EMBA Automotive Industry

ACADEMY FOR
CONTINUING
EDUCATION

FMEA application to ensure cybersecurity of technical products

A Master's Thesis submitted for the degree of
“Executive Master of Business Administration”

supervised by
Dr. Alexander Schloske

Mayara Balboena Bregalda

51910001

Vienna, 30.07.2023

Affidavit

I, **MAYARA BALBOENA BREGALDA**, hereby declare

1. that I am the sole author of the present Master's Thesis, "FMEA APPLICATION TO ENSURE CYBERSECURITY OF TECHNICAL PRODUCTS", 89 pages, bound, and that I have not used any source or tool other than those referenced or any other illicit aid or tool, and
2. that I have not prior to this date submitted this Master's Thesis as an examination paper in any form in Austria or abroad.

Vienna, 30.07.2023

Signature

Acknowledgment

I would like to express my heartfelt gratitude to all those who have played a vital role in successfully completing my Master's thesis as part of my EMBA in the Automotive Industry at TU Wien.

First and foremost, I am incredibly thankful to my parents and sister for their unwavering support and belief in me. They went beyond their means to help finance my education, even from the other side of the ocean. I always promise to do my best to make them proud.

I sincerely appreciate my colleagues and professors at TU Wien, who provided me with valuable insights, knowledge, and countless weekends of learning, cultural exchange, and fun. Special thanks to my supervisor, Professor Schloske, a true master in FMEA, who came up with the idea for this fascinating topic.

I cannot forget my dear colleague from Bosch AG, whose constant encouragement and support played a significant role in my journey toward completing this thesis.

Last but not least, heartfelt thanks to my partner, whose unwavering encouragement, assistance, and patience were crucial in helping me navigate through the challenges of this academic endeavor.

Each of you has contributed to this milestone in my academic journey, and I am grateful for your invaluable support and encouragement.

Thank you all from the bottom of my heart.

Table of content

List of figures

Abbreviations and acronyms

- AD

Autonomous Driving

- ADAS

Autonomous Driving Assistance System

- AIAG

Automotive Industry Action Group

- CAN

Controller Area Network

- CPS

Cyber-Physical system

- DIN

German Institute for Standardization

- ECU

Electronic Control Unit

- E/E

Electrics and Electronics

- FMEA

Failure Mode Effects and Analyzes

- HARA

Hazard Analysis and Risk Assessment

- IEEE

Institute of Electrical and Electronics Engineers

- ISO

International Organization for Standardization

- OEM

Original Equipment Manufacturer

- SPI

Serial Peripheral Interface

- SAE

Society of Automotive Engineer

- TARA

Threat Analysis and Risk Assessment

- VDA

Verband der Automobilindustrie (German Association of the Automotive Industry)

1 Introduction

1.1 Current condition

"Vehicle (noun): a machine, usually with wheels and an engine, used for transporting people or goods, especially on land." That is how the Cambridge dictionary defines a vehicle [1]. However, in the wake of Nicolaus Otto's pioneering invention of internal combustion engines, the conventional perception of a vehicle has undergone notable transformations. Beyond being a mode of conveyance, vehicles now serve as emblematic representations of status and authority in certain societies, while in others, they embody a passionate pursuit or collectible artifact. Furthermore, vehicles have evolved into intricate systems, encompassing a bundle of components and functionalities, surpassing their earlier iterations in complexity.

The automotive industry has played a substantial role in the global economy over the years, yet the emergence of advanced technologies and interconnectedness has brought forth a critical challenge in the form of cybersecurity risks. Rapid technological advancements continue to redefine the boundaries of vehicle manufacturing, prompting a reevaluation of the traditional understanding of automobiles. In this context, vehicles can be conceived as intricate systems encompassing electrical, electronic, and mechanical components, seamlessly integrating an array of emerging technologies. These include, but are not limited to, advancements such as reduced emissions, the proliferation of electric motors and fuel cells, digitalization, connectivity, car-sharing platforms, ADAS, autonomous driving capabilities, and the imperative need for robust cybersecurity measures. The list of technological advancements continues to expand, ushering in a new era of automotive innovation.

As the automotive industry continues to advance technologically, it becomes imperative to address the escalating concern of cyberattacks and safeguard vehicles from potential threats. OEMs are compelled to stay at the forefront of market dynamics, adapt quickly to changes, and meet the evolving demands of customers. This necessitates a delicate balance between maintaining competitiveness and ensuring robust cybersecurity measures. With a broadened connotation of vehicles as complex mechanisms comprising electrical, electronic, and mechanical components, the industry must embrace emerging technologies such as reduced emissions, electric motors, fuel cells, digitalization, connectivity, car-sharing platforms, ADAS, autonomous driving, and cybersecurity. It is essential to proactively adapt to these transformative shifts while consistently prioritizing customer satisfaction.

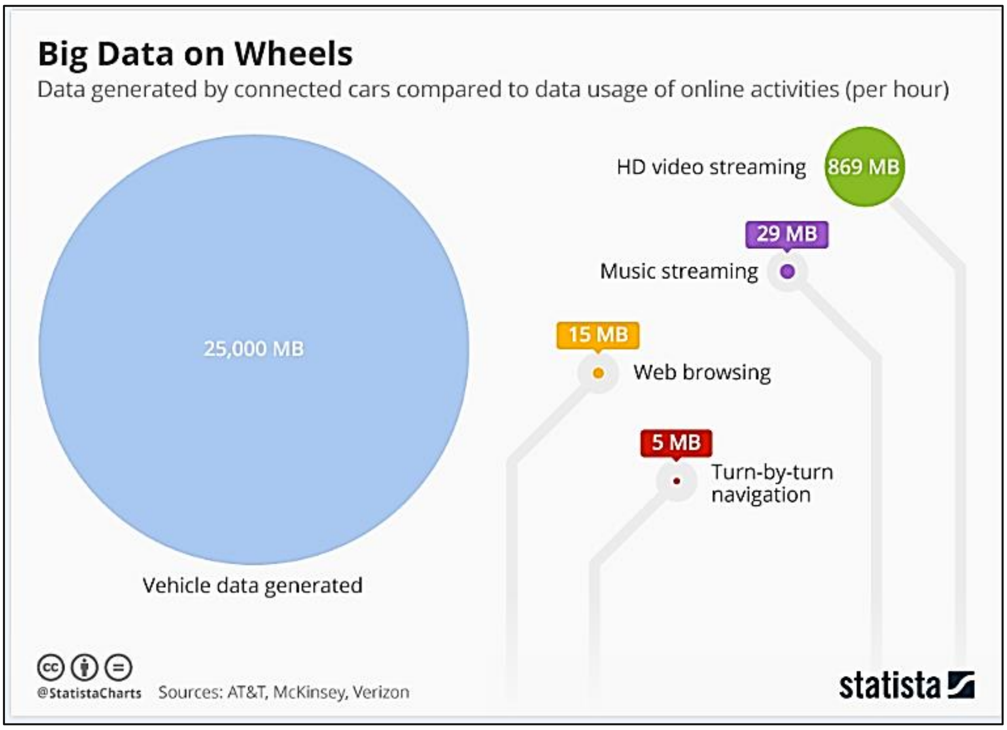


Figure 1 – Amount of data exchange in a vehicle [2]

The incorporation of new features in vehicles, driven by market and customer demands, has resulted in a significant increase in data transmission and storage requirements, as shown in Figure 1. In the context of advancing connectivity, the future of automotive applications is poised to generate vast volumes of data exchange across vehicle systems, interconnectivity with other vehicles, cloud services, and the surrounding environment. This networked structure formed by vehicles holds the potential to store and transmit a wide range of personal information, encompassing customer data from smartphones, manufacturer settings, proximate parked cars, real-time traffic conditions, nearby commercial establishments, and more. From a safety standpoint, this paradigm presents both opportunities and challenges, prompting a heightened focus on cybersecurity measures. The plausibility and severity of potential attacks necessitate a comprehensive examination of the benefits and barriers surrounding cybersecurity within this evolving automotive landscape [3].

1.2 Challenges

As vehicles have evolved and acquired increasingly intricate attributes, accompanied by the integration of additional functionalities, it becomes feasible to classify them as CPS. This entails the interconnection of computational components with physical systems. In the realm of automotive CPS, intricate configurations may involve over 100 ECUs and a substantial number of internal communication channels. Modern cars incorporate numerous features that rely heavily on software implementations, thereby transferring a significant portion of responsibility from the driver to embedded vehicle intelligence. This paradigm shift underscores the growing significance of intelligent systems within vehicles [4]. In order to ensure the integrity of systems and safeguard against potential risks, it is vital to acknowledge the intricate relationship between events transpiring in the digital domain and their ramifications in the tangible world. This interdependence poses significant challenges that necessitate careful consideration and proactive measures[5].

The significance of security concerns related to cyber-attacks within the automotive industry cannot be understated, as evidenced by reported breaches from notable manufacturers such as Fiat Chrysler, Tesla Autonomous Vehicle, BMW, and Mitsubishi. These breaches are often referred to as "hacks," a term that has become commonplace in both technological discourse and everyday vocabulary. The concept of hacking was initially defined by MIT in 1955, and the first known instance of hacking occurred in 1963. As the volume of data continues to grow exponentially, hacking will remain a top priority in ensuring safety and security. In the words of Ginni Rometty, the executive chairman of IBM Corp., data has become the world's new natural resource. It serves as the foundation for gaining a competitive edge and is transforming every profession and industry. Given this reality and the projected global data volume expected to reach 200 zettabytes by

2025, it is evident that cybercrimes will only escalate further in magnitude and impact [6]. Based on the presented graph, it is evident that despite the existing security measures implemented by the industry, hacking incidents continue to constitute a significant proportion of overall attacks.

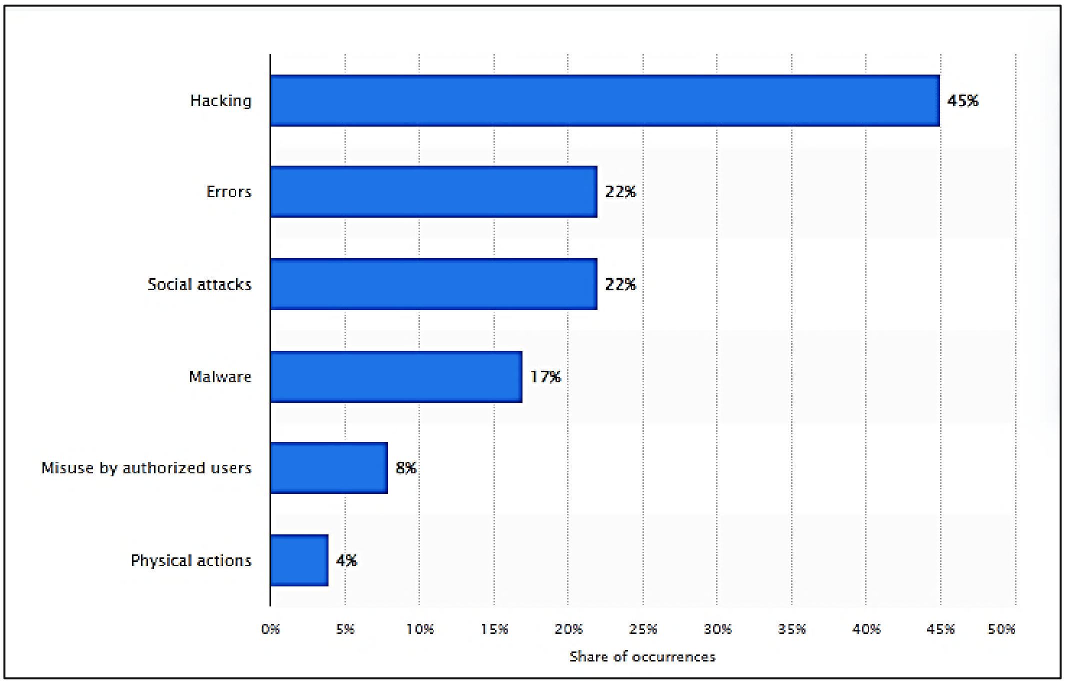


Figure 2 - Most common action varieties in data breaches worldwide in 2019 [7]

Within the automotive sector, OEMs employ diverse methodologies to address potential security concerns on a case-by-case basis during the vehicle creation process. This entails an expansive range of processes, contingent upon the specific automotive system under consideration and the expertise of the team involved. An effective approach involves conducting comprehensive risk assessments and analyses to gather pertinent data and ascertain the implications of introducing new elements, designs, or manufacturing processes. The Failure Mode Effects and Analysis (FMEA) method, a well-established and widely recognized concept within the industry, was initially devised to evaluate the reliability and safety of hardware components [8]. Assessing the safety implications of software components presents a greater challenge compared to physical components, as software does not exhibit failure in the same manner [9].

The convergence of connectivity trends with the assessment of software and hardware components introduces a heightened level of inherent complexity and uncertainty. Consequently, the risk of cyber-attacks becomes increasingly pronounced. Regardless of whether these attacks directly impact safety or not, it is crucial to effectively mitigate and contain them. This realization merely scratches the surface of a larger issue: the automotive industry's current standards must adequately address cybersecurity concerns in order to ensure the integrity and resilience of vehicles [10].

1.3 Research questions and aim

The integration of connected and autonomous functionalities in automotive vehicles has transformed automotive manufacturers into software innovators. However, this paradigm shift introduces complexity and knowledge gaps that only a limited number of OEMs are equipped to handle. The findings of a survey conducted by the Ponemon Institute, which involved 593 automotive component security professionals, validate the concerns regarding the lack of expertise in software security within the industry. The survey reveals that over 80% of participants believe that software security struggles to keep pace with technological advancements in the automotive sector, as illustrated in the accompanying chart. This finding assumes significance in light of the increasing prominence of Cyber-Physical Systems, where accessing the required expertise remains a formidable challenge [3].

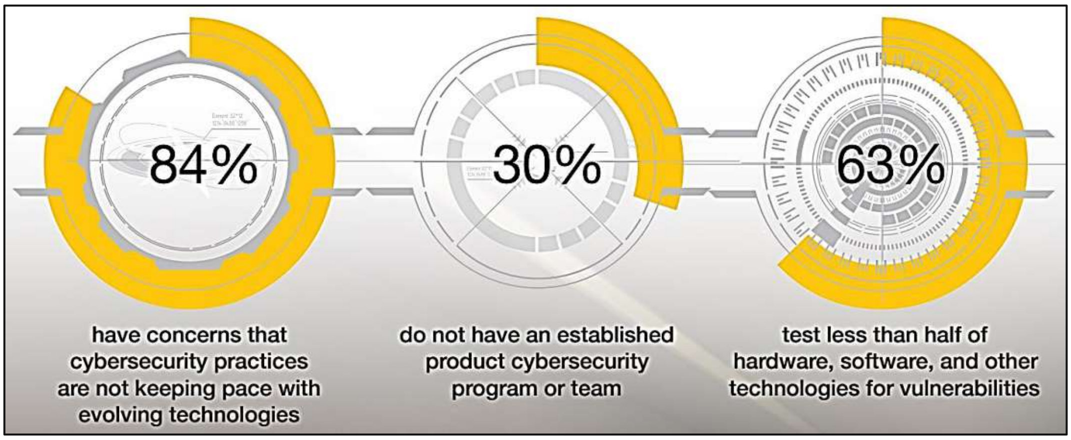


Figure 3 – Survey chart [11]

As the automotive industry experiences a rapid surge in software-implemented functions, reaching approximately 30% [11], it becomes evident that companies and professionals are inadequately equipped to effectively address the associated vulnerabilities. Against this backdrop, this Master's Thesis aims to answer the following questions:

- If the method FMEA is so recognized and extensively used with accuracy, can it be applied to ensure the cybersecurity of technical products?
- How should such a Cybersecurity FMEA be structured?

Despite the existence of standards and norms governing cybersecurity in the automotive industry, there remains a gap that necessitates a more user-friendly and comparable method aligned with established practices. Thus, the objective of this academic endeavour is to propose a pilot method that can effectively support the assessment of cybersecurity in technical products. By bridging this gap, the research aims to enhance the industry's capabilities in addressing cybersecurity risks comprehensively.

1.4 Methodological approach and expected results

The methodological approach of this Master's Thesis is structured into six distinct steps, as illustrated in Figure 4. These steps serve as a roadmap to facilitate the completion of the research. The introduction section provides a comprehensive overview of the current state and challenges of cybersecurity in the automotive industry. It concludes with the research questions outlined in the first chapter, which serve as the guiding objectives of this study.

Chapters 2 and 3 are dedicated to an in-depth exploration of the state-of-the-art literature on cybersecurity in the automotive industry and related works. These chapters lay the foundation for understanding the existing knowledge and research gaps in the field. Additionally, Chapter 3 introduces the framework of FMEA as a relevant reference to guide the author's investigation and findings throughout this thesis.

Chapter 4 forms the core of this Master's Thesis, presenting the author's analysis of a cybersecurity breach and its correlation with the development process. This chapter delves into the intricacies of the breach incident, exploring the underlying causes and factors involved. It provides valuable insights into the vulnerabilities and shortcomings within the development process, contributing to a comprehensive understanding of the cybersecurity landscape in the automotive industry.

Continuing the research journey, Chapter 5 focuses on addressing the remaining research questions. It presents the findings and conclusions derived from the investigation, shedding light on the implications and potential solutions to mitigate cybersecurity risks. This chapter serves as a critical milestone in advancing knowledge and understanding within the field.

Finally, the concluding chapter wraps up the thesis, summarizing the key findings, highlighting their significance, and offering suggestions for future research and development. It provides a comprehensive overview of the contributions made by this study and outlines potential avenues for further exploration and improvement in the realm of automotive cybersecurity. Overall, the methodological approach outlined in this chapter provides a clear roadmap for the execution of this Master's Thesis, ensuring a systematic and rigorous exploration of cybersecurity in the automotive industry.

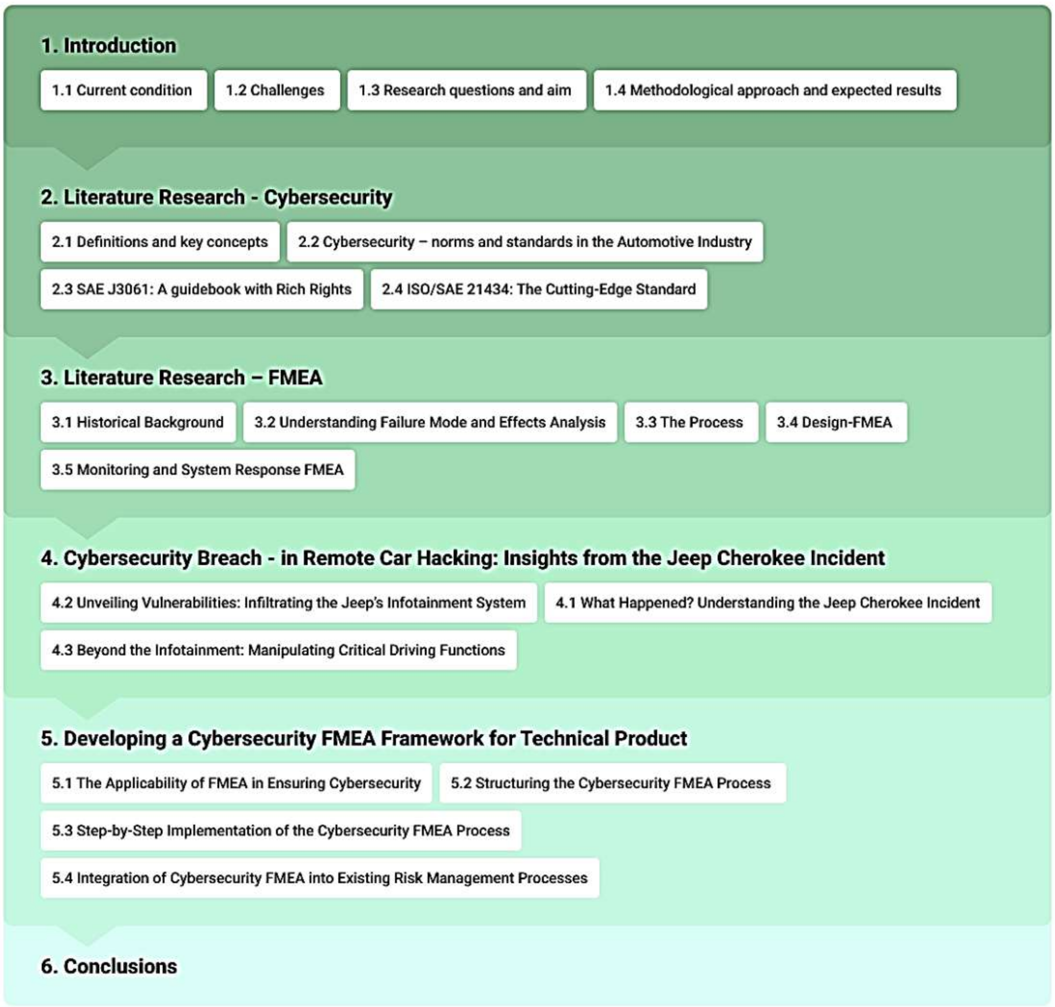

1. Introduction
1.1 Current condition
1.2 Challenges
1.3 Research questions and aim
1.4 Methodological approach and expected results
2. Literature Research - Cybersecurity
2.1 Definitions and key concepts
2.2 Cybersecurity – norms and standards in the Automotive Industry
2.3 SAE J3061: A guidebook with Rich Rights
2.4 ISO/SAE 21434: The Cutting-Edge Standard
3. Literature Research – FMEA
3.1 Historical Background
3.2 Understanding Failure Mode and Effects Analysis
3.3 The Process
3.4 Design-FMEA
3.5 Monitoring and System Response FMEA
4. Cybersecurity Breach - in Remote Car Hacking: Insights from the Jeep Cherokee Incident
4.2 Unveiling Vulnerabilities: Infiltrating the Jeep's Infotainment System
4.1 What Happened? Understanding the Jeep Cherokee Incident
4.3 Beyond the Infotainment: Manipulating Critical Driving Functions
5. Developing a Cybersecurity FMEA Framework for Technical Product
5.1 The Applicability of FMEA in Ensuring Cybersecurity
5.2 Structuring the Cybersecurity FMEA Process
5.3 Step-by-Step Implementation of the Cybersecurity FMEA Process
5.4 Integration of Cybersecurity FMEA into Existing Risk Management Processes
6. Conclusions

Figure 4 – Thesis Structure

2 Literature Research - Cybersecurity

2.1 Definitions and key concepts

The understanding of certain concepts and definitions associated with the topic of cybersecurity in the automotive industry is often intertwined and requires clarification. This chapter serves the purpose of providing a comprehensive description and explanation of these concepts. By delineating and clarifying the key terms and expressions, this chapter aims to establish a solid conceptual framework that will underpin the subsequent analysis and findings of this research.

2.1.1 Cyberattack

"An assault on system Cybersecurity that derives from an intelligent act, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade Cybersecurity services and violate the Cybersecurity policy of a system" [12].

2.1.2 Cybersecurity

A condition is achieved by measures designed to ensure the protection of a cyber-physical system against threat scenarios, unauthorized access, or attack [12,13].

2.1.3 CPS

"The cyber-physical systems are systems that have interactions between computational components and physical systems" [5].

2.1.4 Hacker

"A person who illegally attempts to gain access to or gains access to a system with the intent to gain something or to cause losses from a stakeholder perspective; e.g., fame, financial, terrorist attack" [12].

2.1.5 Hacker chatter

"On-line blogs or conventions, etc. where hackers hold conversations about what they try to do" [12].

2.1.6 Hazard

“Potential source of harm” [14].

2.1.7 Item

“Component or set of components that implements a function at the vehicle level” [13].

2.1.8 PII – Personally Identifiable Information

“It is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context” [12].

2.1.9 Safety x Security

In the context of the automotive industry, it is essential to clearly comprehend the difference between safety and security. While these terms may seem synonymous to some individuals due to their overlapping characteristics [15], it is crucial to establish a precise delineation. Some perceive security as a physical aspect, while safety evokes a sense of being free from harm or danger.

However, when addressing cybersecurity and related topics within the industry, it becomes imperative to recognize the distinction between safety and security. Both safety and security rely on the integrity of data [15]. Consequently, two distinct types of cyberattacks can be identified: safety-related attacks that jeopardize human lives, and non-safety-related attacks that primarily affect users' privacy [16].

Although the meanings of these two terms may vary, it is vital to undertake a comparative evaluation of their similarities and objectives during the product development process. Notably, the cybersecurity lifecycle proposed by SAE J3061 draws significant influence from ISO 26262, a standard predominantly focused on safety. This convergence suggests that technical solutions are increasingly aligning their processes in a similar direction. In fact, there is a possibility that both safety and security considerations may be incorporated into the design and development phases in the near future, as illustrated in Figure 5 [17].

2.1.10 Safety-critical systems

“A system that may cause harm to life, property, or the environment if the system does not behave as intended or desired” [12].

2.1.11 Threats

“A circumstance or event with the potential to cause harm, where harm may be with respect to financial, reputation, privacy, safety, or operational” [12].

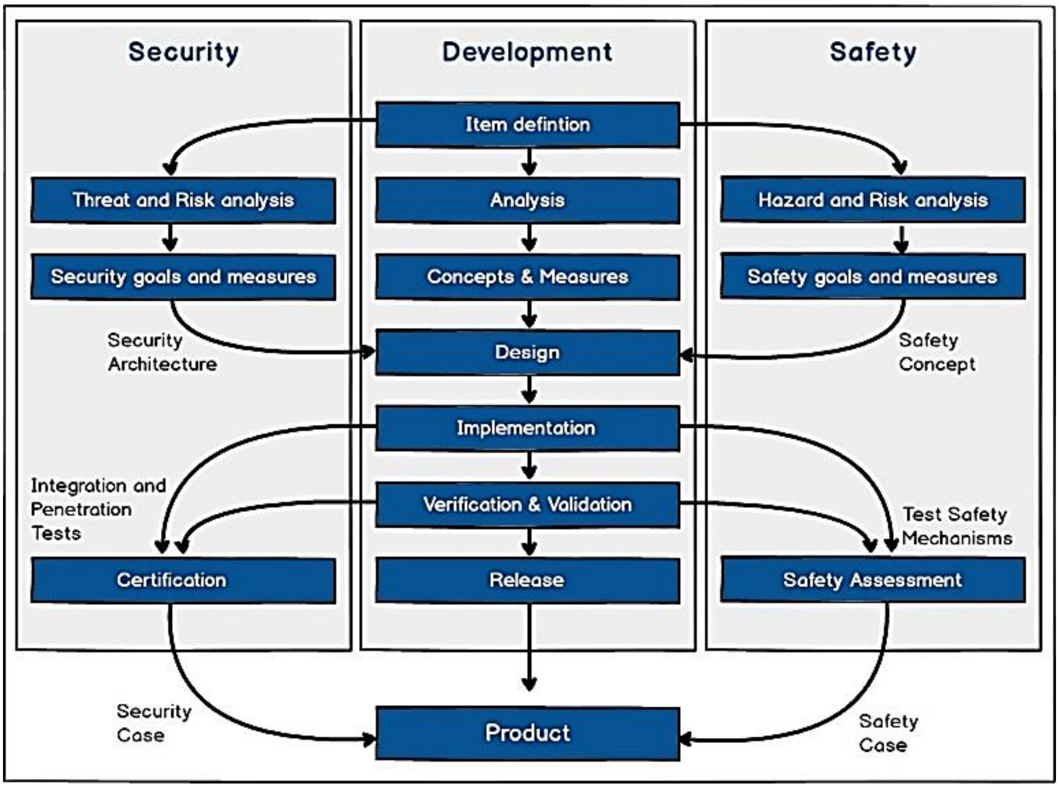


Figure 5 - Comparison of the abstract development process of safety and security [15]

2.1.12 Trigger

“Criterion for triage (analysis to determine the relevance of cybersecurity information to an item or component)” [13].

2.1.13 Vulnerability

“Weakness that can be exploited as part of an attack path” [13].

2.1.14 Weakness

“Defect or characteristic that can lead to undesirable behaviour” [13].

2.2 Cybersecurity – norms and standards in the Automotive Industry

2.2.1 Evolution and Updates

The automotive industry operates within a framework of various norms and standards aimed at enhancing the quality, consistency, and reliability of its products. As original equipment manufacturers continue to innovate and evolve, it becomes imperative for current standards to be periodically updated, while new ones are introduced to address emerging challenges and technological advancements.

2.2.2 Influence on Cybersecurity

In the realm of cybersecurity within the automotive industry, numerous norms have a significant impact on shaping the landscape and ensuring the optimal implementation of new vehicle features. Notably, several standards hold relevance in this context. These include:

1. ISO/SAE 21434 - Road Vehicles - Cybersecurity Engineering: This standard provides guidelines and requirements for integrating cybersecurity into the engineering processes of road vehicles. It offers a comprehensive framework to address cybersecurity risks throughout the vehicle's lifecycle.

2. SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems: This guidebook focuses on cybersecurity practices specific to cyber-physical vehicle systems. It offers valuable insights and recommendations for developing and implementing effective cybersecurity strategies.

3. ISO 26262 - Road Vehicles - Functional Safety: While primarily focusing on functional safety, ISO 26262 indirectly influences cybersecurity in the automotive industry. It provides a systematic approach for managing safety-related risks

throughout the development process, which can serve as a foundation for addressing cybersecurity concerns.

Additionally, there are other relevant quality norms, such as IATF 16949, which outline requirements for quality management systems in the automotive industry. Although not specific to cybersecurity, these norms contribute to ensuring the overall integrity and reliability of automotive products. The interplay of these norms and standards plays a crucial role in shaping cybersecurity practices in the automotive industry. They provide a framework and guidelines for OEMs to address cybersecurity challenges effectively and foster a secure environment for the integration of advanced vehicle features.

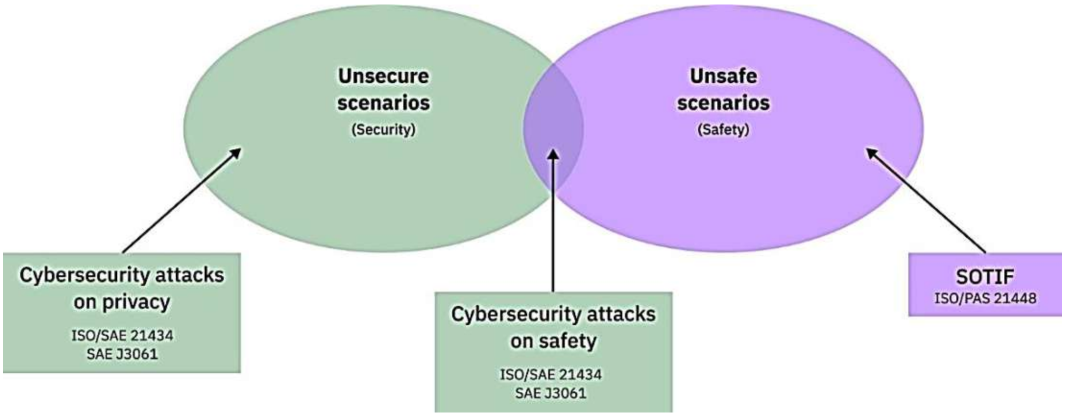


Figure 6 – Intersection between norms in Automotive regarding Safety and Security – adapted from “Engineering a Safer World” [16]

ISO 21434 stands as a cutting-edge standard in addressing cybersecurity in the automotive industry. In contrast, SAE J3061, though older, serves as a valuable guidebook offering insights on the practical application of the former. In the subsequent sections, a thorough analysis of these two specifications will be presented to shed light on their significance and implications. In the subsequent sections of this thesis, we will explore deeper into these two significant specifications. A comprehensive analysis of ISO 21434 will showcase its advanced approach to cybersecurity engineering in the automotive domain. Simultaneously, an in-depth examination of SAE J3061 will highlight its role as a valuable companion to ISO 21434, offering supplementary guidance and practical applications. By exploring these standards, we aim to gain a comprehensive understanding of the current state-of-the-art cybersecurity practices in the automotive industry.

2.3 SAE J3061: A guidebook with Rich Rights

While SAE J3061 predates ISO 21434, it remains a valuable resource in the field of automotive cybersecurity. Functioning as a guidebook, it offers crucial information on how to implement the principles outlined in ISO 21434. This guidebook provides industry professionals with practical insights, best practices, and recommendations for developing and implementing effective cybersecurity strategies within cyber-physical vehicle systems.

As a response to a significant gap in the automotive industry, the creation of SAE J3061 emerged, addressing an area that was previously deemed irrelevant [9]. This comprehensive guidebook on cybersecurity provides valuable insights and techniques specifically tailored for the automotive industry and its processes. Its primary objective is to ensure the safety and security of activities involved in the development of new vehicles within the context of Cyber-Physical Systems.

By establishing this set of guidelines, organizations operating in the automotive sector can navigate through uncharted territory with clear instructions. The guidelines serve to define a life-cycle implementation framework for cybersecurity, drawing inspiration from the V-model and heavily influenced by ISO 26262 [2,9]. This tailored framework ensures that cybersecurity considerations are integrated throughout the entire automotive development process, providing a robust foundation for safeguarding the integrity and security of vehicles.

Within SAE J3061, a range of guidelines encompass valuable information on existing tools, methods, and best practices for implementing cybersecurity measures. These guidelines serve as a solid foundation for further development activities in the field, addressing the complexities and challenges associated with cybersecurity. SAE J3061 offers a structured approach that integrates system safety and cybersecurity within the context of CPS. It encompasses guiding principles for

CPS and provides an overview of the cybersecurity process, management, implementation, as well as insights into relevant tools and methods.

The guidelines also highlight the importance of conducting an initial assessment to determine the need for a cybersecurity process. This assessment aids in evaluating potential threats, estimating risks, and determining the feasibility of implementing a cybersecurity approach. While the assessment can be conducted at various levels of detail, the results can be derived from sources such as conference discussions, hacker chatter, past experiences, and another relevant knowledge. By following the actions outlined in SAE J3061, organizations can streamline the cybersecurity process and effectively address the complexities associated with safeguarding automotive systems.

Regarding the incorporation of safety-related vehicle features, an additional initial assessment can be conducted to evaluate the potential presence of high-risk safety-related threats. As specified in section 1.2 of J3061, it is essential for cybersecurity experts and safety experts to maintain continuous contact and exchange information. This collaborative effort ensures the comprehensive identification and acknowledgment of all potential safety-related threats, irrespective of their anticipated Automotive Safety Integrity Level.

Chapter 2 of this thesis serves the purpose of presenting the references applied in the implementation of J3061. Moreover, these chapters include the provision of comprehensive definitions for terms and acronyms assigned to facilitate a thorough understanding of the subject matter.

2.3.1 System safety vs. System cybersecurity

Chapter 4 discusses the intricate relationship between system safety and system cybersecurity, elucidating the definitions attributed to each domain. In accordance with the guideline, the following definitions are in use [12]:

- System safety - the state of a system that does not cause harm to life, property, or the environment.
- System cybersecurity - the state of a system that does not allow exploitation of vulnerabilities to lead to losses of any kind.

A comprehensive analysis of the provided definitions, explanations, and illustrative examples reveals a significant observation cyberattacks targeting a safety-critical system possess the potential to result in safety-related losses. Conversely, the inverse relationship does not hold true, as cyberattacks directed towards a cybersecurity-critical system may not necessarily jeopardize human life. Instead, such attacks often lead to losses of financial nature or breaches of privacy.

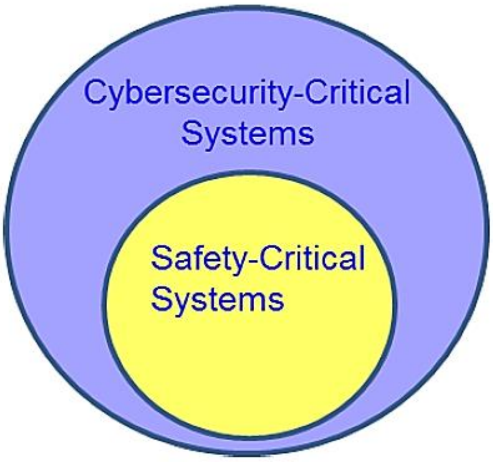


Figure 7 - Cybersecurity-critical x Safety-critical systems according to SAE J3061

Furthermore, it is noteworthy that system safety and system cybersecurity encompass distinct perspectives, despite the potential convergence in the identification of their respective outputs. Notably, each domain employs its unique set of tools for hazard and threat identification, namely Hazard Analysis and Risk Assessment (HARA) and Threat Analysis and Risk Assessment (TARA). While the overall roadmap for both methods may exhibit a similar structure, the TARA process necessitates speculation on the mindset and actions of potential attackers to formulate an appropriate response. In contrast, HARA relies on the analysis of component and system behaviour to ascertain potential risks and hazards.

2.3.2 Guiding Principles and Cybersecurity Process

SAE J3061 provides comprehensive guidance for the adoption of recommended practices across all departments within a vehicle company. Chapter 5 of the guide highlights the significance of integrating the principles and processes outlined in the document throughout the organization. It further elucidates that the guide leverages the best practices from Microsoft's Security Development Lifecycle (SDL) and IEEE's Avoiding the Top 10 Software Security Design Flaws, thereby tailoring the instructions to ensure their applicability and effectiveness [12].

Emphasizing the significance of system cybersecurity, this thesis highlights the need to comprehend vulnerabilities and integrate key principles throughout the entire product lifecycle, from concept and design to development and validation. Notably, SAE J3061 extends its scope beyond the traditional project development lifecycle, encompassing crucial aspects such as the incident response process, over-the-air (OTA) updates, and cybersecurity considerations related to PII when ownership of the vehicle changes [17].

Immediately following, the Cybersecurity Process Overview emphasizes the significance of integrating the cybersecurity process throughout the entire product development path, rather than treating it as an isolated step at the end of development. The authors refer to this approach as WDWS, which stands for a well-defined and well-structured system. By adopting this approach, the procedure becomes less susceptible to incorrect, incomplete, or inconsistent cybersecurity controls, thereby minimizing the introduction of unknown vulnerabilities into the system. The ISO 26262 process scheme serves as a valuable framework for establishing a strategy that facilitates and supports the implementation of the cybersecurity process. As a result, companies with a well-established functional safety working process have a competitive advantage when implementing the concepts outlined in the guideline for the first time.

Figure 8, derived from SAE J3061, offers a comprehensive representation of potential activities and checkpoints for product development, highlighting the central role of cybersecurity management and activities within the V-model framework. As the guideline progresses, several appendices are presented, encompassing various resources and references. These include examples of analysis, techniques for cybersecurity analysis, templates for work products, databases containing information on vulnerabilities and potential classification schemes, as well as test tools that can be valuable to the automotive industry.

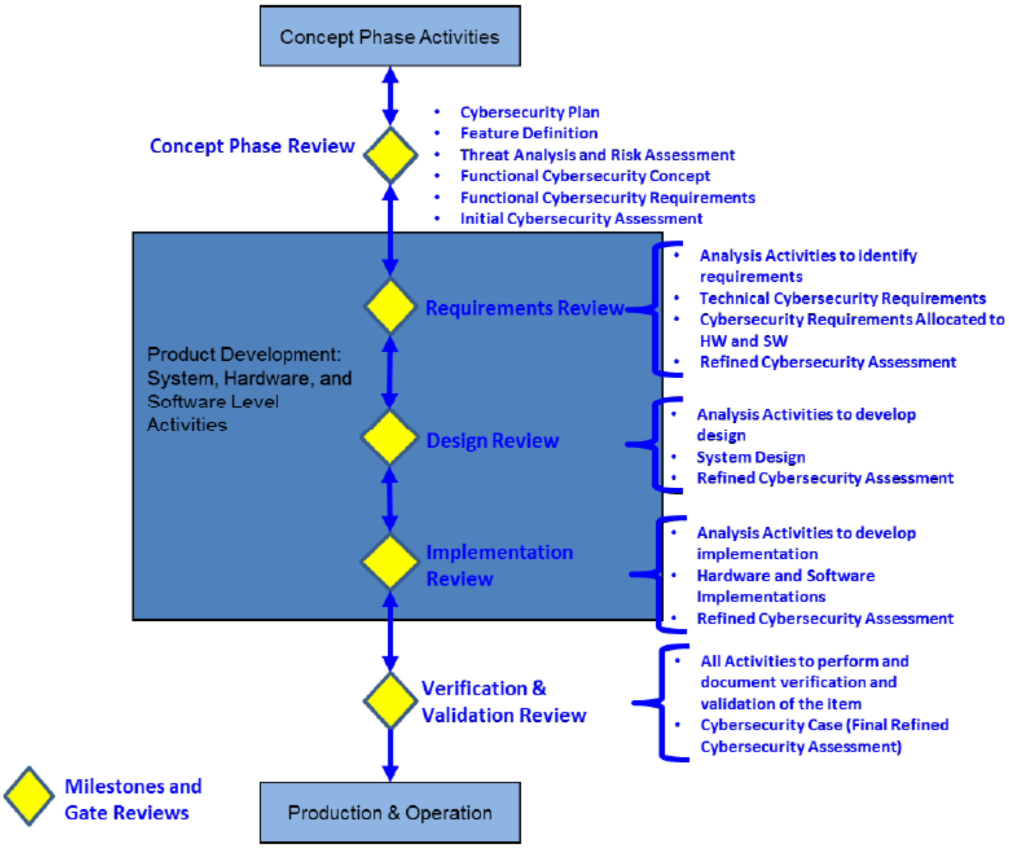

Concept Phase Activities
Concept Phase Review
Cybersecurity Plan
Feature Definition
Threat Analysis and Risk Assessment
Functional Cybersecurity Concept
Functional Cybersecurity Requirements
Initial Cybersecurity Assessment
Product Development: System, Hardware, and Software Level Activities
Requirements Review
Analysis Activities to identify requirements
Technical Cybersecurity Requirements
Cybersecurity Requirements Allocated to HW and SW
Refined Cybersecurity Assessment
Design Review
Analysis Activities to develop design
System Design
Refined Cybersecurity Assessment
Implementation Review
Analysis Activities to develop implementation
Hardware and Software Implementations
Refined Cybersecurity Assessment
Verification & Validation Review
All Activities to perform and document verification and validation of the item
Cybersecurity Case (Final Refined Cybersecurity Assessment)
Milestones and Gate Reviews
Production & Operation

Figure 8 - Overview of possible activities and gates [12]

2.4 ISO/SAE 21434: The Cutting-Edge Standard

ISO 21434 stands at the forefront of cybersecurity standards when discussing the automotive industry. As a comprehensive and up-to-date specification, it sets the benchmark for integrating cybersecurity measures into the engineering processes of road vehicles. This standard addresses the evolving cyber threats and provides essential guidelines and requirements to ensure the robustness and resilience of automotive cybersecurity systems.

Belatedly in August 2021, the state-of-the-art ISO/SAE 21434 - Road Vehicles - Cybersecurity Engineering was introduced. This groundbreaking standard aims to facilitate the engineering of E/E systems, enabling them to adapt to advanced technologies and evolving methods of cyber-attacks. The document is thoughtfully organized, encompassing various areas as depicted in Figure 9. Furthermore, the standard provides helpful annexes that summarize cybersecurity activities and work products, offering additional guidance and support to implement effective cybersecurity measures.

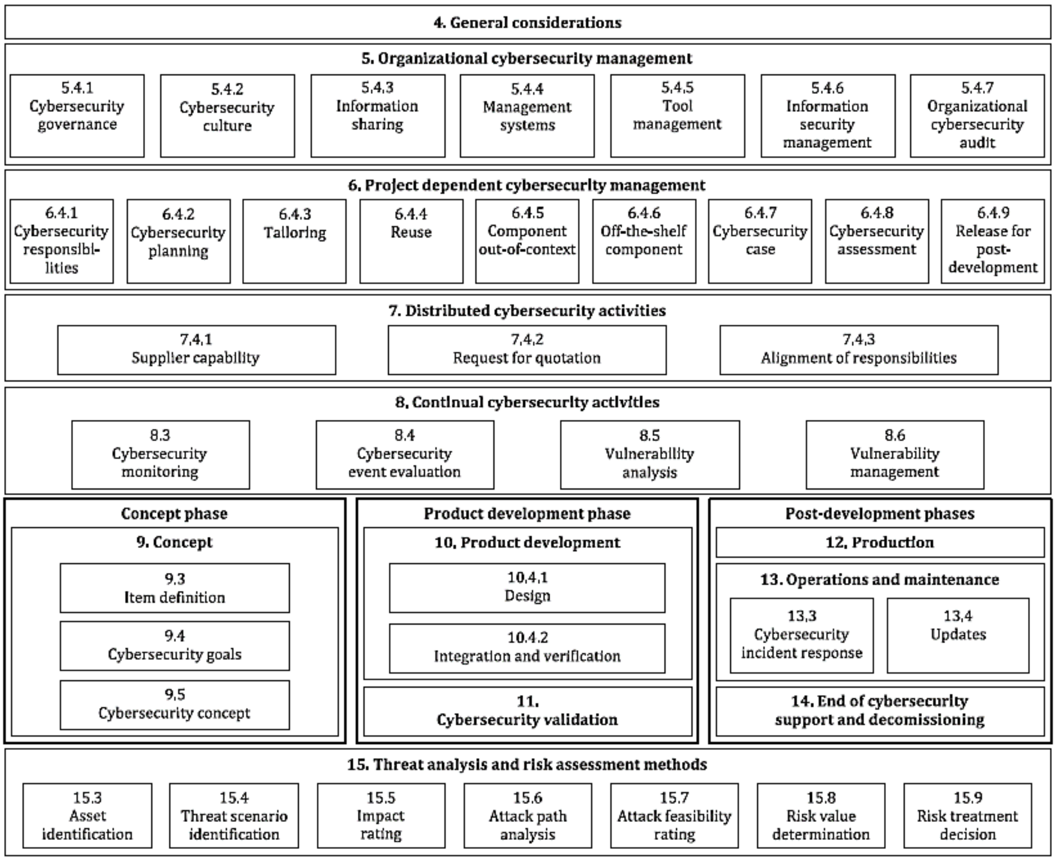

4. General considerations
5. Organizational cybersecurity management
5.4.1 Cybersecurity governance
5.4.2 Cybersecurity culture
5.4.3 Information sharing
5.4.4 Management systems
5.4.5 Tool management
5.4.6 Information security management
5.4.7 Organizational cybersecurity audit
6. Project dependent cybersecurity management
6.4.1 Cybersecurity responsibi-lities
6.4.2 Cybersecurity planning
6.4.3 Tailoring
6.4.4 Reuse
6.4.5 Component out-of-context
6.4.6 Off-the-shelf component
6.4.7 Cybersecurity case
6.4.8 Cybersecurity assessment
6.4.9 Release for post-development
7. Distributed cybersecurity activities
7.4.1 Supplier capability
7.4.2 Request for quotation
7.4.3 Alignment of responsibilities
8. Continual cybersecurity activities
8.3 Cybersecurity monitoring
8.4 Cybersecurity event evaluation
8.5 Vulnerability analysis
8.6 Vulnerability management
Concept phase
9. Concept
9.3 Item definition
9.4 Cybersecurity goals
9.5 Cybersecurity concept
Product development phase
10. Product development
10.4.1 Design
10.4.2 Integration and verification
11. Cybersecurity validation
Post-development phases
12. Production
13. Operations and maintenance
13.3 Cybersecurity incident response
13.4 Updates
14. End of cybersecurity support and decomissioning
15. Threat analysis and risk assessment methods
15.3 Asset identification
15.4 Threat scenario identification
15.5 Impact rating
15.6 Attack path analysis
15.7 Attack feasibility rating
15.8 Risk value determination
15.9 Risk treatment decision

Figure 9 - Structure of SAE/ISO 21434 [13]

The literature review primarily focuses on specific chapters within the ISO/SAE 21434 standard that pertain to ongoing risk assessments and vulnerability management of E/E systems. Chapter 9 specifically delves into the concept phase and explores various activities related to identifying cybersecurity risks, establishing cybersecurity goals, and defining cybersecurity requirements for E/E system components.

While the detailed discussions of these chapters will be presented in subsequent sections, it is important to provide a brief overview of the entire document. ISO/SAE 21434 is a comprehensive standard that addresses the need for robust cybersecurity engineering in the road vehicle industry. It provides guidance and requirements for effectively managing cybersecurity risks throughout the entire product development lifecycle. The standard covers various aspects such as risk assessment, threat analysis, vulnerability management, and security requirements specification. By following the guidelines outlined in ISO/SAE 21434, automotive manufacturers and stakeholders can enhance the security of their E/E systems, adapt to emerging cybersecurity threats, and ensure the safety and reliability of their vehicles. The standard emphasizes the importance of integrating cybersecurity practices early in the development process and maintaining a proactive approach to address potential vulnerabilities.

This literature review will delve deeper into the relevant chapters of ISO/SAE 21434 to provide a comprehensive understanding of the activities and concepts associated with ongoing risk assessments and vulnerability management in E/E systems.

2.4.1 Considerations and Organizational Cybersecurity Management

In the sphere of cybersecurity engineering, it is crucial to comprehend the fundamental aspects of individual items. For original equipment manufacturers, where collaborative models between suppliers and manufacturers can vary, cybersecurity risk management extends throughout the entire supply chain. Activities undertaken throughout a project may differ for each organization involved, necessitating tailored cybersecurity activities to adapt to specific requirements.

During analysis activities, potential malicious actions and the resulting damage that could impact the cybersecurity of a road vehicle's electrical/electronic systems can be identified. To address the challenge of identifying and managing weaknesses and vulnerabilities in these systems, cybersecurity monitoring, remediation, and incident response measures are employed.

Chapter 5 of the standard emphasizes the activities and objectives of Organizational Cybersecurity Management. In order to establish and implement effective cybersecurity management systems, companies must have an applied quality management system and utilize appropriate tools to facilitate the process. The primary objectives include defining a cybersecurity policy, assigning responsibilities for cybersecurity activities, managing cybersecurity risks, and fostering a cybersecurity culture that promotes awareness and continuous improvement. The organization should also conduct regular cybersecurity audits to ensure that tools and practices do not compromise cybersecurity. The following diagram illustrates the recommended framework for cybersecurity governance as outlined in the standard.

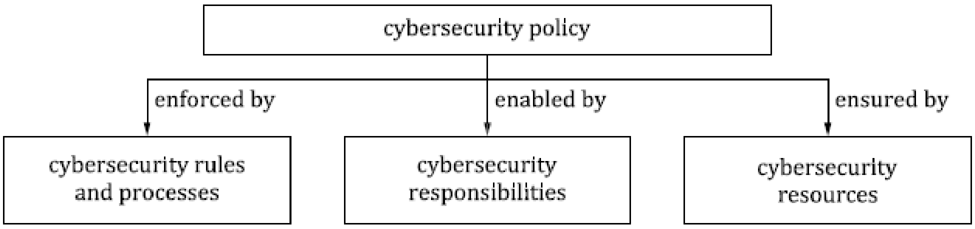


Figure 10 - Cybersecurity governance according ISO21434 [13]

This chapter sheds light on the essential considerations and organizational practices related to cybersecurity management. By adhering to these principles and implementing robust cybersecurity measures, organizations can enhance their overall cybersecurity posture and effectively mitigate risks throughout their operations.

2.4.2 Project-dependent and ongoing activities

Due to the diverse range of available items and components, it is often necessary to define requirements in a more generic manner. Section 6 of the standard outlines how responsibilities are allocated, cybersecurity activities are planned, and tailored approaches are implemented based on this consideration. Common scenarios that require tailoring include reusing components, dealing with components out of context, and managing updates.

Within the ISO framework, a cybersecurity case serves as an input for a cybersecurity assessment. However, it is important to note that not all circumstances warrant a cybersecurity assessment, and there may be specific cases where it is deemed unnecessary post-development. Incorporating cybersecurity into the entire life cycle of a product, whether it is a component or a system, requires a range of ongoing activities. These activities include:

1. Cybersecurity Monitoring: This involves collecting cybersecurity information and conducting analyses to identify potential cybersecurity events. Through defined triggers and thresholds, cybersecurity events are triaged to determine their significance and potential impact.

2. Events Evaluation: The evaluation process aims to determine whether a cybersecurity event poses a weakness to the item or component. It involves assessing the nature of the event, its potential consequences, and the likelihood of exploitation.

3. Vulnerability Analysis: Vulnerability analysis focuses on identifying vulnerabilities derived from weaknesses that could be exploited by potential attackers. This involves examining the system's design, implementation, and configurations to identify potential security flaws and weaknesses.

4. Vulnerabilities Management: Once vulnerabilities are identified, it is crucial to track and oversee their treatment in the affected items. This involves managing a comprehensive process for addressing and mitigating vulnerabilities, such as applying patches, implementing security updates, or utilizing other remediation measures.

Throughout the development of this thesis, more specific details will be provided regarding these activities based on the relevant norms and their application. These activities are critical for ensuring a proactive and comprehensive approach to cybersecurity, mitigating potential risks and ensuring the security of the product throughout its life cycle.

3 Literature Research – FMEA

3.1 Historical Background

Continuing our exploration, we have come across a widely employed approach in the industry. It is indisputable that Failure Mode and Effects Analysis (FMEA) holds great familiarity and has a rich historical background dating back to the 1940s, FMEA has established itself as an indispensable tool. Originally developed by the USA Military to assess equipment and system reliability, FMEA quickly found applications in notable endeavors like NASA's Apollo project, cementing its status as an indispensable tool across various domains.

The spotlight on FMEA intensified when a series of incidents involving Ford Pintos exposed the vulnerability of their gas tanks to explosions in rear-end accidents. In response, Ford made a strategic decision in 1977 to implement FMEA as part of their product development and safety approach [18,19]. This pivotal event marked a defining moment in the automotive industry, propelling the widespread adoption of FMEA and highlighting its critical role in enhancing product safety and risk mitigation.

Ford's influence extended beyond the automotive industry. In 1994, the collaborative effort of Ford, Chrysler, and General Motors resulted in the release of the first FMEA manual, known as QS-9000 at the time. Based on DIN EN ISO 9001:1994-2008, this manual standardized FMEA implementation. The German Association of the Automotive Industry (VDA) further promoted FMEA adoption, ensuring a uniform approach across various technological fields.

The impact of Ford's adoption of FMEA reached far and wide, influencing companies beyond the automotive sector and fostering a culture of continuous improvement and proactive risk management. Aerospace, manufacturing, electronics, and other industries embraced FMEA as they witnessed the tangible benefits derived from its implementation. Lessons learned from Ford's experience shaped industry best practices, established standards, and influenced regulations, all emphasizing the pivotal role of FMEA in enhancing product reliability and safety.

The widespread adoption of FMEA in diverse industries underscores its effectiveness and the enduring significance of Ford's contribution. This methodology has transcended its automotive origins, finding applications in areas beyond technology. As the service sector's definition of "quality" expands, FMEA has been successfully applied to non-technology-related fields, enhancing its versatility and relevance[19].

In the domain of cybersecurity, the Human FMEA approach provides valuable insights by considering human behavior [19], particularly in addressing varied perceptions of threats. By embracing this method and incorporating human factors, organizations can better understand and mitigate potential risks in the multi-layered nature of cybersecurity. This is particularly crucial as studies have shown that individuals with anxiety may struggle to accurately identify cybersecurity threats, highlighting the importance of human factors in threat assessment [20].

In the subsequent sections of this thesis, we will delve into the details of the FMEA methodology. We will explore its principles, processes, and applications. By understanding the historical context and industry-wide adoption of FMEA, we can gain a comprehensive understanding of its significance and its relevance to the field of product development and risk management.

3.2 Understanding Failure Mode and Effects Analysis

This section aims to perform a comprehensively exploration of Failure Mode and Effects Analysis as a fundamental concept within the automotive industry. FMEA is widely recognized as a crucial tool for analysing and mitigating risks associated with various processes and systems. It enhances operational efficiency, product quality, and overall performance. By studying the underlying principles and techniques of FMEA, this research aims to provide valuable insights into identifying the reasons behind items or processes not performing their intended functions and subsequently implementing targeted improvements [21]. In addition to identifying and mitigating failures, FMEA plays a vital role in verifying and improving designs and processes. It supports the identification of shortcomings and design faults, enabling organizations to address them effectively and optimize their systems. By integrating FMEA into the design and development stages, organizations can proactively identify and address potential risks, thereby minimizing the occurrence of failures and enhancing overall reliability.

The comprehensive analysis of FMEA provides organizations in the automotive sector with a strategic approach to optimize their processes, enhance system reliability, and ensure the delivery of high-quality products. Organizations can gain valuable insights that drive continuous improvement and facilitate informed decision-making by systematically examining failure modes, their effects, and the underlying causes. Moreover, the utilization of FMEA as an integral part of the automotive industry ensures compliance with industry standards and regulatory requirements, further reinforcing the significance and relevance of this methodology. This section includes necessary definitions and key concepts to establish a solid foundation for understanding and applying FMEA effectively. By providing a clear understanding of the terminology associated with FMEA, readers can easily navigate this methodology's complexities. This clarity will be especially beneficial for future analyses that implement cybersecurity-friendly procedures as organizations increasingly focus on safeguarding their systems against potential cyber threats.

3.2.1 Definition of Key Concepts in FMEA

Given that FMEA is primarily concerned with failures, discussing, and defining essential concepts related to failure types is imperative. Prior to depth diving into the explanation of FMEA's purpose, goals, and technical aspects, this chapter provides comprehensive definitions of these key concepts, including the various types of failures encountered in the automotive industry. Defining these concepts and failure types lays the groundwork for a comprehensive exploration of FMEA, enabling a deeper understanding of its purpose, goals, and technical nuances. A thorough understanding of these fundamental elements enables organizations and researchers to effectively employ FMEA to identify and mitigate risks, optimize processes, and enhance overall performance within the automotive sector. To begin, let us define the key terms associated with failures and hazards:

- Failure Cause: A failure cause refers to a circumstance or scenario that triggers a failure. It can occur during a product or system's design, production, processing, or use [21]. Understanding the underlying causes of failures is crucial to address and prevent them effectively.
- Failure Effect: The failure effect pertains to the outcome or consequence directly resulting from a failure. It impacts the failed item or its immediate surroundings explicitly [21]. Examining failure effects helps understand the extent and severity of the consequences of failures.
- Failure Mode: Failure mode refers to how a product or process can experience functional failure or lose its intended function or state transition. There are multiple ways in which a product or process can fail, known as failure modes. It is important to note that human failure is also possible, which results from a loss of function due to human action [21,22]. Another perspective on failure mode involves analyzing the performance criteria of a component. Any changes in performance indicate that the component cannot fulfill its assigned function [23]. Understanding failure modes is crucial in identifying potential risks and devising appropriate mitigation strategies.
- Hazardous Situation: A hazardous situation refers to an occurrence where one or more forms of harm are encountered by individuals, property, or the environment. It involves situations that pose risks and can lead to undesirable consequences [21]. Recognizing hazardous situations is vital for implementing preventive measures and ensuring the safety of individuals and the environment.

A stronger foundation has been established by defining and elucidating these key terms, facilitating a comprehensive understanding of FMEA. This interpretation of the concepts is crucial for examining the methodology employed by FMEA and conducting a thorough analysis. The definitions provided serve as building blocks for further exploration and analysis of FMEA in subsequent sections of this thesis. With a solid understanding of these fundamental elements, organizations and researchers can effectively apply FMEA to identify, analyze, and address failures and risks, optimize processes, and enhance overall performance within the automotive sector.

3.2.2 The Purpose and Advantages of FMEA

Applying Failure Mode and Effects Analysis within the automotive industry serves multiple crucial organizational purposes. It is imperative to incorporate FMEA in the development and production planning stages as early as possible to maximize its benefits [24]. The primary objective of FMEA is to mitigate risks and enhance customer satisfaction by proactively anticipating and preventing failures or defects. This is achieved through a systematic process that visualizes product functions, process steps, and their associated failure modes, consequences, and causes, providing a comprehensive overview.

By leveraging the insights gained from the FMEA process, organizations are empowered to develop robust designs, improve reliability, and enhance safety measures by effectively identifying weaknesses in processes or products [24]. These findings also enable the documentation and tracking of risk minimization measures, ensuring appropriate actions are taken to address potential failures. The valuable insights FMEA provides regarding potential failure modes and their impacts play a crucial role in informed decision-making and efficient resource allocation [25].

Both the German Association of the Automotive Industry (VDA) and the Automotive Industry Action Group (AIAG) emphasize the systematic and qualitative nature of FMEA, highlighting key objectives [25]:

- Assessing technical risks of failure associated with the product or process.
- Identifying the causes and consequences of errors.
- Documenting preventive and detection measures.
- Providing recommendations to minimize risks.

Furthermore, FMEA plays a vital role in evaluating the adequacy of planned error avoidance and detection measures. This ensures that organizations can effectively address potential risks and take necessary actions to optimize the effectiveness of their risk mitigation strategies. The historical perspective highlights the significance of early failure detection during product development or launch, as delayed recognition of failures can lead to exponentially more significant negative impacts [26].

FMEA's advantages go beyond risk reduction; it supports organizations in achieving operational excellence, delivering high-quality products, and meeting customer expectations. As organizations implement FMEA, they gain valuable benefits such as the prevention of disturbances during the start of production (SOP), the establishment of a knowledge base, and exoneration in claims for product liability [24,25]. FMEA's comprehensive analysis and proactive approach enables continuous improvement, effective resource allocation, and process optimization within the automotive industry.

3.2.3 FMEA’s limitations

In addition to the numerous benefits and applications of FMEA, it is a requirement to acknowledge and understand the limitations inherent in this methodology. Particularly when considering the focus on cybersecurity within Cyber-Physical Systems, similar challenges arise that require careful consideration. This chapter explores the limitations of FMEA and CPS risk assessments, shedding light on the areas where improvements and alternative approaches are necessary.

One of the key limitations of FMEA and CPS risk assessments is their focus on analyzing single failures. While this approach is valuable for identifying and addressing specific failure modes, it may not fully capture CPS's complex interactions and interdependencies. This limitation can fail to identify potential cascading effects or systemic failures that arise from these interdependencies. To overcome this limitation, it is essential to develop methodologies that account for the intricate relationships and interdependencies among system components. Moreover, the absence of weighting on parameters in FMEA and CPS risk assessments undermines the reliability of the methods when applied to CPS environments. The inability to assign appropriate weights to different parameters limits the accuracy and effectiveness of risk assessment outcomes. Developing approaches incorporating weighting mechanisms can enhance the precision and reliability of risk assessments within CPS [23].

Another significant limitation of FMEA is its heavy reliance on the expertise and knowledge of the analysis team. The accuracy and effectiveness of the analysis heavily depend on the team's ability to identify potential failure modes and assess their severity, occurrence, and detection. The quality of the analysis is directly influenced by the capabilities and experience of the team members, and their individual decisions shape the overall outcome. To mitigate this limitation, organizations should invest in training and knowledge-sharing initiatives to enhance the analysis team's expertise.

Furthermore, the focus on analyzing single failures in FMEA restricts its ability to capture the intricate interactions and dependencies between system components within CPS. This limitation can lead to a failure to identify potential cascading effects or systemic failures arising from these interdependencies. A more comprehensive approach that considers the systemic behavior and interactions of CPS components is required to address this limitation. This could involve the integration of other risk assessment methodologies or developing specialized approaches that account for these complex dependencies.

Lastly, FMEA is primarily qualitative and does not provide quantitative measures. While it enables identifying and prioritizing failure modes based on their potential impact, it does not quantify the exact probability or frequency of their occurrence. This limitation makes it challenging to derive precise, quantifiable actions from the analysis results. Developing quantitative measures and incorporating probabilistic models into the analysis can provide a more comprehensive understanding of the risks associated with CPS.

These combined limitations underscore the need for further research and development of specialized risk assessment approaches that address CPS's unique characteristics and challenges. By acknowledging these limitations and actively working towards their mitigation, organizations can enhance their ability to identify and mitigate risks associated with CPS, ensuring these advanced systems' safe and reliable operation. Future studies should address these limitations and develop comprehensive risk assessment frameworks that integrate qualitative and quantitative approaches to enable effective risk management within CPS environments.

3.3 The Process

A systematic step-by-step process is followed by organizations when conducting FMEA. As per the latest update from the German Association of the Automotive Industry, this process consists of seven distinct steps. Each step plays a crucial role in comprehensively understanding potential problems and guiding subsequent improvement efforts. By following this structured approach, organizations can effectively identify and mitigate risks associated with product design, manufacturing processes, and system operations.

During the FMEA process, the effects of individual failure modes are meticulously determined and evaluated. This evaluation involves analyzing the potential consequences of each failure mode and assessing its severity, occurrence probability, and detection capability. This analysis allows organizations to prioritize their efforts and allocate resources to address the most critical failure modes. Different types of analyses are conducted to address specific aspects of risk management. Two primary variants of FMEA are commonly employed: Design FMEA (DFMEA) and Process FMEA (PFMEA). Each variant focuses on specific aspects of risk management in different stages of the product lifecycle. DFMEA is concerned with identifying potential failure modes related to the product's design or specific features [21]. It ensures that the design meets the required functionality, reliability, and safety standards. On the other hand, PFMEA scrutinizes and mitigates risks inherent in manufacturing and assembly processes. It identifies failure modes impacting product quality, production efficiency, and worker safety.

In addition to DFMEA and PFMEA, another variant has emerged as a significant focus area within the field of FMEA. This variant is known as FMEA-MSRs (System FMEA). System FMEA encompasses a broader examination of failures within a complex system. It goes beyond individual components or processes and considers the overall system and interdependencies. This expanded scope is crucial in maintaining operational integrity and safety during normal operating conditions [27]. System FMEA involves the examination of concept failures, detailed analysis of potential failures, and the consequential impact on the overall system.

The inclusion of System FMEA reflects the evolving landscape of FMEA, which has adapted to new technologies and the recognition of the need to address risks at the system level. As automotive systems become increasingly complex and interconnected, assessing and managing risks holistically is vital. By adopting System FMEA, organizations can proactively identify and mitigate potential failures and their cascading effects throughout the system.

The comprehensive scope of FMEA, encompassing DFMEA, PFMEA, and System FMEA, ensures that organizations have a robust framework to address risks across the product lifecycle. By employing these different variants of FMEA, organizations can optimize product design, improve manufacturing processes, and enhance their systems' overall safety and reliability. The continued evolution and adoption of FMEA methodologies reflect its adaptability to new technologies and its ongoing relevance in mitigating risks within the automotive industry.

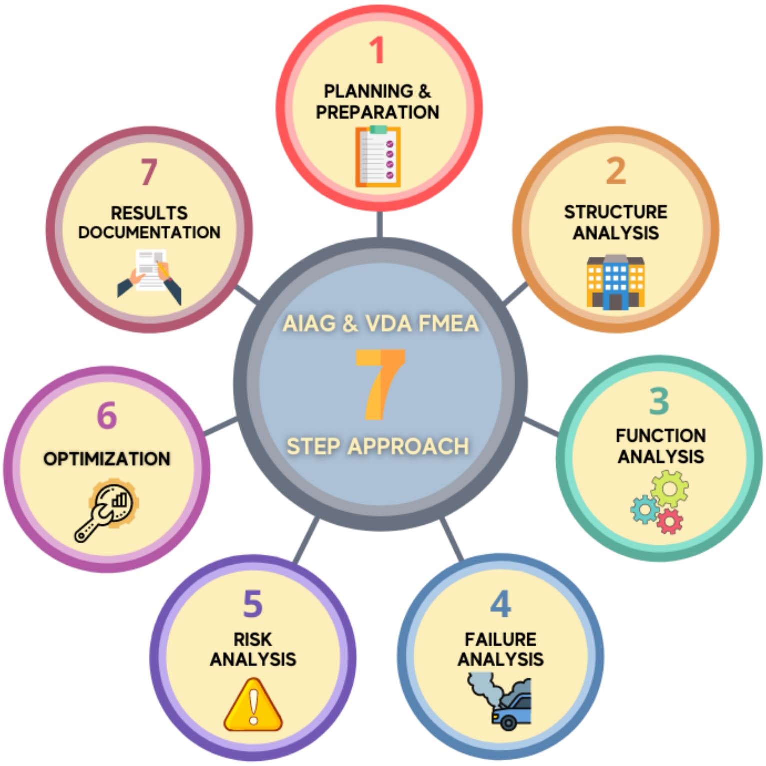


Figure 11 - 7 steps from FMEA according to AIAG&VDA [28]

Within the literature, there is a notion that the FMEA approach can be divided into three distinct phases: planning, performing, and recording. However, it is important to note that this division differs from the framework proposed by the VDA. System analysis, failure and risk analysis, and communication are the three areas into which the VDA framework divides the FMEA process (see Figure 12).

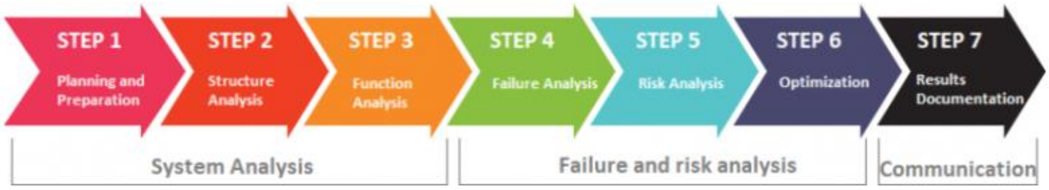


Figure 12 - Steps with area divisions [28]

These zones provide a structured approach for conducting FMEA and ensure comprehensive coverage of the necessary steps and activities involved in the analysis. In the following sections, the focus will be on two types of FMEA: Design and System, both will be thoroughly discussed, exploring their methodologies, applications, and benefits. In the following sections, we will go into great detail about each form of FMEA and the planning stage.

3.3.1 FMEA Planning: Establishing a Solid Foundation

The Planning Phase of FMEA holds excellent significance and plays an equally essential role in both Design FMEA and System FMEA, especially when addressing cybersecurity aspects. During this phase, thoroughly examining the technical requirements associated with the product and method/process is imperative. It is necessary to gather comprehensive, accurate, and quantitative information pertaining to these standards [24]. In addition to technical prerequisites, other factors highlighted by Beverly White and The Practitioners Guide (as shown in the image below) contribute to the effectiveness and comprehensiveness of the FMEA. These factors, depicted in the accompanying image, provide valuable insights for incorporating into the planning phase. By considering these factors, organizations can enhance the risk assessment and mitigation process, particularly within cybersecurity.

Figure 13 - Five T’s to FMEA preparation [29]

To mitigate the risk of "scope creep" and ensure the delivery of a high-quality outcome, incorporating the Five T's [29], as depicted in the accompanying image, proves invaluable in guiding the necessary considerations.

1. Scope (inTent): Clearly defining the boundaries of the FMEA analysis is crucial. It involves identifying what is included and what falls outside its scope. Organizations can focus on the most critical aspects by establishing a well-defined scope and avoiding unnecessary diversions.

2. Timing: A thorough understanding of the FMEA timelines and milestones is essential. It is important to align them with the overall product/process development cycle to ensure seamless integration and timely completion. By synchronizing the FMEA activities with the broader project timeline, organizations can effectively allocate resources and ensure that the analysis is conducted at the appropriate stages.

3. Team: Assessing the availability of a competent and adequately resourced team is crucial for the successful execution of FMEA. The team should possess the necessary expertise and experience to conduct the analysis effectively. By ensuring a capable team, organizations can enhance the quality and reliability of the risk assessment outcomes.

4. Tasks: Identifying the tasks and responsibilities assigned to the team members ensures clarity and accountability throughout the FMEA process. By clearly defining the roles and responsibilities, organizations can streamline the workflow, avoid duplication of efforts, and facilitate effective collaboration among team members.

5. Tools: Determining the necessary tools, such as specialized software, required to conduct and complete the FMEA effectively is essential. These tools enhance the

efficiency and accuracy of the analysis by providing automated calculations, documentation capabilities, and data management features. By utilizing the appropriate tools, organizations can streamline the FMEA process and improve the overall effectiveness of their risk assessments.

Organizations can establish a solid foundation for their FMEA endeavors by addressing these Five T's. Minimizing scope uncertainties, managing timelines effectively, allocating appropriate resources, clarifying tasks, and utilizing the necessary tools contribute to achieving comprehensive and reliable risk assessments.

3.4 Design-FMEA

One of the earliest designations for the modified version of Failure Mode and Effects Analysis can be traced back to the VDA of 1986, referred to as Design-FMEA or DFMEA for short. Alternatively, it is also known as Product FMEA, as its primary focus lies in the design phase of a product. DFMEA is an analytical technique that proactively identifies and addresses potential failure modes and their corresponding causes or mechanisms before the product is released for production (SOP). In conducting a DFMEA, a comprehensive evaluation should encompass all end items, including related systems, subsystems, and components [25,30]. Depending on the scope, the analysis may encompass both hardware and software components. Keeping this comprehensive overview in mind during the planning phase of the DFMEA is binding to ensure consistency, agreement, and a clear focus on the analysis objectives.

3.4.1 Performing a DFMEA and its specifics characteristics

In the context of conducting a Design-Failure Mode and Effects Analysis, the team must align their efforts with the fundamental objectives of identifying and analyzing potential failures associated with product malfunctions, shortened product life, and safety hazards during product usage [31]. It is advantageous to have essential documents such as blueprints, offer drawings, prototypes, bills of materials (BOM), and schematics to facilitate a more efficient and streamlined process before initiating the DFMEA. These documents serve as valuable resources that contribute to better preparation and facilitate a smoother flow in subsequent analysis steps.

In achieving a successful implementation, emphasizing a preventive rather than a reactive approach is essential. Key to this success is executing the project within a tight timeline. When scheduling the DFMEA, the team should consider specific criteria that have been shown to yield better results, as cited by VDA. These criteria include novelty/level of innovation, history of quality/reliability, complexity, the safety of people and systems, cyber-physical systems (including cyber-security), compliance with legal and regulatory requirements, and the availability of catalog and standard parts [25]. By considering these factors, the team can enhance the effectiveness of the DFMEA process and increase the likelihood of identifying and mitigating potential failures.

System DFMEAs play a crucial role in comprehensively assessing the various attributes and interactions within complex systems. These DFMEAs involve the analysis of subsystems and components, which collectively contribute to the functioning of the overall system. Depending on the perspective or responsibility, the definitions and boundaries of system DFMEAs may vary. Typically, these DFMEAs focus on systems that provide functions at the vehicle level, such as the vehicle itself, the drivetrain system, or the brake system, among others. To facilitate analysis, these functions are further broken down into subsystems and components.

In the context of system DFMEAs, it is important to consider the interfaces and interactions that occur not only between different systems and subsystems but also with the environment and customers. These customers can range from suppliers (Tier N), original equipment manufacturers (OEMs), to end-users [25]. By incorporating this broader perspective, system DFMEAs enable a comprehensive evaluation of the interdependencies and potential risks that arise from these interfaces and interactions.

3.4.2 Structural Analysis – step 2

In the structural analysis phase, the primary objective is to systematically identify and break down the scope of the FMEA into its constituent elements, including systems, subsystems, components, and individual pieces. This breakdown is essential for conducting a comprehensive engineering risk analysis. Depending on the specific scope being considered, the structural analysis encompasses both hardware and software elements, reflecting the diverse nature of modern systems [25].

The structural analysis step aims to provide a clear and thorough understanding of the product or process being analyzed. It establishes the boundaries of the system under evaluation and identifies the interfaces between its various components. This depiction of the system's structure is visualized using a structure tree, which showcases the overall system and its hierarchical elements. The main focus and critical areas, where failure effects will be examined, are typically represented at the first level of the structure tree, situated on the far left. As the analysis proceeds, the level of detail can extend to encompass even the design specifics of individual parts [24].

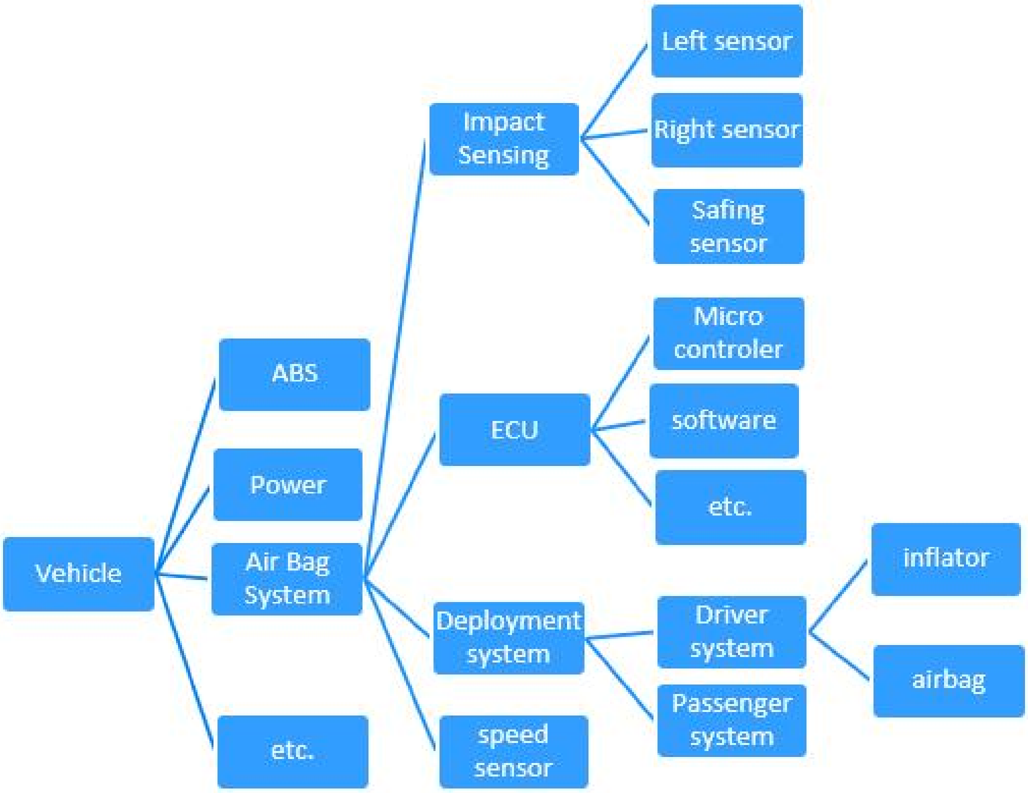


Figure 14 - Structural analysis example [32]

By conducting a comprehensive structural analysis, organizations gain a deeper understanding of the system's composition and its interrelationships. This detailed examination facilitates the identification and assessment of potential failure modes, contributing to effective risk mitigation strategies. The structure tree serves as a valuable tool for visualizing and organizing the elements under analysis, ensuring that no critical aspects are overlooked. Ultimately, this step enhances the overall effectiveness and accuracy of the subsequent FMEA process.

3.4.3 Functional Analysis – step 3

This step within the FMEA process holds significant importance as it focuses on accurately assigning the appropriate elements to their respective functions. To achieve this objective, all parties involved must clearly understand the functional description and requirements. During this step, it becomes essential to clarify the operating conditions and interactions between the system under analysis and its interconnected components [24]. It is essential to highlight that a function represents the intended purpose of a system element. A single system element can encompass multiple functions as well as product characteristics. When discussing the functions of a particular element, it is referred to as the focus element. The entire structure of the function-analysis tree is developed around this element in conjunction with the overall tree structure [33].

By ensuring a thorough understanding of the functions and its characteristics within the system, the analysis can effectively identify and evaluate potential failure modes associated with each function. This step lays the foundation for comprehensive risk assessment and mitigation strategies. Clear and precise functional descriptions enable a more accurate evaluation of the potential failure modes and their corresponding effects, allowing for targeted mitigation efforts. Moreover, considering operating conditions and interactions is crucial to capture the full scope of potential risks. By clarifying the operating conditions, including environmental factors and usage scenarios, and understanding the interactions between the system under analysis and its connected components, the analysis can identify dependencies and potential sources of failures. This integrated approach provides a comprehensive understanding of the system's functionality and aids in uncovering any potential vulnerabilities.

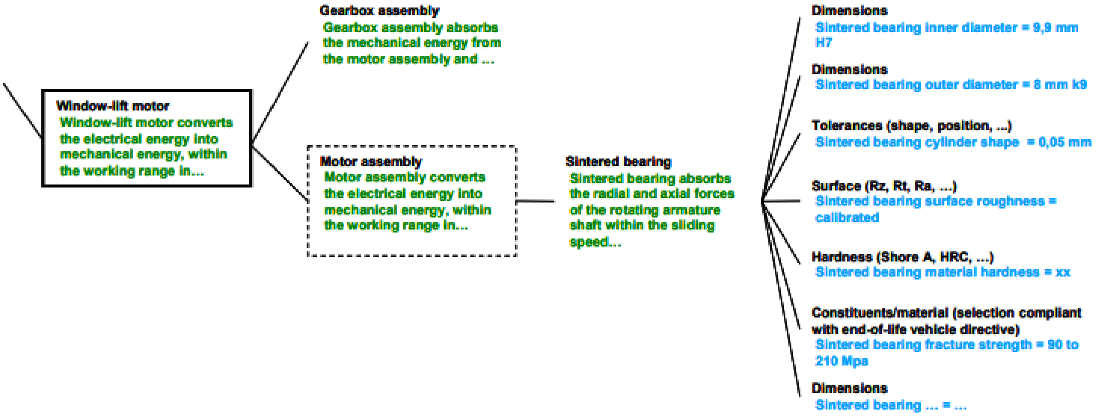

Window-lift motor
Window-lift motor converts the electrical energy into mechanical energy, within the working range in...
Gearbox assembly
Gearbox assembly absorbs the mechanical energy from the motor assembly and ...
Motor assembly
Motor assembly converts the electrical energy into mechanical energy, within the working range in...
Sintered bearing
Sintered bearing absorbs the radial and axial forces of the rotating armature shaft within the sliding speed...
Dimensions
Sintered bearing inner diameter = 9,9 mm H7
Dimensions
Sintered bearing outer diameter = 8 mm k9
Tolerances (shape, position, ...)
Sintered bearing cylinder shape = 0,05 mm
Surface (Rz, Rt, Ra, ...)
Sintered bearing surface roughness = calibrated
Hardness (Shore A, HRC, ...)
Sintered bearing material hardness = xx
Constituents/material (selection compliant with end-of-life vehicle directive)
Sintered bearing fracture strength = 90 to 210 Mpa
Dimensions
Sintered bearing ... = ...

Figure 15 - Function Net with functions and product characteristics [24]

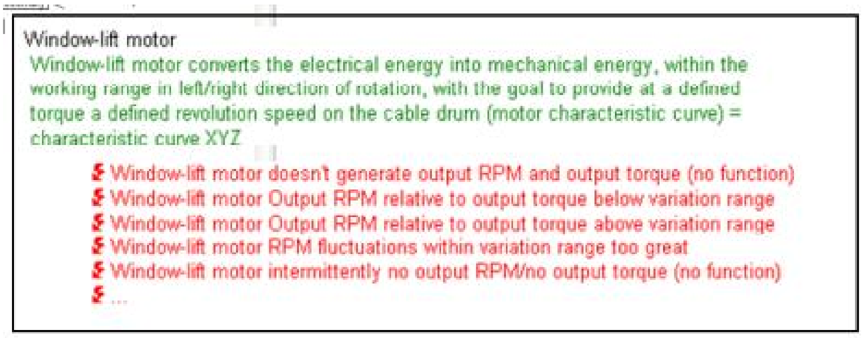
Developing the function-analysis tree structure around the focus element helps organize and visualize the functions within the system. It enables a systematic analysis of each function and its potential failure modes. This structured approach facilitates identifying relationships and dependencies between different functions, providing a comprehensive overview of the system's functional interactions. As we progress from the left side of the structure to the right, the level of detail gradually increases. The functions on the right side specify how the functions on the left side are executed or fulfilled, while the functions on the left side define the objectives that need to be accomplished by the functions on the right side.

3.4.4 Failure Analysis – step 4

In this phase, commonly referred to as error analysis, the fourth step of the FMEA process is undertaken. Its primary objective is to identify failure sequences, types, and causes, and establish their relationships to conduct a comprehensive risk assessment [25]. Each product function or characteristic that was defined in the previous step requires a detailed analysis to ensure that any potential malfunctions, which refer to the failure to fulfill the intended functions, are properly identified and adequately represented. A thorough analysis of malfunctions is essential to avoid any gaps or omissions in the subsequent steps of the FMEA process.

It is important to note that this analysis does not solely focus on complete failures, but also encompasses malfunctions caused by loss, degradation, intermittency, partial functioning, and unintended functionality or non-performance of a specific function or characteristic. By considering all possible malfunctions, the analysis ensures a comprehensive evaluation of potential failure modes and their impacts on the system's functionality and performance.

Moreover, during this step, not only can elements identified in the previous step have multiple functions, but it is also possible to assign multiple errors to each function. By allowing for the inclusion of multiple errors, the analysis can capture a broader range of potential failure scenarios and their associated causes. However, it is indispensable to provide clear and detailed error descriptions to enhance the accuracy and completeness of the subsequent analysis steps.



Window-lift motor

Window-lift motor converts the electrical energy into mechanical energy, within the working range in left/right direction of rotation, with the goal to provide at a defined torque a defined revolution speed on the cable drum (motor characteristic curve) = characteristic curve XYZ

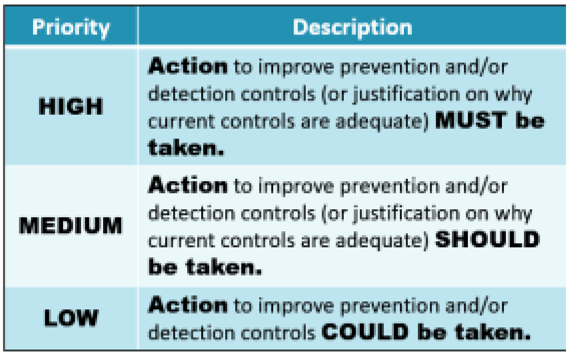
- Window-lift motor doesn't generate output RPM and output torque (no function)
- Window-lift motor Output RPM relative to output torque below variation range
- Window-lift motor Output RPM relative to output torque above variation range
- Window-lift motor RPM fluctuations within variation range too great
- Window-lift motor intermittently no output RPM/no output torque (no function)
- ...

Figure 16 - Example of failures description [24]

The quality of the error descriptions significantly influences the effectiveness of the following steps in the FMEA process. A precise and comprehensive description of errors facilitates a more thorough and accurate analysis in the subsequent steps. It provides the necessary foundation for identifying potential risks, evaluating their severity and occurrence, and devising appropriate mitigation strategies. The detailed error descriptions enable the analysis team to fully understand the nature and impact of each error, ensuring a comprehensive assessment of the system's failure modes.

3.4.5 Risk Analysis – step 5

The main objective of risk analysis is to assess and prioritize risks based on the severity of failure effects, the likelihood of failure causes, and the detection capabilities within the cause-and-effect chain. An Action Priority Table (AP) is utilized to determine the need for action, assigning priority to actions aimed at reducing the risk of failure to the system's function rather than assessing the risk itself.



Priority	Description
HIGH	**Action** to improve prevention and/or detection controls (or justification on why current controls are adequate) **MUST be taken.**
MEDIUM	**Action** to improve prevention and/or detection controls (or justification on why current controls are adequate) **SHOULD be taken.**
LOW	**Action** to improve prevention and/or detection controls **COULD be taken.**

Figure 17 - Action Priority Table levels [29]

3.4.5.1 Severity, Occurrence, and Detection Ratings

Severity, occurrence, and detection are rated on a scale of 0 to 10, with predefined tables aiding in the rating process. Severity (S) reflects the impact of a specific failure mode and considers factors such as customer impact. For instance, a severity rating of 10 signifies an extremely serious failure with implications for safety and compliance with legal regulations, occurring without warning. Occurrence (O) evaluates the likelihood of each failure cause based on control measures. A rating of 7 or 8 for occurrence indicates a high likelihood of repeated occurrence concerning the failure cause/mode, such as systems/components using new or problematic technologies. Detection (D) assesses the system's ability to prevent or detect failure modes or causes before customer handover through investigative measures. For example, a detection rating of 1 represents a high chance of detecting malfunctions or failure mechanisms using proven testing methods from previous generations [24].

3.4.5.2 Prevention and Detection measures

In fault prevention and defect detection, it is customary to establish prevention measures for addressing the causes of faults and detection measures for identifying defects. These measures are considered before assigning Severity-Occurrence-Detection (S-O-D) ratings for each case. Nevertheless, here are some noteworthy examples of both prevention and detection measures [25].

- Prevention Measures:

1. Mechanical Redundancy:

Having redundant elements minimizes the likelihood of faults occurring due to component failure. This preventive measure enhances the general reliability and robustness of the system.

2. Heat Treatment Specification on Drawing:

Heat treatment specification on drawing refers to the explicit instructions on technical drawings regarding the appropriate heat treatment process for specific components.

3. System Design according to Simulation:

The utilization of simulation techniques during system design allows for comprehensive analysis and optimization before implementation.

- Detection Measures:

1. Design of Experiments (DoE):

DoE involves conducting systematic experiments to explore the effects of various factors on a system or process. DoE enables a thorough understanding of the system's behavior and aids in optimizing detection mechanisms.

2. Function Test:

Function tests are conducted to assess whether a system or component performs its intended functions accurately and reliably. Function tests are required to detect defects affecting the system's overall performance.

3. Endurance Test:

Endurance tests involve subjecting a system or component to prolonged operational conditions to evaluate its durability and performance over time. Endurance tests are essential in detecting defects that may emerge during extended periods of operation.

3.4.5.3 Action Prioritization

Once initial ratings and the Action Priority (AP) matrix are established, the team can analyze and propose actions to reduce risk. The primary focus is lowering occurrence, as reducing severity is often more challenging. Failure modes categorized as 'high' necessitate preventive and/or detection controls, while lower-rated modes can be addressed with less urgency, with a particular emphasis on those classified as medium.

After prioritizing actions based on risk analysis, the groundwork is laid for additional analysis, if required, to ensure effective mitigation or further reduction in fault ratings. This step enables a comprehensive evaluation of the existing prevention and detection measures, identifying gaps or areas requiring additional attention.

The risk analysis and mitigation efforts form an iterative improvement process whereby the team continuously assesses and refines the prevention and detection measures. This iterative approach allows for ongoing optimization and adaptation to evolving risks and changing system requirements.

3.4.6 Risk Optimization – step 6

The optimization phase in FMEA concerns enhancing the reliability and performance of a system or process. Steps six and seven of FMEA, similar to DFMEA and PFMEA, mark a significant milestone in the methodology.

The design or process has been established at this stage, leaving little room for further refinement. The focus shifts towards defining new risk reduction measures and evaluating their effectiveness. The FMEA team thoroughly reviews the risk analysis results conducted in previous steps and identifies specific measures to decrease the likelihood of failure causes or enhance detection controls for failure causes or modes.

The SMART principle is applied to the action plan to ensure effective implementation. Each action should be specific, measurable, achievable, relevant, and time bound. This involves assigning responsibility to individuals or teams who will oversee the completion of each action and setting target dates for their achievement [33]. Evaluating the effectiveness of implemented actions is necessary in assessing their impact on risk reduction and system improvement. Completed actions are related to estimating their effectiveness and provide valuable insights for future analyses.

Throughout the optimization phase, the FMEA team may determine that no further action is necessary. This decision could be based on comprehensive risk reduction measures already implemented or the conclusion that certain measures are not feasible or required. In such cases, the "Remarks" column in the FMEA documentation contains entries indicating that no further action or revision is planned [25].

3.4.7 Results Documentation - step 7

In the final phase of FMEA, it is essential to document the results and achievements obtained throughout the process. This documentation serves multiple purposes, including demonstrating to stakeholders and customers that identified issues have been addressed or mitigated effectively. Furthermore, it provides a comprehensive record of the FMEA analysis, serving as a valuable reference for future reviews and ensuring the retention of intellectual property by the developing company.

An important aspect of the documentation phase is creating a report summarizing the FMEA results and planning. While this report does not replace the necessary content reviews by stakeholders, it serves as a concise summary for the FMEA team and other relevant parties. It ensures that each task has been completed and the results have undergone thorough review and assessment. The level of detail included in the report can be tailored depending on the intended audience and company policies. The report is a comprehensive repository of analysis information, reflecting the efforts and decisions made during the FMEA.

When documenting and presenting the results, the following key points may be incorporated [25]:

- Final Status and Objectives: The report should provide information on the final status of the project compared to the initial objectives defined in the Project Plan.
- Scope and Content: Include a description of the FMEA's scope and any additional content incorporated during the analysis.
- Function Derivation: An explanation of how the functions were derived is crucial for understanding the functional aspects of the system or process

under evaluation. This section outlines the fundamental functions and their relationships within the analyzed system.

- Summary of Findings: A concise summary of the findings and their corresponding Severity-Occurrence-Detection (S-O-D) ratings should be included. This summary helps communicate the identified risks and their prioritization to stakeholders, clearly understanding the potential areas of concern.
- Action Overview: The report should provide an overview of the actions defined throughout the FMEA process. This section highlights the measures recommended to address identified risks and their current status, indicating whether they have been implemented or are still in progress.
- Timeline for Optimization Activities: A timeline outlining the schedule for optimization activities within the FMEA should be included.

By effectively documenting the results and achievements of the FMEA, organizations can demonstrate their commitment to addressing potential risks and ensuring the reliability and safety of their systems or processes. The comprehensive report serves as a valuable reference, enabling stakeholders to review and verify the actions taken and decisions made.

In conclusion, by presenting the information clearly and concisely, organizations can provide stakeholders with a comprehensive understanding of the identified risks, the actions to mitigate them, and the ongoing optimization efforts. The documentation is a valuable tool for future reviews, ensuring the continued improvement and success of the analyzed system or process.

3.5 Monitoring and System Response FMEA

3.5.1 Introduction to MSR-FMEA

Another essential Failure Mode and Effects Analysis type that warrants consideration is the MSR-FMEA, also known as System FMEA or Mechatronic FMEA. While the DFMEA primarily focuses on reliability and potential failures resulting from design or component issues, the MSR-FMEA, or Monitoring and

System Response FMEA, takes a different perspective. This newer type of FMEA examines failures that may occur during the use of the system, specifically looking at the consequences rather than the underlying causes. The rising importance of self-diagnostic and monitoring systems in modern vehicles, such as self-driving systems, has brought attention to potential failures not adequately addressed by existing FMEA types. Consequently, the MSR-FMEA has emerged to address this cluster of issues.

However, what precisely is an MSR-FMEA? The primary objective is to ensure the system maintains a safe state during operation. While systems may experience failures during regular operation, assessing the associated risks and consequences is necessary. The MSR-FMEA provides a framework for evaluating these risks, focusing on maintaining safety and addressing potential failures that can impact the system's overall performance and functionality. The introduction of MSR-FMEA aligns with the requirements set forth by ISO 26262, which emphasizes the safety goals of vehicle systems, particularly those related to electrical and electronic components [27].

ISO 26262 plays a vital role in ensuring the safety of vehicles and their complex mechatronic systems. This standard sets stringent requirements for functional safety to prevent and mitigate risks associated with potential failures. The MSR-FMEA methodology is essential for fulfilling these safety goals, providing a comprehensive analysis of potential failures and their impact on system performance. By adopting MSR-FMEA, automotive manufacturers and developers can proactively identify and address potential risks, ensuring mechatronic systems' safe and reliable operation. This approach considers design and component failures and focuses on the overall system behavior and response in various operational scenarios.

The application of MSR-FMEA enables a thorough evaluation of the system's potential failure modes and their effects, considering the dynamic nature of mechatronic systems. It provides valuable insights into potential risks, allowing designers and engineers to implement appropriate monitoring and response mechanisms. Additionally, it facilitates the identification of necessary safety measures and implementation of robust countermeasures to mitigate risks and ensure system safety.

The adoption of MSR-FMEA represents a significant advancement in automotive safety analysis. It acknowledges the growing complexity of modern vehicles and the need to address potential failures that may arise from advanced features and self-diagnostic systems. By incorporating MSR-FMEA into the safety assessment process, automotive manufacturers can enhance their ability to deliver vehicles that meet the highest safety standards and provide reliable performance in various scenarios.

3.5.2 Methodology and Process

Having explored the step-by-step process of Design Failure Mode and Effects Analysis (DFMEA) in detail, it is now required to delve into the key differentiating factors of MSR-FMEA. By comparing these two methodologies, we can comprehensively understand how MSR-FMEA diverges from its predecessor. While DFMEA focuses on analyzing errors during the development phase, MSR-FMEA takes a different approach by examining errors already occurring in the field.

The shift in focus allows for a deeper understanding of system behavior and the implementation of appropriate responses to ensure safety. MSR-FMEA identifies errors and determines how the system should respond to them, emphasizing mitigating risks and safeguarding occupants and other road users [34]. This approach is particularly important as vehicles incorporate advanced features and self-diagnostic systems. By integrating MSR-FMEA into the analysis process, manufacturers gain insights into system performance in real-world scenarios, enabling the development of proactive response mechanisms.

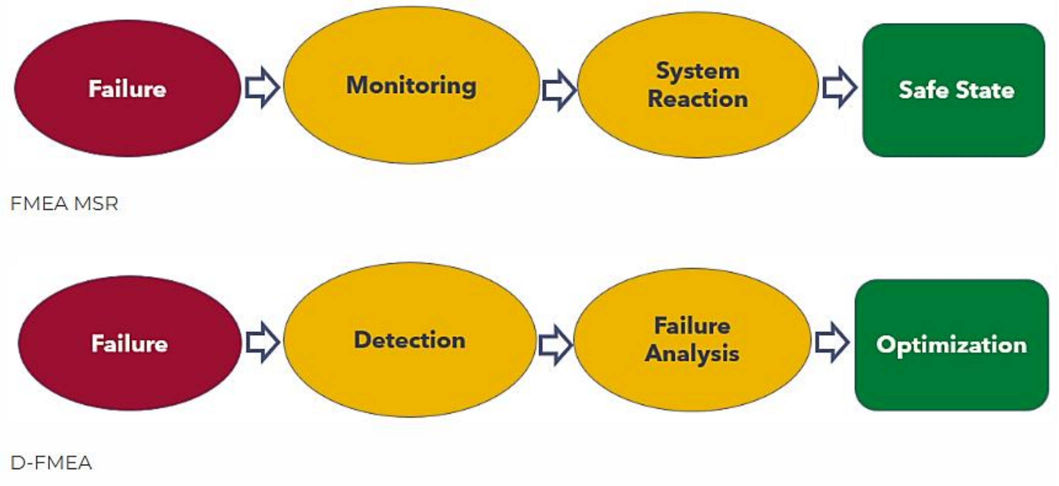


Figure 18 - Comparison between DFMEA and MSR-FMEA approach [34]

The unique focus of MSR-FMEA on errors occurring during operation sets it apart from the preventive nature of DFMEA. This comprehensive approach considers the complexities of real-world scenarios, leading to a more accurate assessment of risks and the formulation of appropriate response actions.

MSR-FMEA offers a comprehensive evaluation of risks, extending beyond personal injury considerations to encompass quality defects and system functions' potential loss or limitation. Its primary objective is to prevent failure sequences that trigger system responses, aiming to replace them with new failures that have a minor impact on the system's safe state. The FMEA-MSR methodology facilitates decisions regarding safety requirements objectives, enabling recommendations such as the addition of monitoring sensors, system redundancies, or improved malfunction detection checks [25].

MSR-FMEA provides organizations with a thorough analysis of potential vulnerabilities and risk mitigation strategies by assessing personal injury risks, quality defects, and functional limitations. These recommendations enhance system safety and performance, ensuring reliability even during failures. The versatility of MSR-FMEA allows for targeted safety measures tailored to the specific needs of mechatronic systems.

3.5.2.1 The Differentiating Factors of MSR-FMEA

One key distinction is observed in step 2, where the structure tree within MSR-FMEA focuses on both the intended and unintended functions of systems and subsystems. The structure here must be compatible with an existing safety concept whenever it is already in place. While the scope of MSR-FMEA is generally limited to the system elements highlighted in the corresponding DFMEA, there may be instances where the analysis extends to include interfaces with other systems, as depicted in the accompanying figure. This expanded scope ensures a more comprehensive assessment of potential risks and allows for a thorough understanding of how system elements interact within the broader context.

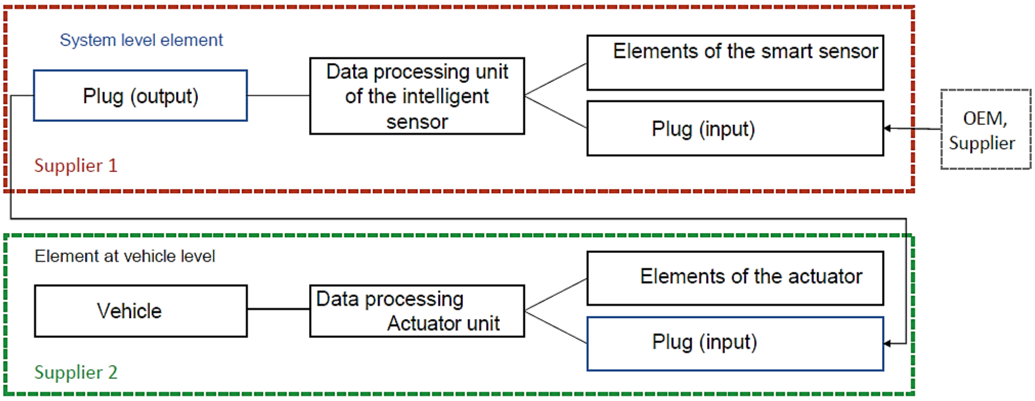


Figure 19 - MSR-FMEA structure tree within an interface element [25]

Step 3 builds upon the same principle as the previous step but introduces an additional layer of complexity by incorporating monitoring and system states. This involves implementing functions such as redundancy checks, detecting values that fall outside the acceptable range, initiating emergency mode, and issuing driver warnings in response to errors. The comprehensive evaluation of these functions necessitates the assessment of sensor signals as well, further enriching the analysis in this phase. By considering the interplay between these elements, MSR-FMEA provides a more robust understanding of potential risks and enhances the system's overall safety [25].

MSR-FMEA adopts the same structure as DFMEA in the failure analysis stage, including identifying possible failure causes, monitoring mechanisms, and system responses. A meaningful comparison between the two methodologies lies in the failure chain. In MSR-FMEA, if a component can detect an error, it initiates an event with a less severe impact than the original fault. It is important to note that errors related to the monitoring procedure are not evaluated within MSR-FMEA, as they fall within the scope of DFMEA if deemed necessary for the project analysis. By maintaining this clear distinction, both methodologies work synergistically to assess potential failures and their effects on system performance comprehensively.

In the final step that impacts the differences in MSR-FMEA, the risk analysis stage introduces notable differences that influence the methodology. The focus shifts to the impact on the user, aligning with the construction principles outlined in the DFMEA manual. Three criteria are employed for evaluation within the risk assessment, presenting a slight deviation from the DFMEA framework. The Probability of Occurrence (O) and Probability of Detection (D) categories are now replaced by Frequency (F) and Monitoring (M) in MSR-FMEA, resulting in the following key considerations:

1. Meaning (B): This criterion assesses the significance of the error sequence, capturing its implications and potential consequences.

2. Frequency (H): The frequency category examines how often the problem occurs or is likely to occur during vehicle usage, considering various operating situations and scenarios.

3. Monitoring (M): The monitoring criterion evaluates the effectiveness and quality of the monitoring functions implemented within the system, ensuring that potential failures are promptly detected and addressed.

By integrating these revised evaluation criteria, MSR-FMEA provides a comprehensive risk analysis framework that considers the impact on the user, occurrence frequency, and the effectiveness of monitoring functions [35].

In addition, the risk analysis step in MSR-FMEA utilizes the Action Priority (AP) table, similar to DFMEA, to prioritize the identified risks. The AP table categorizes risks into three levels of prioritization: low, medium, and high. This aids in determining the appropriate actions and allocating resources to address the identified risks effectively. By applying this systematic approach to risk prioritization, MSR-FMEA ensures that critical risks receive the necessary attention and enables the development of targeted mitigation measures. The utilization of the AP table further enhances the overall risk analysis process and reinforces the importance of proactive risk management within the context of mechatronic system safety analysis.

The optimization step in MSR-FMEA is vital for driving continuous improvement and enhancing system safety. It involves analyzing the results of the risk analysis and identifying areas for enhancement. By implementing preventive measures, improving detection controls, or making changes to component designs, the team aims to eliminate the causes of faults or enhance the monitoring of fault causes [25]. Regular assessments are conducted to evaluate the effectiveness of implemented actions and identify opportunities for further improvement. This iterative process ensures that safety measures are continuously optimized and aligned with mechatronic systems' evolving needs and challenges.

4 Cybersecurity Breach - in Remote Car Hacking: Insights from the Jeep Cherokee Incident

In recent years, the rapidly evolving landscape of technology and connectivity has brought forth new challenges and vulnerabilities in automotive cybersecurity, particularly with the rise of incidents related to remote car hacking. These occurrences have garnered significant attention and emphasized the potential risks associated with interconnected vehicles. One prominent case that has drawn considerable interest is the remote car hacking of a Jeep Cherokee. In this chapter, we aim to delve into this cybersecurity breach from the perspective of OEMs.

Notably, an analysis conducted by KPMG revealed a stunning 300% increase in cyber-attacks in the automotive industry between 2017 and 2019 [36]. The same report emphasized that an average cyber-attack costs the manufacturer more than 10 million dollars, raising a red flag for OEMs to address the growing threats to their systems and vehicles. Through this examination, we seek to understand the implications of the Jeep Cherokee incident and explore practical strategies to enhance automotive cybersecurity. By leveraging available articles and studies, we aim to shed light on the vulnerabilities exploited in the breach, the potential consequences for vehicle security and user safety, and the role of OEMs in fortifying their defenses. With these insights, we desire to equip OEMs with valuable guidance and countermeasures to safeguard their connected vehicles and technical products effectively.

This chapter aims to analyze the Jeep Cherokee incident and explore its implications for ensuring cybersecurity of technical products. With the widespread recognition and accurate application of Failure Mode and Effects Analysis in various industries, the first research question arises: "Can FMEA be effectively utilized to enhance the cybersecurity of technical products?". While the initial intention of this paper was to gather insights directly from industry professionals and employees involved in addressing the breach, the extensive confidentiality surrounding the incident necessitated a different approach. Consequently, this chapter will utilize available articles and studies to examine the breach and its significance comprehensively.

By analyzing existing research and publications, we aim to shed light on the vulnerabilities exploited in the Jeep Cherokee incident, the potential consequences for vehicle security and user safety, and the applicability of FMEA to enhance cybersecurity. The insights gained from this analysis will contribute to answering the research question and provide valuable guidance for OEMs in the automotive industry. Through this examination, we strive to highlight the critical lessons learned from the Jeep Cherokee incident and explore the potential of utilizing FMEA to strengthen cybersecurity practices. By understanding the implications of such breaches and leveraging effective methodologies, OEMs can develop robust countermeasures, ensuring the safety and security of connected vehicles and other technical products.

Disclaimer: The information presented in this chapter is based on publicly available articles and studies related to the Jeep Cherokee remote car hacking incident. Due to the abovementioned limitations, the chapter does not include direct access to confidential or proprietary information."

4.1 What Happened? Understanding the Jeep Cherokee Incident

The rapid evolution of technology and connectivity has introduced new challenges and vulnerabilities in automotive cybersecurity. Recent years have seen a surge in remote car hacking incidents, spotlighting the potential risks associated with interconnected vehicles. One prominent case that has garnered considerable attention is the remote car hacking of a Jeep Cherokee. This pivotal event prompted us to delve into this cybersecurity breach from the perspective of OEMs.

Concerns over vehicle systems ' vulnerability and passengers ' safety have escalated between the increasing awareness of cyberattacks and the criticality of cybersecurity in modern cars. A group of professionals known as white hat hackers have emerged in response to these challenges. Companies or individuals legally authorize these skilled individuals to probe and identify weaknesses in specific systems. Their activities, conducted with permission, distinguish them from other hackers in terms of ethics and purpose [37]. As the automotive industry confronts the potential risks posed by cyber threats, the presence of white hat hackers has become more prominent. Leveraging their expertise and ethical approach, these professionals offer valuable insights into the weaknesses and entry points that malicious hackers could exploit. Through authorized hacking attempts, they play a crucial role in helping the automotive industry identify and rectify vulnerabilities, ultimately ensuring the safety and security of vehicles and their occupants. In an era where connectivity and digitalization are integral to modern cars, their involvement has become increasingly indispensable.

During 2014 and 2015, the automotive industry witnessed a significant demonstration of vulnerabilities in modern vehicles' security features. White hat hackers Charlie Miller and Chris Valasek orchestrated an eye-opening experiment involving a 2014 Jeep Cherokee. They aimed to underscore the potential risks and lack of security measures in unmodified vehicles, particularly concerning remote attacks. This demonstration was a stark reminder of the need for enhanced cybersecurity measures within the automotive industry. The vulnerabilities they successfully exploited could compromise vehicle occupants' safety and privacy. Their groundbreaking work was a wake-up call for automakers, propelling them to prioritize cybersecurity in their design and development processes. The findings from Miller and Valasek's research catalyzed a paradigm shift within the industry, prompting increased efforts to fortify vehicle systems against potential cyber threats. To this day, their pioneering work continues to influence the development of robust security features aimed at safeguarding against remote attacks and ensuring the safety of vehicle users.

The research paper containing 91 pages [38], explores specific vehicle features that amplified its vulnerability to potential attackers. While some of these features were designed to enhance driving experience and safety, it is essential to recognize that these technological advancements can also serve as potential entry points for hackers. The paper examines features such as Adaptive Cruise Control (ACC), Forward Collision Warning Plus (FCW+), Lane Departure Warning (LDW+), and Park Assist System (PAM). It incorporates Bluetooth and Wi-Fi connectivity, further augmenting the vehicle's potential attack points. Furthermore, the paper delves into illustrative examples where white hat hackers effectively manipulated these vulnerabilities, showcasing their ability to control various vehicle functions remotely.

Charlie and Chris successfully accessed Jeep's infotainment system, enabling them to control non-critical features such as the radio and wipers. However, they escalated their intrusion by manipulating critical functions like steering and braking, a development that sent shockwaves through security experts and customers alike. This starkly highlighted the real risks posed by cyber threats to vehicle safety. With the increasing proliferation of electronic control units in modern vehicles, remote control attacks have become increasingly plausible. Safeguarding vehicles against such cyberattacks has never been more critical for passenger and road user safety. The Jeep Cherokee hack triggered a much-needed focus on cybersecurity research and development within the automotive industry. As this incident serves as both a cautionary tale and a catalyst for ongoing efforts to mitigate cyber risks in the automotive landscape, it reinforces the urgency and importance of enhancing cybersecurity practices to protect connected vehicles and other technical products.

4.2 Unveiling Vulnerabilities: Infiltrating the Jeep’s Infotainment System

After carefully selecting the model and manufacturer for their hack, Charlie Miller and Chris Valasek faced the formidable task of comprehending the intricate workings of the 2014 Jeep Cherokee's system. Delving into the vehicle's architecture, they made a strategic assumption that gaining control over the radio control unit would grant them the power to send commands to the ECUs responsible for managing the car's physical features. The architecture of the 2014 Jeep Cherokee is visually depicted in Figure 20 below, providing a glimpse into the interconnected components that became their target of interest.

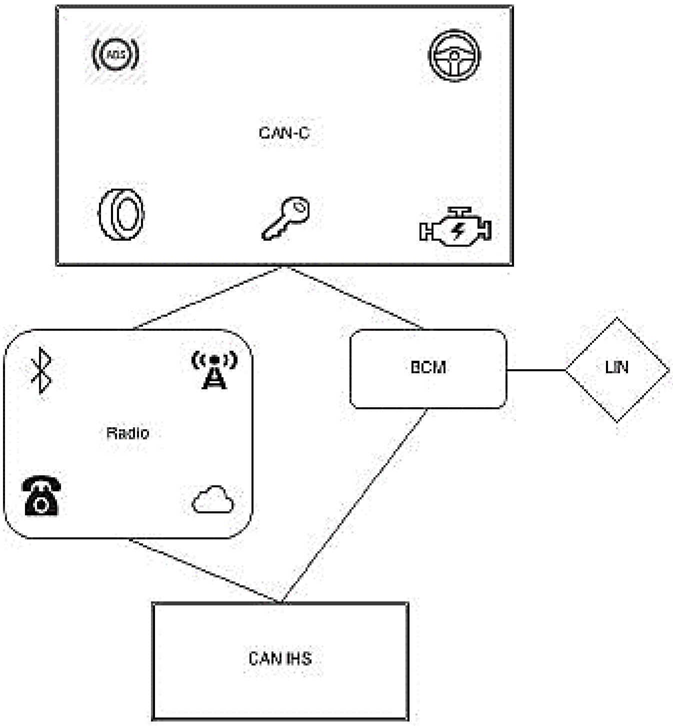


Figure 20 - Jeep Architecture [38]

In automotive cybersecurity, white hackers have consistently pointed out the telematics system's significance as a prime entry point for potential attacks. This system presents a wide array of access points, rendering it an alluring target for malicious intrusions. Its vulnerability stems from the fact that telematics in vehicles encompasses various systems, making them susceptible to potential breaches through channels like GPS, wireless telematics, and more. To further compound the issue, the complex nature of vehicle telematics often involves the convergence of the Internet of Things (IoT), cloud technologies, and software solutions [39]. These interconnections expose a larger attack surface, necessitating robust security measures to safeguard against potential cyber threats.

Moreover, the researchers' paper brought to light the vulnerability of Wi-Fi, which is integrated into numerous devices within modern vehicles. Even if attackers cannot directly access the vehicle's central system, they can exploit potential loopholes through any device connected to the vehicle's Wi-Fi network. While we will not dive deep into the intricate technicalities of the code or explore the specifics of breaching such systems, it is essential to acknowledge this susceptibility and prioritize stringent security measures to fend off potential attacks.

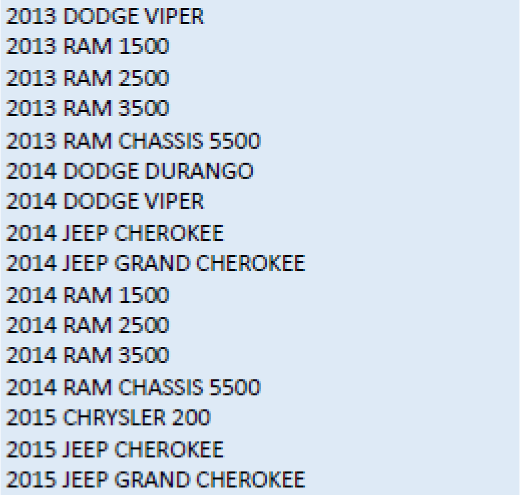
The main entry point for hackers into the 2014 Jeep Cherokee's systems was through its touchscreen infotainment system (chip OMAP). They masterfully executed their attack by treating it as a touchscreen computer susceptible to compromise. Once they gained control, Miller and Valasek held authority over functions unrelated to driving, enabling them to manipulate the radio and adjust HVAC settings. However, these may seem harmless functions during regular driving; losing control or being unaware of such actions could instill panic in the driver. For instance, the driver who experienced the Jeep Cherokee attack described, "Though I had not touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next, the radio switched to the local hip-hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass." This chilling excerpt vividly illustrates the initial stages of the vehicle hack, as Andy Greenberg detailed in an article on Wired's website [40].

As the automotive industry wrestles with the escalating challenge of cybersecurity, understanding these vulnerabilities and the potential consequences is critical. Examining the Jeep Cherokee incident sheds light on the urgent need for robust security measures, protecting the safety and well-being of vehicle users and prompting the automotive community to prioritize cybersecurity research and development. By comprehending the implications of such breaches and leveraging effective methodologies like Failure Mode and Effects Analysis (FMEA), our aim here, OEMs and cybersecurity experts can collaboratively devise and implement innovative countermeasures, safeguarding connected vehicles and other technical products from potential cyberattacks.

4.3 Beyond the Infotainment: Manipulating Critical Driving Functions

With their sights set on influencing driving functions, the hackers embarked on the arduous task of developing custom firmware to take control of a chip responsible for managing the vehicle's physical components. Unlike the chip governing the infotainment system, this chip boasted distinct properties, demanding a different approach to hacking. Ordinarily, attempting to hack one chip via another would be an insurmountable challenge, as Miller and Valasek pointed out. However, the unique circumstances in the Jeep Cherokee case, where the hackers already held dominion over the infotainment chip, presented an opportunity for them to install the meticulously crafted firmware, thus paving the way for a successful hack.

Before exploring the specific physical features that succumbed to the hackers' attack, it is vital to emphasize the broader implications of their research. A comprehensive scan conducted by the researchers revealed a disconcerting list of potentially vulnerable vehicle models, hinting at the far-reaching impact of such attacks. While these vehicles did not undergo the same hack investigated in the research paper, their susceptibility to remote interaction without requiring any form of authentication serves as a compelling cautionary note. This alarming discovery should prompt the automotive industry to prioritize robust cybersecurity measures, fortifying their vehicles against potential threats across a broad spectrum of connected models.



2013 DODGE VIPER
2013 RAM 1500
2013 RAM 2500
2013 RAM 3500
2013 RAM CHASSIS 5500
2014 DODGE DURANGO
2014 DODGE VIPER
2014 JEEP CHEROKEE
2014 JEEP GRAND CHEROKEE
2014 RAM 1500
2014 RAM 2500
2014 RAM 3500
2014 RAM CHASSIS 5500
2015 CHRYSLER 200
2015 JEEP CHEROKEE
2015 JEEP GRAND CHEROKEE

Figure 21 - Possible vehicles that can be vulnerable [38]

The researchers' concern was amplified when they extrapolated their findings, using a formula to estimate the number of vulnerable vehicles, revealing an even more staggering statistic than the number of affected models. The estimated range of vulnerable vehicles stood between 292,000 and 471,000, sending shockwaves through the automotive community. With such a vast number of vehicles potentially at risk, the ramifications of remote attacks on driving functions could be catastrophic. The significant number of vulnerable vehicles caught the attention of OEMs, further amplifying concerns within the industry. Responding to the researchers' findings and mitigating potential risks, a recall of 1.4 million vehicles was initiated. The recall scale demonstrated the gravity of the situation.

4.3.1 The V850 chip

During a presentation at DEF CON 23 [41], Charlie and Chris embarked on exploration beyond the confines of the infotainment unit, seeking an entry point into the broader system of the car. Immersed in their analysis of the vehicle's architecture, as already depicted in Figure 20, they unearthed intriguing connections that hinted at potential pathways for their hacking endeavors. In this phase of their research, a pivotal realization dawned upon them. While they adeptly manipulated the radio's functions, they encountered an obstacle in their quest to influence the car's physical aspects. Despite the radio system's communication with external components and the two CAN (Controller Area Network) units, they discerned the presence of two distinct chips that wielded dominion over essential functions, effectively acting as the gateway to complete control of the entire vehicle. This revelation presented a formidable challenge in their relentless pursuit to access and manipulate critical driving functions.

As the hackers set their sights on taking control of the vehicle's critical driving functions, their path led them to the OMAP chip, responsible for orchestrating the management of the infotainment system. However, a direct approach to sending information to the braking system and prompting immediate action proved unfeasible. Unfazed by this roadblock, they turned their attention to an alternative approach that would prove pivotal in their hacking quest. Their breakthrough came as they delved into the firmware of the V850 chip, which assumed the role of the central controller governing the vehicle's physical features. To their astonishment, they made a critical discovery - the V850 chip's firmware could be updated conveniently from an easily accessible web version, available for download by virtually anyone with an internet connection.

With this newfound knowledge, the hackers devised a strategic move to execute their remote hack. They seamlessly introduced a USB connection to the infotainment unit, cleverly paving the way to update the V850 chip through the OMAP. This cunning maneuver was further supported by the absence of robust authentication or validation rules safeguarding against unauthorized firmware overwriting. This vulnerability in the chip's firmware proved to be the Achilles' heel that unlocked the gateway to manipulating critical driving functions, empowering their actions to impact the vehicle's physical performance directly.

Each meticulous step in their hacking journey evolved as the hackers successfully established a seamless pathway to transmit commands from the OMAP chip to the V850 using the SPI (Serial Peripheral Interface). This communication link between the two chips enabled them to interact and exchange information fluidly, connecting the gap between the infotainment unit and the central control of critical driving functions. With this entry point to the vehicle's core components established, their efforts culminated in realizing their objectives - the remote attack's broad impact extended beyond the infotainment system to enclose the manipulation of the vehicle's physical components. This newfound authority over critical driving functions yielded the vehicle susceptible to their control.

Having mastered the art of sending exploitative messages to the vehicle's systems, identifying pathways for impactful actions during driving scenarios, and accessing privileged operations, the hackers encountered their next challenge: reverse engineering the codes within the Jeep Cherokee ECU. This step was essential to enable them to send customized messages rather than relying on pre-defined ones already in the system.

4.3.2 Exploiting Driving Features

In this critical stage, they encountered the most alarming aspect that haunts those concerned about cyber-attacks. Their investigation led them to uncover a method to kill the engine by turning off a specific fuel injector through a diagnostic routine on the chip. Although this action was only viable at low speeds, the potential harm it could inflict on individuals was deeply concerning. Moreover, Charles and Chris made another unsettling discovery. By initiating a diagnostic session of the ABS ECU, they gained the ability to send commands to bleed all brakes, effectively rendering the vehicle's brakes inoperable. This revelation further heightened the gravity of the vulnerabilities they had encountered.

In their relentless pursuit, the hackers also targeted the steering system, which had proven more resilient than the previous ones. Despite the challenges, they ingeniously found a way to transmit messages with precise torque specifications, enabling them to dictate the wheel's steering direction. As they concluded this investigation phase, the depth of vulnerabilities exposed in the driving features left them deeply concerned about the implications of such attacks.

This passage powerfully illustrates the sheer panic induced by these malicious attacks, emphasizing the gravity of the situation. Andy was aware that the researchers would eventually hack his Jeep Cherokee. As the experiment unfolded, he experienced the chilling effects firsthand. The moment he realized the accelerator was unresponsive, anxiety set in, and he desperately pressed the pedal, watching the RPMs climb with no corresponding increase in speed. The Jeep's movement slowed to a crawl, leaving him stranded on a long overpass with no shoulder for escape. What started as an experiment became a terrifying ordeal as the interstate began to slope upward, causing the Jeep to lose even more momentum and barely inch forward. The impotence of the situation was evident as cars lined up behind his vehicle, honking in frustration. The sense of vulnerability was heightened when an 18-wheeler approached in his rearview mirror, making him hope that the driver would see his predicament and understand he was paralyzed on the highway [40].

5 Developing a Cybersecurity FMEA Framework for Technical Products

This chapter explores the potential application of Failure Mode and Effects Analysis to ensure cybersecurity of technical products, with a specific emphasis on the automotive industry. With the growing concern over cybersecurity breaches in modern vehicles, the importance of implementing robust security measures has never been more critical. In response to these challenges, the aim is to address the research questions raised earlier and develop and present a comprehensive Cybersecurity FMEA framework.

Via exhaustively examining existing literature and industry practices, we aim to establish the relevance and adaptability of FMEA in cybersecurity. By leveraging FMEA's strengths and understanding its limitations, it is possible to pave the way for a comprehensive Cybersecurity FMEA framework tailored to the unique challenges of protecting technical products from cyber threats.

To ensure seamless integration into existing cybersecurity practices, we explore how the Cybersecurity FMEA framework aligns with industry standards and requirements. Harmonizing FMEA with established guidelines such as SAE J3061 and ISO/SAE 21434 strengthens an organization's cybersecurity posture and fosters compliance with industry best practices.

5.1 The Applicability of FMEA in Ensuring Cybersecurity

FMEA is a powerful tool to enhance cybersecurity in technical products, aligning with its core objective of anticipating and preventing failures. In this section, we explore the seamless connection between FMEA and the fundamental principles of cybersecurity, where protection against threat scenarios lies at the forefront.

To establish a solid foundation for employing FMEA in cybersecurity cases, we bridge the definitions and concepts of both methodologies. By interlacing these disciplines, we unlock the viability of effectively exploiting FMEA to harden cybersecurity measures. To create a seamless synergy, we contextualize cybersecurity's key definitions within the world of FMEA.

For instance, drawing parallels between a ‘Hazardous Situation’ (section 3.2.1) and the occurrence of harm leading to unsatisfactory consequences, we extrapolate its relevance to encompass the domain of ‘Cyberattacks’ and ‘Threats.’ In the context of vehicles, unsatisfactory consequences could involve the violation of safety for individuals within and around the vehicle and the potential loss of system functionalities. Extending this definition allows us to address cybersecurity risks and their implications on technical products.

Furthermore, significant parallels are evident between ‘Failure Causes’ in FMEA and concepts in cybersecurity, such as ‘Trigger’ (section 2.1.12), ‘Vulnerability’ (section 2.1.13), and ‘Weakness’ (section 2.1.14). In FMEA, failure causes represent circumstances initiating a failure, while in cybersecurity, these concepts lead to events that could cascade into a cyberattack. Identifying these alignments reinforces the interconnectedness of FMEA and cybersecurity practices in effectively mitigating potential threats and vulnerabilities.

Since 'Cyberattacks' are frequently executed by a human factor – hackers, it creates a compelling connection with 'Failure Mode.' As elucidated in section 3.2.1, failure mode delves into how failures occur, and an essential link emerges: Human failure. While a cyberattack itself might not be considered a human failure, the hackers' staged attack involves human elements that profoundly influence both FMEA and Cybersecurity. This acknowledgment underscores the interplay between human actions and technical vulnerabilities in the context of cybersecurity breaches and highlights the significance of considering human factors in enhancing FMEA's application in cybersecurity.

Identifying commonalities between Failure Mode and Effects Analysis (FMEA) and cybersecurity lays the foundation for addressing the first research question:

- "If the method FMEA is so recognized and extensively used with accuracy, can it be applied to ensure the cybersecurity of technical products?"

The answer to this question is affirmative, as evident from the seamless connection between both methodologies' fundamental definitions and concepts. FMEA's efficacy in anticipating and preventing failures can be effectively applied to bolster cybersecurity measures. Cybersecurity essential to acknowledge that while the applicability of FMEA in cybersecurity is evident, it remains a relatively unexplored territory. Further in-depth exploration and research are essential to fully leverage FMEA's potential in enhancing cybersecurity practices.

By leveraging the strengths of FMEA, particularly in anticipating potential failure modes, organizations can adapt this method to identify and mitigate vulnerabilities in technical products susceptible to cyber threats. The systematic and proactive approach of FMEA aligns with the objectives of cybersecurity, where preemptively identifying weaknesses and potential threats is paramount. Integrating FMEA's methodology into cybersecurity practices can provide a more comprehensive and proactive defense against cyberattacks.

Moreover, the interplay between human factors and technical vulnerabilities in cybersecurity breaches necessitates an approach considering both aspects. FMEA's ability to assess human failures in the context of failure modes makes it relevant in addressing the human element involved in cyberattacks. Understanding the human factors contributing to vulnerabilities in technical products can help organizations implement measures to strengthen their cybersecurity posture.

While FMEA's applicability to cybersecurity holds promise, challenges lie ahead. Adapting FMEA to the dynamic and rapidly evolving landscape of cyber threats requires continuous research and development. Cybersecurity FMEA must address emerging attack vectors and consider the broader context of interconnected systems, which can introduce new risks. Moreover, ensuring seamless integration into existing cybersecurity practices and industry standards is crucial to facilitate its adoption by organizations.

In conclusion, the alignment of FMEA with cybersecurity principles presents a compelling opportunity to enhance the security of technical products. By leveraging FMEA's systematic approach and addressing human factors in cybersecurity, organizations can develop a comprehensive Cybersecurity FMEA framework tailored to the unique challenges of protecting against cyber threats. However, realizing its full potential requires concerted research efforts and a collaborative approach among academia, industry, and cybersecurity experts. Embracing this synergistic approach can foster a safer technological landscape and contribute to the overall cybersecurity resilience of technical products in the automotive and other industries.

5.2 Structuring the Cybersecurity FMEA Process

Having thoroughly explored the Cybersecurity Standards and gained a comprehensive understanding of FMEA principles, we are now well-equipped to determine the optimal structure for a Cybersecurity FMEA. To address our second research question regarding the most effective approach, we must examine potential similarities with other FMEA types, including DFMEA, PFMEA, or MSR-FMEA. This analysis aims to identify the most effective cybersecurity FMEA framework, ensuring that cybersecurity risks are mitigated effectively.

As a result of the Cybersecurity Standards, we gain a greater understanding of the unique challenges posed by cyber threats, underlining the necessity of proactive and systematic risk assessment. We can adapt and tailor FMEA methodologies to address specific cybersecurity concerns based on their proven effectiveness across various domains. By aligning the Cybersecurity FMEA with existing FMEA types, we can leverage best practices and lessons learned from diverse industries, fortifying interconnected systems and safeguarding digital assets. By recognizing both commonalities and distinctions, we can create a comprehensive framework that effectively addresses cybersecurity vulnerabilities while seamlessly integrating with the existing risk management processes.

Furthermore, our solid foundation in Cybersecurity Standards and FMEA methodologies ensures the compatibility and applicability of the structured Cybersecurity FMEA across diverse technological environments. As technology evolves rapidly, this adaptability becomes paramount in securing digital ecosystems against emerging cyber threats. With a clear direction for the Cybersecurity FMEA's structure, the forthcoming sections will explore its step-by-step implementation. We will investigate its significance in enhancing cybersecurity and fortifying digital ecosystems against potential threats, contributing to a more secure and resilient technological landscape.

5.2.1 Integrating FMEA with Cybersecurity Standards and Requirements

Efficiently merging FMEA with Cybersecurity requires thoughtful consideration of the standards and requirements set in Cybersecurity. ISO21434, the State of Art Cybersecurity Standards, offers valuable guidance, highlighting essential elements specified in section 2.4.2. These elements encompass Cybersecurity Monitoring, Events Evaluation, Vulnerability Analysis, and Vulnerabilities Management. Aligning the FMEA process with these core aspects ensures a comprehensive approach to addressing Cybersecurity concerns effectively.

Incorporating a cybersecurity expert within the FMEA team plays a vital role during the definition phase. This step ensures that the team thoroughly understands crucial Cybersecurity points and fosters a collaborative approach in the risk assessment process. By leveraging the insights and expertise of the cybersecurity expert, the FMEA team can comprehensively identify potential Cybersecurity vulnerabilities and implement proactive measures to mitigate risks effectively.

Moreover, drawing insights from the guidebook SAE J3061 reinforces the integration of FMEA and Cybersecurity. The guidebook emphasizes the importance of adopting an exemplary structure during the product development process, offering valuable reference points for designing a robust Cybersecurity FMEA framework. Adhering to these recommendations ensures organizations optimize their risk assessment process and seamlessly align it with Cybersecurity objectives, ensuring the safety and security of their products. By combining the guidance from ISO21434 and SAE J3061 and involving a cybersecurity expert within the FMEA team, organizations can enhance their approach to Cybersecurity FMEA, reinforcing their automotive systems' overall safety and resilience.

5.3 Step-by-Step Implementation of the Cybersecurity FMEA Process

The Cybersecurity FMEA process initiates with step 1, mirroring the planning and preparation phase seen in other FMEA types. However, given the distinct cybersecurity context, specific adaptations are essential. This section will steer through a systematic and comprehensive implementation of the Cybersecurity

FMEA, ensuring the necessary adjustments are made to effectively address cybersecurity risks and vulnerabilities.

The subsequent sections collectively tackle the second research question:

- How should such a Cybersecurity FMEA be structured?

Insights will be developed and guidance on creating a robust Cybersecurity FMEA framework tailored to safeguard technical products against cyber threats by exploring the process step by step.

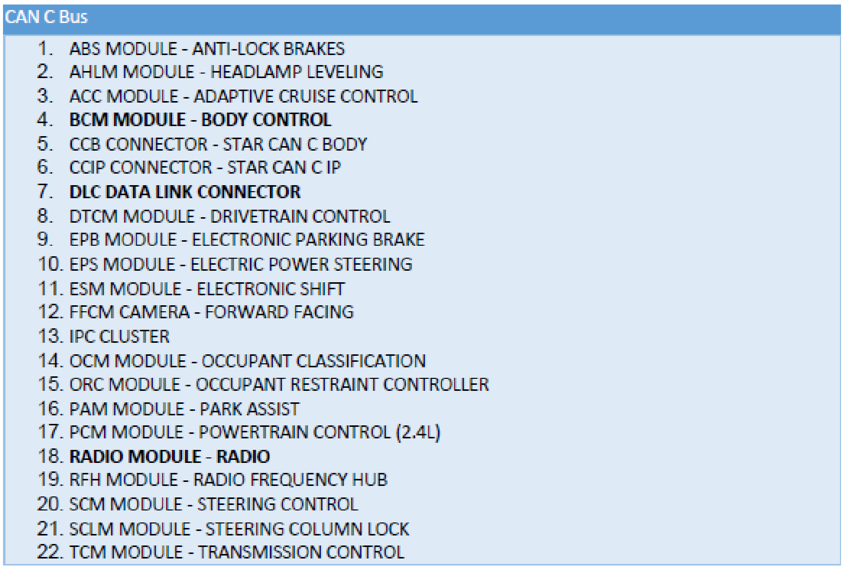
5.3.1 Step 1: Setting the Foundation

In this initial phase of the Cybersecurity FMEA, we follow the tried-and-true patterns seen in other FMEA processes. Key activities include defining the analysis scope, purpose, schedule, assembling the expert team, and identifying necessary tools to guide the entire process from construction to the final FMEA result.

It is good to notice that a Cybersecurity FMEA aligns more closely with the MSR-FMEA methodology. Therefore, essential points and documents utilized in MSR-FMEA also prove valuable in defining Cybersecurity FMEA. These important documents contain HARA, TARA, technical requirements, diagrams, parts lists, and function types accessible to the vehicle user within the system. Additionally, understanding how the OEM plans to release future software updates becomes paramount. With these matters firmly established and the scope well-defined for the team, we can proceed to the next phase of the Cybersecurity FMEA implementation.

5.3.2 Step 2: Constructing the Cybersecurity Structure Tree

Continuing with a familiar approach, we employ the same logic seen in Figure 14 of this paper to build the Cybersecurity FMEA's structure tree. In this step, we focus on software and architecture enclosing the systems susceptible to cyber threats. Unlike other FMEA types that might display hardware and individual parts on the structure tree, the Cybersecurity FMEA emphasizes items predisposed to attacks.



CAN C Bus

1. ABS MODULE - ANTI-LOCK BRAKES
2. AHLM MODULE - HEADLAMP LEVELING
3. ACC MODULE - ADAPTIVE CRUISE CONTROL
4. **BCM MODULE - BODY CONTROL**
5. CCB CONNECTOR - STAR CAN C BODY
6. CCIP CONNECTOR - STAR CAN C IP
7. **DLC DATA LINK CONNECTOR**
8. DTCM MODULE - DRIVETRAIN CONTROL
9. EPB MODULE - ELECTRONIC PARKING BRAKE
10. EPS MODULE - ELECTRIC POWER STEERING
11. ESM MODULE - ELECTRONIC SHIFT
12. FFCM CAMERA - FORWARD FACING
13. IPC CLUSTER
14. OCM MODULE - OCCUPANT CLASSIFICATION
15. ORC MODULE - OCCUPANT RESTRAINT CONTROLLER
16. PAM MODULE - PARK ASSIST
17. PCM MODULE - POWERTRAIN CONTROL (2.4L)
18. **RADIO MODULE - RADIO**
19. RFH MODULE - RADIO FREQUENCY HUB
20. SCM MODULE - STEERING CONTROL
21. SCLM MODULE - STEERING COLUMN LOCK
22. TCM MODULE - TRANSMISSION CONTROL

Figure 22 - CAN C Bus from Jeep Cherokee [38]

For instance, let us consider the hack described in Chapter 4 involving the Jeep Cherokee architecture, which includes CANs and Radio networks. To fill in the structure tree for this system, we would identify the modules present in each network, shedding light on possible hackable units that could compromise the vehicle's integrity, driver safety, or information privacy. Figure 22 provides an example of the Jeep Cherokee CAN C Bus with its corresponding modules. By following this approach, the Cybersecurity FMEA structure tree becomes vital in understanding the vulnerabilities within interconnected systems and proactively and comprehensively guiding risk assessment.

Presented below is an illustrative representation of how the structure tree might be organized:

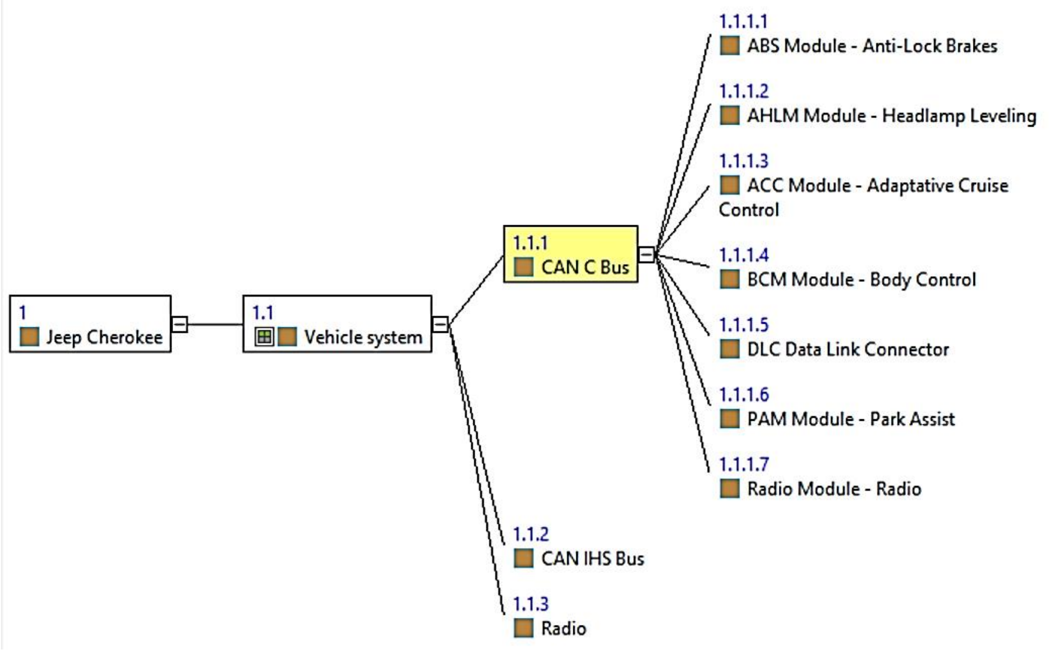


Figure 23 - Example of a structure tree for a Cybersecurity FMEA

Please note that this is just an example, and the actual structure of the tree may vary depending on the specific vehicle model and its cybersecurity aspects.

5.3.3 Step 3: Functional Analysis

Building upon the MSR-FMEA's foundation, the next step is conducting a comprehensive analysis of the system's functions. In this phase, we identify and depict the functions within the system that may be vulnerable to cyberattacks. Like the "special characteristics" in DFMEA, the Cybersecurity FMEA might consider specific functions that could be targeted at any level, requiring varying degrees of security against potential attacks. This functional analysis is crucial in understanding the system's potential weak points and allows us to devise tailored security measures to fortify these critical functions against cybersecurity threats.

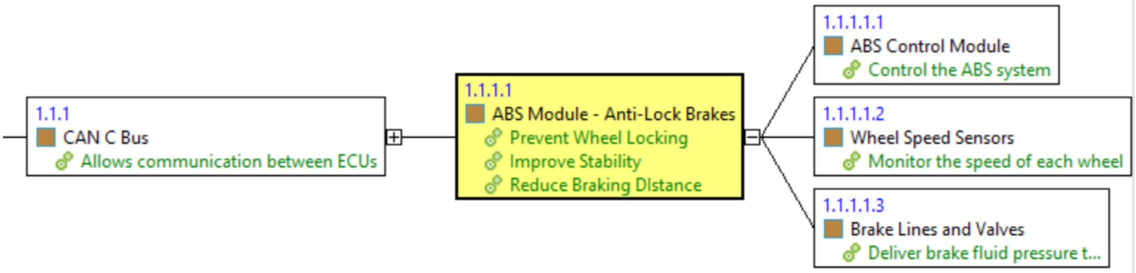


Figure 24 - Function tree for the structure defined

5.3.4 Step 4: Failure Analysis

Moving on to the most critical step of the Cybersecurity FMEA, key aspects are outlined that ensure a coherent analysis between the previously defined functions and the potential failure causes, which involve triggers, vulnerabilities, or weaknesses in the case of the Cybersecurity FMEA. Similar to the DFMEA, it is vital to avoid vague or poorly described malfunctions that may lead to insignificant results. For the Cybersecurity FMEA, improperly allocated vulnerabilities, such as "can be hacked," can restrain a comprehensive risk analysis later.

With the foundation set and the Cybersecurity FMEA structure tree in place, we progress to Step 4. Here, the focus is on identifying the potential failure causes that align with the functions outlined in Step 3. These failure causes may lead to cybersecurity breaches or attacks on the system. In this step, it is necessary to establish a clear and coherent relationship between the functions and the identified failure causes. A well-defined mapping ensures that all function's potential vulnerabilities are accurately assessed, and appropriate mitigation strategies can be planned to enhance cybersecurity measures.

To illustrate this process, let us keep using the example of the ABS module in the Jeep Cherokee 2014 Model:

➢ Function: Prevent Wheel Locking
- Possible Vulnerability: Exploitable Weakness in the ABS Control Module's Software
- Failure Cause: Inadequate Software Security Measures

➢ Function: Improve Stability
- Possible Vulnerability: Susceptibility of Wheel Speed Sensors to Tampering
- Failure Cause: Insufficient Physical Protection of Wheel Speed Sensors

➢ Function: Reduce Braking Distance
- Possible Vulnerability: Vulnerable Communication on the CAN C Bus
- Failure Cause: Lack of Secure Communication Protocols

By identifying these specific failure causes that correspond to the functions of the ABS module, we can gain a comprehensive understanding of potential cybersecurity risks associated with this critical component. This failure analysis is essential in guiding subsequent steps in the Cybersecurity FMEA, such as risk assessment and implementing tailored security measures.

As we proceed with the Cybersecurity FMEA, it is important to remember that the effectiveness of the analysis relies on the accuracy and clarity of the identified failure causes. A precise and well-structured analysis will pave the way for robust cybersecurity measures, ensuring the protection of technical products against cyber threats and supporting the overall strength of the automotive industry in the face of evolving cybersecurity challenges.

5.3.5 Step 5: Risk Analysis - Bridging ISO21434 and Cybersecurity FMEA

In the risk analysis phase, we have a valuable opportunity to integrate elements from ISO21434, particularly Chapter 8, to further enhance the Cybersecurity FMEA process. This step involves evaluating action priorities and requires collaboration with cybersecurity specialists to gain a comprehensive overview of addressing risks effectively and efficiently. Through this collaboration, we can identify areas that demand swift and targeted action and those that may require more extensive changes when prevention or mitigation actions prove challenging.

ISO21434's Cybersecurity Monitoring, which involves analyzing potential cybersecurity events, aligns seamlessly with the risk analysis phase of Cybersecurity FMEA. By combining strategies used in ISO21434 with the risk analysis process, we can more accurately assess the significance and potential impact of failures. This merger allows for a comprehensive evaluation of potential consequences and the likelihood of exploitation, enhancing the overall risk analysis.

The risk analysis in Cybersecurity FMEA draws on the rich methodology of ISO21434, enabling a comprehensive approach to address specific cybersecurity concerns effectively. This convergence of methods and principles entrusts organizations to make informed decisions on prioritizing actions and allocating resources to fortify technical products against cyber threats.

By leveraging ISO21434's insights, methodologies, and specific items, the risk analysis phase becomes a pivotal step in the Cybersecurity FMEA process. Collaborating with cybersecurity specialists ensures that the risk analysis remains accurate and relevant, making it a fundamental aspect of constructing a robust Cybersecurity FMEA framework.

5.3.6 Step 6: Optimization - Strengthening Cybersecurity Measures

The Cybersecurity FMEA team has completed defining and ranking all the main activities at this stage. The focus now shifts to prioritizing tasks that aim to reduce or mitigate cyberattacks, ensuring that each vulnerability identified earlier has a well-defined action plan. Setting deadlines and assigning responsible individuals for each task is crucial to facilitate effective follow-up and implementation.

Establishing a robust system for exchanging documentation related to these tasks becomes imperative to ensure seamless coordination and efficiency. Keeping track of progress and maintaining clear communication channels among team members will foster a proactive approach to addressing cybersecurity risks.

5.3.7 Step 7: Results Documentation - Communicating and Archiving Findings

As the Cybersecurity FMEA analysis concludes at this step, the paramount focus lies in communicating the results effectively. Sharing the findings with relevant stakeholders ensures that key insights and risk mitigation strategies are distributed across the organization.

Additionally, maintaining a comprehensive archive of these documents is of utmost importance. This information storage will be valuable for future consultations, supporting ongoing improvement efforts and strengthening the organization's cybersecurity resilience. By documenting the results meticulously, the Cybersecurity FMEA process becomes a valuable knowledge base, continuously contributing to enhancing cybersecurity measures.

5.4 Integration of Cybersecurity FMEA into Existing Risk Management Processes

With the Cybersecurity FMEA analysis completed and results at hand, the next crucial step involves seamlessly integrating the findings into the active Cybersecurity Management processes of the companies. Chapter 6 of the State-of-the-Art Cybersecurity Standards for Vehicles encompasses three vital sections: Cybersecurity Case, Cybersecurity Assessment, and Release to post-development. If the Original Equipment Manufacturer (OEM) already has these processes in place, the Cybersecurity FMEA results can be seamlessly incorporated into the Cybersecurity Case and Assessment.

The Cybersecurity FMEA provides invaluable insights that might not have been previously considered in the Technical Architecture Risk Assessment and other methods used during the vehicle system's implementation. By utilizing the Cybersecurity FMEA results, companies can enhance their understanding of potential vulnerabilities and devise more robust activities to mitigate cyber threats effectively. Integrating these insights into the existing Cybersecurity Management processes further strengthens the overall security posture of the vehicle system, contributing to a safer and more resilient technological landscape.

6 Conclusion

This thesis extensively explored cybersecurity for technical products, particularly in the automotive industry. With the continuous evolution of vehicles, incorporating advanced technologies such as connectivity, automation, and IoT, the need for robust cybersecurity measures has become paramount. However, ensuring the seamless integration of cybersecurity throughout the product development process poses significant challenges for engineers, safety experts, and development staff.

To address this complexity and soothe the limitation of cybersecurity implementation, the study focused on an in-depth investigation of cybersecurity norms and standards, drawing insights from real-world incidents and leveraging the proven efficacy of Failure Mode and Effects Analysis. A practical and effective solution, the Cybersecurity FMEA, was developed by combining these elements.

The key concepts of cybersecurity and the norms and standards guiding the automotive industry in securing technical products were thoroughly examined throughout the research. Understanding the implications of the Jeep Cherokee incident shed light on potential vulnerabilities and underscored the urgency of robust cybersecurity measures.

The approach was tailored to align with cybersecurity demands based on the knowledge acquired during the thesis process. The Cybersecurity FMEA framework emerged as a viable and promising solution, offering a systematic and proactive methodology to effectively identify and mitigate cybersecurity risks. As with any new concept, further refinement and adaptation are necessary to ensure the seamless integration of the Cybersecurity FMEA within OEMs and other technical product development processes. The framework's potential benefits and tangible results make it an exciting avenue for future research and implementation.

In conclusion, this thesis highlights the significance of cybersecurity in the automotive industry and presents a promising approach to address cybersecurity challenges through the Cybersecurity FMEA framework. By continuously advancing our understanding of cybersecurity, refining the methodology, and collaborating across disciplines, a safer and more secure technological landscape can be formed, protecting customers and automotive systems from cyber threats.

7 References

[1] “vehicle,” URL: https://dictionary.cambridge.org/dictionary/english/vehicle [retrieved 24 June 2023].

[2] Richter, F., “Big Data on Wheels,” *Statista*, 9 Feb 2017, URL: https://www.statista.com/chart/8018/connected-car-data-generation/ [retrieved 22 March 2023].

[3] Martin, H., Ma, Z., Schmittner, C., Winkler, B., Krammer, M., et al., “Combined automotive safety and security pattern engineering approach,” *Reliability Engineering & System Safety*, Vol. 198, 2020, p. 106773. doi: 10.1016/j.ress.2019.106773

[4] Ghadhab, M., Junges, S., Katoen, J.-P., Kuntz, M., and Volk, M., “Safety analysis for vehicle guidance systems with dynamic fault trees,” *Reliability Engineering & System Safety*, Vol. 186, 2019, pp. 37–50. doi: 10.1016/j.ress.2019.02.005

[5] Schmittner, C., Ma, Z., Schoitsch, E., and Gruber, T., “A Case Study of FMVEA and CHASSIS as Safety and Security Co-Analysis Method for Automotive Cyber-physical Systems,” *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security,* ASIA CCS '15: 10th ACM Symposium on Information, Computer and Communications Security, Singapore Republic of Singapore, 14 04 2015 14 03 2015, edited by J. Zhou and D. Jones, ACM, New York, NY, USA, 2015, pp. 69–80. doi: 10.1145/2732198.2732204

[6] Cybercrimemag, “Cybercrime To Cost The World $10.5 Trillion Annually By 2025,” URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ [retrieved 13 March 2023].

[7] Statista, “Leading global data breach methods 2019 | Statista,” URL: https://www.statista.com/statistics/221390/share-of-hacking-methods-across-organizations/ [retrieved 13 March 2023].

[8] Christoph, S., Gruber, T., Puschner, P., and Schoitsch, E., “Security Application of Failure Modes and Effect Analysis (FMEA),”.

[9] Altawairqi, A. and Maarek, M., “Attack Modeling for System Security Analysis,” *Computer Safety, Reliability, and Security,* edited by S. Tonetta, E.

Schoitsch and F. Bitsch, Springer International Publishing, Cham, 2017, pp. 81–86.

[10] Schmittner, C., Ma, Z., Reyes, C., Dillinger, O., and Puschner, P., “Using SAE J3061 for Automotive Security Requirement Engineering,” *Computer Safety, Reliability, and Security,* edited by A. Skavhaug, J. Guiochet, E. Schoitsch and F. Bitsch, Springer International Publishing, Cham, 2016, pp. 157–170.

[11] Synopsys, “Securing the Modern Vehicle - A Study of Automotive Industry Cybersecurity Practices,” URL: https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/securing-the-modern-vehicle.pdf [retrieved 13 March 2023].

[12] Vehicle Cybersecurity Systems Engineering Committee, “J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,” SAE International, 400 Commonwealth Drive, Warrendale, PA, United States.

[13] International Standard, “ISO/SAE 21434 - Road vehicles - Cybersecurity engineering,” ISO/SAE International, 2021.

[14] “IEC 60050 - International Electrotechnical Vocabulary - Details for IEV number 351-57-01: "hazard",” URL: https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=351-57-01 [retrieved 16 April 2023].

[15] YSEC, “Safety vs. security - how can divergence become convergence?,” URL: https://www.security-analyst.org/safety-vs-security-how-can-divergence-become-convergence/ [retrieved 23 April 2023].

[16] Leveson, N., *Engineering a safer world. Systems thinking applied to safety,* The MIT Press, Cambridge, Massachusetts, 2017, 534.

[17] James, M., “Threats versus hazards: The role of SAE J3061 in automotive software development - LDRA,” URL: https://ldra.com/threats-versus-hazards-the-role-of-sae-j3061-in-automotive-software-development/ [retrieved 7 May 2023].

[18] “Case: The Ford Pinto | Business Ethics,” URL: https://philosophia.uncg.edu/phi361-matteson/module-1-why-does-business-need-ethics/case-the-ford-pinto/ [retrieved 7 June 2023].

[19] *FMEA - Einführung und Moderation. Durch systematische Entwicklung zur übersichtlichen Risikominimierung : mit 114 Abbildungen,* 2nd ed., Springer Vieweg, Wiesbaden, op. 2012, XXI, 265 str.

[20] Khalid Khan, S., Shiwakoti, N., and Stasinopoulos, P., "A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles," *Accident; analysis and prevention*, Vol. 165, 2022, p. 106515.
doi: 10.1016/j.aap.2021.106515

[21] Beverly White, *Risk Analysis Using Failure Modes and Effects Analysis (FMEA). FMEA Made Easy,* Independently published, 2022.

[22] Mohammed Hamed Ahmed Soliman, *Risk Assessment Using FMEA. A Case of Reliable Improvement,* Independently published, 2021.

[23] Oliveira, J., Carvalho, G., Cabral, B., and Bernardino, J., "Failure Mode and Effect Analysis for Cyber-Physical Systems," *Future Internet*, Vol. 12, No. 11, p. 205.

[24] OG_C1, "Booklet No. 14 Failure Mode and Effects Analysis FMEA," URL: https://assets.bosch.com/media/global/bosch_group/purchasing_and_logistics/information_for_business_partners/downloads/quality_docs/general_regulations/bosch_publications/booklet-no14-failure-mode-and-effects-analysis_EN.pdf [retrieved 24 June 2023].

[25] Automotive Industry Action Group, *The FMEA handbook. Failure mode and effects analysis,* Automotive Industry Action Group, Southfield, Michigan, 2019, 236.

[26] Quality-One | Quality and Reliability Consulting - Training - Facilitation, "FMEA | Failure Mode and Effects Analysis | Quality-One," URL: https://quality-one.com/fmea/ [retrieved 19 June 2023].

[27] QualityTrainingPortal, "What is an FMEA-MSR? Here are some quick answers," *Resource Engineering, Inc./QualityTrainingPortal.com*, 24 Jan 2018, URL: https://fmea-training.com/fmea-msr-facts/ [retrieved 25 June 2023].

[28] Team, R., “A Guide to AIAG & VDA FMEAs in Relyence,” *Relyence Corporation*, 2 May 2022, URL: https://relyence.com/2022/05/02/a-guide-to-aiag-vda-fmeas-in-relyence/ [retrieved 25 June 2023].

[29] “The Practitioners Guide: 2019 AIAG-VDA FMEAs,” URL: https://mcusercontent.com/59732fafdc1daae4f3d97568a/files/9f67b1ff-701b-12b1-3fdb-0f090e1444e7/practitioners_guide_aiag_vda_fmeas.02.pdf?mc_cid=91330bf29f&mc_eid=fb0b719539 [retrieved 25 June 2023].

[30] “SAE_FMEA,” 2nd Edition, 1995, URL: https://www.lehigh.edu/~intribos/Resources/SAE_FMEA.pdf [retrieved 6 March 2023].

[31] QualityTrainingPortal, “Design vs. Process FMEAs,” *Resource Engineering, Inc./QualityTrainingPortal.com*, 23 Jul 2016, URL: https://fmea-training.com/design-vs-process-fmeas/ [retrieved 25 June 2023].

[32] Hunt, J., “Introducing the AIAG-VDA DFMEA,” 3 Jul 2019, URL: https://my.omnex.com/articles/introducing-the-aiag-vda-dfmea/ [retrieved 2 July 2023].

[33] Mary Rowzee, “Understanding AIAG-VDA’s FMEA Process and Approach,” URL: https://www.qualitydigest.com/inside/lean-article/understanding-aiag-vda-s-fmea-process-and-approach-061820.html [retrieved 4 July 2023].

[34] Dijaz Maric, “FMEA monitoring and system response,” *Lorit Consultancy GmbH*, 3 May 2023, URL: https://lorit-consultancy.com/en/2023/05/fmea-monitoring-and-system-response/ [retrieved 9 July 2023].

[35] Daniel Mormul, “FMEA for Monitoring and System Response,” *PROQUAL Management Institute*, 15 Dec 2021, URL: https://proqual.pl/en/knowledge-zone/fmea-for-monitoring-and-system-response/ [retrieved 9 July 2023].

[36] Team ZCySec, “Automotive Cyber Security In 2023,” URL: https://zcybersecurity.com/car-automotive-cyber-security/ [retrieved 10 July 2023].

[37] Security, P., “White Hat Hackers: How Ethical Hacking Works - Panda Security,” URL: https://www.pandasecurity.com/en/mediacenter/panda-security/white-hat-hacker/ [retrieved 17 July 2023].

[38] Dr. Charlie Miller, Chris Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” 2015.

[39] “What is Vehicle Telematics? Definition and FAQs | HEAVY.AI,” URL: https://www.heavy.ai/technical-glossary/vehicle-telematics [retrieved 21 July 2023].

[40] Greenberg, A., “Hackers Remotely Kill a Jeep on the Highway—With Me in It,” *WIRED*, 21 Jul 2015, URL: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [retrieved 21 July 2023].

[41] YouTube, “DEF CON 23 - Charlie Miller & Chris Valasek - Remote Exploitation of an Unaltered Passenger Vehicle,” URL: https://www.youtube.com/watch?v=OobLb1McxnI [retrieved 24 July 2023].