, 26 potential hazards, and derived 14 damage scenarios were meticulously assessed. Moreover, 45 system assets were examined, along with their associated Cybersecurity Properties. Remarkably, the use of the Medini Tool led to the identification of a staggering 943 threat scenarios for this system, necessitating further in-depth evaluations.The largest number of threats were connected with Loss of Authenticity and Loss of integrity,

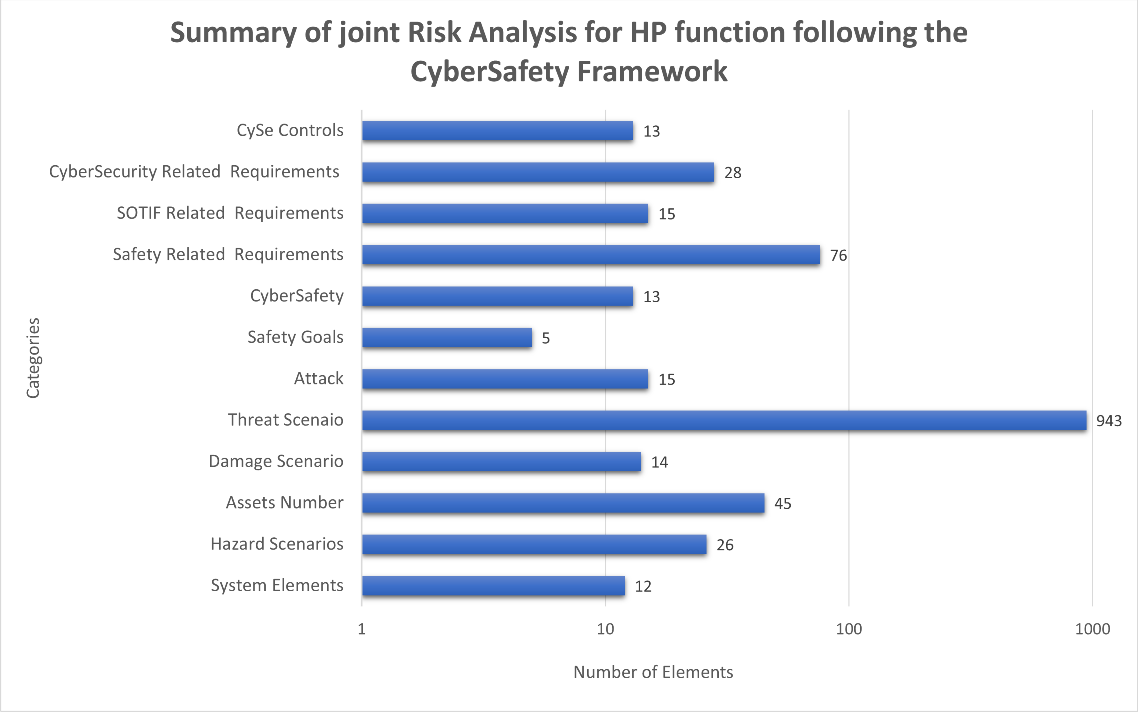


Figure 4.28: Summary of joint Risk Analysis for HP function following the CyberSafety framework.

respectively 254 and 251, what is represented in Figure 4.29. For all of the losses 15 basic Attacks were defined and further evaluated.

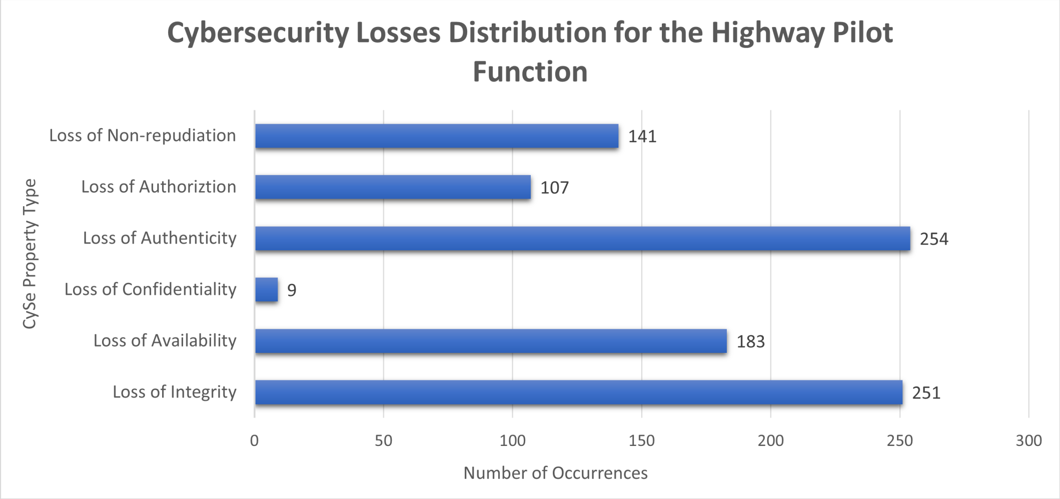


Figure 4.29: Cybersecurity Losses Distribution for the Highway Pilot Function.

To effectively manage the exhaustive scope of potential threats, the effort concentration was on threats linked to prominent attacks, such as Denial-of-Service or Tampering, with a specific focus on the impact on Availability, a crucial cybersecurity property. Consequently, 13 overarching CyberSafety goals were identified, which, in turn, led to the formulation of 28 additional requirements tailored to fulfill these goals.

Finally, in pursuit of a comprehensive evaluation, 13 cybersecurity controls were devised, drawing on the established Security Pattern Definition for Automotive Systems. These controls were meticulously applied to enhance the overall security posture of the system with the main focus on the Intrusion Detection and Prevention System (IDPS).

The study reinforces the notion that the joint TARA and HARA approach, augmented by SOTIF considerations, provides a solid foundation to identify and address potential security and safety challenges. The cohesive integration of CyberSafety goals, requirements, and cybersecurity controls further enhances the overall resilience of the system against multifaceted threats, ensuring a safer and more secure operation. These findings underscore the importance of a holistic approach to risk assessment and mitigation in complex engineering systems, particularly in the context of safety-critical domains such as automotive systems.

4.2.1 Cybersecurity Impact on Safety

During the evaluation of Damage Scenarios, the Impact Rating plays a crucial role, adhering to the guidelines set forth in [13]. This rating offers valuable insights into the potential impact on various aspects, including Safety, Financial, Operational, and Privacy, for the item analyzed, which in this case is the HP system.

For the HP system, all the identified Damage Scenarios have a notable impact on system safety, with ratings falling into both the moderate and severe categories. Of these scenarios, 8 are associated with severe impacts on system safety, as observed in Figure 4.30. This significant connection between the Damage Scenarios and system safety underscores the importance of linking the analysis to the FuSa and SOTIF domains.

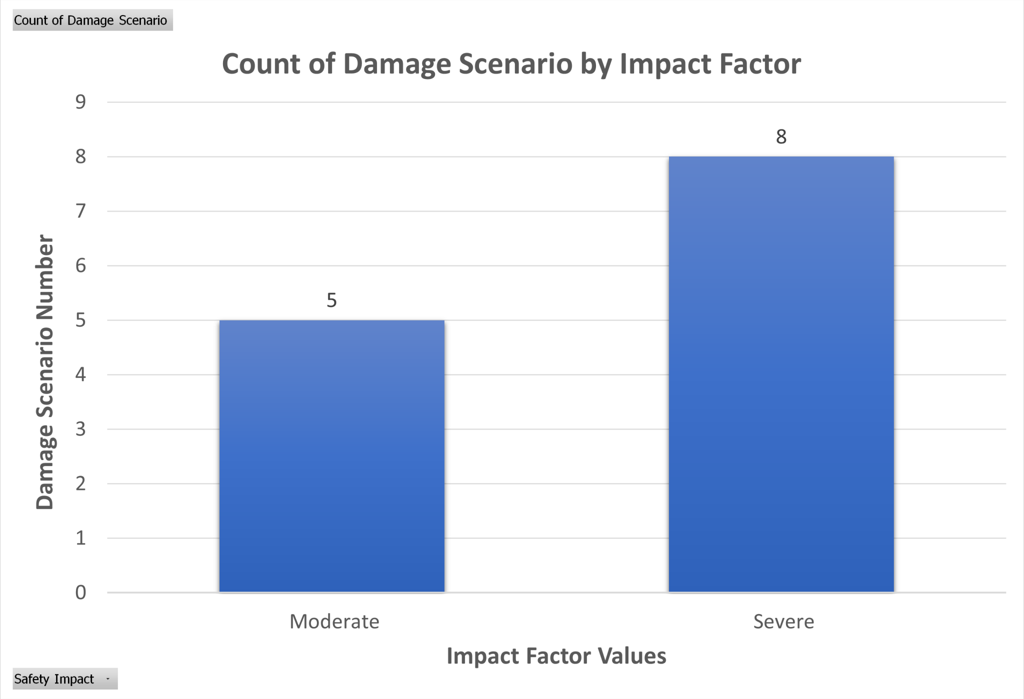


Figure 4.30: Count of Damage Scenario by Impact Factor.

The identification of common goals and requirements becomes particularly crucial, as they serve as essential components of both the safety and security posture of the HP system. The shared goals and requirements address critical aspects that influence both safety and security, resulting in a cohesive approach that serves the overall resilience and robustness of the system.

The strong connection between the identified Damage Scenarios and FuSa analysis and requirements further validates the efficacy of adopting a CyberSafety framework for the HP system. Shared goals and requirements act as essential pillars in enhancing both safety and security, reinforcing the commitment to delivering a reliable, safe, and secure system.

By considering the Impact Rating, the analysis gains deeper insight into the potential consequences of the identified Damage Scenarios and their ramifications on the overall functionality and well-being of the HP system. The focus on both safety and security ensures that appropriate measures are implemented to minimize risks, maintain system integrity, and provide a safe and secure environment for users and occupants.

4.2.2 Attack Analysis HP System Attack Analysis

When summarizing the attacks identified for the HP system, a comprehensive evaluation was carried out, taking into account various factors to determine the Attack Feasibility Rating, following the attack potential-based approach as outlined in ISO 21434 Annex G.Table 4.3

The superiority of attack-based potential analysis over other methods lies in its ability to provide a more comprehensive and context-specific evaluation of cybersecurity risks and potential threats facing a system. While other methodologies, such as generic risk assessments or vulnerability scanning, offer valuable insight, attack-based potential analysis adds specificity and depth to the evaluation process. By focusing on actual attack scenarios and their feasibility, organizations can implement more targeted and effective security measures, ultimately enhancing the overall cybersecurity posture and reducing the likelihood of successful cybernetics.

The core parameters considered in this assessment include:

- **Elapsed Time** - includes the time to identify a vulnerability and develop and (successfully) apply an exploit;

- **Specialist expertise** - The level of expertise possessed by attackers influences the complexity and sophistication of their methods. Attacks carried out by highly skilled experts may be more challenging to detect and counteract;

- **Knowledge of the Item or Component** - An attacker's understanding of the targeted system's vulnerabilities and weaknesses significantly impacts their likelihood of success;

- **Window of Opportunity** - The duration during which a system is exposed and vulnerable to attacks plays a crucial role in assessing the potential for successful exploitation;

- **Equipment** - The resources and tools available to attackers affect the range of attack strategies they can employ, thus influencing the feasibility of attacks.

By conducting a detailed analysis of the number of attacks based on the elapsed time parameter, it becomes evident that a significant portion of these attacks can be executed within a short time frame, typically less than a day, as seen in Figure 4.31. Such vulnerabilities, where the identification, preparation, and execution of the exploit can be accomplished rapidly, are commonly referred to as "0-day vulnerabilities."

Given the criticality of the safety aspects within the entire HP system, it is imperative to prioritize the mitigation of these 0-day vulnerabilities. Addressing these vulnerabilities in the initial stages of system development and deployment is of utmost importance to bolster the overall security posture and safeguard against potential threats.

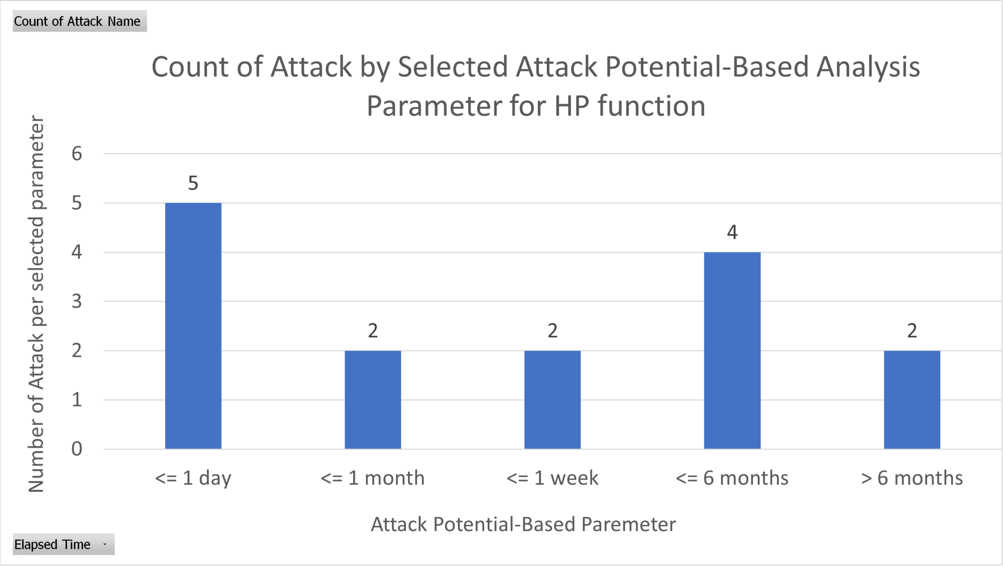


Figure 4.31: Count of Attack by Attack Elapsed Time.

In addition to the time-sensitive nature of the identified vulnerabilities, it is crucial to acknowledge that the HP function demands a high level of expertise and domain knowledge from potential attackers. To effectively analyze the system, comprehend its intricacies, and discern the various signals and dependencies, attackers must possess significant expertise in the relevant domain.

Figure 4.32 illustrates that a majority of the identified attacks (5 attacks) require the level of expertise typically associated with "Expert" attackers, while an additional 6 attacks necessitate the proficiency level of "Proficient" attackers. These findings emphasize that the HP system is potentially exposed to sophisticated and knowledgeable adversaries, capable of executing targeted attacks that exploit system vulnerabilities with precision.

Considering the skill level required by potential attackers, it becomes evident that the HP system's security must be fortified with advanced defense mechanisms and stringent security controls. Combining the understanding of time-critical vulnerabilities and the demand for specialized expertise, it is imperative to prioritize proactive security measures to thwart potential attacks effectively.

Indeed, while an attack on the HP system does require a certain level of expertise and knowledge of the system, it is crucial to recognize that certain basic information is publicly accessible, particularly concerning the utilized sensors, their localization, and fundamental knowledge about the data transmitted to the main component.

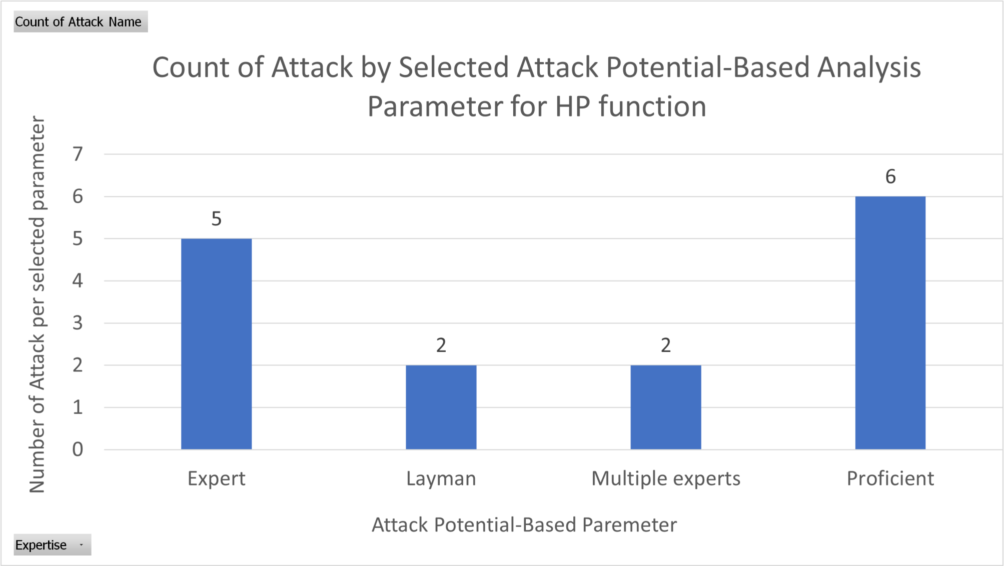


Figure 4.32: Count of Attack by Attack Expertise.

Figure 4.33 illustrates that the publicly available information lays the foundation for potential attackers to understand the basic components and interactions of the system. However, it is important to note that the truly sensitive and confidential information is residing within the fusion and decision algorithms, which constitute the core components of the HP function.

To protect these critical algorithms and proprietary information, more sophisticated and robust security measures must be deployed. Given the significance of the fusion and decision algorithms to the function's core functionality, protecting these confidential data becomes paramount to ensuring the system's overall security and reliability.

The insights derived from Figure 4.33 highlight the need for a strategic balance between publicly available information and protecting the core elements of the HP function. Through comprehensive security measures and ongoing vigilance, the system can effectively defend itself against both external and internal threats, ensuring the continuous delivery of safe and secure driving experiences.

The analysis of the vehicle system's "Window of Opportunity" parameter presents a challenging aspect to mitigate. The vehicle often remains stationary, providing potential attackers with ample time and opportunity to analyze the system. However, it is interesting to note that despite this extended window of opportunity, most of the attacks on this specific system require a "Moderate" window of opportunity. This suggests that attacks are mainly focused on instances when the vehicle is in motion, activating the HP system, what is shown in Figure 4.34.

Nevertheless, when the vehicle is parked in a publicly accessible space, it exposes its external interfaces, offering relatively easy access to potential attackers. This becomes a critical attack path, providing unauthorized individuals with the opportunity to break into the system, manipulate the components of the HP system, or even install malicious software.

Given the scenario of a parked vehicle and the accessibility of its external interfaces, it is essential to implement robust security measures to fortify these entry points. This includes physical security measures,

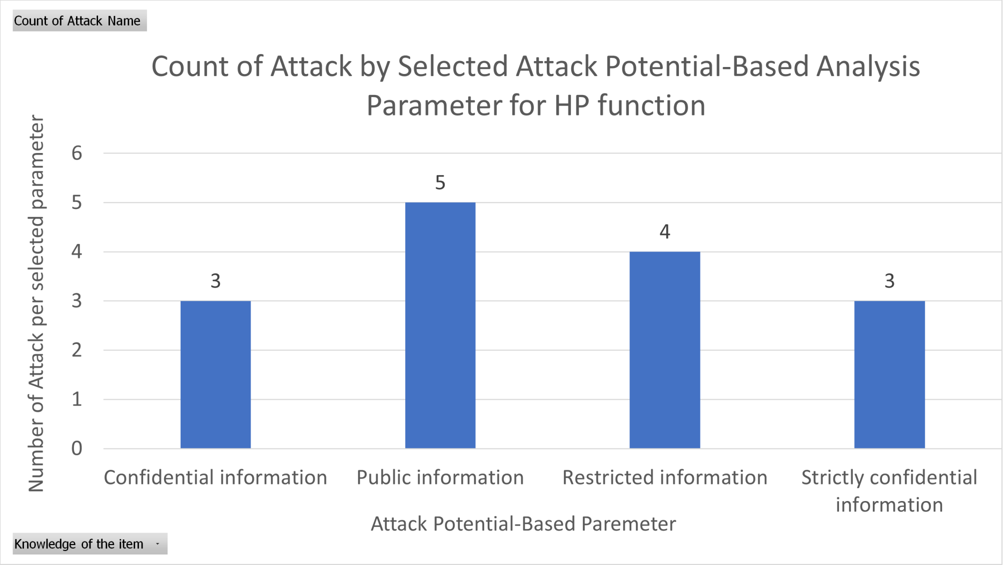


Figure 4.33: Count of Attack by Knowledge of the item or component.

such as tamper-resistant locks, as well as cybersecurity protocols to prevent unauthorized access to the system's interfaces.

Moreover, deploying intrusion detection systems and real-time monitoring can bolster the system's ability to detect and respond swiftly to any potential breaches.

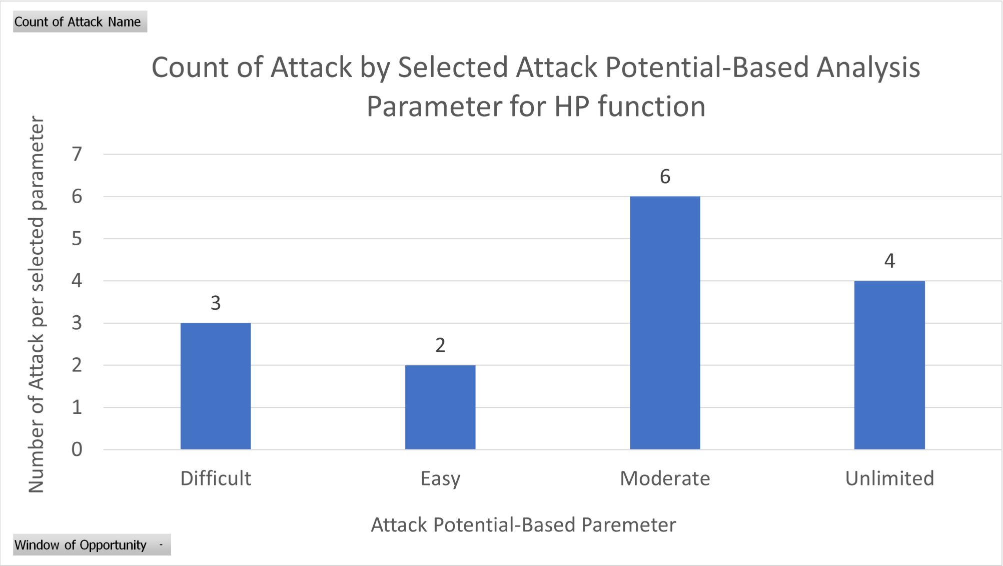


Figure 4.34: Count of Attack by Window of opportunity.

The automotive industry, being a specialized domain, has traditionally relied on specific automotive protocols and equipment for the development of automotive functions. As a result, many attacks targeting automotive systems typically require specialized equipment and knowledge. However, with the advent of remote connectivity and the adoption of Ethernet as a backbone network in modern vehicles, there has been a shift towards the utilization of more commonly used standard hacking tools.

Figure 4.35 provides valuable insight, revealing that a considerable number of attacks identified for the HP system only require standard equipment commonly employed in hacking practices. This indicates a potential shift towards leveraging more readily available tools for exploiting vulnerabilities in the automotive system.

As these attacks that rely solely on standard equipment become more prevalent, it becomes imperative to prioritize their analysis and mitigation. Ensuring the security of the system against such attacks is of paramount importance, as their widespread accessibility could increase the risk of successful intrusions.

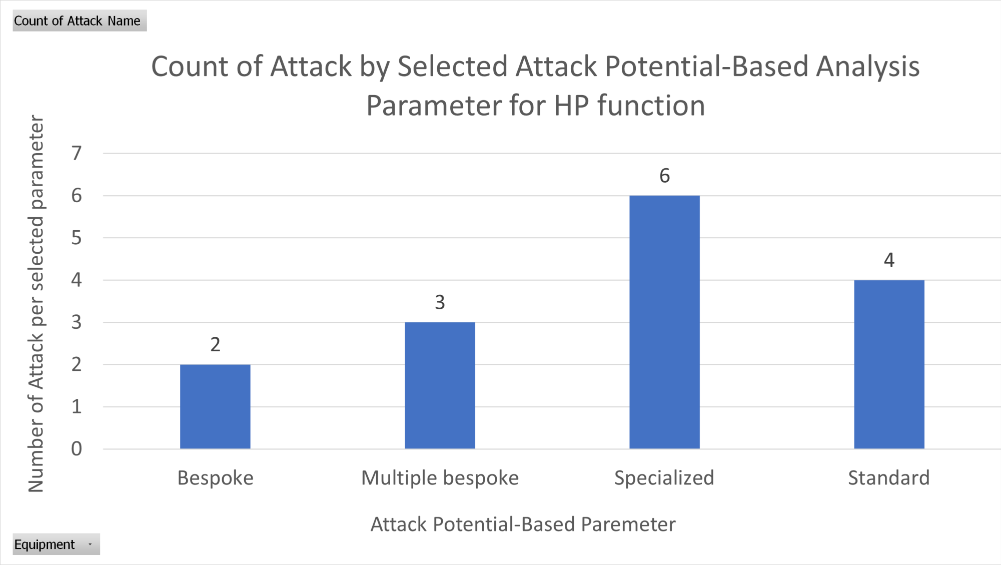


Figure 4.35: Count of Attack by needed Equipment.

The combination of Elapsed Time and Expertise knowledge in Figure 4.36 provides a crucial indication that vulnerabilities within the system can be exploited by both Layman and Proficient hackers. This finding underscores the critical importance of implementing a robust mitigation strategy to address attacks that can be executed by individuals with varying levels of expertise.

In particular, the presence of attacks that can be conducted by Layman hackers with relatively limited knowledge and skills underscores the need for immediate attention. Such attacks may have an immediate impact on the system and can potentially lead to severe consequences if not addressed promptly.

In response to this critical insight, an effective mitigation strategy should be devised and deployed to safeguard the system against both Layman and Proficient attackers.

The further analysis focused on calculating the Attack Feasibility Rating (AFR) for each attack identified for the HP system, considering the following equation based on [13].

The AFR provides a quantitative measure of the feasibility of each attack, considering the common elements or factors shared among the attacks compared to the total number of elements in the system. Higher AFR values indicate that the attack is more feasible due to the presence of shared items, which may contribute to a higher likelihood of successful exploitation.

By applying equation (4.1) to each identified attack in the HP system, it becomes possible to rank attacks based on their feasibility, prioritize mitigation efforts for attacks with higher AFR values, and effectively allocate resources to address the most critical vulnerabilities. For each parameter from 4.1, numerical values

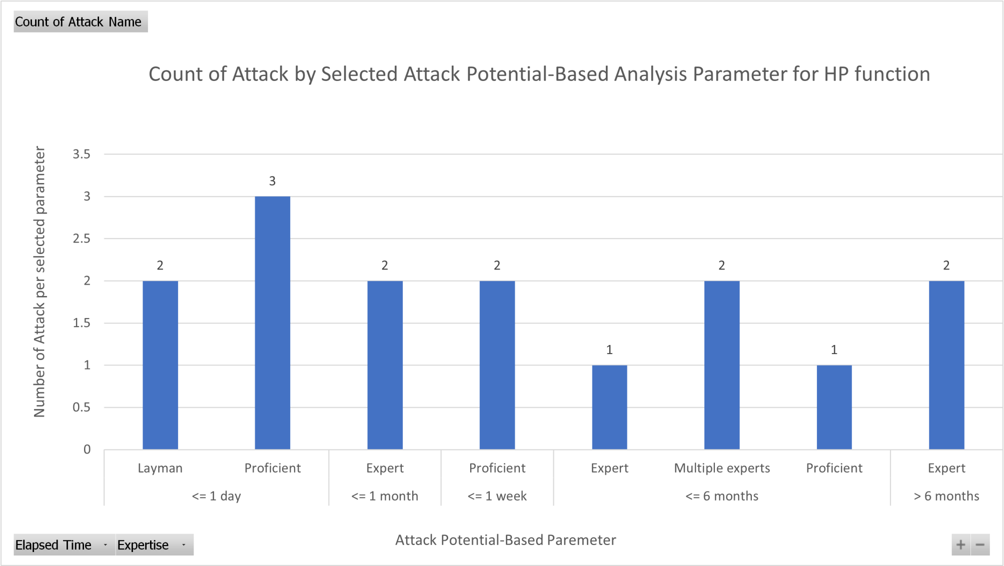


Figure 4.36: Count of Attack by Elapsed Time and Expertise.

can be defined. For this analysis, an example of the aggregation of the attack potential based on Annex G from [13] was used. Table 4.3. This data-driven approach helps make informed decisions to enhance the overall cybersecurity posture of the HP system and ensure its safe and secure operation.

$$AFR = \sum_{i=1}^{5} X_i = X_1 + X_2 + X_3 + X_4 + X_5 \tag{4.1}$$

where:

X_1 represents Elapsed Time (ET),

X_2 represents Expertise (EXP),

X_3 represents Knowledge of the item (KIT),

X_4 represents Window of Opportunity (WoO),

X_5 represents Equipment (EQP).

The mapping of the final Attack Feasibility Rating (AFR) is carried out using the guidelines provided in Table 4.4, as specified in [13]. This table defines the rating categories and their corresponding value ranges. By associating the calculated AFR values with the appropriate rating category, the severity and feasibility of each attack can be quantified and classified.

Using Table 4.4, the identified attacks are categorized into different levels, such as "High," "Medium", "Low", or "Very Low," based on their AFR values. The AFR rating obtained for each attack serves as a valuable tool for prioritizing mitigation efforts and effectively allocating resources.

Using the ISO 21434 guidelines and Table 4.4 ensures a standardized approach to evaluating the feasibility of attacks, making it easier for stakeholders to understand the security implications and take appropriate actions to address the identified vulnerabilities. This systematic approach helps strengthen the cybersecurity defenses of the HP system and contributes to the assurance of its overall safety and security.

Table 4.3: Example aggregation of attack potential based on Table G.6 from [13].

Elapsed time		**Specialist expertise**		**Knowl. of the item or component**		**Window of opportunity**		**Equipment**	
Enum.	**Val.**	**Enum.**	**Val.**	**Enum.**	**Val.**	**Enum.**	**Val.**	**Enum.**	**Val**
≤1 day	0	Layman	0	Public	0	Unlimited	0	Standard	0
≤1 week	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
≤1 month	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
≤6 months	17	Multiple experts	8	Strictly confidential	11	Difficult/ none	10	Multiple bespoke	9
>6 months	19								

Table 4.4: Example attack potential mapping. Based on Table G.7 from [13].

Rating	**Values**
High	0 – 9
	10 – 13
Medium	14 – 19
Low	20 – 24
Very Low	≥ 25

The analysis of the AFR has provided valuable information, as shown in Figure 4.37. The ranking of AFR values has shed light on the criticality of various identified attacks, allowing a focused approach to cybersecurity mitigation efforts.

It is notable that certain attacks, such as Social Engineering and Traffic Sign Spoofing, have received high AFR scores. However, it is important to recognize that these attacks fall outside the system boundaries and are not within the scope of cybersecurity mechanisms for this specific system. Therefore, the focus of mitigation efforts should remain directed towards attacks within the system's operational domain.

The analysis has highlighted the significance of Denial-of-Service (DoS) attacks, with an AFR of 8, as one of the most critical threats to the system. These attacks can severely impact the availability and functionality of the HP system, necessitating robust countermeasures to protect against their potential exploitation.

Additionally, attacks related to external data gathering (e.g., GPS, Sensor Data) have been identified as posing considerable risks to the system, particularly concerning the accurate calculation of routes when the HP system is active. Mitigating these risks is crucial to ensure the safe and reliable operation of the HP function.

Furthermore, physical access attacks have been recognized as potentially leading to severe consequences for the system, including tampering with the Human-Machine Interface (HMI). Preventing physical access to the vehicle is a crucial aspect of the overall cybersecurity strategy, as such attacks can result in unauthorized control and manipulation of critical system components.

It is essential to consider the chain of events that can lead to certain attacks, such as vehicle hijacking or theft, as highlighted in the analysis. Addressing vulnerabilities in these stages is vital to breaking the attack chain and preventing possible physical access attacks.

By understanding the ranking of AFR values and the specific risks posed by each attack, stakeholders can effectively allocate resources to implement targeted security measures. Mitigating the most critical threats will strengthen the overall cybersecurity posture of the HP system, enhancing its resilience against potential cyber incidents, and ensuring the safety and security of the system's operation.

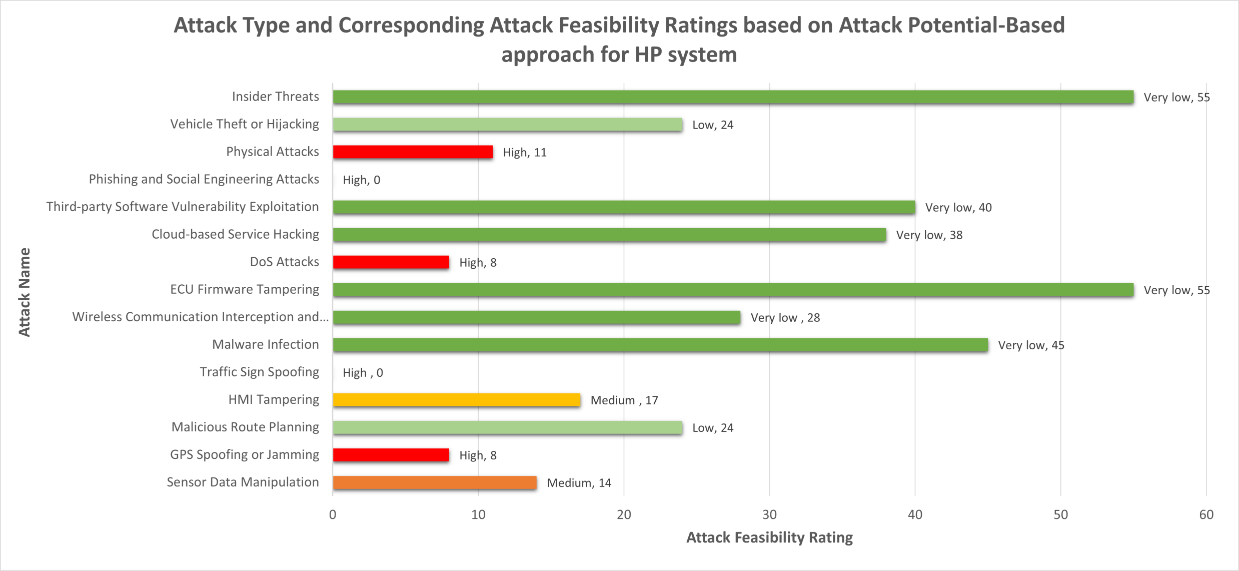


Figure 4.37: Attack Type and Corresponding Attack Feasibility Ratings based on Attack Potential-Based approach for HP system.

The introduction of security meditations to minimize identified risks is a crucial step in enhancing the overall cybersecurity posture of the HP system. To achieve this, the use of security patterns is employed as comprehensive and state-of-the-art solutions to address the defined CySe (Cybersecurity) related threats effectively.

Security patterns offer well-established and proven methodologies to counter various types of cyber-threats. By adopting these patterns, organizations can implement robust and standardized security measures, ensuring a consistent and structured approach to cybersecurity.

To further optimize the selection and implementation of security controls, the Attack-Potential-Based approach is utilized. This involves analyzing each security control provided based on its effectiveness in mitigating potential attacks. AFR is calculated for each security control, providing a quantitative measure of its impact on reducing the feasibility of attacks.

By assessing the AFR for each security control, stakeholders can prioritize and focus on controls that have a higher potential for reducing the overall risk. Security controls with lower AFR values are considered more effective in mitigating attacks and are thus given higher priority in the implementation process.

The use of the AFR per security control presents a valuable opportunity to reduce risk by strategically applying specific security measures to counter identified attacks. With this approach, Ansys Medini provides informative visualizations to users, indicating how the AFR is reduced for particular attack paths using a color-based convention, as depicted in Figure 4.20.

The color-based convention enables users to quickly identify the effectiveness of individual security controls in mitigating specific attack scenarios. By visualizing the reduction in AFR, users can understand the direct impact of each security control on the overall feasibility of an attack.

When a security control is applied to an attack path, the corresponding reduction in AFR is represented by a distinct color code. A more significant reduction in AFR is indicated by a color that stands out, visually highlighting the effectiveness of security control in thwarting the attack.

This interactive and intuitive visualization empowers users to make informed decisions regarding the selection and deployment of security controls. By identifying and implementing the most effective controls for specific attack paths, overall risk is systematically reduced, contributing to a more robust cybersecurity defense.

The evaluation of the defined Security Controls has provided valuable information on their potential effectiveness in mitigating cyberthreats. The analysis assumes that the majority of these controls require more than 6 months for an attacker to successfully exploit them. Additionally, it is based on the reasonable assumption that the probability of a 0-day vulnerability on a correctly implemented Security Control is extremely low, as shown in Figure 4.38.

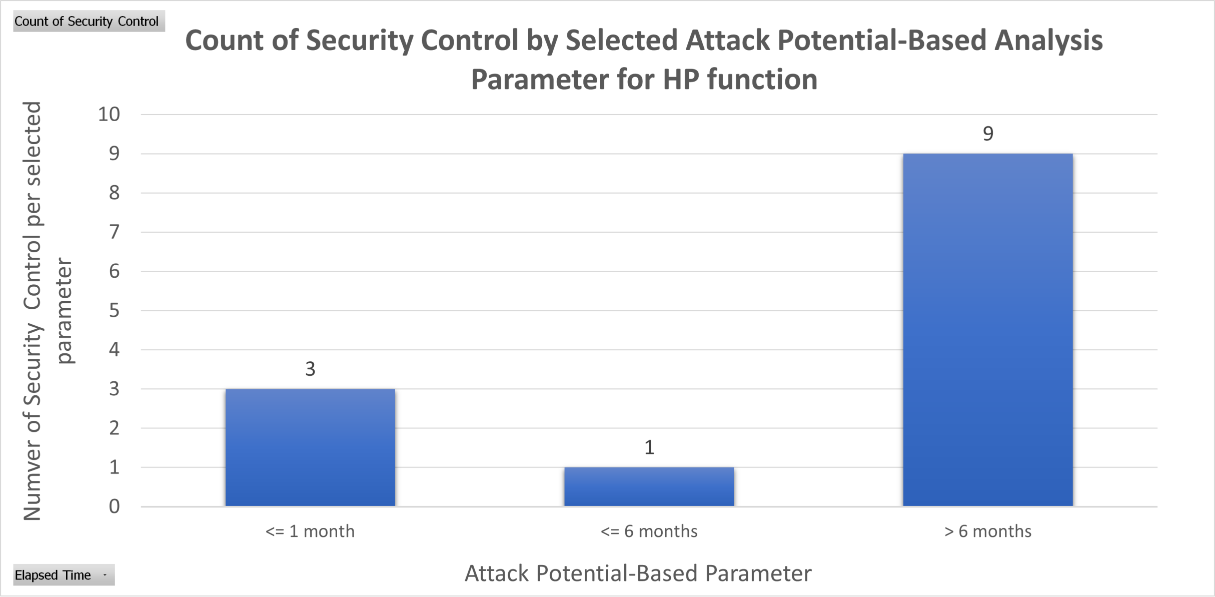


Figure 4.38: Count of Security Control by Elapsed Time.

Controls that demand more than 6 months for successful exploitation, showcasing their strength in providing long-term protection against cyberthreats. The extended elapsed time significantly reduces the likelihood of successful attacks, bolstering the system's overall cybersecurity defense.

The assumption that the defined Security Controls employ state-of-the-art solutions and secure cryptography adds a significant layer of protection to the HP system. Such advanced measures make it considerably challenging for potential attackers to break the implemented controls.

Given the complexity and sophistication of these security measures, the analysis assumes that multiple expert-level knowledge and expertise are required to breach the Security Controls successfully, as presented in Figure 4.39. This assumption is well-founded, as secure cryptography and advanced solutions are designed to resist attacks from knowledgeable and skilled adversaries.

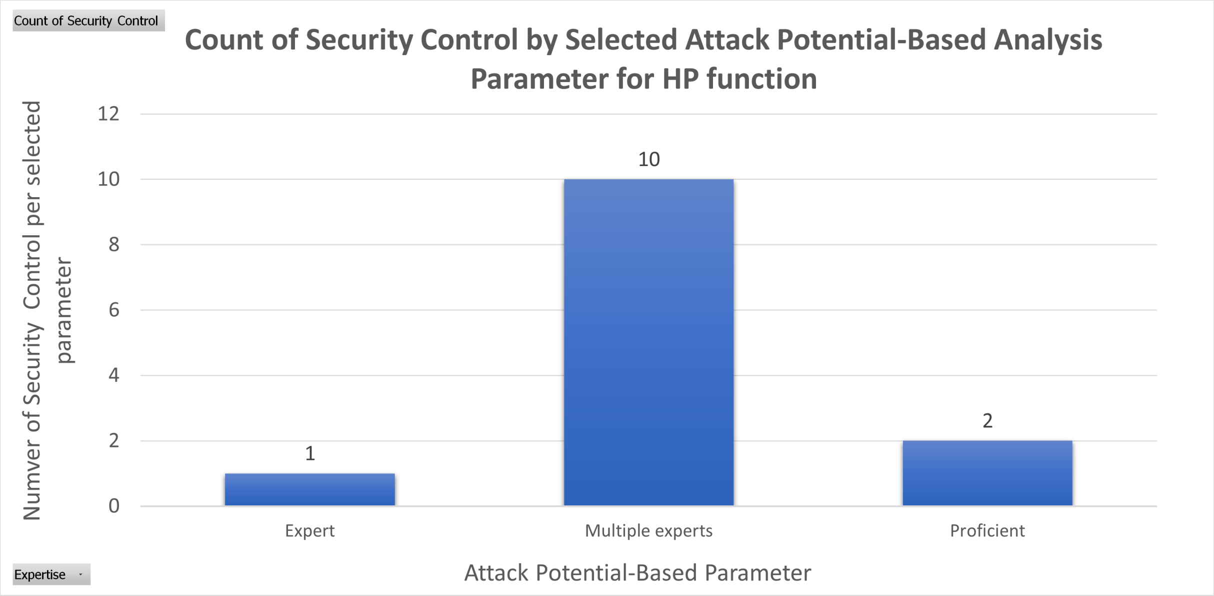


Figure 4.39: Count of Security Control by needed Expertise.

The completion of the AFR calculation for the defined Security Controls involves making specific assumptions about their properties. These assumptions contribute to understanding the feasibility of potential attacks and the effectiveness of controls to mitigate them.

Detailed knowledge of the applied security measures is assumed to be strictly confidential. This confidentiality adds a layer of protection, as potential attackers would face significant challenges in obtaining critical information about the security mechanisms, what can be seen in Figure 4.40.

The Security Mechanisms are designed to resist long exposure to potential attacks. As a result, the window of opportunity for attackers is significantly reduced, making it difficult for them to exploit vulnerabilities, as summarized in Figure 4.41.

To breach the Security Mechanisms, it is assumed that specialized and bespoke tools are required, and such equipment is not freely available to potential attackers. This assumption raises the bar for attackers, making it challenging for them to carry out successful attacks, as summarized in Figure 4.42.

By incorporating all of the mentioned assumptions into the AFR calculation for the Security Controls, the analysis gains a more comprehensive understanding of the system's resilience against cyberthreats. The identified Security Controls are designed to be robust, resistant to prolonged attacks, and dependent on confidential knowledge and specialized equipment. These attributes significantly contribute to reducing the feasibility of the attack and improving the overall cybersecurity posture of the HP system.

The application of the best-suited Security Controls on the analyzed Attack Paths is a critical step in mitigating identified risks and enhancing the overall cybersecurity resilience of the HP system. By strategically

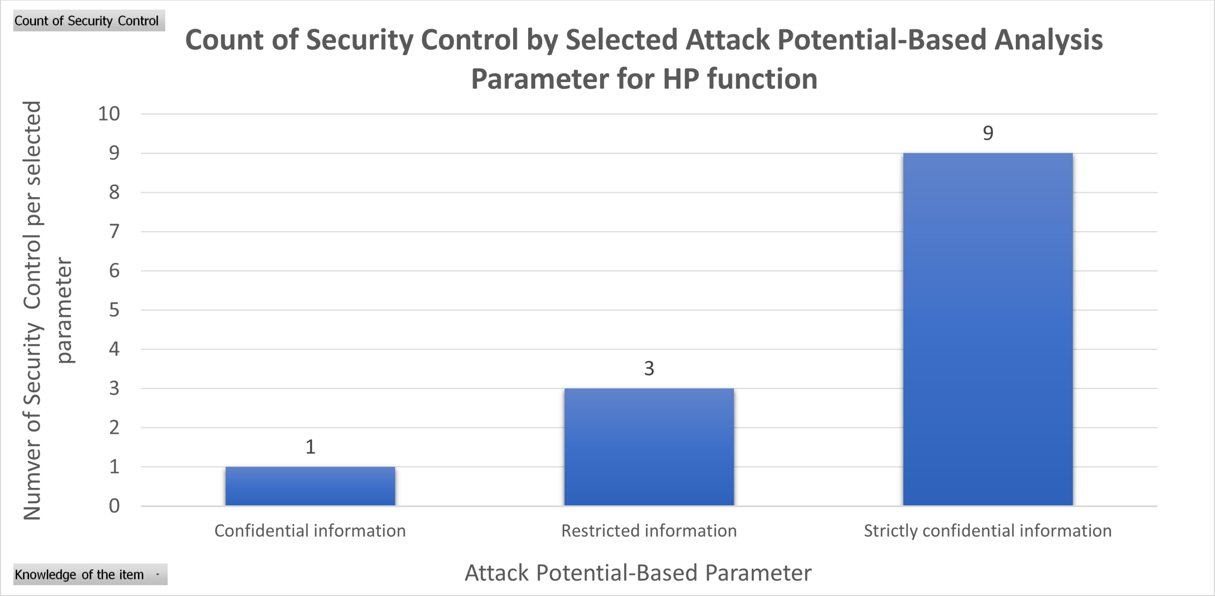


Figure 4.40: Count of Security Control by Knowledge of an item or component.

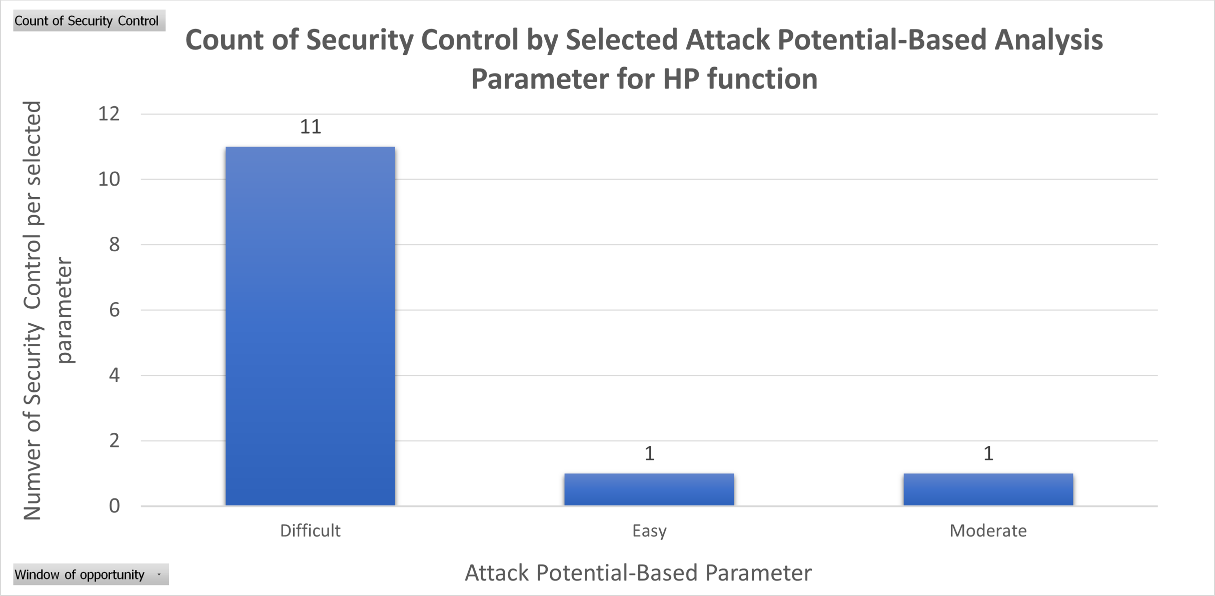


Figure 4.41: Count of Security Control by Window of opportunity.

implementing these controls, the initial system's vulnerability to the most dangerous attacks is significantly reduced, translating high and medium risks to very low, as observed in Figure 4.43.

The selection of the best-suited Security Controls is based on their respective AFR and their effectiveness in countering specific attack scenarios. Controls with lower AFR values are prioritized for implementation, as they demonstrate a higher potential for reducing attack feasibility and improving the system's overall security posture.

Through this approach, the most critical attack paths are fortified against potential cyberthreats. By addressing vulnerabilities and applying effective Security Controls, the system gains robust protection, making it more resilient to attacks and ensuring its safe and secure operation.

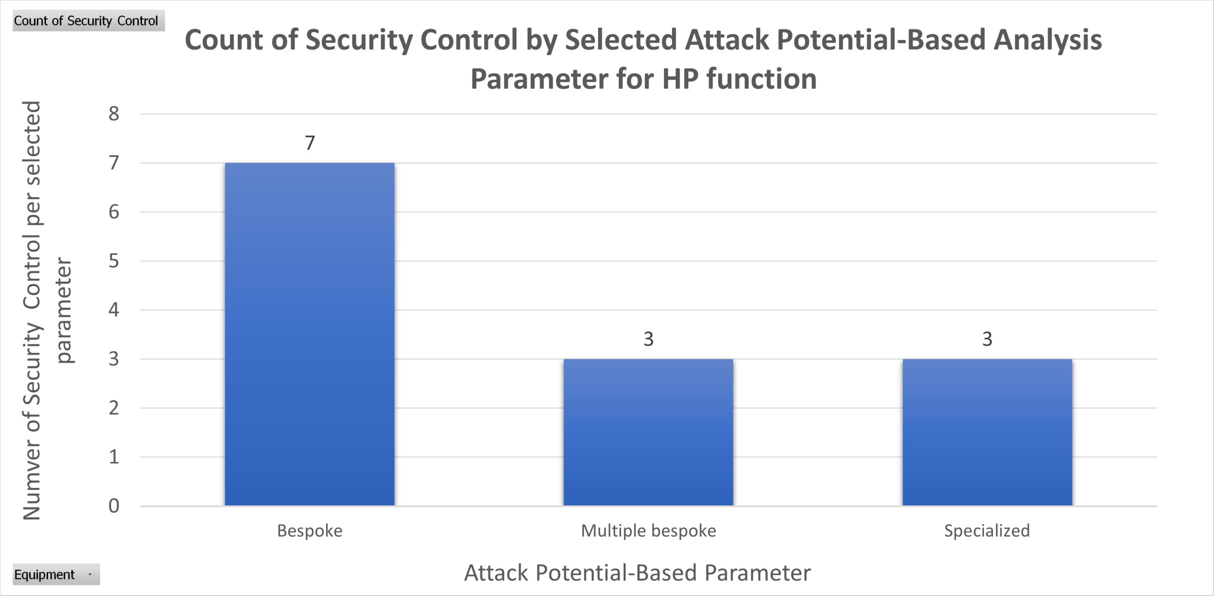


Figure 4.42: Count of Security Control by needed equipment.

By reducing the identified risks from high or medium to very low, the HP system becomes better equipped to handle potential cyber-incidents and maintain its operational integrity. This risk reduction effort aligns with industry best practices and cybersecurity standards, ensuring that the system adheres to a proactive and data-driven approach to address cyber threats.

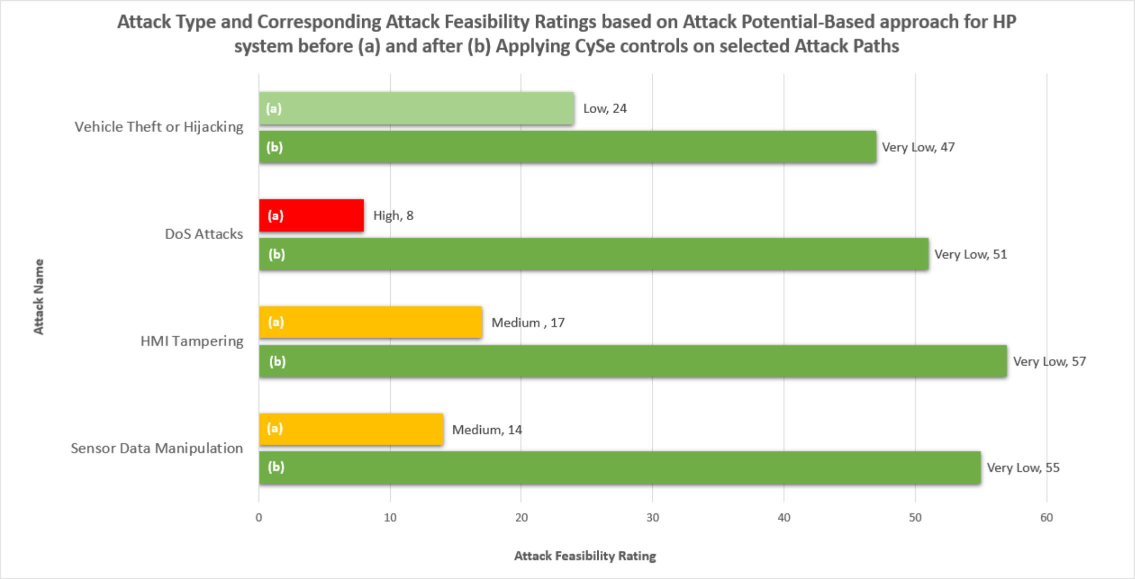


Figure 4.43: Attack Type and Corresponding Attack Feasibility Ratings based on Attack Potential-Based approach for HP system before (a) and after (b) Applying CySe controls on selected Attack Paths. Used AFR color coding: Red - High, Yellow - Medium, Light green - Low, Dark Green - Very Low.

4.2.3 Risk Mitigation Analysis

Risk analysis serves as the final step in the comprehensive risk assessment process for the HP system. Upon calculating the Attack Feasibility Rating (AFR) for each identified threat, the final risk associated with specific threats can be determined. In this study, the most critical threats based on their potential severe impact on system safety were prioritized, that is:

T1 - Tampering of Object List leads to Unjustified Strong Deceleration due to data unintended manipulation;

T2 - Denial of Service of Object List leads to Unjustified Strong Deceleration due to data unintended manipulation;

T846 - Denial of Service of EmeBrk leads to Unjustified Strong Deceleration due to data unintended manipulation;

These threats were subjected to detailed attack analysis through the creation of Attack Trees using the Medini Analysis tool, enabling a thorough exploration of potential vulnerabilities.

To quantify the risks associated with each threat, Equation 4.2 was used, as presented in the example analysis of Annex H of [13]. In addition, the Risk Mitigation Matrix (Table 4.5) and the Translation Matrix (Table 4.6) were used to determine risk values. It is worth noting that organizations may also define risk values using their customized risk formula.

$$R = 1 + I \times F \tag{4.2}$$

where:

R represents Risk Value,

I Impact Rating,

F Attack Feasibility.

As seen in Figure 4.44, in red (a), initially, that is, before mitigation, the risks of these identified threats were rated at the highest level, with a Risk Value of 5. Signifying their potential significant impact. Consequently, strategic risk reduction measures, marked in green (b) were adopted to address these critical risks. By applying the appropriate Cybersecurity Controls, the AFR was effectively reduced to Very Low, significantly mitigating the overall risk associated with the identified threats, which now stands at a reduced value of 2.

The comprehensive analysis carried out in this study involved evaluating FuSa + SOTIF, CySe, and cybersecurity threats, resulting in a significant improvement in the safety level of the entire vehicle. This approach is in line with an overarching safety posture strategy, reinforcing the system's reliability and resilience.

Through this rigorous risk assessment and mitigation process, the results successfully identify, prioritize, and address potential threats, demonstrating the practicality and effectiveness of incorporating Cybersecurity

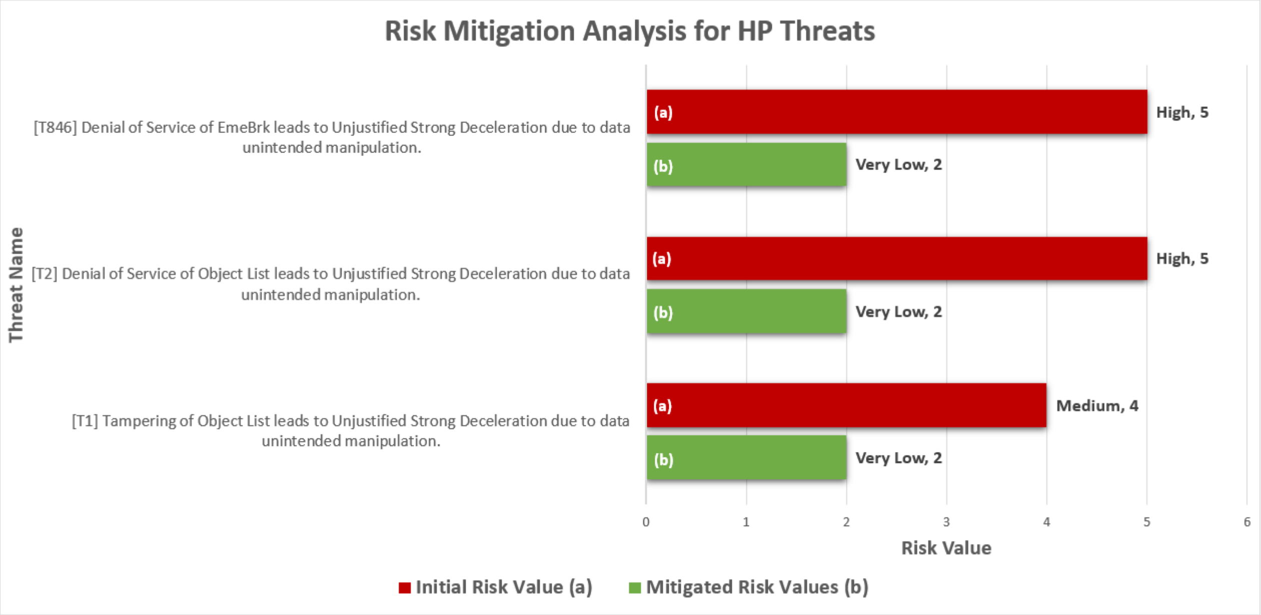


Figure 4.44: Risk Mitigation Analysis for HP Threats - (a) Initial Risk Values, (b) Mitigated Risk. Values.

Controls into the HP system design. The use of risk assessment methodologies and data-driven decisions allows for an informed risk management strategy, ultimately strengthening the overall security and safety posture of the system.

Table 4.5: Risk matrix example based on Table H.8 [13].

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	**2**	**3**	**4**	**5**
	Major	**1**	**2**	**3**	**4**
	Moderate	**1**	**2**	**2**	**3**
	Negligible	**1**	**1**	**1**	**1**

Table 4.6: Example Translation of impact and attack feasibility to numerical values based on Table H.10 from Annex H [13].

Impact rating	**Numerical value I for impact**
Negligible	0
Moderate	1
Major	1,5
Severe	2

Attack feasibility rating	**Numerical value F for attack feasibility**
Very low	0
Low	1
Medium	1,5
High	2

4.2.4 Design Work Products Effort Reduction

Based on the HP pilot analysis, which follows the prepared CyberSafety framework, there was a possibility to evaluate how much effort can be reduced by the introduction of common analysis work products for the design phase.

In order to calculate the effort reduction the Effort Reduction Coefficient was introduced. Equation (4.3). The Effort Reduction Coefficient (ERC) is calculated as follows:

$$ERC = \frac{NOSI}{TNOSI} \times 100\% \tag{4.3}$$

where:

ERC represents Effort Reduction Coefficient,

$NOSI$ is the Number of Shared Items,

$TNOSI$ is the Total Number of Items.

At this stage of the analysis, several key components were taken into consideration, namely Item Elements Definition, Risk Scenario Definition, Goals Definition, and Requirement Definition. The reduction in effort resulting from the application of the CyberSafety framework for the design phase of the HP system is summarized in Table 4.7.

The most significant effort reduction was observed in Item Elements Definition, as it played a pivotal role in both the FuSa and CySe aspects. The presence of 11 common damage scenarios between CySe and FuSa further reinforced the overall effort reduction, resulting in a substantial 37.93% reduction. Similarly, the identification of common CySe goals contributed to a total effort reduction of 38.46%, as 5 defined goals were found to be applicable to both FuSa and CySe.

The second largest effort reduction was observed in Requirement Definition, where the overlaps between FuSa and CySe were particularly pronounced. Of the 119 entirely defined requirements, a significant portion (76) impacted both CySe and FuSa, leading to notable effort reduction in this area.

In total, the effort reduction achieved through the application of the CyberSafety framework for the design phase of the HP system amounts to an impressive 66.50%. This substantial reduction highlights the strong correlation and overlap between the FuSa and CySe domains, highlighting the advantages of adopting a common CyberSafety framework. The benefits extend beyond mere effort reduction, as this approach also leads to time and cost savings.

Moreover, the early adoption of CyberSafety measures during development not only reduces the number of design iterations, but also improves overall product quality. By addressing potential safety and security aspects upfront and establishing a stable system architecture, the need for complex and last-minute solutions is minimized, resulting in a more robust and reliable product.

The analysis underscores the importance of integrating the principles and measures of cyber security into the development process from an early stage. The close correlation between FuSa+SOTIF and CySe aspects confirms the efficacy of a unified approach, which ultimately leads to improved efficiency, reduced effort, and higher product quality. Embracing a common CyberSafety framework proves to be a prudent and rewarding strategy to realize safer, more secure, and better performing systems like the HP function.

Table 4.7: Product Design Analysis Effort Reduction based on HP function.

Work Item Type	**[ERC%]**
Item Elements Definition	100
Risk Scenario Definition *	37.93
Goals Definition	38.46
Requirement Definition	63.87
Total	**66.50**

Note: Hazard and Damage Scenarios are merged into Risk Scenario.

4.2.5 Proposal of the Weighted Safety Score

Presented in the previous section, the risk calculation and reduction strategy was based on guidelines provided by the ISO 21434 [13] standard, specifically focusing on the cybersecurity perspective. However, to fully assess the overall risk score for automotive systems, it is essential to incorporate additional factors that include both safety and security considerations. This section introduces a more robust risk scoring methodology that extends the ISO 21434 risk analysis guidelines by integrating safety elements and providing an early indication of the likelihood and detectability of the threat.

In the complex landscape of modern automotive systems, it is crucial to ensure complete risk management. Automotive systems are increasingly interconnected and software-driven, highlighting both potential safety hazards and cybersecurity threats. Traditional risk assessment methods, while effective within their specific domains, often do not address the full spectrum of risks that arise from the convergence of cybersecurity and safety concerns.

To bridge this gap, a multifaceted risk evaluation method is proposed that amalgamates safety and security metrics into a single coherent risk score. This approach not only aligns with the established practices outlined in ISO 21434 but also integrates principles from safety standards, such as ISO 26262, to create a unified risk assessment model. By considering both Hazard Safety Indicator (HaSI) and Threat Risk Score (ThRS), this methodology provides a holistic view of potential risks.

HaSI - Hazard Safety Indicator

HaSI is derived from the ASIL score, which takes into account the severity of potential injuries (S), the exposure frequency of hazardous events (E), and the controllability of those events by drivers or systems (C). Equation (4.4) represents how the HaSI is calculated.

$$HaSI = \sum S_i \times E_i \times C_i \tag{4.4}$$

where:

S Severity,

E Exposure,

C Controllability.

Each hazard is scored based on its potential impact, frequency of exposure, and ability to control or mitigate it. Based on [5], clasess of Severity, Exposure and Controllability has assigned numerical values, which are taken into account during HaSI calculation. Table 4.8 provides porposed scores for Class of Severity, Table 4.9 provides scores for Class of Exposure and Table 4.10 provides scores for Class of Controllability.

Table 4.8: Classes of Severity.

Class of Severity	Description	Severity Level
S0	No injuries	0
S1	Light and moderate injuries	1
S2	Severe and life-threatening injuries	2
S3	Life-threatening injuries (survival uncertain), fatal injuries	3

Table 4.9: Classes of Exposure.

Class of Exposure	Description	Exposure Level
E0	Incredible	0
E1	Very Low probability	1
E2	Low Probability	2
E3	Medium Probability	3
E4	High Probability	4

ThRS - Threat Risk Score

ThRS however, is rooted in cybersecurity principles, focusing on the potential impact of threats, their likelihood of occurrence, and the ease with which they can be detected.This index measures the risk associated with potential threat, which extends the impact rating suggested in ISO 21434 [13]. Equation (4.5) represents how the ThRS is calculated.

Table 4.10: Classes of Controllability.

Class of Controllability	Description	Controllability Level
C0	Controllable in general	0
C1	Simply controllable	1
C2	Normally controllable	2
C3	Difficult to control or uncontrollable	3

$$ThRS = \sum I_j \times L_j \times D_j \tag{4.5}$$

where:

I Impact,

L Likelihood,

D Detectability.

Each threat is scored based on its impact (I), likelihoood (L), and detectability (D) . Clasess of Impact, Likelihood, and Detectability has assigned numerical values, which are taken into account during ThRS calculation. Table 4.11 provides proposed scores for Class of Impact, Table 4.12 provides scores for Class of Likelihood and Table 4.13 provides scores for Class of Detectability.

Table 4.11: Impact level score and description.

Class of Impact	Description	Impact Level
I1	Negligible impact	1
I2	Minor impact	2
I3	Moderate impact	3
I4	Significant impact	4
I4	Catastrophic impact	5

Table 4.12: Likelihood level score and description.

Class of Likelihood	Description	Likelihood Index
L1	Rare - Unlikely to occur.	1
L2	Unlikely - Could occur at some time.	2
L3	Possible - Might occur at some time.	3
L4	Likely - Will probably occur.	4
L5	Almost certain - Expected to occur in most circumstances.	5

Table 4.13: Detectability level score and description.

Class of Detectability	Description	Detectability Index
C1	Very high - Almost certain to be detected.	1
C2	High - High probability of being detected.	2
C3	Moderate - Moderate probability of being detected.	3
C4	Low - Low probability of being detected.	4
C5	Very low - Very unlikely to be detected.	5

WSS - Weighted Safety Score

By combining HaSI and ThRS, Weighted Safety Score (WSS) can be calculated that offers a holistic view of the risk landscape, accounting for both safety and security aspects. Equation (4.6) represents how the WSS is calculated.The WSS calculation involves assigning appropriate weight factors w_T (Weight Threat) and w_H (Weight Hazard) to the HaSI and ThRS, reflecting the relative importance of hazards and threats in various automotive domains such as safety-critical systems, user experience applications, sensors, body control, and connectivity. Table 4.14 consists of proposed weigths for hazards and threats scores based on the following rationale:

$$WSS = w_H \times HSI + w_T \times TRS \tag{4.6}$$

w_T Weight Threat,

w_H Weight Hazard,

Table 4.14: Weight Factors for Different System Types.

Domain	Weight Hazard (w_H)	Weight Threat (w_T)
Safety	0.8	0.2
User Experience	0.3	0.7
Sensor	0.5	0.5
Body	0.7	0.3
Connectivity	0.2	0.8

- Safety - In the safety domain, particularly for ADAS applications, safety is paramount. The focus is on ensuring the system is free from hazards that could lead to severe consequences. Therefore, a higher weight is given to hazard-related risks;
- User Experience - User applications typically involve a higher exposure to cybersecurity threats but are less critical in terms of safety. Thus, a higher weight is assigned to threat-related risks to reflect the importance of protecting against security breaches;

- Sensor - In the sensor domain, both safety and security are equally important. Sensors can impact vehicle operation (safety) and be vulnerable to tampering or attacks (security).Therefore, equal weight is given to both hazard and threat-related risks;

- Body - The body domain includes components that are crucial for the structural integrity and safety of the vehicle. Although security is important, the emphasis is more on ensuring the safety of the vehicle's physical components. Hence, a higher weight is given to hazard-related risks;

- Connectivity - The connectivity domain is highly susceptible to cybersecurity threats such as hacking, data breaches, and malicious attacks. While connectivity-related issues can lead to indirect safety consequences (e.g., disabling critical systems through a cyber-attack), the primary concern is not the immediate safety hazard but rather the security breach that could eventually lead to unsafe conditions.

The final safety indicator, which incorporates both the severity of the threat and the threat risk, provides a holistic view of the system's safety profile. Using standardized ranges for impact, likelihood and detection, this approach ensures a comprehensive and consistent risk assessment. This enables better informed decision making on risk mitigation and system safety improvements.

To ensure that the WSS score is meaningful, interpretative, and comparable across different contexts and domains, a standard range of 0 - 100 is proposed, and the calculation is shown in Equation (4.7).

$$NormalizedWWSS = \frac{w_H \times TotalHaSI + w_T \times TotalTRS}{w_H \times maxHaSI + w_T \times maxThSI} \times 100 \tag{4.7}$$

The WSS ranges with associated risk level and interpretation are proposed in 4.15.

By establishing these ranges and interpreting the WSS accordingly, organizations can make informed decisions about the safety of their systems, prioritize risk mitigation efforts, and ensure that they maintain an acceptable level of safety for their operations.

This method ensures that the overall risk assessment is not only comprehensive, but also domain-specific, allowing for more targeted risk mitigation strategies. The weighted factors for different domains are carefully chosen to align with their unique risk profiles, thereby providing a balanced assessment that can guide engineering decisions and enhance the safety and security of automotive systems. WSS can be calculated as a consolidated factor for an individual characteristic or function, as well as for an individual threat, providing greater granularity of information that can be used when assigning or decomposing functions.

In summary, the introduction of the Weighted Safety Score represents a significant advancement in risk analysis methodology by integrating safety and security perspectives, improving the precision and relevance of risk assessments in the automotive industry.

Table 4.15: The WSS ranges and their interpretation

WSS Range	**Risk Level**	**Interpretation**
0-20	Very Low Risk	The system is considered very safe. Minimal or no additional safety measures are required. Continous monitoring is recommended.
21-40	Low Risk	The system has a low level of risk. Basic safety and security measures are in place and are adequate. Regular reviews and minor improvements may be needed.
41-60	Moderate Risk	The system has a moderate level of risk. Additional safety and security measures should be considered. Regular monitoring and periodic safety assessments are necessary.
61-80	High Risk	The system has a high level of risk. Significant safety and security improvements are required. Enhanced monitoring and frequent safety and security reviews are essential.
81-100	Very High Risk	The system is considered very unsafe. Immediate and extensive safety measures are necessary. Continuous and intensive monitoring is required.

4.2.6 Highway Pilot Weighted Safety Score Evaluation

In this section, the introduced WSS score is validated by selecting specific hazards and threats for the HP function. For each identified hazard, the corresponding WSS score is calculated based on the relevant threat scenarios.

Table 4.16 consists of the safety evaluation of HP function selected hazard scenarios. For each severity of the hazard, the exposure and controllability classes are derived based on ISO 26262 [5] resulting in ASIL level.

In Table 4.17 the evaluation of the threat risk is performed based on the proposed classless classification, encompassing impact, likelihood, and detection. At this stage, in the absence of any proposed CySe measures, all classes exhibit high values. For threats related to data tampering, the impact, likelihood, and detectability classes are considered higher, as the available safety mechanisms will not be activated and, therefore, will not mitigate this threat. In contrast, for threats related to denial of service, safety mechanisms may remain active and support the mitigation strategy.

Table 4.18 presents the threat classes following the implementation of the Intrusion Detection System (IDS) as a security measure. The detectability class is significantly reduced, as the IDS is assumed to be highly effective in detecting threats, thereby decreasing the associated impact and likelihood classes.

Table 4.16: Hazard Risk Evaluation for Highway Pilot selected scenarios.

Hazard Description	**Hazard ID**	**Severity Class**	**Exposure Class**	**Controllability Class**
Unjustified Strong Deceleration (ASIL D)	H1	S3	E4	C3
Collision with a solid object on road or roadside (ASIL A)	H2	S3	E1	C3
Leaving assigned driving corridor or lane (ASIL B)	H3	S3	E2	C3

Table 4.17: Threat Risk Evaluation for Highway Pilot selected scenarios.

Threat Description	**Threat ID**	**Impact Class**	**Likelihood Class**	**Detectability Class**
Threat Tampering Object List	T1	I5	L3	D5
Threat Denial of Service on Emergency Braking	T2	I4	L4	D4
Threat Denial of Service on Object List	T3	I4	L4	D4

Table 4.18: Threat Risk Evaluation for Highway Pilot selected scenarios after applying Intrusion Detection System.

Threat Description	**Threat ID**	**Impact Class**	**Likelihood Class**	**Detectability Class**
Threat Tampering Object List	T1	I4	L2	D2
Threat Denial of Service on Emergency Braking	T2	I3	L3	D1
Threat Denial of Service on Object List	T3	I4	L2	D1

Table 4.19: Normalized Weighted Safety Score before and after applying Intrusion Detection System.

Hazard ID	**Threat ID**	**Normalized WSS Before IDS**	**Normalized WSS After IDS**
H1	T1	81.4	59.5
H1	T2	83.2	56.9
H1	T3	77.32	56.5
H2	T1	36.8	14.9
H2	T2	38.7	12.3
H2	T3	32.7	11.9
H3	T1	45.7	23.8
H3	T2	47.6	21.2
H3	T3	41.6	20.8

In result, the Normalized Weighted Safety Sore is calculated on considered data for mitigated and not mitigated threats. Table 4.19 includes the calculated values. Since HP is assumed to be part of the safety domain, w_H and w_T according to 4.14 are selected. The result shows the highest score for hazards with the highest safety value, which according to 4.15 results in a high or very high risk level for the system. The respectively low and very low WSS score is calculated for H2 and H3, which have a safety score ASIL A and ASIL B. After applying IDS as a CySe measure, the most critical risk of H1 is mitigated to a moderate value, which can be considered acceptable assuming that HP core function can be isolated from the rest of non-critical vehicle functions.

4.3 Process Indicators

Despite the availability of standards and methodologies, there is a significant need to assess and improve the effectiveness of engineering processes that combine CySe and FuSa activities. A critical aspect of this assessment is to define clear and representative indicators or Key Performance Indicators (KPI)s that can measure the process's performance. These KPI are essential for identifying gaps, driving improvements, and ensuring compliance with standards.

Establishing a robust set of KPIs is crucial for several reasons:

- Regulatory Compliance: Ensures that the development process meets the stringent requirements of ISO 26262 and ISO 21434;
- Risk Management: Helps in identifying and mitigating potential risks early in the development process;
- Process Improvement: Provides a basis for continuous improvement by highlighting areas of inefficiency or non-compliance;
- Stakeholder Communication: Facilitates clear and objective communication among stakeholders regarding process performance and areas for improvement.

Previous studies have explored various aspects of process improvement in the context of software development, agile methodologies, and process mining. For example, [130] work on entropy metrics for agile development processes highlights the challenges of measuring complexity and quality in a rapidly evolving development environment. Similarly, the systematic review by [131] on complex process modeling in process mining underscores the need for a unified view of complexity reduction approaches and the importance of understanding the complexity of the process model.

With the focus on the design phase of a product development the following KPIs are defined:

- Security And Safety Risk Identification Rate (SSRIR)
- Risk Assessment Coverage (RAC)
- Design Review Effectiveness (DRE)
- Mitigation Strategy Completeness (MSC)
- Design Compliance Rate (DCR)
- Residual Risk Level (RRL)
- Security and Safety Requirements Coverage (SSRC)
- Design Complexity Index (DCI)
- Design Change Request Rate (DCRR)

Security And Safety Risk Identification Rate (SSRIR)

$$SSRIR = \frac{NumberofIdentifiedRisks}{TotalNumberofDesignElementsReviewed} \tag{4.8}$$

Ensures that potential risks are identified early. A high SSRIR indicates a thorough risk identification process. An acceptable score would be 90% or higher, suggesting that almost all potential risks are identified during the design phase.

Risk Assessment Coverage (RAC)

$$RAC = (\frac{NumberofAssessedRisks}{TotalNumberofIdentifiedRisks}) \times 100\% \tag{4.9}$$

Confirms a thorough risk assessment. All identified risks should be assessed for severity and likelihood. An acceptable score is 100%, indicating comprehensive risk assessment coverage.

Design Review Effectiveness (DRE)

$$DRE = (\frac{NumberofissuesIdentifiedinReviewes}{TotalNumberofIssues}) \times 100\% \tag{4.10}$$

Evaluates the effectiveness of design reviews. Effective design reviews should identify a high percentage of potential issues. An acceptable score would be 85% or higher, indicating that most issues are being caught during the review process.

Mitigation Strategy Completeness (MSC)

$$MSC = (\frac{NumberofRiskswithCompleteMitigationStrategies}{TotalNumberofIdentifiedRisks}) \times 100\% \tag{4.11}$$

Ensures that all risks have mitigation strategies.All identified risks should have complete mitigation strategies. An acceptable score is 100%, ensuring that every risk has a documented and actionable mitigation plan.

Design Compliance Rate (DCR)

$$DCR = (\frac{NumberofCompliantDesignElements}{TotalNumberofDesignedElements}) \times 100\% \tag{4.12}$$

Verifies compliance with standards.Design elements should comply fully with relevant standards (ISO 26262, ISO 21434). An acceptable score is 100%, indicating full compliance.

Residual Risk Level (RRL)

$$RRL = \frac{\sum ResidualRiskScore}{TotalNumberofRisks} \tag{4.13}$$

Measures the effectiveness of risk mitigation. Residual risk should be minimized after implementing mitigation strategies. An acceptable score is low, preferably between 0 and 20, indicating effective risk mitigation.

Security and Safety Requirement Coverage (SSRC)

$$SSRC = (\frac{Number of Implemented Requirements}{Total Number of Requirements}) \times 100\% \tag{4.14}$$

Ensures all requirements are met.All security and safety requirements should be implemented in the design. An acceptable score is 100%, ensuring complete coverage of the requirements.

Design Complexity Index (DCI)

$$DCI = (\frac{Number of Interconnections}{Total Number components}) \tag{4.15}$$

Manages design complexity. The complexity of the design should be manageable to avoid security and safety vulnerabilities. An acceptable score is moderate, indicating balanced and manageable complexity.

Design Change Request Rate (DCRR)

$$DCRR = (\frac{Number of Design Change Requests}{Total Number of Design Elements}) \tag{4.16}$$

Indicates the robustness of the initial design. The initial design should be robust and require few changes. An acceptable score is 10% or lower, indicating a well-thought-out and stable design.

The summary of CySa indicators with proposed target value is provided in Table 4.20.

Table 4.20: CyberSafety process indicators description with target values.

Indicator	**Target Value**
Security and Safety Risk Identification Rate (SSRIR)	$\geq 90\%$
Risk Assessment Coverage (RAC)	100%
Design Review Effectiveness (DRE)	$\geq 85\%$
Mitigation Strategy Completeness (MSC)	100%
Design Compliance Rate (DCR)	100%
Residual Risk Level (RRL)	Low (0-20 on a 0-100 scale)
Security and Safety Requirement Coverage (SSRC)	100%
Design Complexity Index (DCI)	Moderate (1-3 on a relative scale)
Design Change Request Rate (DCRR)	$\leq 10\%$

4.3.1 CyberSafety Process Indicators Evaluation

Introducing the CySa development process and its improvements significantly changes the approach to the design of automotive systems by identifying complete risks at an early stage, thus driving design decisions. Thanks to the process indicators described in the previous section, the process can be better validated. Since CySe and FuSa-related risks can be analyzed together, the SSRIR score can reach 100%, which proves the holistic identification of risk. Furthermore, since all identified risks can be covered during the assessment, the assumed RAC score reaches 100% as well.

Thanks to the definition of all interfaces between CySe and FuSa, all issues related to design and review methods can be addressed. Therefore, the DCR score can reach 100%. Mitigation techniques are crucially important, and by identifying overlaps between CySe and FuSa, the MSC factor reaches 100

Since CySa is designed according to the standards ISO 21434, ISO 26262 and ISO 21448, all work products are considered and therefore the DCR score can be calculated as 100%. In principle, the CySa process framework is applicable to any vehicle domain. However, while focusing on the safety domain, the factors of safety play a significant role, and the initial risk score is considered high or very high. After proper indication of risks and the provision of appropriate controls and measures, it has been proven that the RRL may drop, in the worst case, to a moderate value.

Thanks to joint efforts in the CySe and FuSa domains, the requirements coverage score, i.e., SSRC, reaches 100%. While evaluating the HP example with IDS as a proposed mitigation measure for both CySe and FuSa, the assumed DCI index may reach a moderate value. This is because basic safety mechanisms still need to be implemented, while defined CySe measures add more interfaces and connections.

The THA and DCRR scores were not thoroughly evaluated, as they require real-time data in the field. Nevertheless, by following CySa, organizations can expect a low DCRR rate since all critical design considerations are already addressed at the beginning. The summary of CySa indicators is shown in Table 4.21.

Table 4.21: CyberSafety process indicators description with evaluated values in context of Safety Domain.

Indicator	**Target Value**
Security and Safety Risk Identification Rate (SSRIR)	100%
Risk Assessment Coverage (RAC)	100%
Design Review Effectiveness (DRE)	100%
Mitigation Strategy Completeness (MSC)	100%
Design Compliance Rate (DCR)	100%
Residual Risk Level (RRL)	Moderate
Security and Safety Requirement Coverage (SSRC)	100%
Design Complexity Index (DCI)	Moderate

Chapter 5

Conclusions and Future Work

5.1 Research Summary

The automotive industry is undergoing a major transformation, moving from product-centric to service-oriented, based on software capabilities. This shift is driven by innovations in electric and autonomous vehicles, which require robust cybersecurity measures to protect communications and improve overall vehicle safety. Integrating cybersecurity into the core of vehicle design, in addition to collaboration between traditionally isolated functional safety and cybersecurity teams, has become paramount Chapter 1.

The research landscape reveals a marked contrast between the maturity of Functional Safety (FuSa) and the emerging field of Cybersecurity (CySe) within the automotive industry. FuSa has a well-established body of literature, while a significant increase in cybersecurity-related publications coincides with the introduction of the ISO 21434 standard in 2021, highlighting the growing importance of cybersecurity in vehicle development. However, it is clear that the relevant standards are still in the process of being refined.

As vehicles become more interconnected, they face a growing risk of cyber threats. Ensuring the cybersecurity resilience of these systems is essential to protect them from external malicious attacks. Traditional risk analysis for automotive systems with a high degree of autonomy has focused primarily on safety concerns, often overlooking the cybersecurity aspect. This oversight has resulted in significant hazards, as demonstrated by incidents such as the Jeep Cherokee hack and other documented vulnerabilities in automotive systems [14–17, 126, 127].

Crucially, confidence in vehicles depends on the creation of comprehensive common work products that recognize the inextricable link between safety and security. However, there are differences, as certain vehicle systems operate independently of software control, which requires different safety and security considerations. The rapid evolution of cyber-security threats highlights the need for continued vigilance Chapter 2.

To address these challenges, a paradigm shift towards close collaboration between engineering teams at the early stages of product development is imperative Figure 5.1. This shift helps identify architectural challenges early on, preventing costly changes in later development phases. Aligning strategy, analysis, and design processes between safety and security is vital in resolving inconsistencies Figure 5.2.

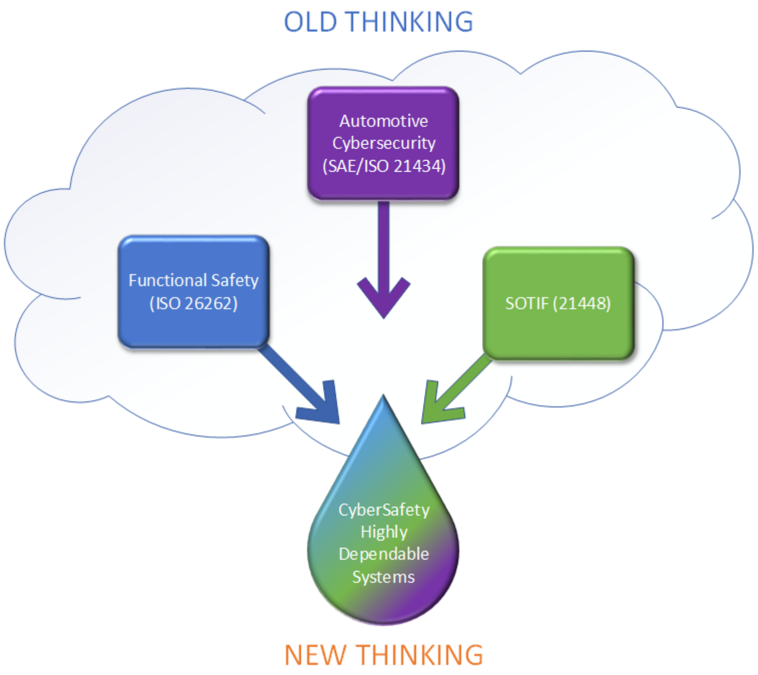

OLD THINKING
Automotive Cybersecurity (SAE/ISO 21434)
Functional Safety (ISO 26262)
SOTIF (21448)
CyberSafety Highly Dependable Systems
NEW THINKING

Figure 5.1: Old vs New way of thinking on vehicle safety landscape.

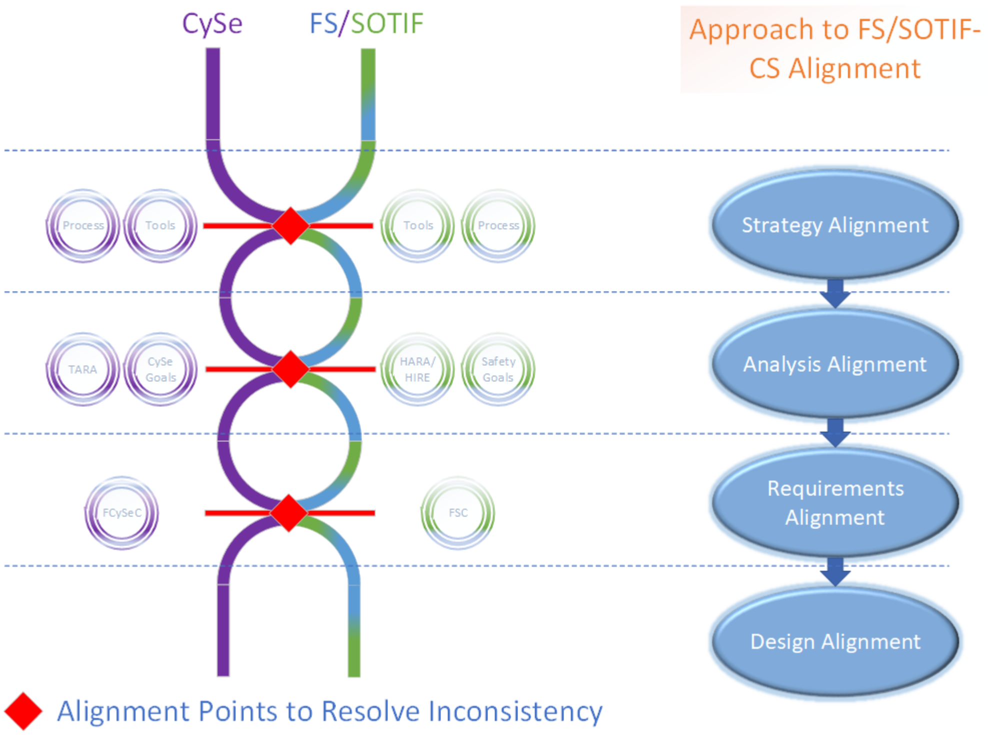


Figure 5.2: Old vs New way of thinking on vehicle safety landscape.

This integrated approach requires a holistic perspective to address the full spectrum of highly autonomous system design and production. The application of well-established lean management principles in manufacturing is also relevant in the design phase. These principles streamline processes, eliminate waste, and improve overall system quality. In addition, the adoption of Model-Based Systems Engineering (MBSE) principles allows organizations to achieve a more unified and holistic view of system architecture. MBSE introduces a structured approach that uses visual models and simulations to systematically analyze and optimize system design Chapter 2.

The primary objective of this PhD research was twofold. Firstly, to develop a practical and implementable approach to the design and implementation of advanced control systems in highly automated vehicles, aimed at improving system reliability, fostering synergy among development teams, minimizing duplication of effort and accelerating overall development. This objective addressed the urgent need for synergy between safety and security in the dynamic automotive industry. The significant research effort, marked by an exhaustive review of the literature, a careful analysis of standards and guidelines, and extensive expert consultation, culminated in the development of the CyberSafety (CySa) process. This process has been designed to fulfill the overarching objectives of this thesis Chapter 3.

Secondly, the research aims to propose a reference organizational design model and technical methodology tailored for application within the research and development departments of automotive companies. This model goes beyond theoretical constructs and aims to provide a tangible framework for the effective integration of safety and security principles in an industrial environment, enhancing collaboration and communication within teams. The robustness of this organizational model was rigorously evaluated through its application in a real-world example of and ADAS system i.e. Highway Pilot (HP) Chapter 4.

Central to these objectives was the hypothesis that early collaboration on integrated safety and security throughout the product development life cycle will yield superior reliability and quality for high-autonomy automotive embedded systems by minimizing risks and ensuring robust performance. Developing a novel development model that equips companies with comprehensive tools and methodologies for efficiently managing the intricate design of complex, mixed-criticality, high-autonomy automotive embedded systems, while integrating safety and security throughout the entire process, will significantly improve system reliability, reduce development efforts, and enhance overall vehicle safety and security. This hypothesis serves as the cornerstone of the research methodology and guides the investigation efforts in Chapter 3.

The CyberSafety (CySa) process has been thoroughly designed, grounded in existing standards, and structured to address the critical interfaces between security and safety processes. It also establishes clear roles and responsibilities for development teams. At the same time, defining the common work products is needed from the perspective of the process. Importantly, it integrates seamlessly with the current automotive standards landscape, ensuring its relevance and applicability. This process, modeled using the BPMN language and implemented using the Bizagi Modeller tool, is easily adaptable to the specific workflows of automotive companies.

Significant emphasis has been placed on the design phase within the CyberSafety process, recognizing its key role in the development lifecycle. In addition, consistent attention has been paid to continuous vulnerability management, especially during the product maintenance phase. This focus has been driven by the ongoing product maintenance requirements that OEMs typically impose within the automotive industry.

In light of proposed CySa framework there is a need to define clear and representative Key Performance Indicatorss to effectively measure the performance of the process. Establishing robust KPIs serves several essential purposes: ensuring regulatory compliance, facilitating risk management, driving continuous process improvement, and enhancing communication among stakeholders.

Focusing on the design phase of the product development, a set of KPIs has been defined, including the Security And Safety Risk Identification Rate (SSRIR), Risk Assessment Coverage (RAC), Design Review Effectiveness (DRE), Mitigation Strategy Completeness (MSC), Design Compliance Rate (DCR), Residual Risk Level (RRL), Security and Safety Requirement Coverage (SSRC), Design Complexity Index (DCI), and Design Change Request Rate (DCRR). These KPIs ensure comprehensive risk identification, assessment and mitigation, compliance with relevant standards, and manageable design complexity.

The introduction of the CySa development process marks a significant change in the design of automotive systems by identifying risks in a comprehensive way at an early stage, thus guiding design decisions more effectively. The defined KPIs facilitate the validation of the process, ensuring that CySe and FuSa-related risks are jointly analyzed and addressed, leading to high scores in the defined metrics. This integrated approach ensures that all interfaces between CySe and FuSa are defined, all mitigation strategies are complete, and compliance with the ISO 21434, ISO 26262, and ISO 21448 standards is achieved. The result is a robust and holistic engineering process framework that can be applied across various vehicle domains.

The fundamental objective of the dissertation of formulating a highly practical and implementable approach to the design and implementation of advanced control systems in highly automated vehicles has been reached and rigorously validated. This validation was achieved through a careful evaluation process carried out within the widely recognized Ansys Medini tool, where cross-functional analysis has been proposed. The example chosen for this evaluation was the Highway Pilot system, carefully selected for its role as a representative of a highly automated and complex safety function. This choice was crucial, as it required a comprehensive evaluation taking into account both safety and security aspects.

The suggested solution expands Cybersecurity (CySe) analysis to new domains, eliminating its customary deep integration with the Electrical/Electronic (EE) vehicle architecture. Instead, it focuses on abstracted system functional architectural components, their relationships, use case data flows, and communication patterns. This abstraction enables the identification of hazards independent of physical implementations, allowing for early detection and mitigation of possible problems before finalizing physical architectural decisions and functional allocations. Without such an evaluation, unjustified risks would remain in the system Chapter 4.

The evaluation results provide compelling empirical evidence to support the research hypothesis. Figure 4.44 shows a substantial reduction in cybersecurity risks and safety hazards (from very high to low). Moreover, Table 4.7 shows a significant decrease in development effort, particularly in the system design phase (up to 60%). Importantly, this reduction in effort is achieved while maintaining adherence to established standards, highlighting the approach's ability to deliver high-quality and secure products.

Modern automotive systems, increasingly interconnected and software driven, present complex safety and cybersecurity challenges. Traditional risk assessments often do not address the full spectrum of these risks. Furthermore, as already experienced during the execution of professional projects in the automotive industry, conducting Cybersecurity (CySe) and Functional Safety (FuSa) analyses in isolation often leads to conflicting objectives, particularly in mission-critical real-time systems. In particular, this issue arises in the exchange of data between components, where cryptographic checks may introduce delays that hinder the timely completion of safety verifications. To bridge this gap, a multifaceted risk evaluation method is proposed that combines safety and security metrics into a unified risk score. This approach is aligned with ISO 21434 and integrates the principles of ISO 26262, using the Hazard Safety Indicator (HaSI) and Threat Risk Score (ThRS) to offer a comprehensive risk perspective. The Hazard Safety Indicator (HaSI) is calculated from the ASIL score, considering severity, exposure, and controllability, while the Threat Risk Score (ThRS) evaluates impact, likelihood, and detectability. The combined Weighted Safety Score (WSS) accounts for both hazards and threats, with weight factors tailored to various automotive domains. This method ensures a comprehensive domain-specific risk assessment, guiding engineering decisions to improve the safety and security of the automotive system. The Weighted Safety Score (WSS) provides a holistic view of the risk landscape of the system, supporting better informed decision making for risk mitigation and safety improvements. WSS score ranges has been defined in Table 4.15 and evaluated in the context of the Highway Pilot (HP) ADAS system that proves its value, as presented in Table 4.19.

Research operates within specific limitations and assumptions, relying on industry standards and available tools at the time. Section 1.3. Future integration of newer versions and more versatile tools is planned. Model evaluation focuses predominantly on the design phase and uses the Highway Pilot system as a representative example. The research primarily adopts a cybersecurity perspective, addressing highly critical threats and hazards. The assumed process flow is iterative and agile. Despite challenges related to standardized joint development practices, direct communication with tool vendors has led to anticipated enhancements. These limitations and assumptions define the scope of the research, which extends to potential applications beyond the automotive industry.

5.2 Discussions

Fully autonomous vehicles, in which the driver is completely removed from the driving process, remain a distant concept. Their realization requires the development of an entire ecosystem that includes not only the vehicles themselves but also a comprehensive road infrastructure and robust, high-quality wireless connectivity. These requirements pose significant challenges, particularly in areas outside urban centers, where building such an infrastructure can be particularly difficult.

One of the most significant hurdles in the transition to fully autonomous systems lies in the intermediate phase. This phase involves the coexistence of fully autonomous and semi-autonomous vehicles on the road. During this period, eliminating the human factor, which often contributes to accidents, is proving a formidable task. This co-existence raises questions about how human drivers interact with autonomous vehicles and the potential safety risks associated with this complex dynamic.

Despite the considerable distance that separates us from achieving a "zero accident" world, where the human factor is entirely eliminated, it is imperative that we diligently chart the right course and work towards standardizing solutions. This is especially critical given the increasing prevalence of connected vehicles, which are highly exposed to cyber-threats.

As we look to the future, it becomes evident that standardization efforts should include the integration of security patterns into existing cybersecurity standards. Such an approach would complement the ongoing work in standardization working groups dedicated to defining parameters such as the Cybersecurity Assurance Level (CAL) and Targeted Attack Feasibility (TAF) within ISO/SAE 8475 [77]. Furthermore, it would align with efforts related to Cybersecurity Verification and Validation outlined in ISO/PAS 8477 [78], and broader initiatives addressing Information Security, Cybersecurity, and Privacy Protection as articulated in ISO/IEC 5888. These measures are vital to fortifying the security posture of connected vehicles and ensuring their safe operation in an increasingly digital landscape.

In addition to the essential standardization and procedural efforts, there is a significant engineering aspect to consider. One of the key steps towards a seamlessly connected and intelligent vehicle is the concept of the Software-Defined Vehicle.

The term "software-defined vehicle" refers to a vehicle whose functions and capabilities are primarily enabled by software. This represents a fundamental shift in the automotive industry, transforming vehicles from primarily hardware-based products to sophisticated software-centric electronic devices on wheels.

Today's premium vehicles already contain up to 150 million lines of software code, spread across a complex network of more than 100 electronic control units, coupled with a growing array of sensors, cameras, radar systems, and light detection and ranging (lidar) devices. Mass-market vehicles are quickly following suit. Three overarching trends, electrification, automation, and connectivity, are fundamentally changing consumer expectations. As a result, automakers are increasingly turning to software to meet these evolving demands.

Traditionally, automakers differentiated their products through mechanical features such as horsepower and torque. However, today's consumers are looking for features that are predominantly software-defined, such as advanced driver assistance systems, innovative infotainment solutions, and smart connectivity features. The evolution from driver assistance to fully autonomous driving increases the need for sophisticated software. As consumers expect richer content in their information technology systems, the volume of digital content managed by vehicles continues to grow. And as vehicles become an integral part of the Internet of Things (IoT), transmitting significant amounts of data to and from the cloud, software is essential to efficiently process, manage, and distribute these data.

The benefits of the software-defined vehicle go beyond unlocking new safety, comfort, and convenience features. It represents a paradigm shift that offers several other notable advantages over its hardware-defined predecessor.

A key aspect of the evolution of the software-defined vehicle is the separation of software and hardware development. This transition parallels the change seen in the evolution of mobile phones. Initially, the software and hardware in mobile phones were closely intertwined, but with the advent of smartphones, mobile phones underwent a profound change. They became software platforms capable of supporting an extensive ecosystem of applications, regardless of the underlying hardware.

Similarly, the automotive industry is currently experiencing a similar shift in vehicle software development. Car manufacturers are beginning to create what can be described as 'walled gardens' for applications. In these controlled environments, vehicle manufacturers, together with other approved parties, can actively participate in the development and integration of software solutions that improve vehicle functionality.

This transition marks a significant step towards the software-defined vehicle, where the software ecosystem becomes a driving force, independent of the specific hardware it runs on.

The software-defined vehicle of the future promises a host of benefits, including enhanced safety and security features, increased levels of autonomy, the ability to receive regular functional and security updates, and a software platform for a range of connected services, including state-of-the-art information technology. This transformation of vehicle capabilities is not limited to technical advances; it also opens up entirely new business models and revenue streams. Services such as theft prevention, emergency assistance alerts, and personalized travel guides are just a few examples of the exciting possibilities that the software-defined vehicle will bring to both consumers and original equipment manufacturers. The full extent of these opportunities has yet to be fully explored and realized.

However, as we embrace the software-driven future, it is important to recognize the increased potential for cyber-attacks. Using established IT concepts, we can implement a comprehensive defense strategy to protect against these threats. This approach involves defining security zones within the vehicle network, effectively creating a ’vehicle fortress’.

Defining these security zones allows us to implement security measures at multiple levels within the vehicle’s architecture. Each security zone acts as an individual layer of defense, focusing on securing the components within its limits. This layered approach has several benefits: it reduces the risk of unauthorized access, limits the impact of potential security breaches, and strengthens the overall cybersecurity resilience of the vehicle.

Vehicle security zones play an important role in the broader defense-in-depth strategy. They establish clear boundaries and separation between components with similar cybersecurity requirements. This separation facilitates the implementation of tailored security controls, monitoring systems, and incident response protocols within each zone. In essence, security zones are the building blocks of a robust vehicle cybersecurity framework.

Integrating artificial intelligence AI technology into the automotive design process provides a breakthrough potential to strengthen cybersecurity protocols and efficiently address safety problems. Design teams can ensure robust cybersecurity integration from the start by leveraging AI-driven functionalities such as automated test case generation for functional and safety requirements, customer requirement analysis and generation, security artifact creation, and training data integrity evaluation. AI may also serve as a secure coding copilot, providing developers with real-time feedback on coding habits and creating customized, secure code for the hardware design. Furthermore, AI-powered dynamic fuzzing and analysis tools speed up vulnerability identification, while automated vulnerability processing and patch development reduce response times. These developments jointly strengthen automotive systems against cyber-attacks and reinforce safety measures, encouraging trust in the car. Moreover, AI methods may help with verification and validation in the automotive lifecycle, assisting in test cases creation, execution, and pre-analysis of results.

5.3 Closing Statement

The long-term vision of a connected, autonomous, and environmentally friendly transport system may seem distant, but it is important to remember that monumental achievements often take time. Rome, as the saying goes, was not built in a day. With the rapid pace of technological breakthroughs and innovation, this ambitious vision has a real chance of becoming a reality.

To turn this vision into a practical and achievable goal, it is vital that experts and professionals from different areas of engineering come together. By pooling our collective knowledge and understanding of the ultimate goal, we can chart a course towards this transformative future. History has shown time and again that collaboration can lead to extraordinary achievements, and this will not be the first time that humanity has achieved remarkable things by working together.

In this age of artificial intelligence and advanced technologies, progress can be made at an astonishing rate. However, it is important to recognize that the human factor remains a critical consideration. Even with the most advanced technologies at our disposal, ensuring overall safety will always depend on our ability to address and mitigate human challenges and risks.

This dissertation dived into the dynamic world of innovation to uncover the profound essence of true innovation. It is not just about incremental progress; it embodies a transformative spirit that reshapes paradigms and unlocks innovative solutions to the most complex challenges. At its core, innovation weaves together imagination, experimentation, and the relentless pursuit of progress, all fueled by the creative spirits that dare to explore uncharted territories and challenge established norms. True innovation is rooted in people: people with the courage to challenge the status quo, the vision to imagine a better future, and the extraordinary ability to connect the dots differently. These innovators are marked by their persistence, unwavering resilience, and their profound capacity to learn and grow from failures. It is these innovators who drive the industry forward, fostering the kind of breakthroughs that fundamentally reshape our world.It is important to note that innovators are not born, they are made. Anyone can learn to think and act with an innovative mindset. In addition to the innovator virtues already mentioned, one should also be empathetic, create innovations for the benefit of others, take risks, embrace uncertainty, and actively collaborate to discover together. These additional qualities enrich the innovative spirit and make it a force for positive change and social progress.

Appendix A

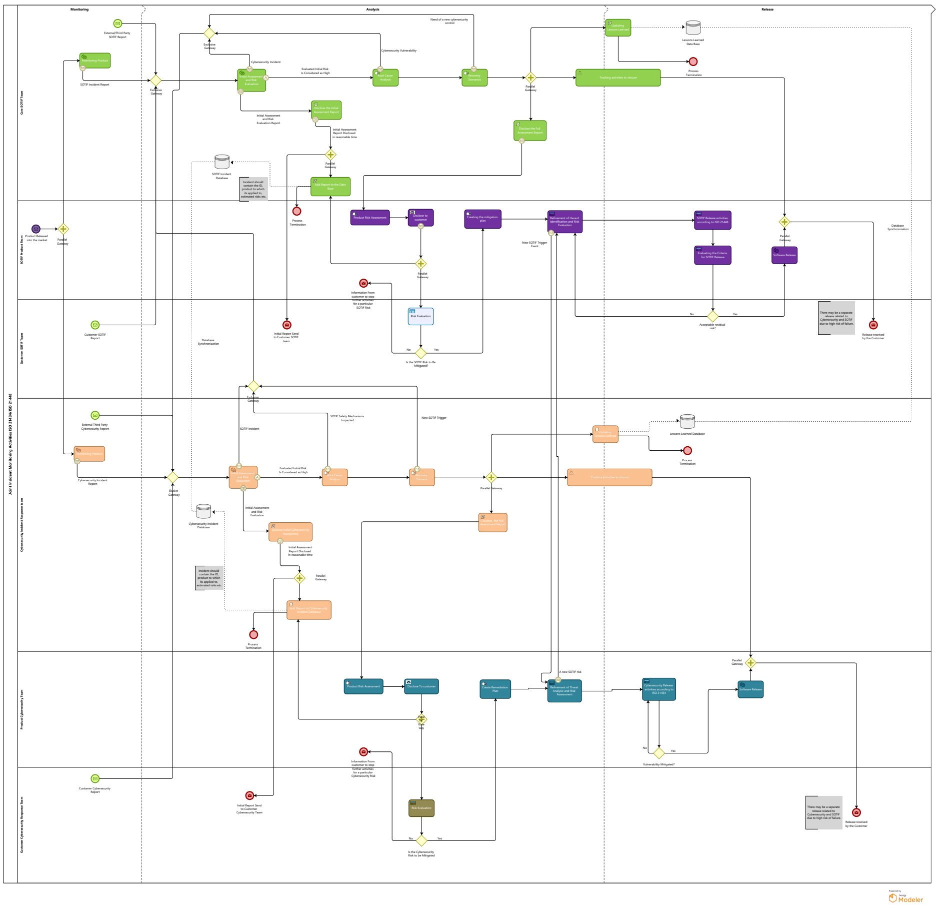
Appendix A - Bizagi - CyberSafetyFramework

CyberSafetyFramework

Bizagi Modeler

Table of Contents

1 COMBINEDINCIDENTMONITORINGANDRESPONCEPROCESS


Joint Incident Monitoring Activities ISO 21434/ISO 21448
Monitoring
Analysis
Release
Core SOTIF Team
SOTIF Product Team
Customer SOTIF Team
Cybersecurity Incident Response team
Product Cybersecurity Team
Customer Cybersecurity Response Team
External/Third Party SOTIF Report
Monitoring Product
SOTIF Incident Report
Exclusive Gateway
Cybersecurity Incident
Initial Assessment and Risk Evaluation
Evaluated Initial Risk Is Considered as High
Root Cause Analysis
Cybersecurity Vulnerability
Need of a new cybersecurity control
Recovery Scenarios
Parallel Gateway
Updating Lessons Learned
Lessons Learned Data Base
Process Termination
Tracking activities to closure
Disclose the Initial Assessment Report
Initial Assessment and Risk Evaluation Report
Initial Assessment Report Disclosed in reasonable time
Disclose the Full Assessment Report
SOTIF Incident Database
Incident should contain the ID, product to which its applied to, estimated risks etc.
Add Report to the Data Base
Product Released into the market
Product Risk Assessment
Disclose to customer
Creating the mitigation plan
Refinement of Hazard Identification and Risk Evaluation
New SOTIF Trigger Event
SOTIF Release activities according to ISO 21448
Evaluating the Criteria for SOTIF Release
Software Release
Database Synchronization
Information From customer to stop further activities for a particular SOTIF Risk
Risk Evaluation
No
Yes
Is the SOTIF Risk to Be Mitigated?
Customer SOTIF Report
Initial Report Send to Customer SOTIF team
Acceptable residual risk?
There may be a separate release related to Cybersecurity and SOTIF due to high risk of failure.
Release received by the Customer
External Third Party Cybersecurity Report
Cybersecurity Incident Report
SOTIF Incident
SOTIF Safety Mechanisms Impacted
New SOTIF Trigger
Root Cause Analysis
Recovery Scenario
Initial Assessment and Risk Evaluation
Disclose Initial Cybersecurity Assessment
Cybersecurity Incident Database
Add Report to Cybersecurity Incident Database
Lessons Learned Database
Tracking Activities to closure
Disclose the Full Assessment Report
Disclose To customer
Create Remediation Plan
A new SOTIF risk
Refinement of Threat Analysis and Risk Assessment
Cybersecurity Release activities according to ISO 21434
Vulnerability Mitigated?
Information From customer to stop further activities for a particular Cybersecurity Risk
Customer Cybersecurity Report
Initial Report Send to Customer Cybersecurity Team
Is the Cybersecurity Risk to be Mitigated
Powered by
Modeler

Version:

1.0

Author:

rj2v4c

1.1 JOINT INCIDENT MONITORING ACTIVITIES ISO 21434/ISO 21448

1.1.1 PROCESS ELEMENTS

1.1.1.1 Root Cause Analysis

Description

- Root Cause Analysis is performed if the related risk score for Cybersecurity Incident is High.
- It shall include the detailed information about Cybersecurity related risk and impact on the system.
- The Root Cause Analysis shall be conducted in a reasonable time (to be mutually agreed between supplier and customer).
- If the SOTIF Safety impact is identified, it should be sent to the Core SOTIF Team for further analysis.

Performers

Cybersecurity Core Analyst

Accountable

Cybersecurity Core Manager

Consulted

CyberSafety Manager

Informed

SOTIF Project Manager, Cybersecurity Product Manager, Project Manager

1.1.1.2 Recovery Scenario

Description

- Root Cause Analysis is performed if the related risk score for Cybersecurity Incident is High.
- It shall include the detailed information about Cybersecurity related risk and impact on the system.
- The Root Cause Analysis shall be conducted in a reasonable time (to be mutually agreed between supplier and customer).

- If a new SOTIF trigger is identified, the information shall be sent to the Core SOTIF team.

Performers

Cybersecurity Core Analyst

Accountable

Cybersecurity Core Manager

Consulted

CyberSafety Manager

Informed

SOTIF Project Manager, Project Manager, Cybersecurity Product Manager

1.1.1.3 Parallel Gateway

Description

If recovery scenario is prepared, in parallel Updating Lessons Learned, Trancing activities to closure, Disclose the Full Assessment Report processes shall be triggered.

1.1.1.4 Disclose the Full Assessment Report

Description

Releasing the Full Assessment Report to Customer.

Performers

Cybersecurity Core Analyst

Accountable

Cybersecurity Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Core Manager, Cybersecurity Product Manager

Informed

Project Manager

1.1.1.5 Product Risk Assessment

Description
Conducting a Risk Assessment on a product level.

Performers

Cybersecurity Product System Analyst

Accountable

Cybersecurity Product Manager

Consulted

CyberSafety Manager, Cybersecurity Product System Analyst

Informed

Project Manager

1.1.1.6 Disclose To customer

Description
Releasing the Assessment Report to Customer.

Performers

Cybersecurity Product Manager

Accountable

Cybersecurity Product Manager

Consulted

CyberSafety Manager, Project Manager, Cybersecurity Product System Analyst

Informed

Customer SOTIF Team, Cybersecurity Core Manager

Implementation

WebService

1.1.1.7 Parallel Gateway

Description
If the Full Assessment Report is disclosed it shall be in parallel send to customer as well as stored in the Cybersecurity Incident Database.

1.1.1.8 Risk Evaluation

Description

Customer is evaluating the Cybersecurity risk.

Performers

Customer Cybersecurity Incident Response Team

Consulted

Cybersecurity Core Analyst

Informed

CyberSafety Manager, Cybersecurity Product Manager, Project Manager

1.1.1.9 ◇Is the Cybersecurity Risk to be Mitigated

Description

Decision point at customer side if the Cybersecurity related risk shall be mitigated.

Gates

Yes

No

1.1.1.10 Create Remediation Plan

Description

Creating a remediation plan how to mitigate a Cybersecurity related risk on a product level.

Performers

Cybersecurity Product Manager

Accountable

Cybersecurity Product System Analyst

Consulted

CyberSafety Manager, Project Manager, Cybersecurity Product Software Engineer

Informed

Release Manager

1.1.1.11 Information From customer to stop further activities for a particular Cybersecurity Risk

Description

Information From customer to stop further activities for a particular Cybersecurity Risk

1.1.1.12 Tracking Activities to closure

Description

This process represents a monitoring activities from the Core Cybersecurity Incident Response team to check the progress on a project team level.

Performers

Cybersecurity Core Manager

Accountable

Cybersecurity Core Manager

Consulted

CyberSafety Manager, Cybersecurity Product Manager, Project Manager, SOTIF Project Manager

Informed

Release Manager

1.1.1.13 Updating Lessons Learned

Description

Updating the Lessons Learned Database of Core Cybersecurity Incident Response team.

Performers

Cybersecurity Core Analyst

Accountable

Cybersecurity Core Manager

Consulted

Cybersecurity Product Manager

Informed

CyberSafety Manager, SOTIF Product System Analyst, SOTIF Project Manager, Project Manager

1.1.1.14 Process Termination

Description

After updating the Lessons Learned this process threat is terminated.

1.1.1.15 Parallel Gateway

Description

If the Full Assessment Report is disclosed it shall be in parallel send to customer as well as stored in the SOTIF Incident Database.

1.1.1.16 Risk Evaluation

Description

Customer is evaluating the SOTIF risk.

Performers

Customer SOTIF Team

Accountable

Customer SOTIF Team

Informed

CyberSafety Manager, SOTIF Project Manager, Project Manager

1.1.1.17 Is the SOTIF Risk to Be Mitigated?

Description

Decision point at customer side if the SOTIF related risk shall be mitigated.

Gates

Yes

No

1.1.1.18 Creating the mitigation plan

Description

Creating a plan how to mitigate a SOTIF related risk on a product level.

Performers

SOTIF Project Manager

Accountable

SOTIF Product System Analyst

Consulted

CyberSafety Manager, Project Manager, SOTIF Product Software Engineer

Informed

Release Manager

1.1.1.19 Refinement of Hazard Identification and Risk Evaluation

Description

Having the mitigation plan and Product Risk Assessment the Hazard Identification and Risk Evaluation shall be revisited.

- If during Hazard Identification and Risk Evaluation the new threat scenario is identified it shall be communicated to the Cybersecurity System Architect.

- If during Threat Analysis and Risk Assessment a new safety impact is identified it shall be communicated to the SOTIF System Architect.

Performers

SOTIF Product System Analyst

Accountable

SOTIF Project Manager

Consulted

CyberSafety Manager, Cybersecurity Product System Analyst, Cybersecurity Product Manager, SOTIF Product Software Engineer

Informed

Project Manager

1.1.1.20 SOTIF Release activities according to ISO 21448

Description

Performing all release activities according to the ISO 21448

Performers

SOTIF Project Manager

Accountable

SOTIF Project Manager

Consulted

SOTIF Product System Analyst, SOTIF Product Software Engineer

Informed

Project Manager

1.1.1.21 Evaluating the Criteria for SOTIF Release

Description

Checking if the release fulfills the SOTIF criteria according to ISO 21448.

Performers

SOTIF Product System Analyst

Accountable

SOTIF Product System Analyst

Consulted

SOTIF Project Manager, SOTIF Product Software Engineer, CyberSafety Manager

Informed

Project Manager

1.1.1.22 Acceptable residual risk?

Description

Decision point if a residual risk can be accepted.

Gates

No

Yes

1.1.1.23 Software Release

Description

Internal Release Activities.

Performers

Release Manager

Accountable

Release Manager

Consulted

CyberSafety Manager, Project Manager, SOTIF Project Manager

Informed

Cybersecurity Core Analyst

Implementation

WebService

1.1.1.24 Information From customer to stop further activities for a particular SOTIF Risk

Description

Information From customer to stop further activities for a particular SOTIF Risk

1.1.1.25 Root Cause Analysis

Description

- Root Cause Analysis is performed if the related risk score for SOTIF Incident is High.
- It shall include the detailed information about SOTIF related risk and impact on the system.
- The Root Cause Analysis shall be conducted in a reasonable time (to be mutually agreed between supplier and customer).
- If the Cybersecurity Vulnerability is detected, it should be sent to the Cybersecurity Incident Response Team for further analysis.

Performers

SOTIF Core Analyst

Accountable

SOTIF Core Manager

Consulted

CyberSafety Manager

Informed

Cybersecurity Core Analyst, Cybersecurity Product Manager, Project Manager, SOTIF Project Manager

1.1.1.26 Recovery Scenarios

Description

- Root Cause Analysis is performed if the related risk score for SOTIF Incident is High.
- It shall include the detailed information about SOTIF related risk and impact on the system.
- The Root Cause Analysis shall be conducted in a reasonable time (to be mutually agreed between supplier and customer).
  - If a need for a new Cybersecurity control is identified in shall be send to the Core Cybersecurity Incident Response team.

Performers

SOTIF Core Analyst, SOTIF Core Manager

Accountable

SOTIF Core Manager

Consulted

CyberSafety Manager

Informed

Cybersecurity Core Analyst, Cybersecurity Product Manager, Project Manager, SOTIF Project Manager

1.1.1.27 Parallel Gateway

Description

If recovery scenario is prepared, in parallel Updating Lessons Learned, Trancing activities to closure, Disclose the Full Assessment Report processes shall be triggered.

1.1.1.28 Tracking activities to closure

Description

This process represents a monitoring activities from the Core SOTIF team to check the progress on a project team level.

Performers

SOTIF Core Manager

Accountable

SOTIF Core Manager

Consulted

CyberSafety Manager, Cybersecurity Product Manager, Project Manager, Release Manager, SOTIF Project Manager

Informed

Release Manager

1.1.1.29 Parallel Gateway

Description

As Convergence: is used to merge alternative paths, the gateways waits for all incoming flows before it continues.

1.1.1.30 Release received by the Customer

Description
Release received by the Customer

1.1.1.31 Updating Lessons Learned

Description
Updating the Lessons Learned Database of Core SOTIF team.

Performers
SOTIF Core Analyst

Accountable
SOTIF Core Manager

Consulted
SOTIF Project Manager

Informed
Cybersecurity Core Analyst, Cybersecurity Product Manager, Project Manager, CyberSafety Manager

1.1.1.32 Process Termination

Description
After updating the Lessons Learned this process threat is terminated.

1.1.1.33 Disclose the Full Assessment Report

Description
Releasing the Full Assessment Report to Customer.

Performers
SOTIF Core Analyst

Consulted
CyberSafety Manager, SOTIF Core Manager, SOTIF Project Manager

Informed
Project Manager

1.1.1.34 Refinement of Threat Analysis and Risk Assessment

Description
Having the mitigation plan and Product Risk Assessment the Threat Analysis and Risk Assessment shall be revisited.

- If during Hazard Identification and Risk Evaluation the new threat scenario is identified it shall be communicated to the Cybersecurity System Architect.

- If during Threat Analysis and Risk Assessment a new safety impact is identified it shall be communicated to the SOTIF System Architect.

Performers

Cybersecurity Product System Analyst

Accountable

Cybersecurity Product Manager

Consulted

CyberSafety Manager, SOTIF Product System Analyst, SOTIF Project Manager, Cybersecurity Product Software Engineer

Informed

Project Manager

1.1.1.35 Cybersecurity Release activities according to ISO 21434

Description

Performing all release activities according to the ISO 21434.

Performers

Cybersecurity Product Manager

Accountable

Cybersecurity Product Manager

Consulted

Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst

Informed

Project Manager

1.1.1.36 Vulnerability Mitigated?

Description

Decision point if a risk is properly mitigated.

Gates

No

Yes

1.1.1.37 Software Release

Description
Internal Release Activities.

Performers

Release Manager

Accountable

Release Manager

Consulted

CyberSafety Manager, Cybersecurity Product Manager, Project Manager

Informed

Cybersecurity Core Analyst

Implementation

WebService

1.1.1.38 Parallel Gateway

Description
As Convergence: is used to merge alternative paths, the gateways waits for all incoming flows before it continues.

1.1.1.39 Release received by the Customer

Description
Release received by the Customer

1.1.1.40 Parallel Gateway

Description
If Initial Assessment Report is ready it should in parallel be stored in database and send to customer.

1.1.1.41 Add Report to the Data Base

Description

Adding the SOTIF Incident Report to the Organization Data base.

Performers

SOTIF Core Analyst

Consulted

CyberSafety Manager, SOTIF Core Manager, SOTIF Project Manager

Informed

Project Manager

1.1.1.42 Process Termination

Description

After adding the information to a SOTIF Incident Data Base this process threat shall be terminated.

1.1.1.43 Initial Report Send to Customer SOTIF team

Description

Initial Report Send to Customer SOTIF team

1.1.1.44 Parallel Gateway

Description

If Initial Assessment Report is ready it should in parallel be stored in database and send to customer.

1.1.1.45 Add Report to Cybersecurity Incident Database

Description

Adding the Cybersecurity Incident Incident Report to the Organization Data base.

Performers

Cybersecurity Core Analyst

Accountable

Cybersecurity Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Core Manager, Cybersecurity Product Manager

Informed

Project Manager

1.1.1.46 Process Termination

Description

After adding the information to a Cybersecurity Incident Data Base this process threat shall be terminated.

1.1.1.47 Initial Report Send to Customer Cybersecurity Team

Description

Initial Report Send to Customer Cybersecurity Team

1.1.1.48 Exclusive Gateway

Description

If any Cybersecurity Incident, or Cybersecurity Vulnerability or a Need of a new Cybersecurity control message is triggered, this information shall be passed to Cybersecurity Incident Response team.

Gates

Elusive Gateway

1.1.1.49 Product Released into the market

Description

Indication from the Product them that SOTIF product reach the commercial market.

1.1.1.50 Parallel Gateway

Description

Once the Product is release to the market, SOTIF and Cybersecurity Monitoring Activities shall be triggered in parallel.

1.1.1.51 Monitoring Product

Description

ε Monitoring SOTIF Product on the market based on the internal and external inputs.

Performers

Customer SOTIF Team, SOTIF Core Analyst

Accountable

SOTIF Core Manager

Consulted

CyberSafety Manager, SOTIF Core Manager

Informed

Cybersecurity Product Manager, Project Manager, SOTIF Project Manager

Implementation

WebService

1.1.1.52 Monitoring Product

Description

- Monitoring Cybersecurity Product on the market based on the internal and external inputs.

Performers

Customer Cybersecurity Incident Response Team, Cybersecurity Core Analyst

Accountable

Cybersecurity Product System Analyst

Consulted

CyberSafety Manager, Cybersecurity Core Manager

Informed

Project Manager, Cybersecurity Product Manager, SOTIF Project Manager

Implementation

WebService

1.1.1.53 Exclusive Gateway

Description

If any SOTIF Incident, or New SOTIF Trigger or SOTIF Safety Mechanism is identified, this information shall be passed to SOTIF Incident Response team.

Gates

Exclusive Gateway

1.1.1.54 External/Third Party SOTIF Report

Description

External SOTIF Report may come from an independent organization monitoring the market for the SOTIF incidents i.e. market regulator, university, foundation etc.

1.1.1.55 Customer SOTIF Report

Description

SOTIF report indicating the vulnerability found my the car producer.

1.1.1.56 Exclusive Gateway

Description

If an Incident Report comes from any defined source, the Initial Assessment and Risk Evaluation shall be triggered.

Gates

Initial Assessment and Risk Evaluation

1.1.1.57 Initial Assessment and Risk Evaluation

Description

Conducting an initial assessment and risk evaluation of and incident.

- If a SOTIF incident has Cybersecurity criteria fulfilled , should be also passed to the Core Cybersecurity Incident Response Team.

- The Initial Assessment and Risk Evaluation shall be conducted in an reasonable time (to be discussed mutually between supplier and customer).

- If the Evaluated Risk is considered as High, the Core SOTIF team should perform a Root Cause Analysis.

- Initial Assessment and Risk Evaluation shall focus on a high level system impact and rank it accordingly for a decision if a detailed analysis is needed.

Performers

SOTIF Core Analyst

Accountable

SOTIF Core Manager

Consulted

CyberSafety Manager

Informed

Cybersecurity Core Analyst, Cybersecurity Product Manager, Project Manager, SOTIF Project Manager

Implementation

WebService

1.1.1.58 Product Risk Assessment

Description

Conducting a Risk Assessment on a product level.

Performers

SOTIF Product System Analyst

Accountable

SOTIF Project Manager

Consulted

CyberSafety Manager, SOTIF Product Software Engineer

Informed

Project Manager

1.1.1.59 Disclose to customer

Description

Releasing the Assessment Report to Customer

Performers

SOTIF Project Manager

Accountable

SOTIF Project Manager

Consulted

CyberSafety Manager, Project Manager, SOTIF Product System Analyst

Informed

Customer SOTIF Team, SOTIF Core Manager

Implementation

WebService

1.1.1.60 External Third Party Cybersecurity Report

Description

External Cybersecurity Report may come from an independent organization monitoring the market for the Cybersecurity incidents i.e. market regulator, university, foundation etc.

1.1.1.61 Customer Cybersecurity Report

Description

Cybersecurity report indicating the vulnerability found my the car producer.

1.1.1.62 Elusive Gateway

Description

If an Incident Report comes from any source, the Initial Assessment and Risk Evaluation shall be triggered.

Gates

Initial Assessment and Risk Evaluation

1.1.1.63 Initial Assessment and Risk Evaluation

Description

Conducting an initial assessment and risk evaluation of and incident.

- If a Cybersecurity Event incident has Safety implications , should be also passed to the Core SOTIF Incident Response Team.

- The Initial Assessment and Risk Evaluation shall be conducted in an reasonable time (to be discussed mutually between supplier and customer).

- If the Evaluated Risk is considered as High, the Core Cybersecurity Incident Response team should perform a Root Cause Analysis.

- Initial Assessment and Risk Evaluation shall focus on a high level system impact and rank it accordingly for a decision if a detailed analysis is needed.

Performers

Cybersecurity Core Analyst

Accountable

Cybersecurity Core Manager

Consulted

CyberSafety Manager

Informed

Cybersecurity Core Analyst, SOTIF Project Manager, Cybersecurity Product Manager, Project Manager

Implementation

WebService

1.1.1.64 Disclose the Initial Assessment Report

Description

Initial Assessment Report Should be disclosed to The Customer in a reasonable time period.

Exact timing shall be mutually agreed between supplier and customer.

Performers

SOTIF Core Analyst

Consulted

CyberSafety Manager, SOTIF Project Manager, SOTIF Core Manager

Informed

Project Manager

1.1.1.65 Disclose Initial Cybersecurity Assessment

Description

Initial Assessment Report Should be disclosed to The Customer in a reasonable time period.

Exact timing shall be mutually agreed between supplier and customer.

Performers

Cybersecurity Core Analyst

Accountable

Cybersecurity Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Product Manager, Cybersecurity Core Manager

Informed

Project Manager

1.1.1.66 SOTIF Incident Database

Description

Database entity which stores the SOTIF Incidents.

1.1.1.67 Lessons Learned Data Base

Description

Storage of Lessons Learned of SOTIF incidents activities.

1.1.1.68 Cybersecurity Incident Database

Description

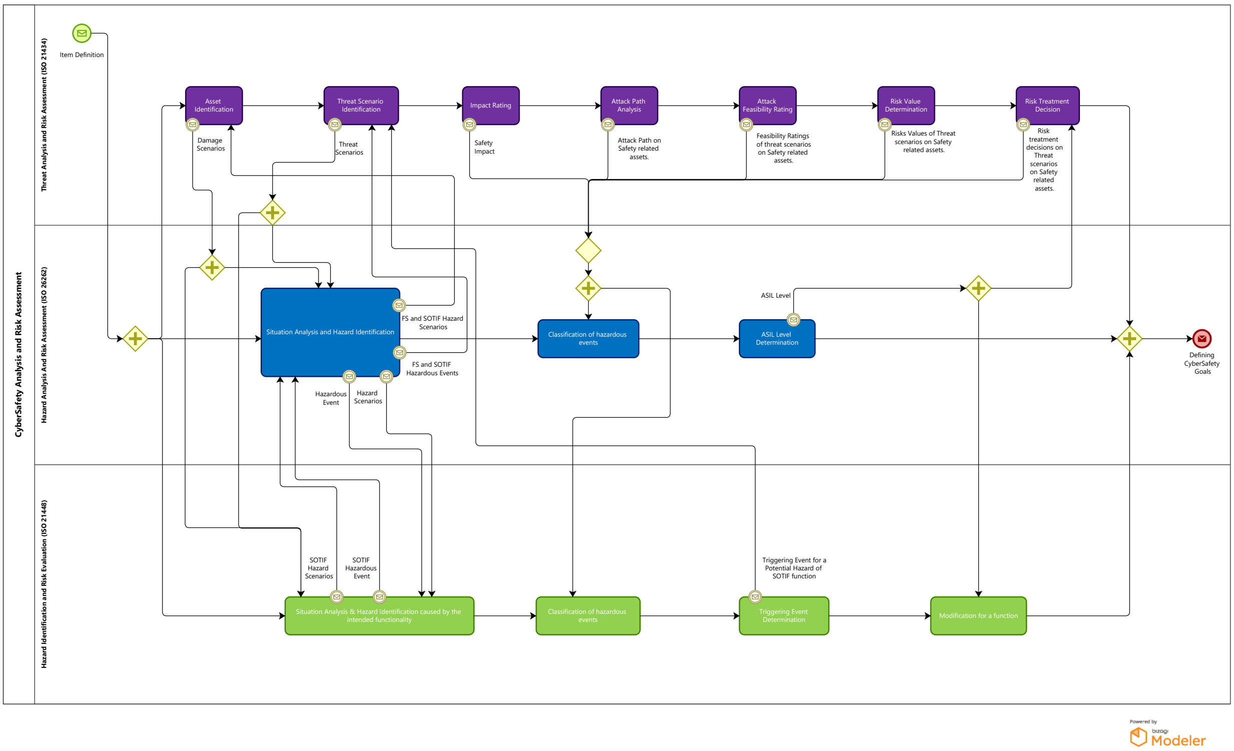
Storage of Cybersecurity Incident Reports.

1.1.1.69 Lessons Learned Database

Description

Storage of Lessons Learned of Cybersecurity incidents activities.

2 CYBERSAFETY ANALYSIS AND RISK ASSESMENT


CyberSafety Analysis and Risk Assessment
Threat Analysis and Risk Assessment (ISO 21434)
Hazard Analysis And Risk Assessment (ISO 26262)
Hazard Identification and Risk Evaluation (ISO 21448)
Item Definition
Asset Identification
Threat Scenario Identification
Impact Rating
Attack Path Analysis
Attack Feasibility Rating
Risk Value Determination
Risk Treatment Decision
Damage Scenarios
Threat Scenarios
Safety Impact
Attack Path on Safety related assets.
Feasibility Ratings of threat scenarios on Safety related assets.
Risks Values of Threat scenarios on Safety related assets.
Risk treatment decisions on Threat scenarios on Safety related assets.
Situation Analysis and Hazard Identification
FS and SOTIF Hazard Scenarios
FS and SOTIF Hazardous Events
Hazardous Event
Hazard Scenarios
Classification of hazardous events
ASIL Level
ASIL Level Determination
Defining CyberSafety Goals
SOTIF Hazard Scenarios
SOTIF Hazardous Event
Situation Analysis & Hazard Identification caused by the intended functionality
Classification of hazardous events
Triggering Event for a Potential Hazard of SOTIF function
Triggering Event Determination
Modification for a function
Powered by bizagi Modeler

Version:

1.0

Author:

rj2v4c

2.1 CYBERSAFETY ANALYSIS AND RISK ASSESSMENT

2.1.1 PROCESS ELEMENTS

2.1.1.1 Asset Identification

Description

Prerequisites:

- Item Definition

Further Supporting Information

- Cybersecurity Specifications

Requirements and recommendations

- Damage scenarios shall be identified.
- Assets with cybersecurity properties whose compromise leads to a damage scenario shall be identified.

Work Products

- Damage scenarios
- Assets with cybersecurity properties

Performers

Cybersecurity Product System Analyst

Accountable

Cybersecurity Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Software Engineer, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Software Architect

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

2.1.1.2 Threat Scenario Identification

Description

Prerequisites:

- Item Definition

Further Supporting Information

- Cybersecurity Specifications
- Damage Scenarios
- Assets with Cybersecurity properties

Requirements and recommendations

- Threat scenarios shall be identified and include:
  - targeted asset;
  - compromised cybersecurity property of the asset
  - cause of compromise of the cybersecurity property

- Assets with cybersecurity properties whose compromise leads to a damage scenario shall be identified.

Work Products

- Threat scenarios

Performers

Cybersecurity Product System Analyst

Accountable

Cybersecurity Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Product Software Engineer, SOTIF Software Architect

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

2.1.1.3 □Impact Rating

Description

Prerequisites:

- Damage Scenarios

Further Supporting Information

- Item Definition
- Assets with Cybersecurity Properties

Requirements and recommendations

- The damage scenarios shall be assessed against potential adverse consequences for road users in the impact categories of safety, financial, operational, and privacy (S, F, O, P) respectively
- The impact rating of a damage scenario shall be determined for each impact category to be one of the following:
  - severe
  - major
  - moderate
  - negligible
- Safety related impact ratings shall be derived from ISO 26262-3:2018
- If a damage scenario results in an impact rating and an argument can be made that every impact category is considered less critical , then further analysis for that other impact category my be omitted.

Work Products

- Impact ratings with associated impact categories.

Performers

Cybersecurity Product System Analyst

Accountable

Cybersecurity Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect

Informed

Core Quality Product Engineer, Quality Product Engineer, Project Manager

2.1.1.4 Attack Path Analysis

Description

Prerequisites:

- Item definition or cybersecurity specifications
- Threat scenarios

Further Supporting Information

- Weaknesses from cybersecurity events
- Weaknesses found during product development
- Architectural Design
- Previously identified Attack Paths, if available
- Vulnerability Analysis

Requirements and recommendations

- The threat scenarios shall be analyzed to identify attack paths.
- An attack path shall be associated with the threat scenarios that can be realized by the attack path

Work Products

- Attack paths

Performers

Cybersecurity Product System Analyst

Accountable

Cybersecurity Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

2.1.1.5 Attack Feasibility Rating

Description

Prerequisites:

- Attack paths

Further Supporting Information

- Architectural design;
- Vulnerability Analysis;

Requirements and recommendations

- For each attack path, the attack feasibility rating shall be determined with an assigned rating
- The attack feasibility rating method should be defined based on one of the following approaches;
  - attack potential-based approach;
  - CVSS-based approach;
  - attack-vector based approach

- If an attack potential-based approach is used, the attack feasibility rating should be determined based on core factors including:
  - elapsed time;
  - specialist expertise;
  - knowledge of the item or component;
  - window of opportunity;
  - equipment.
- If a CVSS-based approach is used, the attack feasibility rating should be determined based on the exploitability metrics of the base metric group, including:
  - attack vector;
  - attack complexity;
  - privileges required;
  - user interaction
- If an attack vector-based approach is used, the attack feasibility rating should be determined based on evaluating the predominant attack vector of the attack path

Work Products

- Attack feasibility ratings

Performers

Cybersecurity Product System Analyst

Accountable

Cybersecurity Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

2.1.1.6 Risk Value Determination

Description

Prerequisites

- Threat Scenarios
- Impact ratings with associated impact categories
- Attack feasibility ratings

Further Supporting Information

- None

Requirements and recommendations

- For each threat scenario the risk value shall be determined from the impact of the associated damage scenarios and the attack feasibility of the associated attack paths.
- The risk value of a threat scenario shall be a value between 1 and 5, where a value 1 represents minimal risk

Work Products

- Risk values

Performers

Cybersecurity Product System Analyst

Accountable

Cybersecurity Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

2.1.1.7 Situation Analysis & Hazard Identification caused by the intended functionality

Description

Prerequisites:

- Item Definition

Requirements and recommendations

- The hazards, caused by the unintended behavior of the function, are determined systematically. This systematic identification is primarily based on knowledge about the function and its possible deviations. This can be achieved by applying the methods proposed in ISO 26262-3:2018 while considering performance limitations of the intended functionality.

- The operational situations and operating modes in which an item's malfunctioning behavior, considering performance limitations of the intended functionality, will result in a hazardous event shall be described; both when the vehicle is correctly used and when it is incorrectly used in a reasonably foreseeable way.

- The hazards shall be determined systematically based on possible malfunctioning behavior of the item.

- Hazards caused by malfunctioning behavior of the item, considering performance limitations of the intended functionality, shall be defined at the vehicle level.

- If there are hazards identified in this clause that are outside of the scope of ISO 26262, then these hazards shall be addressed according to organization specific procedures.

- Relevant hazardous events shall be determined.

- The consequences of hazardous events shall be identified.

Work Products

- Systems Hazards Scenarios related to SOTIF

- Hazardous Events related to SOTIF

Performers

SOTIF Product System Analyst

Accountable

Cybersecurity Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Cybersecurity Test Engineer, Functional Safety Core Manager, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Functional Safety Test Engineer, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer, Project Software Architect, Project System Architect, Cybersecurity Core Analyst, Cybersecurity Core Manager, SOTIF Core Manager

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

2.1.1.8 □Classification of hazardous events

Description

Prerequisites:

- Item Definition
- System Hazard Scenarios related to SOTIF
- Hazardous Events related to SOTIF

Requirements and recommendations

- The harm and controllability of hazardous events can be estimated using the method described in ISO 26262-3:2018, Clause 6 but their evaluation for an individual hazardous event can be specific to a given SOTIF related hazard.
- The severity and controllability of the potentially hazardous behavior, in a given scenario, are considered to determine whether a credible harm can result. For hazardous event classification a delayed or no reaction to control the hazard, from the involved persons, can be considered.
- All hazardous events identified shall be classified, except those that are outside the scope of ISO 26262-3.
- The severity of potential harm shall be estimated based on a defined rationale for each hazardous event. The severity shall be assigned to one of the severity classes S0, S1, S2 or S3 in accordance with ISO 26262-3
- There are operational situations that result in harm (e.g. an accident). A subsequent malfunctioning behavior of the item in such an operational situation can increase, or fail to decrease, the resulting harm. In this case the classification of the severity may be limited to the difference between the severity caused by the initial operational situation (e.g. the accident) and the malfunctioning behavior of the item.
- The severity class S0 may be assigned if the hazards analysis and risk assessment determines that the consequences of a malfunctioning behavior of the item are clearly limited to material damage. If a hazardous event is assigned severity class S0, no ASIL assignment is required.
- The probability of exposure of each operational situation shall be estimated based on a defined rationale for each hazardous event. The probability of exposure shall be assigned to one of the probability classes, E0, E1, E2, E3 or E4 in accordance with ISO 26262-3
- The number of vehicles equipped with the item shall not be considered when estimating the probability of exposure.
- Class E0 may be used for those operational situations that are suggested during hazards analysis and risk assessment, but that are considered incredible, and therefore not explored further. A rationale shall be recorded

for the exclusion of these situations. If a hazardous event is assigned exposure class E0, no ASIL assignment is required.

- The controllability of each hazardous event, by the driver or other persons involved in the operational situation shall be estimated based on a defined rationale for each hazardous event. The controllability shall be assigned to one of the controllability classes C0, C1, C2 or C3 in accordance with ISO 26262-3

- Class C0 may be used for hazards addressing the unavailability of the item if they do not affect the safe operation of the vehicle (e.g. some driver assistance systems) or if an accident can be avoided by routine driver actions. If a hazardous event is assigned controllability class C0, no ASIL assignment is required.

Work Products

- Severity Class of a hazards scenario of SOTIF function

- Exposure Class of a hazards scenario of SOTIF function

- Controllability Class of a hazard scenario of SOTIF function

Performers

SOTIF Product System Analyst

Accountable

SOTIF Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Core Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Cybersecurity Test Engineer, Functional Safety Core Manager, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Functional Safety Test Engineer, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer, Project Software Architect, Project System Architect

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

2.1.1.9 □Triggering Event Determination

Description

Objectives:

Identification and Evaluation of triggering events:

- That can trigger potentially hazardous behavior shall be identified;
- Shall be evaluated for their acceptability with respect to SOTIF;

Prerequisites:

- Item Definition
- System Hazard Scenarios related to SOTIF
- Hazardous Events related to SOTIF
- Classification of hazardous events

Requirements and recommendations

- A systematic method can be established to perform the analysis of triggering events. This method can consider knowledge gained from similar projects and field experience. The analysis aims to identify the system weaknesses (including those of its sensors, algorithms, actuators) and the related scenarios that could lead to an identified hazard.
- The analysis can be conducted in parallel, starting from both:
    - the known limitations of the system components to determine scenarios that could result in hazardous behavior the to these limitations
    - the identified environment conditions and foreseeable missuses to determine the system limitations that could trigger potentially hazardous behavior of the system
- Triggering events related to algorithms, sensors and actuators shall be evaluated
- The identified triggering events are evaluated considering the acceptance criteria that are specified during the SOTIF risk identification and evaluation
- The response of the system to these triggering events can be considered as acceptable with respect to the SOTIF without need of further functional improvement (as described in Clause 8) if:
    - The probability of the system causing a hazardous event is lower than the validation target value
    - There is no systematically unacceptable scenario in relation to a specific vehicle that has the potential to lead to a hazardous event.

Work Products

- Triggering events of hazardous events of SOTIF

Performers

SOTIF Product System Analyst

Accountable

SOTIF Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Core Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Cybersecurity Test Engineer, Functional Safety Core Manager, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Functional Safety Test Engineer, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer, Project Software Architect, Project System Architect

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

2.1.1.10 Risk Treatment Decision

Description

Prerequisites

- Item definition
- Threat scenarios
- Risk Values

Further Supporting Information

- Cybersecurity specifications;
- Previous risk treatment decisions of the item or component, or similar items or components;
- impact ratings with associated impact categories;
- Attack Paths;
- Attack feasibility ratings;

Requirements and recommendations

- For each threat scenario, considering its risk values, one or more of the following risk treatment option(s) shall be determined:
    - avoiding the risk
    - reducing the risk
    - sharing the risk
    - retaining the risk

Work Products

- Risk treatment decisions

Performers

Functional Safety Product System Analyst

Accountable

Cybersecurity Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Project Manager, SOTIF Product System Analyst, SOTIF Software Architect

Informed

Core Quality Product Engineer, Quality Product Engineer, Project Manager

2.1.1.11 Modification for a function

Description

Objectives:

The development activities of the functional modifications to reduce the SOTIF related risks shall achieve the following objectives:

- identification and allocation of measures to avoid, reduce, or mitigate the SOTIF related risks;
- estimation of the effect of the SOTIF related measures on the intended function; and
- improvement of the information required by Clause 5 (Functional and system specification).

Prerequisites:

- Item Definition
- System Hazard Scenarios related to SOTIF

- Hazardous Events related to SOTIF
- Classification of hazardous events
- Definition and evaluation of triggering events

Requirements and recommendations

- This sub-clause deals with identification of measures to avoid, reduce, or mitigate the SOTIF related risks. The function and system descriptions are developed through several iterations and each time the Functional and System specification (required by Clause 5) is updated with information about the identified measures.
- A functional modification to reduce SOTIF related risks may be needed when the identified triggering events:
    - have the possibility to trigger a potentially hazardous behavior leading to a hazardous event with credible harm (according to Clause 6); and
    - cannot be evaluated as acceptable with respect to the safety of the intended functionality (according to Clause 7).
- To support achieving the objectives of this clause, the following information can be considered:
    - information on the system architectural design;
    - the functionality which is defined and described in accordance with Clause 5;
    - the evaluation of the potential outcome of possible hazardous events in accordance with Clause 6;
    - the possible scenarios that can trigger an unintended system behavior leading to a hazardous event in accordance with Clause 7;
    - knowledge derived from previous verification results, where the system and components did not behave as expected for specific use cases during verification in accordance with Clause 10 (if any); and
    - knowledge derived from previous validation results including real-life use cases, where the function did not behave as expected and the system and component limitations cause an unreasonable level of risk in accordance with Clause 11 (if any).

Work Products

- Refined System Specification related to SOTIF

Performers

SOTIF Product System Analyst

Accountable

SOTIF Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Core Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Cybersecurity Test Engineer, Functional Safety Core Manager, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Functional Safety Test Engineer, Project Software Architect, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

2.1.1.12 Situation Analysis and Hazard Identification

Description

Prerequisites:

- Item Definition

Requirements and recommendations

- The operational situations and operating modes in which an item's malfunctioning behavior will result in a hazardous event shall be described; both when the vehicle is correctly used and when it is incorrectly used in a reasonably foreseeable way.

- The hazards shall be determined systematically based on possible malfunctioning behavior of the item.

- Hazards caused by malfunctioning behavior of the item shall be defined at the vehicle level.

- If there are hazards identified in this clause that are outside of the scope of ISO 26262, then these hazards shall be addressed according to organization specific procedures.

- Relevant hazardous events shall be determined.

- The consequences of hazardous events shall be identified.

- It shall be ensured that the chosen level of detail of the list of operational situations does not lead to an inappropriate lowering of the ASIL.

Work Products

- Systems Hazards Scenarios

- Hazardous Events

Performers

Functional Safety Product System Analyst

Accountable

Functional Safety Core Manager

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Functional Safety Manager, Functional Safety Product System Analyst, Functional Safety Product Software Engineer, Project Software Architect, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

2.1.1.13 □Classification of hazardous events

Description

Prerequisites:

- Item Definition

- System Hazard Scenarios
- Hazardous Events

Requirements and recommendations

- All hazardous events identified shall be classified, except those that are outside the scope of ISO 26262-3.
- The severity of potential harm shall be estimated based on a defined rationale for each hazardous event. The severity shall be assigned to one of the severity classes S0, S1, S2 or S3 in accordance with ISO 26262-3
- There are operational situations that result in harm (e.g. an accident). A subsequent malfunctioning behavior of the item in such an operational situation can increase, or fail to decrease, the resulting harm. In this case the classification of the severity may be limited to the difference between the severity caused by the initial operational situation (e.g. the accident) and the malfunctioning behavior of the item.
- The severity class S0 may be assigned if the hazards analysis and risk assessment determines that the consequences of a malfunctioning behavior of the item are clearly limited to material damage. If a hazardous event is assigned severity class S0, no ASIL assignment is required.
- The probability of exposure of each operational situation shall be estimated based on a defined rationale for each hazardous event. The probability of exposure shall be assigned to one of the probability classes, E0, E1, E2, E3 or E4 in accordance with ISO 26262-3
- The number of vehicles equipped with the item shall not be considered when estimating the probability of exposure.
- Class E0 may be used for those operational situations that are suggested during hazards analysis and risk assessment, but that are considered incredible, and therefore not explored further. A rationale shall be recorded for the exclusion of these situations. If a hazardous event is assigned exposure class E0, no ASIL assignment is required.
- The controllability of each hazardous event, by the driver or other persons involved in the operational situation shall be estimated based on a defined rationale for each hazardous event. The controllability shall be assigned to one of the controllability classes C0, C1, C2 or C3 in accordance with ISO 26262-3
- Class C0 may be used for hazards addressing the unavailability of the item if they do not affect the safe operation of the vehicle (e.g. some driver assistance systems) or if an accident can be avoided by routine driver actions. If a hazardous event is assigned controllability class C0, no ASIL assignment is required.

Work Products

- Severity Class of a hazards scenario
- Exposure Class of a hazards scenario

- Controllability Class of a hazard scenario

Performers

Functional Safety Product System Analyst

Accountable

Functional Safety Core Manager

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

2.1.1.14 □ASIL Level Determination

Description

Prerequisites:

- Severity Class of a hazards scenario
- Exposure Class of a hazards scenario
- Controllability Class of a hazard scenario

Requirements and recommendations

- An ASIL shall be determined for each hazardous event based on the classification of severity, probability of exposure and controllability, in accordance with ISO 26262-3
- Four ASILs are defined: ASIL A, ASIL B, ASIL C and ASIL D, where ASIL A is the lowest safety integrity level and ASIL D the highest one.
- In addition to these four ASILs, the class 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.

- If several unlikely situations are combined that result in a lower probability of exposure than E1, QM may be argued for S3, C3 based on this combination.

Work Products

- ASIL Level

Performers

Functional Safety Product System Analyst

Accountable

Functional Safety Core Manager

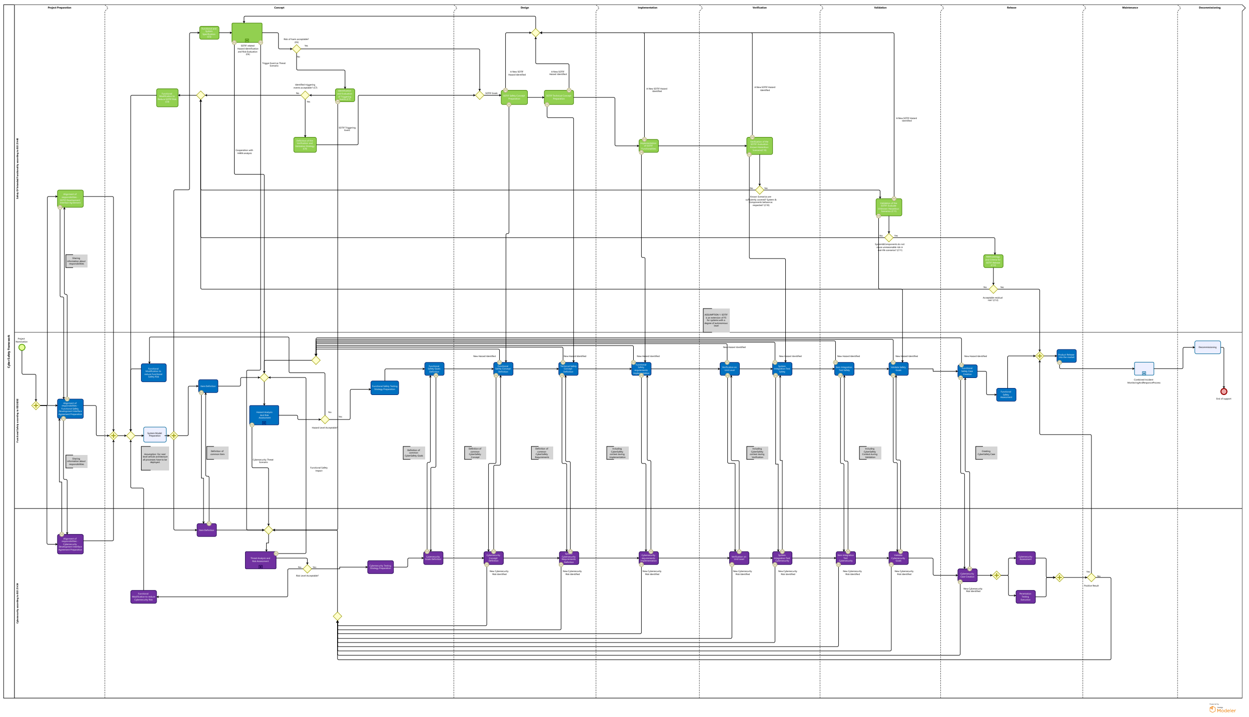
Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Software Architect, SOTIF Project Manager

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

3 CYBERSAFETYFRAMEWORK


Cyber Safety Framework
Safety Of Intended Functionality according to ISO 21448
Functional Safety according to ISO 26262
Cybersecurity according to ISO 21434
Project Preparation
Concept
Design
Implementation
Verification
Validation
Release
Maintenance
Decommissioning
Project Nomination
SOTIF related Hazard Identification and Risk Evaluation (C6)
Risk of harm acceptable? (C6)
Yes
No
Trigger Event as Threat Scenario
Identified triggering events acceptable? (C7)
SOTIF Triggering Event
SOTIF Goals
SOTIF Safety Concept Preparation
SOTIF Technical Concept Preparation
A New SOTIF Hazard Identified

Version:

1.0

Author:

rj2v4c

3.1 CYBER SAFETY FRAMEWORK

3.1.1 PROCESS ELEMENTS

3.1.1.1 □Alignment of responsibilities - Cybersecurity Development Interface Agreement Preparation

Description

Objective:

The objective of this activity is to define the interactions, dependencies, and responsibilities for distributed cybersecurity activities between customers and suppliers.

[RQ-07-04] A customer and a supplier shall specify the distributed cybersecurity activities in a cybersecurity interface agreement including:

a) appointment of customer's and supplier's points of contact regarding cybersecurity;

b) identification of cybersecurity activities that are to be performed by customer and supplier,respectively;

c) if applicable, a joint tailoring of cybersecurity activities;

d) the information and the work products to be shared;

e)milestones regarding the distributed cybersecurity activities

f)definition of the end of cybersecurity support for the item or component

[RC-07-05] The cybersecurity interface agreement should be mutually agreed upon between customer and supplier prior to the start of the distributed cybersecurity activities.

[RQ-07-06] If there is an identified vulnerability to be managed in accordance with [RQ-08-07], the customer and supplier shall agree on actions and responsibility for those actions.

[RQ-07-07] If requirements are unclear, not feasible, or conflict with other cybersecurity requirements or requirements from other disciplines, then customer and supplier shall each notify the other so that appropriate decisions and actions can be taken.

[RC-07-08] Responsibilities should be specified in a responsibility assignment matrix.

Work Products:

[WP-07-01] Cybersecurity interface agreement

Performers

Cybersecurity Product Manager

Accountable

CyberSafety Manager

Consulted

Cybersecurity Core Manager, Functional Safety Manager

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

3.1.1.2 □Alignment of responsibilities - Functional Safety Development Interface Agreement Preparation

Description

Objective:

The Development Interface Agreement (DIA) aims to describe the roles and responsibilities between the customer and supplier for functional safety.

Consequently the safety planning by the customer and supplier is in line with the DIA.

5.4.3.1 The customer and the supplier shall specify a DIA including the following:

- the appointment of the customer’s and the supplier’s safety managers;
- the joint tailoring of the safety activities in accordance with ISO 26262-2:2018;
- the activities of the safety life-cycle to be performed by the customer and the activities of the safety life-cycle to be performed by the supplier;
- the information and the work products to be shared, including distribution and reviews;
- the responsibility assigned to each party for each activity;
- the communication or confirmation of the target values, derived from the system level targets, to each relevant party in order for them to meet the target values for single-point fault metric and latent fault metric in accordance with the evaluation of the hardware architectural metrics and the evaluation of safety goal violations due to random hardware failures (see ISO 26262-5);
- the interface-related processes, methods and tools needed for the collaboration between customer and supplier;
- the agreement on which party (supplier or customer) performs the safety validation in accordance with ISO 26262-4;
- the functional safety assessment activities, in accordance with ISO 26262-2, regarding the elements or work products developed by the supplier;
- the planning of the supplier's functional safety assessment report;
- the agreement between customer and supplier(s) that allows a customer assigned auditor to perform functional safety audits at the supplier's premises.

Work Product:

Development Interface Agreement (DIA)

Performers

Functional Safety Manager

Accountable

CyberSafety Manager

Consulted

Cybersecurity Product Manager, Functional Safety Core Manager

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

3.1.1.3 Alignment of responsibilities - SOTIF Development Interface Agreement

Description

Objective:

The Development Interface Agreement (DIA) aims to describe the roles and responsibilities between the customer and supplier for functional safety.

Consequently the safety planning by the customer and supplier is in line with the DIA.

5.4.3.1 The customer and the supplier shall specify a DIA including the following:

- the appointment of the customer’s and the supplier’s safety managers;
- the joint tailoring of the safety activities in accordance with ISO 21448:2022;
- the activities of the safety life-cycle to be performed by the customer and the activities of the safety life-cycle to be performed by the supplier;
- the information and the work products to be shared, including distribution and reviews;
- the responsibility assigned to each party for each activity;
- the communication or confirmation of the target values, derived from the system level targets
- the interface-related processes, methods and tools needed for the collaboration between customer and supplier;
- the agreement on which party (supplier or customer) performs the safety validation
- the functional safety assessment activities regarding the elements or work products developed by the supplier;
- the planning of the supplier's functional safety assessment report;
- the agreement between customer and supplier(s) that allows a customer assigned auditor to perform functional safety audits at the supplier's premises.

Work Product:

Development Interface Agreement (DIA)

Performers

SOTIF Project Manager

Accountable

CyberSafety Manager

Consulted

Cybersecurity Product Manager, Functional Safety Manager

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

3.1.1.4 System Model Preparation

Description

Objective

- to develop abstract model of a system, with each model presenting a different view or perspective of that system

Recommendations

- System modeling shall consist of following elements:
  - Language
  - Structure
  - Argumentation
  - Presentation
- System model shall include structural and behavioral elements to better express the system relationships.
- The model is used to prove the concept of the design;
- The model must be viewable;

Work product:

System Model

Performers

Project System Architect

Accountable

CyberSafety Manager

Consulted

Cybersecurity Core Analyst, Cybersecurity Product Manager, Cybersecurity Penetration Testing Engineer, Functional Safety Core Manager, Functional Safety Manager, Functional Safety Product System Analyst, Project Software Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Project Manager, SOTIF Software Architect

Informed

Project Manager, Core Quality Product Engineer, Quality Product Engineer

3.1.1.5 Item Definition

Description

Objective:

- define the item, its operational environment and their interactions in the context of cybersecurity

The following information can be considered:

- existing information regarding the item and the operational environment.

Requirements and recommendations:

[RQ-09-01] The following information on the item shall be identified:

- item boundary;
- item functions;
- preliminary architecture;

[RQ-09-02] Information about the operational environment of the item relevant to cybersecurity shall be described.

Work Products:

[WP-09-01] Item definition

Performers

Cybersecurity Product System Analyst

Accountable

Cybersecurity Product Manager

Consulted

Cybersecurity Core Analyst, Cybersecurity Core Manager, Functional Safety Manager, Functional Safety Product System Analyst, Project System Architect, SOTIF Product System Analyst, SOTIF Project Manager

Informed

Cybersecurity Core Manager

3.1.1.6 Threat Analysis and Risk Assessment

Description

Description:

This activity describes methods to determine the extent to which a road user can be impacted by a threat scenario. These methods and their work products are collectively known as a threat analysis and risk assessment (TARA) and are performed from the viewpoint of affected road users. The methods defined in this clause are generic modules that can be invoked systematically, and from any point in the life cycle of an item or component:

- asset identification
- threat scenario identification
- impact rating
- attack path analysis
- attack feasibility rating
- risk value determination
- risk treatment decision

The objectives are to:

- identify assets, their cybersecurity properties and their damage scenarios;
- identify threat scenarios;
- determine the impact rating of damage scenarios;
- identify the attack paths that realize threat scenarios;
- determine the ease with which attack paths can be exploited;
- determine the risk values of threat scenarios; and
- select appropriate risk treatment options for threat scenarios.

Requirements and recommendations:

[RQ-15-01] Damage scenarios shall be identified.

[RQ-15-02] Assets with cybersecurity properties whose compromise leads to a damage scenario shall be identified.

Work Products:

- Damage scenarios,
- Assets with cybersecurity properties

Performers

Cybersecurity Product System Analyst

Accountable

Cybersecurity Core Analyst

Consulted

CyberSafety Manager, Cybersecurity Core Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Functional Safety Manager, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, Cybersecurity Test Engineer, SOTIF Test Engineer

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

Process

3.1.1.7 CyberSafety Analysis and Risk Assesment - CyberSafety Analysis and Risk Assessment Cybersecurity Testing Strategy Preparation

Description

Objectives:

1. A verification and validation strategy shall be defined such that:
    - It supports the rationale for the cybersecurity
    - The necessary evidence is generated
    - The procedures to generate the evidence are developed

2. A verification and validation strategy shall include:
    - Level and scope of testing strategy for defined cybersecurity specification;
    - Level and scope of penetration tests;
    - Level and scope of Vulnerability Scanning;
    - Level and scope of Fuzz testing;
    - The robustness of the system or function;
    - The ability of the system to prevent cybersecurity risks;

Work Product:

Cybersecurity Test Strategy

Performers

Cybersecurity Test Engineer

Accountable

Cybersecurity Product Manager

Consulted

CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Core Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Functional Safety Core Manager, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Functional Safety Test Engineer, Project System Architect, Project Software Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

3.1.1.8 Cybersecurity Goals Definition

Description

Objective:

- Defining Cybersecurity requirements, to protect asses against a threat scenario.

Requirements and recommendations:

- A verification shall be performed to confirm completeness, correctness and consistency of the cybersecurity goals with respect to the risk treatment decisions

- A verification shall be preformed to confirm consistency of all cybersecurity goals of the item

Work product:

- Cybersecurity Goals

Performers

Cybersecurity Product System Analyst

Accountable

Cybersecurity Product Manager

Consulted

CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Core Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Cybersecurity Test Engineer, Functional Safety Core Manager, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Functional Safety Test Engineer, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

3.1.1.9 Cybersecurity Concept Definition

Description

Objectives:

- To define technical operational cybersecurity controls and their interactions to achieve cybersecurity goals, which take into account dependencies between functions of the item and cybersecurity claims. Description can include conditions for achieving cybersecurity goals and functions dedicated to address specific aspects of threat scenarios.

Requirements:

- The cybersecurity requirements shall be allocated to the item, and if applicable to one or more of its components.

- Cybersecurity concept should be verified to confirm completeness, correctness and consistency with respect to cybersecurity goals and consistency with respect to cybersecurity claims

Work Products:

- Cybersecurity Concept

- Verification report for the Cybersecurity Concept

Performers

Cybersecurity Product System Analyst

Accountable

Cybersecurity Product Manager

Consulted

CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect

Informed

Core Quality Product Engineer, Cybersecurity Test Engineer, Functional Safety Test Engineer, SOTIF Test Engineer, Quality Product Engineer

3.1.1.10 System Cybersecurity Requirements Definition

Description

Objectives:

- Definition of cybersecurity specification of the interfaces between sub-components of defined architectural design related to the fulfillment of the defined cybersecurity concept requirements including their usage, static and dynamic aspects.

Requirements and recommendations:

- When defining cybersecurity requirements, cybersecurity implications of post-development phases can be considered, e.g. secure management of the key store; deactivation of debug interfaces; procedures to delete personally identifiable information

- The cybersecurity specification can include the identification of configuration and calibration parameters relevant for fulfilling the cybersecurity requirements, as well as their settings or permitted range of values, e.g. the correct configuration for the integration of the hardware security module

- Capability of a component necessary to implement the cybersecurity controls can be considered, .e.g processor performance, memory resources.

- **[RQ-10-08]** The defined cybersecurity specifications shall be verified to ensure completeness, correctness, and consistency with the cybersecurity specifications from higher levels of architectural abstraction.

Work products:

- Cybersecurity Requirements
- Verification report for the cybersecurity specifications

Performers

Cybersecurity Product System Analyst

Accountable

Cybersecurity Product Manager

Consulted

CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Product System Analyst, SOTIF Product Software Engineer, SOTIF Project Manager, SOTIF Software Architect

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

3.1.1.11 Cybersecurity requirements Implementation

Description

Objective:

- To implement cybersecurity requirements according to the cybersecurity requirement specification

Requirements and Recommendations:

- **[RC-10-06]** Established and trusted design and implementation principles should be applied to avoid or minimize the introduction of weaknesses.

- **[RQ-10-05]** Criteria for suitable design, modeling or programming languages for cybersecurity that are not addressed by the language itself shall be covered by design, modeling and coding guidelines, or by the development environment.

Work Products:

- Software unit design specification

Performers

Cybersecurity Product Software Engineer

Accountable

Cybersecurity Product System Analyst

Consulted

Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Functional Safety Manager, Functional Safety Product System Analyst, Functional Safety Product Software Engineer, Functional Safety Test Engineer, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer, Test Engineer

Informed

Core Quality Product Engineer, Release Manager, Test Engineer, SOTIF Test Engineer, Cybersecurity Test Engineer, Project Manager

3.1.1.12 Verification on Unit Level

Description

Objective:

- To verify if the isolated written code is working according to the software requirements.

Work Products:

- Unit Level Test results

Performers

Cybersecurity Product Software Engineer

Accountable

Cybersecurity Product System Analyst

Consulted

CyberSafety Manager, Cybersecurity Product System Analyst, Functional Safety Manager, Functional Safety Product Software Engineer, Project Software Architect, Project System Architect, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, Cybersecurity Product Manager

Informed

Core Quality Product Engineer, Project Manager, Release Manager, Quality Product Engineer

3.1.1.13 System Integration Test Cybersecurity

Description

Objective:

- The purpose of the Cybersecurity System Integration and Integration Test process is to integrate the cybersecurity system components to produce an integrated system that will satisfy the cybersecurity architectural design.

Work Product:

- Test evidence is development that all integrated elements fulfill their cybersecurity requirements.

Performers

Cybersecurity Test Engineer

Accountable

Cybersecurity Product System Analyst

Consulted

CyberSafety Manager, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Functional Safety Test Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer, SOTIF Product Software Engineer, Cybersecurity Penetration Testing Engineer

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

3.1.1.14 Item Integration Test Cybersecurity

Description

Objective:

- The purpose of the Cybersecurity Item Test process is to verify if the complete cybersecurity item satisfies cybersecurity concept requirements.

Work Product:

- Test evidence is development that defined item elements fulfill their cybersecurity requirements.

Performers

Cybersecurity Test Engineer

Accountable

Cybersecurity Product System Analyst

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Test Engineer, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Functional Safety Test Engineer, Project Software Architect, Project System Architect, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer, Release Manager

3.1.1.15 Validate Cybersecurity Goals

Description

Objective:

- The purpose of the Cybersecurity Goals Validation process is to verify if the complete cybersecurity item within its operational environmental satisfies cybersecurity goals.

Work Product:

- Test evidence is development that defined item elements fulfill their cybersecurity goals.

Performers

Cybersecurity Test Engineer

Accountable

Cybersecurity Product System Analyst

Consulted

CyberSafety Manager, Cybersecurity Product Manager, Cybersecurity Penetration Testing Engineer, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Functional Safety Test Engineer, Project System Architect, Project Software Architect, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer

Informed

Core Quality Product Engineer, Release Manager, Project Manager, Quality Product Engineer

3.1.1.16 Cybersecurity Case Creation

Description

Objective:

- To provide the argument for the cybersecurity of the item to component, supported by work products

Requirements and Recommendations:

- Parts of the argument can be implicit (e.g. if part of the argument is evident from the compiled set of work products then that part of the argument can be omitted)

- In distributed development, the cybersecurity case of the item can be a combination of the cybersecurity cases of the customer and of the suppliers, which references evidence from the work products generated by the respective parties. Then the overall argument of the item is supported by arguments from all parties

- The cybersecurity case considers the cybersecurity requirements for post-development

Work Products:

- Cybersecurity Case document

Performers

Cybersecurity Product Manager

Accountable

Cybersecurity Core Manager

Consulted

Customer SOTIF Team, SOTIF Project Manager, Functional Safety Manager

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

3.1.1.17 □Cybersecurity Assessment

Description

Objective:

- Cybersecurity assessment shall judge the cybersecurity of the item or component.

Requirements and Recommendations:

- Cybersecurity assessment shall check process implementation against activities defined in the cybersecurity plan

- It should provide an independent judgment that the objectives of cybersecurity process have been adequately achieved by the item or component, and the provided arguments are convincing

Work Products:

- Cybersecurity assessment report

Performers

Cybersecurity Core Analyst

Accountable

Cybersecurity Core Analyst

Consulted

CyberSafety Manager

Informed

Core Quality Product Engineer, Quality Product Engineer, Release Manager, Cybersecurity Product Manager

3.1.1.18 □Penetration Testing Execution

Description

Objective:

- Independent practice of assessing a system, network or web application to find cybersecurity vulnerabilities an attacker could exploit.

Recommendations:

- Penetration Assessment should be conducted by an independent team or a 3rd party company.

Work Products:

- Penetration Assessment Test Report.

Performers

Cybersecurity Penetration Testing Engineer

Accountable

Cybersecurity Product Manager

Consulted

Cybersecurity Core Manager, SOTIF Project Manager, SOTIF Product System Analyst, Functional Safety Product System Analyst, Functional Safety Manager

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

3.1.1.19 Functional Modification to reduce Cybersecurity Risk

Description

Objectives

1. The development activities of the functional modifications to reduce the cybersecurity related risks shall achieve the following objectives:

    - identification and allocation of measures to avoid, reduce, or mitigate the cybersecurity related risks

    - estimation of the effect of the cybersecurity related measures on the intended function

    - improvement of the information required by system specification

Performers

Cybersecurity Product System Analyst

Accountable

Project System Architect

Consulted

CyberSafety Manager, Cybersecurity Product Manager, Cybersecurity Product System Analyst, Functional Safety Manager, Functional Safety Product System Analyst, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect

Informed

Project Manager

3.1.1.20 Item Definition

Description

Objective:

- establishing the definition of the item, including its functionality, interfaces, environmental conditions, legal requirements and hazards. This definition serves to provide sufficient information about the item to the persons who conduct the subsequent sub-phases: "Hazard analysis and risk assessment" and "Functional safety concept"

Requirements and recommendations:

The requirements of the item shall be made available, including:

- legal requirements, national and international standards;
- the functional behavior at the vehicle level, including the operating modes or states;
- the required quality, performance and availability of the functionality, if applicable;
- constraints regarding the item such as functional dependencies, dependencies on other items, and the operating environment;
- potential consequences of behavioral shortfalls including known failure modes and hazards, if any;
- the capabilities of the actuators, or their assumed capabilities

The boundary of the item, its interfaces, and the assumptions concerning its interaction with other items and elements, shall be defined considering:

- the elements of the item;
- the assumptions concerning the effects of the item's behavior on the vehicle;
- the functionality of the item under consideration required by other items and elements;
- the functionality of other items and elements required by the item under consideration;
- the allocation and distribution of functions among the involved systems and elements;
- the operational scenarios which impact the functionality of the item.

Work Products:

Item definition

Performers

Functional Safety Product System Analyst

Accountable

Functional Safety Core Manager

Consulted

CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Product Manager, Cybersecurity Product System Analyst, SOTIF Core Manager, SOTIF Product System Analyst, SOTIF Project Manager

Informed

Project Manager

3.1.1.21 Hazard Analysis And Risk Assessment

Description

Objective:

- to identify and to classify the hazardous events caused by malfunctioning behavior of the item
- to formulate the safety goals with their corresponding ASILs related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.

Requirements and recommendations:

- The hazard analysis and risk assessment shall be based on the item definition;
- The item without internal safety mechanisms shall be evaluated during the hazard analysis and risk assessment, i.e. safety mechanisms intended to be implemented or that have already been implemented in predecessor items shall not be considered in the hazard analysis and risk assessment;
- Hazardous events shall be classified for is severity, exposure and controllability;
- An SAIL shall be determined for each hazardous event based on the classification of severity, probability of exposure and controllability,

Work Products:

- Hazard analysis and risk assessment report
- Verification report of the hazard analysis and risk assessment

Performers

Functional Safety Product System Analyst

Accountable

Functional Safety Core Manager

Consulted

CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Project Software Architect, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product System Analyst, SOTIF Software Architect, Functional Safety Core Manager, Functional Safety Manager, Functional Safety Product System Analyst, Functional Safety Product Software Engineer, Functional Safety Test Engineer, SOTIF Test Engineer

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

Process

3.1.1.22 CyberSafety Analysis and Risk Assesment - CyberSafety Analysis and Risk Assessment □Functional Modification to reduce Functional Safety Risk

Description

Objectives

1. The development activities of the functional modifications to reduce the safety related hazards shall achieve the following objectives:

    - identification and allocation of measures to avoid, reduce, or mitigate the safety related hazards
    - estimation of the effect of the safety related measures on the intended function
    - improvement of the information required by system specification

Performers

Functional Safety Product System Analyst

Accountable

Project System Architect

Consulted

CyberSafety Manager, Cybersecurity Product Manager, Cybersecurity Product System Analyst, Functional Safety Manager, Functional Safety Product System Analyst, SOTIF Project Manager, SOTIF Product System Analyst, SOTIF Software Architect

Informed

Project Manager

3.1.1.23 Functional Safety Testing Strategy Preparation

Description

Objectives:

1. Verification planning shall be carried out for each phase and sub-phase of the safety life-cycle and shall address the following:

    - the content of the work products to be verified;
    - the objective of the verification;
    - the methods used for verification;
    - the pass and fail criteria for the verification;
    - the verification environment, if applicable;
    - the equipment used for verification, if applicable;
    - the resources needed for verification, if applicable;
    - the actions to be taken if anomalies are detected ;
    - the regression strategy;

2. The planning of verification should consider the following:

    - the adequacy of the verification methods to be applied;
    - the complexity of the work product to be verified;
    - prior experiences related to the verification of the subject material;
    - the degree of maturity of the technologies used, or the risks associated with the use of these technologies

3. Verification specification shall specify the methods to be used for the verification, and shall include:

   - review or analysis checklists
   - simulation scenarios
   - test cases, test data and test objects

4. For testing, the specification of each test case shall include:

   - a unique identification;
   - the reference to the version of the associated work product to be verified;
   - the preconditions and configurations;
   - the environmental conditions, if appropriate;
   - the input data, their time sequence and their values ;
   - the expected behavior which includes output data, acceptable ranges of output values, time behavior and tolerance behavior ;
   - the criteria to determine the test case as passed or failed;

5. For testing, test cases shall be grouped according to the test methods to be applied, considering the following aspects:

   - the required test equipment or test environment;
   - the logical and temporal dependencies;
   - the resources

6. For testing, test cases should be reviewed by a different person regarding the author(s) of the work product to be verified

Work Product:

Functional Safety Test Strategy (Verification Specification):

- Verification Plan
- Verification Specification
- Verification Report

Performers

Functional Safety Test Engineer

Accountable

Functional Safety Manager

Consulted

CyberSafety Manager, Cybersecurity Core Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Cybersecurity Test Engineer, Functional Safety Core Manager, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Functional Safety Test Engineer, Project System Architect, Project Software Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Software Architect, SOTIF Test Engineer, SOTIF Project Manager

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

3.1.1.24 Functional and System Specification (C5)

Description

Objectives:

1. Compilation and creation of evidence, which contains the information sufficient to initiate the SOTIF related activities.

2. Update the evidence as necessary after each interaction of the SOTIF related activities.

Description:

1. Functional and System specification

    1. Function related:

- The goals of the intended functionality
- The use cases in which the intended functionality is activated, deactivated and active
- The description of the intended functionality
- The level of automation/authority over the vehicle dynamics
- The dependencies on, and interaction with:
    - the car driver, passengers, pedestrians and other road users
    - relevant environmental conditions
    - the interfaces with the road infrastructure

2. System Related:

- The description of the system and elements implementing the intended functionality
- The description and behavior of the installed sensors, controllers and actuators used by the intended functionality
- The description and behavior of the installed sensors, controllers and actuators used by the intended functionality
- The description and behavior of the installed sensors, controllers and actuators used by the intended functionality
- The concepts and technologies for the system and sub systems
- The limitations and their countermeasures
- The system architecture supporting the countermeasures
- The degradation concept
- The warning strategies
- The dependencies on, and interaction with other functions and systems of the vehicle

Performers

SOTIF Product System Analyst

Accountable

SOTIF Project Manager

Consulted

CyberSafety Manager, Cybersecurity Core Manager, Cybersecurity Product System Analyst, Project System Architect, SOTIF Project Manager

Informed

Project Manager

3.1.1.25 SOTIF related Hazard Identification and Risk Evaluation (C6)

Description

Objectives:

1. The possible hazardous events, caused by functionality that results in potentially hazardous behavior and their potential consequences, are identified and evaluated

2. The acceptance criteria (e.g. a validation target) to evaluate the design in the validation phase are specified

3. The possible hazardous events caused by reasonably foreseeable misuse of the function, by the user, are identified and evaluated

Performers

SOTIF Product System Analyst

Accountable

SOTIF Project Manager

Consulted

CyberSafety Manager, Cybersecurity Core Manager, Cybersecurity Product System Analyst, Project System Architect, SOTIF Core Manager

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

Process

3.1.1.26 CyberSafety Analysis and Risk Assesment - CyberSafety Analysis and Risk Assessment Identification and Evaluation of Triggering Events (C7)

Description

Objectives:

1. Identification of triggering event that can trigger potentially hazardous behavior.

2. Evaluation of triggering events for their acceptability with respect to the SOTIF.

Performers

SOTIF Product System Analyst

Accountable

SOTIF Project Manager

Consulted

CyberSafety Manager, Cybersecurity Core Manager, Cybersecurity Product System Analyst, Project Software Architect

Informed

SOTIF Project Manager

3.1.1.27 Functional Modification to Reduce SOTIF Risk (C8)

Description

Objectives

1. The development activities of the functional modifications to reduce the SOTIF related risks shall achieve the following objectives:

   - identification and allocation of measures to avoid, reduce, or mitigate the SOTIF related risks

   - estimation of the effect of the SOTIF related measures on the intended function

   - improvement of the information required by Clause 5 (Functional and system specification).

Performers

SOTIF Product System Analyst

Accountable

SOTIF Project Manager

Consulted

Cybersecurity Product System Analyst, Cybersecurity Core Analyst, Project System Architect, Project Software Architect, SOTIF Product System Analyst, SOTIF Product Software Engineer, SOTIF Software Architect

Informed

Project Manager

3.1.1.28 □Definition of the Verification and Validation Strategy (C9)

Description

Objectives:

1. A verification and validation strategy shall be defined such that:
   - it supports the rationale for the SOTIF
   - The necessary evidence is generated
   - The procedures to generate the evidence are developed
2. A verification and validation strategy shall include:
   - The ability of sensors and the sensor processing algorithms to model the environment
   - The ability of the decision algorithms to handle both known and unknown situations and to make the appropriate decisions according to the environment model and the system architecture
   - The robustness of the system or function
   - The ability of the HMI to prevent reasonably foreseeable misuse;
   - The manageability of the handover scenario by the driver

Performers

SOTIF Product System Analyst

Accountable

SOTIF Project Manager

Consulted

CyberSafety Manager, Cybersecurity Core Manager, Cybersecurity Product System Analyst, Project Software Architect

Informed

Project Manager

3.1.1.29 □SOTIF Safety Concept Preparation

Description

Preparation of Safety concept, which includes SOTIF related requirements based on defined goals after HIRE analysis.

Performers

SOTIF Product System Analyst

Accountable

SOTIF Project Manager

Consulted

CyberSafety Manager, Cybersecurity Product System Analyst, SOTIF Core Manager

Informed

Project Manager, Core Quality Product Engineer, Quality Product Engineer

3.1.1.30 SOTIF Technical Concept Preparation

Description

Preparation of SOTIF architectural design requirements based on Safety Concept Requirements.

Performers

SOTIF Product System Analyst

Accountable

SOTIF Project Manager

Consulted

Project Software Architect, CyberSafety Manager, Cybersecurity Core Analyst, SOTIF Core Manager

Informed

Project Manager, Core Quality Product Engineer, Quality Product Engineer

3.1.1.31 Implementation of SOTIF Functionalities

Description

Implementation of SOTIF features in defined system.

Performers

SOTIF Product Software Engineer

Accountable

SOTIF Software Architect

Consulted

CyberSafety Manager, Cybersecurity Product System Analyst, Cybersecurity Product Software Engineer

Informed

Project Manager, Core Quality Product Engineer, Release Manager, Test Engineer, SOTIF Test Engineer

3.1.1.32 Verification of the SOTIF: Evaluation Known Hazardous Scenario(C10)

Description

Objectives:

1. The system and components (sensors, algorithms and actuators) shall be verified to show that they behave as expected for known hazardous scenarios and reasonably foreseeable misuse (derived from previous analyses and knowledge). It shall be verified that system and components are covered sufficiently by the tests.

2. To support the achievement of the objectives of this clause, the following information can be considered:

- Verification strategy, as defined in Clause 9
- Functional concept, including sensors, actuators and algorithm specification
- System design specification
- Verification targets
- Vehicle design (e.g. mounting position)
- Analysis of triggering events results

Performers

SOTIF Product Software Engineer

Accountable

SOTIF Product System Analyst

Consulted

CyberSafety Manager, Cybersecurity Core Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Project System Architect, SOTIF Product System Analyst, SOTIF Project Manager, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Project Software Architect

Informed

Project Manager, Core Quality Product Engineer, Release Manager, Quality Product Engineer

3.1.1.33 □Validation of the SOTIF: Evaluate Unknown Hazardous Scenarios (C11)

Description

Objectives:

1. The functions of the system and the components (sensors, decision-algorithms and actuators) shall be validated to show that they do not cause an unreasonable level of risk in real-life use cases . This requires evidence that the validation targets are met

2. Following input can be considered:

- Validation strategy, as defined in Clause 9
- Verification results in defined use cases, as defined in Clause 10
- Functional concept, including sensors, actuators and decision-algorithm specification
- System design specification
- Validation targets, as defined in Clause 6
- Vehicle design (e.g. sensor mounting position);
- Analysis of triggering events results

Performers

SOTIF Test Engineer

Accountable

SOTIF Product System Analyst

Consulted

CyberSafety Manager, Cybersecurity Product System Analyst, Project System Architect, SOTIF Project Manager, Cybersecurity Product Software Engineer, Cybersecurity Product Manager, SOTIF Software Architect

Informed

Core Quality Product Engineer, Release Manager, Quality Product Engineer

3.1.1.34 □Methodology and Criteria for SOTIF Release (C12)

Description

Objectives

1. Review SOTIF activities,

2. Evaluate the acceptability of the residual risk considering the findings of the SOTIF activities.

Inputs:

1. Functional and system specification as defined in Clause 5

2. Verification and validation targets as defined in Clause 6

3. Analysis of triggering events as defined in Clause 7

4. Functional improvements as the result of Clause 8 activities

5. Verification and validation strategy, as defined in Clause 9

6. Results of verification as defined in Clause 10

7. Results of the validation of the SOTIF as defined in Clause 11

Performers

SOTIF Product System Analyst

Accountable

SOTIF Project Manager

Consulted

Customer SOTIF Team, CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Product System Analyst, Project System Architect, Release Manager, SOTIF Core Analyst, SOTIF Product System Analyst

Informed

Project Manager, Release Manager, Core Quality Product Engineer, Quality Product Engineer

3.1.1.35 Functional Safety Goals Definition

Description

Objective:

- A safety goal shall be determined for each hazardous event with an ASIL evaluated in the hazard analysis and risk assessment. If similar safety goals are determined, these may be combined into one safety goal..

Requirements and recommendations:

- The ASIL determined for the hazardous event shall be assigned to the corresponding safety goal. If similar safety goals are combined into a single one, the highest ASIL shall be assigned to the combined safety goal

- The safety goals together with their ASIL shall be specified in accordance with ISO 26262-8:2018, Clause 6.

- Assumptions used for, or resulting from the hazard analysis and risk assessment which are relevant for ASIL determination (if applicable, including hazardous events classified QM or with no ASIL assigned) shall be identified. These assumptions shall be validated in accordance with ISO 26262-4:2018, Clause 8 for the integrated item.

Work product:

- Safety Goals

Performers

Functional Safety Product System Analyst

Accountable

Functional Safety Manager

Consulted

CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Core Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Cybersecurity Test Engineer, Functional Safety Core Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Functional Safety Test Engineer, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

3.1.1.36 Functional Safety Concept Definition

Description

Objectives:

- to specify the functional or degraded functional behavior of the item in accordance with its safety goals;

- to specify the constraints regarding suitable and timely detection and control of relevant faults in accordance with its safety goals;

- to specify the item level strategies or measures to achieve the required fault tolerance or adequately mitigate the effects of relevant faults by the item itself, by the driver or by external measures;

- to allocate the functional safety requirements to the system architectural design, or to external measures;

- to verify the functional safety concept and specify the safety validation criteria.

Requirements and recommendations:

- The functional safety requirements shall be specified in accordance with ISO 26262-8:2018, Clause 6

- The functional safety requirements shall be derived from the safety goals, considering the system architectural design

- At least one functional safety requirement shall be derived from each safety goal

- The functional safety requirements shall specify, if applicable, strategies for

    - fault avoidance;

    - fault detection and control of faults or the resulting malfunctioning behavior;

    - transitioning to a safe state, and if applicable, from a safe state;

    - fault tolerance;

    - the degradation of the functionality in the presence of a fault

    - driver warnings needed to reduce the risk exposure time to an acceptable duration

    - driver warnings needed to increase the controllability by the driver

    - how timing requirements at the vehicle level are met, i.e. how the fault tolerant time interval shall be met by defining a fault handling time interval

    - avoidance or mitigation of a hazardous event due to improper arbitration of multiple control requests generated simultaneously by different functions

- Each functional safety requirement shall be specified by considering the following, as applicable:

    - operating modes;

    - fault tolerant time interval;

    - safe states;

    - emergency operation time interval;

    - functional redundancies

- If a safety goal violation can be prevented by transitioning to, or by maintaining, one or more safe states, then the corresponding safe state(s) shall be specified

    - If a safe state cannot be reached by a transition within an acceptable time interval, an emergency operation shall be specified.

- o If assumptions are made about the necessary actions of the driver, or other persons, in order to prevent the violation of a safety goal, then the following shall apply
    - these actions shall be specified in the functional safety concept
    - the adequate means and controls available to the driver or other persons shall be specified in the functional safety concept

- The functional safety requirements shall be allocated to the elements of the system architectural design
- If the functional safety concept relies on elements of other technologies, then the following shall apply:
    - o the functional safety requirements implemented by elements of other technologies shall be derived and allocated to the corresponding elements of the architecture
    - o the functional safety requirements relating to the interfaces with elements of other technologies shall be specified;
    - o the implementation of functional safety requirements by elements of other technologies shall be ensured through specific measures that are outside the scope of ISO 26262
    - o no ASIL should be assigned to safety requirements allocated to these elements
- If the functional safety concept relies on external measures, then the following shall apply
    - o the functional safety requirements implemented by external measures shall be derived and communicated;
    - o the functional safety requirements of interfaces with external measures shall be specified
    - o if the external measures are implemented by one or more E/E systems, the functional safety requirements shall be addressed using ISO 26262

Work Products:

- Functional Safety Concept
- Verification Report of the Functional Safety Concept

Performers

Functional Safety Product System Analyst

Accountable

Functional Safety Manager

Consulted

CyberSafety Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Functional Safety Manager, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, Cybersecurity Core Analyst

Informed

Core Quality Product Engineer, Cybersecurity Test Engineer, Functional Safety Core Manager, Functional Safety Test Engineer, SOTIF Test Engineer, Quality Product Engineer

3.1.1.37 Technical Safety Concept Definition

Description

Objectives:

- The **technical safety concept -** an aggregation of the technical safety requirements and the corresponding system architectural design that provides rationale as to why the system architectural design is suitable to fulfill safety requirements resulting from activities described in ISO 26262-3 (with consideration of non-safety requirements) and design constraints.

- The **technical safety requirements -** specify the technical implementation of the functional safety requirements at their respective hierarchical level; considering both the item definition and the system architectural design, and addressing the detection of latent failures, fault avoidance, safety integrity and operation and service aspects.

- The **system architectural design** is the selected system-level solution that is implemented by a technical system. The system architectural design aims to fulfill both, the allocated technical safety requirements and the non-safety requirements.

Requirements and recommendations:

- The technical safety requirements shall be specified in accordance with the functional safety concept and the system architectural design of the item considering the following:

    - the safety-related dependencies and constraints of items, systems and their elements;

    - the external interfaces of the system, if applicable;

    - the reconfigurability of the system;

- The technical safety requirements shall specify the stimulus response of the system that affects the achievement of safety requirements. This includes the combinations of relevant stimuli and failures with each relevant operating mode and defined system state.

- If other functions or requirements are implemented by the system or its elements, in addition to those functions for which technical safety requirements are specified, then these functions or requirements shall be specified or their specification referenced.

- Technical safety and non-safety requirements shall not contradict.

- The technical safety requirements shall specify the safety mechanisms that detect faults and prevent or mitigate failures present at the output of the system that violate the functional safety requirements including:
  - o the safety mechanisms related to the detection, indication and control of faults in the system itself;
  - o the safety mechanisms related to the detection, indication and control of faults in other external elements that interact with the system;
  - o the safety mechanisms that contribute to the system achieving or maintaining the safe state of the item;
  - o the safety mechanisms to define and implement the warning and degradation strategy;
  - o the safety mechanisms that prevent faults from being latent.

Safety mechanisms

- For each safety mechanism that enables an item to achieve or maintain a safe state, the following shall be specified:
  - o the transition between states
  - o the fault handling time interval with respect to the timing requirements apportioned from the appropriate architectural level
  - o the emergency operation tolerance time interval, see ISO 26262-1:2018, 3.45, if the safe state of the item cannot be reached within the FTTI
- This requirement applies to ASILs (A), (B), C, and D. If applicable, safety mechanisms shall be specified to prevent faults from being latent.
- This requirement applies to ASILs (A), (B), C, and D. To avoid multiple-point failures, the diagnostic test strategy shall be specified for each safety mechanism implemented to detect multiple-point faults, considering:
  - o the reliability requirements of the hardware components with consideration given to their role in the architecture and their contribution to a multiple-point failure
  - o the specified quantitative target values for the maximum probability of violation of each safety goal due to random hardware failures
  - o the assigned ASIL derived from the related safety goal, the related functional safety requirement or technical safety requirement at a higher hierarchical level
  - o the multiple-point fault detection time interval
- This requirement applies to ASILs (A), (B), C, and D. The development of safety mechanisms that are implemented only to prevent dual point faults from being latent shall at least comply with
  - o ASIL B for technical safety requirements assigned ASIL D;
  - o ASIL A for technical safety requirements assigned ASIL B and ASIL C;

- o QM for technical safety requirements assigned ASIL A

System architectural design specification and technical safety concept

- The system architectural design in this sub-phase and the technical safety concept shall be based on the item definition, functional safety concept and the prior system architectural design

- The consistency of the system architectural design in ISO 26262-3:2018, 7.3.1 and the system architectural design in this sub-phase shall be checked. If discrepancies are identified, an iteration of the activities described in ISO 26262-3:2018 may be necessary

- The system architectural design shall implement the technical safety requirements

- With regard to the implementation of the technical safety requirements, the following shall be considered in the system architectural design

  - o the ability to verify the system architectural design;

  - o the technical capability of the intended hardware and software elements with regard to the achievement of functional safety

  - o the ability to execute tests during system integration.

- The internal and external interfaces of safety-related elements shall be defined such that other elements shall not have adverse safety-related effects on the safety-related elements

- If ASIL decomposition is applied to the safety requirements during system architectural design, it shall be applied in accordance with ISO 26262-9:2018, Clause 5

Safety Analyses and avoidance of systematic failures

- Safety analyses on the system architectural design shall be performed in accordance with ISO 26262-4:2018 Table 1 and ISO 26262-9:2018, Clause 8 in order to:

  - o provide evidence for the suitability of the system design to provide the specified safety-related functions and properties with respect to the ASIL;

  - o identify the causes of failures and the effects of faults;

  - o identify or confirm the safety-related system elements and interfaces;

  - o support the design specification and verify the effectiveness of the safety mechanisms based on identified causes of faults and the effects of failures

- Identified internal causes of failure shall be eliminated, or their effects mitigated where necessary, to comply with the safety goals or requirements.

- Identified external causes of failure shall be eliminated, or their effects mitigated where necessary, to comply with the safety goals or requirements.

- To reduce the likelihood of systematic failures, well-trusted systems design principles should be applied where applicable. These may include the following:
  - re-use of well-trusted technical safety concepts;
  - re-use of well-trusted designs for elements, including hardware and software components;
  - re-use of well-trusted mechanisms for the detection and control of failures;
  - re-use of well-trusted or standardized interfaces.
- An analysis of the suitability of well-trusted design principles shall be performed and documented to ensure consistency and suitability to the product’s application.
- In order to avoid systematic faults, the system architectural design shall exhibit the following properties:
  - modularity;
  - adequate level of granularity
  - simplicity.
- Hazards newly identified during safety analyses or during the system architectural design that are not already covered by a safety goal shall be included in an updated hazard analysis and risk assessment (HARA) in accordance with ISO 26262-3.

Measures for control of random hardware failures during operation

- Measures for the detection, control or mitigation of random hardware failures shall be specified with respect to the system architectural design
- This requirement applies to ASILs (B), C, and D of the safety goal. One of the alternative procedures for the evaluation of violation of the safety goal due to random hardware failures (see ISO 26262-5:2018, Clause 9) shall be chosen and the target values shall be specified for final evaluation at the item level.
- This requirement applies to ASILs (B), C, and D of the safety goal. Appropriate target values for failure rates and diagnostic coverage should be specified at the element level in order to comply with
  - the target values of the metrics in ISO 26262-5:2018, Clause 8
  - the procedures in ISO 26262-5:2018, Clause 9.
- This requirement applies to ASILs (B), C, and D. For distributed developments (see ISO 26262-8:2018, Clause 5) the derived target values shall be communicated to each relevant party.

Allocation to hardware and software

- The technical safety requirements shall be allocated to the system architectural design elements with system, hardware or software as the implementing technology.

- The allocation and partitioning decisions shall comply with the system architectural design.

- Each system architectural design element shall inherit the highest ASIL from the technical safety requirements that it implements.

- If a system architectural design element is comprised of sub-elements with different ASILs assigned, or of safety-related and non-safety-related sub-elements, then each of these shall be treated in accordance with the highest ASIL, unless the criteria for coexistence (in accordance with ISO 26262-9:2018, Clause 6) are met

- If technical safety requirements are allocated to custom hardware elements that incorporate programmable behavior (such as ASICs, FPGA or other forms of digital hardware) an adequate development process, combining requirements from ISO 26262-5 and ISO 26262-6, shall be defined and implemented.

Hardware-software interface (HSI) specification

- The HSI specification shall specify the hardware and software interaction and be consistent with the technical safety concept. The HSI specification shall include the component's hardware parts that are controlled by software and hardware resources that support the execution of the software.

- The HSI specification shall include the following characteristics:

    - the relevant operating modes of the hardware devices and the relevant configuration parameters;

    - the hardware features that ensure the independence between elements or that support software partitioning;

    - shared and exclusive use of hardware resources;

    - the access mechanism to hardware devices;

    - the timing constraints derived from the technical safety concept

- The relevant diagnostic capabilities of the hardware, and their use by the software, shall be specified in the HSI specification

    - the hardware diagnostic features shall be defined

    - the diagnostic features concerning the hardware, to be implemented in software, shall be defined

- The HSI shall be specified during the system architectural design

Production,operation,service and decommissioning

- The requirements addressed in ISO 26262-7:2018 for production, operation, service and decommissioning, identified during the system architectural design, shall be specified. These include:

    - measures required to achieve, maintain or restore the safety-related functions and properties of the item and its elements during production, service or decommissioning;

- o the safety-related special characteristics;
- o the requirements that ensure proper identification of systems or elements;
- o the verification measures for production;
- o the service requirements including diagnostic data and service notes;
- o measures for decommissioning.

- Diagnostic features shall be specified in order to provide the required data that enables field monitoring for the item or its elements according to ISO 26262-2:2018, Clause 7, with consideration being given to the results of safety analyses and the implemented safety mechanisms.

- To restore or maintain functional safety, diagnostic features shall be specified that allow fault identification and the effectiveness of maintenance or repair to be checked during servicing

Verification

- The technical safety requirements shall be verified in accordance with ISO 26262-8:2018, Clauses 6 and 9, to provide evidence for their correctness, completeness, and consistency with respect to the given boundary conditions of the system.

- The system architectural design, the hardware-software interface (HSI) specification and the specification of requirements for production, operation, service and decommissioning and the technical safety concept shall be verified using the verification methods listed in ISO 26262-4:2018 Table 2 to provide evidence that the following objectives are achieved:

    - o they are suitable and adequate to achieve the required level of functional safety according to the relevant ASIL;
    - o there is consistency between the system architectural design and the technical safety concept;
    - o validity of and compliance with system architectural designs of prior development steps.

Work products:

- Technical Safety requirements Specification
- Technical Safety Concept
- System architectural design specification
- Hardware-software interface (HSI) specification
- Specification of requirements for production, operation, service and decommissioning

- Verification report for system architectural design, the hardware-software interface (HSI) specification, the specification of requirements for production, operation, service and decommissioning, and the technical safety concept

- Safety analyses report

Performers

Functional Safety Product System Analyst

Accountable

Functional Safety Manager

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Functional Safety Product Software Engineer, Project System Architect, Project Software Architect, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect

Informed

Core Quality Product Engineer, Cybersecurity Test Engineer, Functional Safety Test Engineer, Project Manager, SOTIF Test Engineer, Quality Product Engineer

3.1.1.38 □Functional Safety requirements Implementation

Description

Objectives:

- to develop a software unit design in accordance with the software architectural design, the design criteria and the allocated software requirements which supports the implementation and verification of the software unit

- to implement the software units as specified

Requirements and recommendations

- The requirements of this sub-clause shall be complied with if the software unit is a safety-related element.

- The software unit design and implementation shall:

    - be suitable to satisfy the software requirements allocated to the software unit with the required ASIL;

    - be consistent with the software architectural design specification ;

    - be consistent with the hardware-software interface specification, if applicable

- To avoid systematic faults and to ensure that the software unit design achieves the following properties, the software unit design shall be described using the notations listed in ISO 26262-6 Table 5.

    - consistency

- comprehensibility;
- maintainability;
- verifiability;

- The specification of the software units shall describe the functional behavior and the internal design to the level of detail necessary for their implementation

- Design principles for software unit design and implementation at the source code level as listed in ISO 2626-6:2018 Table 6 shall be applied to achieve the following properties:

  - correct order of execution of subprograms and functions within the software units, based on the software architectural design;
  - consistency of the interfaces between the software units;
  - correctness of data flow and control flow between and within the software units;
  - simplicity;
  - readability and comprehensibility;
  - robustness;
  - suitability for software modification;
  - verifiability.

Work Products:

- Software unit design specification

Performers

Functional Safety Product Software Engineer

Accountable

Functional Safety Product System Analyst

Consulted

Cybersecurity Product Software Engineer, Cybersecurity Core Analyst, Project Software Architect, Cybersecurity Product System Analyst, Project System Architect, SOTIF Product System Analyst, SOTIF Software Architect, Cybersecurity Penetration Testing Engineer

Informed

Core Quality Product Engineer, Quality Product Engineer, Test Engineer, Cybersecurity Test Engineer, SOTIF Test Engineer

3.1.1.39 □Verification on Unit Level

Description

Objectives:

- to provide evidence that the software unit design satisfies the allocated software requirements and is suitable for the implementation;

- to verify that the defined safety measures resulting from safety-oriented analyses are properly implemented;

- to provide evidence that the implemented software unit complies with the unit design and fulfills the allocated software requirements with the required ASIL;

- to provide sufficient evidence that the software unit contains neither undesired functionalities nor undesired properties regarding functional safety.

Requirements and recommendations:

- The requirements of this sub-clause shall be complied with if the software unit is a safety-related element.

- The software unit design and the implemented software unit shall be verified in accordance with ISO 26262-8:2018, Clause 9 by applying an appropriate combination of methods according to ISO26262-6:2018 Table 7 to provide evidence for:

  - compliance with the requirements regarding the unit design and implementation in accordance with Clause 8;

  - the compliance of the source code with its design specification;

  - compliance with the specification of the hardware-software interface;

  - confidence in the absence of unintended functionality and properties;

  - sufficient resources to support their functionality and properties;

  - implementation of the safety measures resulting from the safety-oriented analyses

- To enable the specification of appropriate test cases for the software unit testing in accordance with ISO 26262-6:2018 9.4.2, test cases shall be derived using the methods as listed in ISO 26262-6:2018 Table 8.

- To evaluate the completeness of verification and to provide evidence that the objectives for unit testing are adequately achieved, the coverage of requirements at the software unit level shall be determined and the structural coverage shall be measured in accordance with the metrics as listed in ISO 26262-6:2018 Table 9. If the achieved structural coverage is considered insufficient, either additional test cases shall be specified or a rationale based on other methods shall be provided.

- The test environment for software unit testing shall be suitable for achieving the objectives of the unit testing considering the target environment. If the software unit testing is not carried out in the target environment, the differences in the source and object code, as well as the differences between the test environment and the target environment, shall be analyzed in order to specify additional tests in the target environment during the subsequent test phases.

Work Products:

- Software verification specification

- Software verification report

Performers

Functional Safety Product Software Engineer

Accountable

Functional Safety Product System Analyst

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Functional Safety Product System Analyst, Project Software Architect, Project System Architect, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer, Functional Safety Manager

Informed

Core Quality Product Engineer, Project Manager, Release Manager

3.1.1.40 □System Integration Test Safety

Description

Objective:

- to define the integration steps and to integrate the system elements until the system is fully integrated

- to verify that the defined safety measures, resulting from safety analyses at the system architectural level, are properly implemented;

- to provide evidence that the integrated system elements fulfill their safety requirements according to the system architectural design

Requirements and recommendations:

- To provide evidence that the system architectural design is compliant with the functional safety and technical safety requirements, integration testing activities shall be performed in accordance with ISO 26262-8:2018, Clause 9 to check:
  - the correct implementation of functional safety and technical safety requirements;
  - the correct functional performance, accuracy and timing of safety mechanisms;
  - the consistent and correct implementation of interfaces;
  - adequate robustness;

- integration and test strategy shall be defined that considers the system architectural design specification, the functional safety concept and the technical safety concept. It shall address:
  - the test goals suitable to provide evidence for functional safety;
  - the integration and testing of the item and its elements that contribute to the safety concepts;
- The fulfillment of each functional safety and technical safety requirement shall be verified (if applicable by testing) at least once in the complete integration sub-phase.
- To enable the appropriate specification of test cases for the integration tests, test cases shall be derived using an appropriate combination of methods, as listed in ISO26262-4:2018 Table 3, and by considering the integration level.

Hardware-software integration and testing:

- The hardware developed in accordance with ISO 26262-5 and the software developed in accordance with ISO 26262-6 shall be integrated and used as the subject of the test activities in ISO26262-4:2018 Table 4 to ISO26262-4:2018 Table 8**.**
- The integrated hardware and software shall be tested for compliance with the requirements addressing the HSI specification.
- Evidence for the correct implementation of the safety-related functions and behavior according to the technical safety requirements at the hardware-software level shall be provided by using test methods listed in ISO26262-4:2018 Table 4.
- This requirement applies to ASIL (A), B, C, and D. The correct functional performance, accuracy and timing of the safety mechanisms at the hardware-software level shall be demonstrated using test methods listed in ISO26262-4:2018 Table 5.
- This requirement applies to ASIL (A), B, C, and D. Evidence for the consistent and correct implementation of the external and internal interfaces at the hardware-software level shall be provided by using test methods listed in ISO26262-4:2018 Table 6.

- This requirement applies to ASIL (A), (B), C, and D. The effectiveness of the hardware fault detection mechanisms at the hardware-software level, with respect to the fault models, shall be demonstrated using test methods listed in ISO26262-4:2018 Table 7.

- This requirement applies to ASIL (A), (B), (C), and D. The level of robustness of the elements at the hardware-software level shall be demonstrated using test methods listed in ISO26262-4:2018 Table 8.

Work Products:

- HSI integration and test strategy

- HSI Integration and test report

Performers

Functional Safety Test Engineer

Accountable

Functional Safety Product System Analyst

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Functional Safety Manager, Functional Safety Test Engineer, Project Software Architect, Project System Architect, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Project Manager, SOTIF Product System Analyst, SOTIF Software Architect, SOTIF Test Engineer

Informed

Core Quality Product Engineer, Release Manager, Quality Product Engineer

3.1.1.41 Item Integration Test Safety

Description

Objectives:

- The individual elements of the system shall be integrated in accordance with the system architectural design, and tested in accordance with the system integration test specification.

- The tests are intended to provide evidence that each system element interacts correctly, complies with the technical and functional safety requirements, and gives an adequate level of confidence that unintended behaviors, that could violate a safety goal, are absent.

- The item shall be integrated into the vehicle and the vehicle integration tests shall be carried out to confirm the safety goals.

- The verification of the interface specification of the item with the in-vehicle communication network and the in-vehicle power supply network shall be performed.

Requirements and recommendations:

- Evidence for the correct implementation of functional safety and technical safety requirements at the system level shall be provided by using test methods as listed in ISO26262-4:2018 Table 9.

- This requirement applies to ASIL (A), (B), (C), and D. The correct functional performance, accuracy, coverage of failure modes at the system level, and timing of the safety mechanisms at the system level shall be demonstrated using test methods listed in ISO26262-4:2018 Table 10.

- Evidence for the consistent and correct implementation of the external and internal interfaces at the system level shall be provided by using test methods listed in ISO26262-4:2018 Table 11.

- The level of robustness at the system level shall be demonstrated using test methods listed in ISO26262-4:2018 Table 12.

- Test goals resulting from the requirements ISO26262-4:2018 7.4.4.2.2 to 7.4.4.2.5 shall be addressed by the application of adequate test methods as listed in the corresponding tables.

- The correct implementation of the functional safety requirements at the vehicle level shall be demonstrated using test methods listed in ISO26262-4:2018 Table 13.

- This requirement applies to ASIL (A), (B), C, and D. The correct functional performance, accuracy and timing of the safety mechanisms at the vehicle level shall be demonstrated using test methods listed in ISO26262-4:2018 Table 14.

- This requirement applies to ASIL (A), (B), C, and D. The consistency and correctness of the implementation of the interfaces internal and external to the vehicle shall be demonstrated using test methods listed in ISO26262-4:2018 Table 15.

- This requirement applies to ASIL (A), (B), C, and D. The level of robustness at the vehicle level shall be demonstrated using test methods listed in ISO26262-4:2018 Table 16.

Work Products:

- Item integration and test strategy

- Item Integration and test report

Performers

Functional Safety Test Engineer

Accountable

Functional Safety Product System Analyst

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Cybersecurity Test Engineer, Functional Safety Product Software Engineer, Project Software Architect, Project System Architect, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer

Informed

Core Quality Product Engineer, Project Manager, Release Manager

3.1.1.42 Validate Safety Goals

Description

Objectives:

- to provide evidence that the safety goals are achieved by the item when being integrated into the respective vehicle(s);

- to provide evidence that the functional safety concept and the technical safety concept are appropriate for achieving functional safety for the item.

Requirements and recommendations:

- The safety goals shall be validated for the item in a representative context at vehicle level

- For the definition of a representative context, representative vehicles based on vehicle types and vehicle configurations shall be considered

- The safety validation specification shall be defined, including:

    - the configuration of the item subjected to safety validation including its calibration data in accordance with ISO 26262-6:2018, Annex C;

    - the specification of safety validation procedures, test cases, driving maneuvers, and acceptance criteria;

  - the equipment and the required environmental conditions

- If testing is used for safety validation, then the same requirements as provided for verification testing (see ISO 26262-8:2018, 9.4.2 and 9.4.3) may be applied.

- The achievement of functional safety for the item when being integrated into the vehicle shall be validated by evaluating the following aspects:

  - the controllability;

  - the effectiveness of the external measures;

  - the effectiveness of the elements of other technologies;

  - assumptions that influence the ASIL in the hazard analysis and risk assessment (see ISO 26262-3:2018, 6.4.4.4) that can be checked only in the final vehicle.

- The safety validation at the vehicle level, based on the safety goals, the functional safety requirements and the intended use, shall be executed as planned using:

  - the safety validation procedures and test cases for each safety goal including detailed pass/fail criteria;

  - the scope of application. This may include issues such as configuration, environmental conditions, driving situations, operational use cases, etc.

- An appropriate set of the following methods shall be applied:

  - repeatable tests with specified test procedures, test cases, and pass/fail criteria;

  - analyses;

  - long-term tests, such as vehicle driving schedules and captured test fleets;

  - operational use cases under real-life conditions, panel or blind tests, or expert panels;

  - reviews.

- The results of the safety validation shall be evaluated to provide evidence that the implemented safety goals achieve functional safety for the item.

Work products:

- Safety validation specification including safety validation environment description

- Safety validation report

Performers

Functional Safety Test Engineer

Accountable

Functional Safety Product System Analyst

Consulted

CyberSafety Manager, Cybersecurity Penetration Testing Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Cybersecurity Test Engineer, Functional Safety Manager, Functional Safety Product Software Engineer, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, SOTIF Test Engineer, Project Software Architect, Project System Architect

Informed

Core Quality Product Engineer, Release Manager, Project Manager

3.1.1.43 Functional Safety Case Creation

Description

Objectives:

- A safety case shall be developed, in accordance with the safety plan, in order to provide the argument for the achievement of functional safety.

Requirements and recommendations:

- The safety case should progressively compile the work products that are generated during the safety life-cycle to support the safety argument.

- In the case of a distributed development, the safety case of the item can be a combination of the safety cases of the customer and of the suppliers, which references evidence from the work products generated by the respective parties. Then the overall argument of the item is supported by arguments from all parties. The interfaces between the customer and a supplier are defined in a Development Interface Agreement (see ISO 26262-8:2018, Clause 5).

- To support safety planning according to ISO26262-2:2018 6.4.6, the intended safety arguments can be identified prior to work products becoming available. To support progressive functional safety assessments according to ISO26262-2:2018 6.4.12.3 the safety case can be released progressively as work products are generated to provide evidence for the safety arguments.

Work Products:

- Safety Case

Performers

Functional Safety Manager

Accountable

Functional Safety Core Manager

Consulted

CyberSafety Manager, SOTIF Project Manager, SOTIF Test Engineer, Cybersecurity Penetration Testing Engineer, Cybersecurity Test Engineer, Functional Safety Product Software Engineer, Functional Safety Product System Analyst, Functional Safety Test Engineer, Project Software Architect, Project System Architect, SOTIF Product System Analyst, SOTIF Product Software Engineer, SOTIF Software Architect, Test Engineer, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst

Informed

Core Quality Product Engineer, Release Manager, Project Manager

3.1.1.44 □Functional Safety Assessment

Description

Objectives:

- For items and elements where the highest ASIL of the safety requirements is ASIL (B), C, or D: a functional safety assessment shall be carried out in accordance with ISO26262-2:2018 6.4.9, to judge the achieved functional safety of the item, or the contribution to the achievement of functional safety by the developed elements.

- A functional safety assessment may be based on a judgment of whether the objectives of the ISO 26262 series of standards are achieved.

Requirements and recommendations:

- A functional safety assessment:
  - shall be planned in accordance with ISO 26262-2:2018 6.4.6.5 f);
  - should be planned at the latest at the beginning of the product development at the system level;
  - should be progressively performed during the product development;
  - shall be finalized before the release for production.

- One or more persons shall be appointed to carry out a functional safety assessment, in accordance with ISO 26262-2:2018 5.4.2.7 and ISO 26262-2:2018 5.4.4. The appointed persons shall provide a report that contains a judgment of the achieved functional safety.

- The persons responsible for performing a functional safety assessment shall be given the authority to perform the functional safety assessment according to their discretion, including:

    - the breadth and depth with which the safety activities and their results, that are within the scope of the functional safety assessment in accordance with 26262-2:2018 6.4.12.7, are assessed;

    - the information to be made available in accordance with 26262-2:2018 6.4.9.3

    - the support deemed necessary to perform the functional safety assessment in accordance with 26262-2:2018 6.4.9.2, such as the availability of the persons responsible for a pertinent work product.

- The functional safety assessor may appoint one or more assistants to support the performance of the functional safety assessment in accordance with 26262-2:2018 6.4.9.2 and 26262-2:2018 5.4.4. Such persons may lack independence from the developers of the corresponding item, elements or work products, but their independence shall be at least I1, as defined in 26262-2:2018 Table 1, and the assessor shall appraise their input to ensure an unbiased opinion is given.

- The scope of a functional safety assessment shall include:

    - the safety plan and all the work products required by the safety plan;

    - the processes required for functional safety;

    - the appropriateness and effectiveness of the performed or implemented safety measures that can be assessed during the development of the item or element;

    - the arguments, if provided, as to why functional safety is achieved considering the achievement of the relevant objectives of the ISO 26262 series of standards;

    - the argument provided in the safety case;

    - the rationales for the safety anomalies managed to closure in accordance with 26262-2:2018 5.4.3.

- functional safety assessment shall consider:

    - the planning of the other confirmation measures [see 26262-2:2018 6.4.6.5 f)];

    - the results from the confirmation reviews and functional safety audit;

    - the recommendations resulting from the previous functional safety assessment and the resulting corrective actions, if applicable (see 26262-2:2018 6.4.12.9 to 26262-2:2018 6.4.12.13 and ISO 26262-8:2018, 8.4.5.2);

    - the results of the functional safety assessment activities regarding the elements or work products developed by suppliers, corresponding with the Development Interface Agreements in accordance with ISO 26262-8:2018, Clause 5, if applicable.

- A functional safety assessment report shall include a recommendation for acceptance, conditional acceptance, or rejection of the functional safety of the item, or of the contribution to the functional safety of the item by the developed elements or work products.

- A functional safety assessment report in accordance with 26262-2:2018 6.4.12.9 may include a recommendation for conditional acceptance provided the functional safety of the item, or the required contribution to functional safety by the developed elements or work products, is achieved, subject to the resolution of the identified conditions for acceptance.

- In the case of a recommendation for conditional acceptance in accordance with 26262-2:2018 6.4.12.10, the functional safety assessment report shall include the conditions for acceptance.

- If the recommendation in a functional safety assessment report in accordance with 26262-2:2018 6.4.12.10 is a conditional acceptance of the achieved functional safety, the corrective actions needed to address the conditions for acceptance documented in the functional safety assessment report shall be carried out.

- If the recommendation in a functional safety assessment report in accordance with 26262-2:2018 6.4.12.9 is a rejection of the achieved functional safety, then:

    - adequate corrective actions shall be performed;

    - the functional safety assessment shall be repeated;

Work Products:

- Functional Safety Assessment Report

Performers

Functional Safety Manager

Accountable

Functional Safety Core Manager

Consulted

CyberSafety Manager, SOTIF Project Manager

Informed

Core Quality Product Engineer, Project Manager, Quality Product Engineer

3.1.1.45 □Product Release into the market

Description

Objectives:

- Releasing the product into the market.

Safety Requirements:

- The safety case in accordance with ISO 26262-2:2018 6.4.8 shall be available prior to the release for production.
- The applicable confirmation measure reports in accordance with ISO 26262-2:2018 6.4.9 to ISO 26262-2:20186.4.12 shall be available prior to the release for production
- The release for production of the item, or elements, shall only be approved if there is sufficient evidence for confidence in the achievement of functional safety.
- The documentation of functional safety for release for production shall include the following information:
    - the name and signature of the person responsible for the release;
    - the versions of the released item or elements;
    - the configuration of the released item or elements;
    - the release date.
- At the release for production, a baseline for the embedded software, including the calibration data, and a baseline for the hardware shall be available and shall be documented in accordance with ISO 26262-8:2018, Clause 10.

Work Product:

- Released Product

Performers

Release Manager

Accountable

Project Manager

Consulted

Cybersecurity Core Manager, Cybersecurity Product Manager, SOTIF Core Manager, SOTIF Project Manager, CyberSafety Manager

Informed

Customer Cybersecurity Incident Response Team, Customer SOTIF Team, External Cybersecurity Entity, External SOTIF Entity

3.1.1.46 Combined Incident MonitoringAndResponceProcess

Description

Managing the cybersafety incidents related to release product.

Performers

Customer Cybersecurity Incident Response Team, Customer SOTIF Team, CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Core Manager, Cybersecurity Product Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, External Cybersecurity Entity, External SOTIF Entity, Project Manager, Project Software Architect, Project System Architect, Release Manager, Software Engineer, Software Test Engineer, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, Test Engineer

Accountable

Project Manager

Consulted

Customer Cybersecurity Incident Response Team, Customer SOTIF Team, CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Core Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Cybersecurity Product Manager, External Cybersecurity Entity, External SOTIF Entity, Project Manager, Project Software Architect, Project System Architect, Release Manager, Software Engineer, Software Test Engineer, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, Test Engineer

Informed

Customer Cybersecurity Incident Response Team, Customer SOTIF Team, CyberSafety Manager, Cybersecurity Core Analyst, Cybersecurity Core Manager, Cybersecurity Product Software Engineer, Cybersecurity Product System Analyst, Cybersecurity Product Manager, External Cybersecurity Entity, External SOTIF Entity, Project Manager, Project Software Architect, Project System Architect, Release Manager, Software Engineer, Software Test Engineer, SOTIF Core Analyst, SOTIF Core Manager, SOTIF Product Software Engineer, SOTIF Product System Analyst, SOTIF Project Manager, SOTIF Software Architect, Test Engineer

Process

3.1.1.47 CombinedIncidentMonitoringAndResponceProcess - Joint Incident Monitoring Activities ISO 21434/ISO 21448□Decommissioning

Description

Objectives:

- Remove product from the market

- The objective of this clause is to define the responsibilities of the organizations and persons responsible for achieving decommissioning

Requirements and Recommendations:

- The organization shall appoint persons with the responsibility and the corresponding authority, in accordance with ISO26262-2:2018 5.4.2.7, to achieve and maintain the functional safety of the item regarding production, operation, service and decommissioning.

- The organization shall institute, execute and maintain processes in order to achieve and maintain the functional safety of the item regarding production, operation, service and decommissioning

- the item changes during production, operation, service or decommissioning, the release for production in accordance with ISO26262-2:2018 6.4.13, shall be updated accordingly.

Work products:

- Evidence of safety decommissioning, resulting from ISO26262-2:2018 7.4.2

Performers

Release Manager

Accountable

Project Manager

Consulted

Cybersecurity Core Manager, Functional Safety Core Manager, SOTIF Core Manager

Informed

Core Quality Product Engineer

4 RESOURCES

4.1 CYBERSECURITY PRODUCT SYSTEM ANALYST (ROLE)

Description

Cybersecurity Product System Analyst is responsible for all Design Products related to Cybersecurity activities in a particural project.

4.2 CYBERSECURITY CORE ANALYST (ROLE)

Description

Cybersecurity Core Analyst is a part of Core Cybersecurity Team, which monitors and analyses the infield products for a Cybersecurity threats.

4.3 CYBERSAFETY MANAGER (ROLE)

Description

CyberSafety Manager is responsible for coordination of Safety and Cybersecurity activities in project.

4.4 CYBERSECURITY PENETRATION TESTING ENGINEER (ROLE)

Description

Cybersecurity Penetration Testing Engineer is reponsible for Penetration Assessment of a developed product.

4.5 CYBERSECURITY PRODUCT SOFTWARE ENGINEER (ROLE)

Description

Cybersecurity Product Software Engineer is responsible for implementation of Cybersecurity functionality into the project.

4.6 FUNCTIONAL SAFETY MANAGER (ROLE)

Description

Responsible for Functional Safety work products management.

4.7 FUNCTIONAL SAFETY PRODUCT SOFTWARE ENGINEER (ROLE)

Description

Functional Safety Product Software Engineer is responsible for implementation of Functional Safety functionality into the project.

4.8 FUNCTIONAL SAFETY PRODUCT SYSTEM ANALYST (ROLE)

Description

Functional Safety Product System Analyst is responsible for all Design Products related to Functional Safety activities in a particural project.

4.9 PROJECT SOFTWARE ARCHITECT (ROLE)

Description

Project Software Architect is responsible for the Software Architecture definition and maintenance.

4.10 PROJECT SYSTEM ARCHITECT (ROLE)

Description

Project System Architect is responsible for the entire System Architecture preparation and analysis. She/He is in charge of any changes in the system.

4.11 SOTIF CORE ANALYST (ROLE)

Description

SOTIF Core Analyst is a part of Core SOTIF Team, which monitors and analyses the infield products for a SOTIF threats.

4.12 SOTIF CORE MANAGER (ROLE)

Description

Manages Core Team Activities, is responsible for a final decision of a risk score.

4.13 SOTIF PRODUCT SOFTWARE ENGINEER (ROLE)

Description

SOTIF Product Software Engineer is responsible for implementation of SOTIF functionality into the project.

4.14 SOTIF PRODUCT SYSTEM ANALYST (ROLE)

Description

SOTIF Product System Analyst is responsible for all Design Products related to SOTIF activities in a particural project.

4.15 SOTIF SOFTWARE ARCHITECT (ROLE)

Description

Software architect responsible for SOTIF related software architecture.

4.16 CORE QUALITY PRODUCT ENGINEER (ROLE)

4.17 PROJECT MANAGER (ROLE)

Description

Project Manager is responsible entire project management, and various competency synchronization to fulfill and organizational, customer and legal standards.

4.18 QUALITY PRODUCT ENGINEER (ROLE)

Description

Quality Product Enigneer is responsible for monitioring the process activities and work products availability according to quality KPIs.

Quality Product Enigneer is also responsible for condicting an internal quality assessment.

4.19 CYBERSECURITY PRODUCT MANAGER (ROLE)

Description

Responsible for Cybersecurity work products management.

4.20 SOTIF PROJECT MANAGER (ROLE)

Description

SOTIF Project Manager is responsible for managing all work products needed according to ISO 21448.

4.21 CYBERSECURITY TEST ENGINEER (ROLE)

Description

Test Engineer responsible for testing Cybersecurity related features.

4.22 FUNCTIONAL SAFETY CORE MANAGER (ROLE)

Description

Manages Core Team Activities, is responsible for a final decision of a risk score.

4.23 FUNCTIONAL SAFETY TEST ENGINEER (ROLE)

Description

Functional Safety Test Engineer is responsbile for testing activities related to functional safety of developed system.

4.24 SOTIF TEST ENGINEER (ROLE)

Description

Test Engineer responsible for testing SOTIF related features.

4.25 CYBERSECURITY CORE MANAGER (ROLE)

Description

Manages Core Team Activities, is responsible for a final decision of a risk score.

4.26 TEST ENGINEER (ROLE)

Description

Test Engineer responsible for feature tests.

4.27 RELEASE MANAGER (ROLE)

Description

Release Manager is responsible for all activities needed for software release preparation.

4.28 CUSTOMER SOTIF TEAM (ROLE)

Description

Customer SOTIF Team is responsible for SOTIF release approval and delivery of infield SOTIF reports from vehicles.

4.29 CUSTOMER CYBERSECURITY INCIDENT RESPONSE TEAM (ROLE)

Description

Customer Cybersecurity Incident Response Team is responsible for a risk mitigation strategy approval, and provides Incident Reports from infield vehicles.

4.30 EXTERNAL CYBERSECURITY ENTITY (ROLE)

Description

An etity, which provides cybersecurity related data to the Cybersecurity team. It can be a non-profit organisation, state governance, univercity etc.

4.31 EXTERNAL SOTIF ENTITY (ENTITY)

Description

External SOTIF Entity provides SOTIF reports. It can be SOTIF Intelligence Platform, Supply Chain Reports, Governance Agencies, Safety Researches.

4.32 SOFTWARE ENGINEER (ROLE)

Description

Software engineer responsbile for feature development.

4.33 SOFTWARE TEST ENGINEER (ROLE)

Description

Test engineer responsbile for software level testing.

Appendix B

Appendix B - Medini Analyze - CyberSafety Analysis Highway Pilot

You can download the necessary files by clicking the following link:

Download ZIP File (Medini Analyze - CyberSafety Analysis Highway Pilot)

List of Figures

Bibliography

[1] Hakob Barseghyan. *The Laws of Scientic Change*. Springer International Publishing Switzerland 2015, 2015.

[2] Saul Perlmutter, Brian Schmidt, and Adam Riess. The nobel prize in physics 2011. *The Royal Swedish Academy of Sciences*, page 50005, 2011.

[3] Kazimierz Kosmowski. *Operational resilience regarding safety and security aspects of industrial automation and control systems*, pages 99–116. Gdynia Maritime University, 01 2023.

[4] Kazimierz T. Kosmowski, Emilian Piesik, Jan Piesik, and Marcin Śliwiński. Integrated functional safety and cybersecurity evaluation in a framework for business continuity management. *Energies*, 15(10), 2022.

[5] ISO Central Secretary. Road vehicles — functional safety. Standard ISO 26262:2018, International Organization for Standardization, Geneva, CH, 2018.

[6] ISO Central Secretary. Road vehicles — safety of the intended functionality. Standard ISO 21448:2019, International Organization for Standardization, Geneva, CH, 2019.

[7] Amund Skavhaug, Jeremie Guiochet, Erwin Schoitsch, and Friedemann Bitsch. *Computer Safety, Reliability, and Security: SAFECOMP 2016 Workshops, ASSURE, DECSoS, SASSUR, and TIPS, Trondheim, Norway, September 20, 2016, Proceedings*. Springer, 2016.

[8] Thomas Quirchmayr, Barbara Paech, Roland Kohl, and Hannes Karey. *Semi-automatic Software Feature-Relevant Information Extraction from Natural Language User Manuals*. Springer, 2017.

[9] Warren Axelrod. Cybersecurity challenges of systems-of-systems for fully-autonomous road vehicles. *2017 13th International Conference and Expo on Emerging Technologies for a Smarter World, CEWIT 2017*, 2018-Janua:1–6, 2017.

[10] Gianfranco Burzio, Giuseppe Faranda Cordella, Michele Colajanni, Mirco Marchetti, and Dario Stabili. Cybersecurity of connected autonomous vehicles : A ranking based approach. *2018 International Conference of Electrical and Electronic Technologies for Automotive, AUTOMOTIVE 2018*, 2018.

[11] Maslina Daud, Rajah Rasiah, Mary George, David Asirvatham, and Govindamal Thangiah. Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations? *International Journal of Business and Society*, 19:161–180, 2018.

[12] Yousik Lee, Samuel Woo, Yunkeun Song, Jungho Lee, and Dong Hoon Lee. Practical vulnerability-information-sharing architecture for automotive security-risk analysis. *IEEE Access*, 8:120009–120018, 2020.

[13] ISO Central Secretary. Road vehicles — cybersecurity engineering. Standard ISO 21434:2021, International Organization for Standardization, Geneva, CH, 2021.

[14] Charlie Miller and Chris Valasek. Hackers remotely kill a jeep on the highway - with me in it, 2014. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [Accessed: Dec2023].

[15] Xugui Zhou, Anna Schmedding, Haotian Ren, Lishan Yang, Philip Schowitz, Evgenia Smirni, and Homa Alemzadeh. Strategic safety-critical attacks against an advanced driver assistance system. In *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 79–87, 2022.

[16] Kyounggon Kim, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, and Huy Kang Kim. Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers and Security*, 103:102150, 2021.

[17] KEEN Security LAB. Car hacking research: Remote attack tesla motors, 2016. https://www.youtube.com/watch?v=c1XyhReNcHY&ab_channel=KeenSecurityLab [Accessed: May2024].

[18] Florian Sommer, Jürgen Dürrwang, and Reiner Kriesten. Survey and classification of automotive security attacks. *Information*, 10(4), 2019.

[19] Aurélien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. *IACR Cryptology ePrint Archive*, 2010:332, 01 2010.

[20] Jürgen Dürrwang, Johannes Braun, Marcel Rumez, Reiner Kriesten, and Alexander Pretschner. Enhancement of automotive penetration testing with threat analyses results. *SAE International Journal of Transportation Cybersecurity and Privacy*, 1:21, 11 2018.

[21] Upstream Security Ltd. Smart mobility cyber attacks repository, 2024. https://www.upstream.auto/research/automotive-cybersecurity/ [Accessed: May2024].

[22] Jonathan Petit, Bas Stotelaar, Michael Feiri, and Frank Kargi. Remote attacks on automated vehicles sensors: Experiments on camera and lidar, 2015. https://api.semanticscholar.org/CorpusID:39608826 [Accessed: Dec2023].

[23] KEEN Security LAB. Experimental security assessment of bmw cars: A summary report, 2019. https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf [Accessed: Dec2023].

[24] Helmut Martin, Zhendong Ma, Christoph Schmittner, Bernhard Winkler, Martin Krammer, Daniel Schneider, Tiago Amorim, Georg Macher, and Christian Kreiner. Combined automotive safety and security pattern engineering approach. *Reliability Engineering and System Safety*, 198, 2020.

[25] Oleg Kirovskii and Vasilii Aleksandrovich Gorelov. Driver assistance systems: Analysis, tests and the safety case. iso 26262 and iso pas 21448. *IOP Conference Series: Materials Science and Engineering*, 534, 2019.

[26] Xinyu Zhang, Wenbo Shao, Mo Zhou, Qifan Tan, and Jun Li. A scene comprehensive safety evaluation method based on binocular camera. *Robotics and Autonomous Systems*, 128:103503, 2020.

[27] Priyadarshini, Simon Greiner, Maike Massierer, and Oum-El-Kheir Aktouf. Feature-based software architecture analysis to identify safety and security interactions. *Proceedings - IEEE 20th International Conference on Software Architecture, ICSA 2023*, page 12 – 22, 2023.

[28] Tim Weilkiens, Lamm Jesko, Stephan Roth, and Markus Walker. *Model-Based System Architecture*. John Wiley and Sons, Inc, 2015.

[29] David Long and Zane Scott. *A Primer for Model-Based Systems Engineering*. Vitech Company, 2012.

[30] Lovric, Tomislav, Schneider-Scheyer, Manuel, and Sarkic, Samir. Sysml as backbone for engineering and safety - practical experience with trw braking ecu. In *SAE 2014 World Congress and Exhibition*. SAE International, apr 2014.

[31] Shiyi Jin, Jin-Gyun Chung, and Yinan Xu. Signature-based intrusion detection system (ids) for in-vehicle can bus network. In *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–5, 2021.

[32] Sergej Japs. Towards the development of the cybersecurity concept according to iso/sae 21434 using model-based systems engineering. In *2021 IEEE 29th International Requirements Engineering Conference (RE)*, pages 486–491, 2021.

[33] Richard Messnarz, Christian Kreiner, Georg Macher, and Alastair Walker. Extending automotive spice 3.0 for the use in adas and future self-driving service architectures. *Journal of Software: Evolution and Process*, 30:1–14, 2018.

[34] Alan Smith and Felix Offodile. Strategic importance of team integration issues in product development processes to improve manufacturability. *Team Performance Management*, 14:269–292, 2008.

[35] Franz Wotawa, Bernhard Peischl, Florian Klück, and Mihai Nica. Quality assurance methodologies for automated driving. *Elektrotechnik und Informationstechnik*, 135:322–327, 8 2018.

[36] Shannon Flumerfelt. Leveraging system complexity for improvement. *Total Quality Management and Business Excellence*, 31:542–549, 4 2020.

[37] Thor Myklebust, Tor Stalhane, and Gunnar Jenssen. Autonomous vehicles-trust, safety and security cases: The complete picture. *Proceedings - Annual Reliability and Maintainability Symposium*, 2023-January, 2023.

[38] Betty Cheng, Bradley Doherty, Nick Polanco, and Matthew Pasco. Security patterns for automotive systems. *Proceedings - 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems Companion, MODELS-C 2019*, pages 54–63, 2019.

[39] Boris Brankovic, Marco Ebster, Katharina Polanec, Christoph Binder, and Christian Neureiter. Towards an automated security-by-design approach in automotive system-of-systems architectures. In *2023 8th International Conference on Smart and Sustainable Technologies (SpliTech)*, pages 1–4, 2023.

[40] Bizagi. Bizagi user guide modeler, 2024. https://help.bizagi.com/process-modeler/en/index.html?events.htm [Accessed: May2024].

[41] Ansys. Automotive transportation and mobility, 2024. https://www.ansys.com/en-in/industries/transportation-and-mobility [Accessed: May2024].

[42] Josef Oehmen, Bohdan Oppenheim, Deborah Secor, et al. *The Guide to Lean Enablers for Managing Engineering Programs*. Joint MIT-PMI-INCOSE Community of Practice on Lean in Program Management, 05 2012.

[43] Karl Ulrich, Steven Eppinger, and Maria Yang. *Product Design and Development, 7th ed.* McGraw-Hill Education, 2020.

[44] Robert Cooper. Stage-gate systems: A new tool for managing new products. *Business Horizons*, 33(3):44–54, 1990.

[45] Taiichi Ohno. *Toyota Production System: Beyond Large-Scale Production*. CRC Press, 1988.

[46] James Womack, Daniel Jones, and Daniel Ross. *The Machine That Changed the World*. Free Press, 1990.

[47] Bohdan Oppenheim. Lean product development flow. *Systems Engineering*, 7:no – no, 10 2004.

[48] Allen Ward. *Lean Product and Process Development*. Lean Enterprises Inst. Inc, 2007.

[49] James Morgan and Jeffrey Liker. *The Toyota Product Development System*. Productivity Press, 2007.

[50] Bohdan Oppenheim. *Lean for Systems Engineering with Lean Enablers for Systems Engineering*. Wiley, 2011.

[51] Josef Oehmen and Eric Rebentisch. *Waste in Lean Product Development*. Initiative LAI-MIT, 2010.

[52] Joakim Pernstal, Robert Feldt, Tony Gorschek, et al. Flex-rca: A lean-based method for root cause analysis in software process improvement. *Software Qual J 27*, page 50005, 2019.

[53] United States Department of Transportation Federal Highway Administration. Systems engineering for intelligent transportation systems, 2007. https://ops.fhwa.dot.gov/publications/seitsguide/seguide.pdf [Accessed: Dec2023].

[54] ISO Central Secretary. Systems and software engineering — system life cycle processes. Standard ISO15288:2015, International Organization for Standardization, Geneva, CH, 2015.

[55] VDA QMC. Automotive spice process assessment / reference model. Standard, Verband der Automobilindustrie, Berlin, DE, 2017.

[56] Alastair Walker. Cybersecurity in safety-critical systems. *Journal of Software: Evolution and Process*, 30:4–9, 2018.

[57] United States Department of Transportation. Nhtsa - national highway traffic safety administration, 2024. https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity [Accessed: Jun2023].

[58] AUTO-ISAC. Automotive information sharing and analysis center, 2020. https://automotiveisac.com/best-practices/ [Accessed: Jun2023].

[59] IPA IT Security Center Information-Technology Promotion Agency Japan. Approaches for vehicle information security information security for networked" vehicles, 2013. https://www.ipa.go.jp/files/000033402.pdf [Accessed: Dec2023].

[60] European Union Agency for Cybersecurity. Enisa good practices for security of smart cars, 2019. https://www.enisa.europa.eu/publications/smart-car [Accessed: Dec2023].

[61] Upstream Security. Global automotive cybersecurity report, 2021. https://upstream.auto/2021report/ [Accessed: Jun2023].

[62] Zachary Collier, Daniel Dimase, Steve Walters, Mark Tehranipoor Mohammad, James H. Lambert, and Igor Linkov. Cybersecurity standards: Managing risk and creating resilience. *Computer*, 47:70–76, 2014.

[63] Philip Stirgwolt. Effective management of functional safety for iso 26262 standard. In *2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS)*, pages 1–6, 2013.

[64] ISO Central Secretary. Quality management systems—particular requirements for the application of iso 9001:2008 for automotive production and relevant service part organizations. Standard ISO 16949:2009, International Organization for Standardization, Geneva, CH, 2009.

[65] UNECE. United nations economic commission of europe, 2020. https://unece.org/ [Accessed: Dec2023].

[66] United Nations Economic and Social Council. Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, 2021. https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf [Accessed: Jun2023].

[67] SAE International. Cybersecurity guidebook for cyber-physical vehicle systems. Standard SAEJ3061:2021, Society of Automotive Engineers, Warrendale, USA, 2021.

[68] Arpad Torok, Zsolt Szalay, and Balazs Saghi. New aspects of integrity levels in automotive industry-cybersecurity of automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, pages 1–9, 2020.

[69] Giedre Sabaliauskaite, Jin Cui, Lin Shen Liew, and Fengjun Zhou. Integrated safety and cybersecurity risk analysis of cooperative intelligent transport systems. *Proceedings - 2018 Joint 10th International Conference on Soft Computing and Intelligent Systems and 19th International Symposium on Advanced Intelligent Systems, SCIS-ISIS 2018*, pages 723–728, 2018.

[70] SAE International. Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. Standard SAEJ30161:2018, Society of Automotive Engineers, Warrendale, USA, 2018.

[71] Yanan Zhang, Peiji Shi, Yangyang Liu, Shengqiang Han, Baoying Mu, and Jia Zheng. Study on incident response system of automotive cybersecurity. In *Security and Privacy in New Computing Environments*, volume 284, pages 198–209. Springer Verlag, 2019.

[72] VDA QMC Quality Management in the Automotive Industry. Quality management in the automotive industry automotive spice ® process reference model process assessment model title: Automotive spice process assessment / reference model, 2017. https://www.automotivespice.com [Accessed: Dec2022].

[73] AUTOSAR. Requirements on intrusion detection system, 2020. https://www.autosar.org/fileadmin/user_upload/standards/foundation/20-11/AUTOSAR_RS_IntrusionDetectionSystem.pdf [Accessed: Dec2023].

[74] AUTOSAR. Specification of intrusion detection system protocol, 2020. https://www.autosar.org/fileadmin/user_upload/standards/foundation/20-11/AUTOSAR_PRS_IntrusionDetectionSystem.pdf [Accessed: Dec2023].

[75] AUTOSAR. Specification of intrusion detection system manager, 2020. https://www.autosar.org/fileadmin/user_upload/standards/classic/20-11/AUTOSAR_SWS_IntrusionDetectionSystemManager.pdf [Accessed: Dec2023].

[76] AUTOSAR. Specification of intrusion detection system manager for adaptive platform, 2020. https://www.autosar.org/fileadmin/user_upload/standards/adaptive/20-11/AUTOSAR_SWS_AdaptiveIntrusionDetectionSystemManager.pdf [Accessed: Dec2023].

[77] ISO Central Secretary. Road vehicles cybersecurity assurance levels (cal) and targeted attack feasibility (taf). Standard ISO 8475, International Organization for Standardization, Geneva, CH, 2024.

[78] ISO Central Secretary. Road vehicles cybersecurity verification and validation. Standard ISO 8477, International Organization for Standardization, Geneva, CH, 2024.

[79] Stefan Brunner, Jurgen Roder, Markus Kucera, and Thomas Waas. Automotive e/e-architecture enhancements by usage of ethernet tsn. In *2017 13th Workshop on Intelligent Solutions in Embedded Systems (WISES)*, pages 9–13, 2017.

[80] Alessio Bucaioni and Patrizio Pelliccione. Technical architectures for automotive systems. In *2020 IEEE International Conference on Software Architecture (ICSA)*, pages 46–57, 2020.

[81] Matthias Traub, Alexander Maier, and Kai L. Barbehön. Future automotive architecture and the impact of it trends. *IEEE Software*, 34(3):27–32, 2017.

[82] Anders Magnusson, Leo Laine, and Johan Lindberg. Rethink ee architecture in automotive to facilitate automation, connectivity, and electro mobility. In *2018 IEEE/ACM 40th International Conference on Software Engineering: Software Engineering in Practice Track (ICSE-SEIP)*, pages 65–74, 2018.

[83] Open Group. Open group standard service-oriented architecture ontology, 2019. https://www.opengroup.org/forum/service-oriented-architecture-soa [Accessed: (Mar2023)].

[84] Harald Proff, Thomas Pottebaum, and Philipp Wolf. Software is transforming the automotive world. *Deloitte.Insights*, page 20, 2020.

[85] Stefaan Sonck Thiebaut, Antonio De Rosa, and Ralph Sasse. Secure embedded hypervisor based systems for automotive. In *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)*, pages 211–212, 2016.

[86] Renesas Electronics Corporation. Rh850 / f1k group, 2016. https://www.renesas.com/br/en/document/man/rh850f1k-group-users-manual-hardware [Accessed: Jun2023].

[87] Christos Tranoris, Spyros Denazis, Lucas Guardalben, João Pereira, and Susana Sargento. Enabling cyber-physical systems for 5g networking: A case study on the automotive vertical domain. In *2018 IEEE/ACM 4th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, pages 37–40, 2018.

[88] Gianfranco Burzio, Giuseppe Faranda Cordella, Michele Colajanni, Mirco Marchetti, and Dario Stabili. Cybersecurity of connected autonomous vehicles : A ranking based approach. *2018 International Conference of Electrical and Electronic Technologies for Automotive*, pages 1–6, 2018.

[89] Christos Kyrkou, Andreas Papachristodoulou, Andreas Kloukiniotis, Andreas Papandreou, Aris Lalos, Konstantinos Moustakas, and Theocharis Theocharides. Towards artificial-intelligence-based cybersecurity for robustifying automated driving systems against camera sensor attacks. *Proceedings of IEEE Computer Society Annual Symposium on VLSI, ISVLSI*, 2020-July:476–481, 2020.

[90] Abdullah Al Mamun, Md. Abdullah Al Mamun, and Abdullatif Shikfa. Challenges and mitigation of cyber threat in automated vehicle: An integrated approach. In *2018 International Conference of Electrical and Electronic Technologies for Automotive*, pages 1–6, 2018.

[91] Michele Scalas and Giorgio Giacinto. Automotive cybersecurity: Foundations for next-generation vehicles. *arXiv*, 2019.

[92] Matan Levi, Yair Allouche, and Aryeh Kontorovich. Advanced analytics for connected car cybersecurity. In *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, volume 2018-June, pages 1–7. Institute of Electrical and Electronics Engineers Inc., 7 2018.

[93] Toru Sakon and Yukikazu Nakamoto. Structured policy-based design method for cybersecurity of automotive e/e system. In *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pages 1617–1622, 2018.

[94] Jesse Edwards, Ameer Kashani, and Gopalakrishnan Iyer. Evaluation of software vulnerabilities in vehicle electronic control units. In *2017 IEEE Cybersecurity Development (SecDev)*, pages 83–84. Institute of Electrical and Electronics Engineers Inc., 10 2017.

[95] Ken Schwaber. *Agile Project Management with Scrum*. Best practices. Microsoft Press, 2004.

[96] Craig Larman and Bas Vodde. *Practices for Scaling Lean & Agile Development: Large, Multisite, and Offshore Product Development with Large-Scale Scrum*. Pearson Education, 2010.

[97] Syeda Komal Anjum, Carsten Wolff, and Nerea Toledo. Adapting agile principles for requirements engineering in automotive software development. In *2022 IEEE European Technology and Engineering Management Summit (E-TEMS)*, pages 166–174, 2022.

[98] Syeda Komal Anjum and Carsten Wolff. Integration of agile methods in automotive software development processes. In *2020 IEEE 3rd International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE)*, pages 000151–000154, 2020.

[99] Magnus Ågren, Rogardt Heldal, Eric Knauss, and Patrizio Pelliccione. Agile beyond teams and feedback beyond software in automotive systems. *IEEE Transactions on Engineering Management*, 69(6):3459–3475, 2022.

[100] Kent Beck, Mike Beedle, Arie van Bennekum, Alistair Cockburn, Ward Cunningham, Martin Fowler, James Grenning, Jim Highsmith, Andrew Hunt, Ron Jeffries, Jon Kern, Brian Marick, Robert C. Martin, Steve Mellor, Ken Schwaber, Jeff Sutherland, and Dave Thomas. Manifesto for agile software development, 2001. `http://www.agilemanifesto.org/` [Accessed: Feb2023].

[101] SEBoK Editorial Board. *The Guide to the Systems Engineering Body of Knowledge (SEBoK)*. The Trustees of the Stevens Institute of Technology, Hoboken, NJ, 2.8 edition, 2023. Accessed Jan2024.

[102] Josef Oehmen, editor. *The Guide to Lean Enablers for Managing Engineering Programs, Version 1.0*. Joint MIT-PMI-INCOSE Community of Practice on Lean in Program Management, Cambridge, MA, 2012.

[103] Aleksander Buczacki, Dariusz Cieślar, Bohdan W. Oppenheim, and Mateusz Stachnik. Lean systems engineering for automotive perception systems. In *2019 24th International Conference on Methods and Models in Automation and Robotics (MMAR)*, pages 548–553, 2019.

[104] Mika Arpe and Cory Ensley. The future of automotive data connectivity. Technical report, Aptiv, 03 2021.

[105] Biter Nabeel. OTA Updates Require Flexible Architecture. Technical report, Aptiv, 02 2021.

[106] Martin Bornemann, Bejnamin Bould, and Cezary Klimasz. Open server platform requires shifts in hardware and software. Technical report, Aptiv, 05 2023.

[107] Glen De Vos. Aptiv's gen 6 adas platform forsoftware-defined vehicles. Technical report, Aptiv, 01 2021.

[108] Brian Witten. Positioning automotive cybersecurity for the future. Technical report, Aptiv, 04 2023.

[109] PricewaterhouseCoopers (PwC). The 2018 strategy & digital auto report, 2018. https://www.strategyand.pwc.com/de/en/industries/automotive/the-future-is-here/digital-auto-report-2018.pdf [Accessed: Jun2023].

[110] UMAR ZAKIR ABDUL HAMID. *Autonomous, Connected, Electric and Shared Vehicles: Disrupting the Automotive and Mobility Sectors*, pages i–xviii. SAE, 2023.

[111] Inc Object Management Group. Business process model and notation, 2010. https://www.omg.org/spec/BPMN/2.0/PDF [Accessed: May2022].

[112] Badr Omair and Ahmad Alturki. Taxonomy of fraud detection metrics for business processes. *IEEE Access*, 8:71364–71377, 2020.

[113] Martin Skoglund, Fredrik Warg, and Behrooz Sangchoolie. In search of synergies in a multi-concern development lifecycle: Safety and cybersecurity. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11094 LNCS:302–313, 2018.

[114] Georg MacHer, Christoph Schmittner, Jürgen Dobaj, Eric Armengaud, and Richard Messnarz. An integrated view on automotive spice, functional safety and cyber-security. *SAE Technical Papers*, 2020-April:1–10, 2020.

[115] Vivek Agrawal, Balasubramanian Achuthan, Asadullah Ansari, Vishal Tiwari, and Vikas Pandey. Threat/hazard analysis and risk assessment: A framework to align the functional safety and security process in automotive domain. *SAE International Journal of Transportation Cybersecurity and Privacy*, 4, 12 2021.

[116] Árpád Török, Zsolt Szalay, and Balázs Sághi. New aspects of integrity levels in automotive industry-cybersecurity of automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 23(1):383–391, 2022.

[117] Guard Knox. Zonal architecture: The foundation for next-generation vehicles, 2021. https://learn.guardknox.com/zonal-architecturethe-foundation-for-next-generation-vehicles [Accessed: Jun2023].

[118] Guard Knox. The automotive paradigm shift & the rise of the cybertech tier, 2022. https://learn.guardknox.com/the-automotive-paradigm-shift-the-rise-of-the-cybertech-tier [Accessed: Jun2023].

[119] Christian Plappert, Daniel Zelle, Henry Gadacz, Roland Rieke, Dirk Scheuermann, and Christoph Krauß. Attack surface assessment for cybersecurity engineering in the automotive domain. In *2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, pages 266–275, 2021.

[120] VDA QMC. Automotive cybersecurity management system audit 1st edition, december 2020. Standard, Verband der Automobilindustrie, Berlin, DE, 2020.

[121] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. Computer security incident handling guide : Recommendations of the national institute of standards and technology, 8 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [Accessed: Jun2023].

[122] Lei Ren, Huilin Yin, Wancheng Ge, and Qian Meng. Environment influences on uncertainty of object detection for automated driving systems. In *2019 12th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, pages 1–5, 2019.

[123] ISO Central Secretary. Road vehicles — guidelines for auditing cybersecurity engineering. Standard ISO 5112:2022, International Organization for Standardization, Geneva, CH, 2022.

[124] ISO Central Secretary. Road vehicles — safety for automated driving systems — design, verification and validation. Standard ISO 5083:2022, International Organization for Standardization, Geneva, CH, 2022.

[125] Liat Haber and Abraham Carmeli. Leading the challenges of implementing new technologies in organizations. *Technology in Society*, 74:102300, 2023.

[126] Aryan Mehta, Ali Asgar Padaria, Dwij Bavisi, Vijay Ukani, Priyank Thakkar, Rebekah Geddam, Ketan Kotecha, and Ajith Abraham. Securing the future: A comprehensive review of security challenges and solutions in advanced driver assistance systems. *IEEE Access*, PP:1–1, 01 2023.

[127] Ben Nassi, Dudi Nassi, Raz Ben-Netanel, Yisroel Mirsky, Oleg Drokin, and Yuval Elovici. Phantom of the adas: Phantom attacks on driver-assistance systems. *IACR Cryptol. ePrint Arch.*, 2020:85, 2020.

[128] Shifat Kayser, Furkan Heybetli, and Mustafa Sinasi Ayas. Model based detection scheme for denial of service attack on lane keeping assist system. In *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pages 1–6, 2022.

[129] Markus Schumacher et al. *"Security Patterns: Integrating Security and Systems Engineering"*. "John Wiley & Sons, Ltd", "Chichester", 2006.

[130] Ozgur Aktunc. Entropy metrics for agile development processes. In *2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops*, pages 7–8, 2012.

[131] Reni Kurnia, Ridi Ferdiana, and Sunu Wibirama. Software metrics classification for agile scrum process: A literature review. In *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, pages 174–179, 2018.