THESIS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

Automotive Cybersecurity: From Risk Assessment to Mitigation

ALJOSCHA LAUTENBACH

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Göteborg, Sweden 2025

Automotive Cybersecurity: From Risk Assessment to Mitigation
Aljoscha Lautenbach
ISBN 978-91-8103-223-9

Acknowledgements, dedications, and similar personal statements in this thesis, reflect the author's own views.

Doktorsavhandlingar vid Chalmers tekniska högskola
Ny serie nr 5681
ISSN 0346-718X

Department of Computer Science and Engineering
Chalmers University of Technology
SE-412 96 Göteborg
Sweden
Phone number: +46 (0)31-772 1000

Printed by Chalmers Digitaltryck
Göteborg, Sweden 2025

Automotive Cybersecurity: From Risk Assessment to Mitigation

Aljoscha Lautenbach

Department of Computer Science and Engineering, Chalmers University of Technology

ABSTRACT

As road vehicles are increasingly defined by their software capabilities and connected service infrastructure, it has become widely accepted that cybersecurity is vital to keep road users and their environment safe and secure. Failures of vehicular cybersecurity can lead to loss of life, severe injuries, financial losses and breaches of privacy.

Automotive system development faces several challenges, including long development lead times and system life-times, highly heterogeneous hardware, multi-tiered supply chains and legal, safety and real-time requirements. These challenges frame the available design choices. An effective cybersecurity concept must be rooted in a thorough understanding of the risks associated with connected vehicles. Furthermore, efficient processes are essential for responding to newly discovered vulnerabilities and incidents. This thesis aims to deepen our understanding of these issues through three primary objectives: (1) to explore the systematization of threat analysis and risk assessment to facilitate cybersecurity requirements engineering, (2) to examine how cybersecurity engineering processes can be implemented to address cybersecurity issues effectively, and (3) to analyze the influence of automotive technology on the design of cybersecurity measures.

The first part of this thesis focuses on risk assessment and standardization by (a) developing a risk assessment methodology which influenced ISO/SAE 21434, an automotive cybersecurity engineering standard, (b) updating the risk assessment methodology to fully align with the standard, and (c) critically analyzing ISO/SAE 21434 to identify conceptual weaknesses, while proposing improvements to its threat analysis and risk assessment framework, and vulnerability and incident handling processes. The second part focuses on the design and implementation of risk mitigation measures by examining (i) common automotive cybersecurity design issues, (ii) memory exploitation and protection techniques for resource-constrained electronic control units, (iii) the impact of the CAN bus's technical constraints on authentication protocols and (iv) the potential of 5G telecommunication technology to strengthen security in vehicle-to-everything communication.

Keywords: Automotive Cybersecurity, Automotive Risk Assessment, ISO/SAE 21434, In-Vehicle Network, CAN authentication, Memory Protection, V2X Security, Vulnerability Management, Incident Handling

LIST OF PUBLICATIONS

This thesis is based on the work contained in the following papers, referred to by roman letters in the text:

A Mafijul Md. Islam, **Aljoscha Lautenbach**, Christian Sandberg and Tomas Olovsson. "A Risk Assessment Framework for Automotive Embedded Systems". In *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security (CPSS '16)*[1]. Pages 3–14. Association for Computing Machinery, New York, NY, USA. 2016.

B **Aljoscha Lautenbach**, Magnus Almgren and Tomas Olovsson. "Proposing HEAVENS 2.0 – an automotive risk assessment model ". In *Proceedings of the 5th ACM Computer Science in Cars Symposium (CSCS '21)*. Article 5, pages 1–12. Association for Computing Machinery, New York, NY, USA. 2021.

C Daniel Grimm, **Aljoscha Lautenbach**, Magnus Almgren, Tomas Olovsson and Eric Sax. "Gap Analysis of ISO/SAE 21434 – Improving the Automotive Cybersecurity Engineering Life Cycle". In *2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC)*. Pages 1904-1911. IEEE. 2023.

D **Aljoscha Lautenbach**, Magnus Almgren and Tomas Olovsson. "Understanding Common Automotive Security Issues and Their Implications". In *Hamid, B., Gallina, B., Shabtai, A., Elovici, Y., Garcia-Alfaro, J. (eds) Security and Safety Interplay of Intelligent Software Systems (CSITS 2018, ISSA 2018)*. Lecture Notes in Computer Science, vol 11552, pages 19 – 34. Springer, Cham. 2019.

E **Aljoscha Lautenbach**, Magnus Almgren and Tomas Olovsson. "What the stack? On Memory Exploitation and Protection in Resource Constrained Automotive Systems". In *D'Agostino, G., Scala, A. (eds) Critical Information Infrastructures Security (CRITIS 2017)*. Lecture Notes in Computer Science, vol 10707, pages 185—193. Springer, Cham. 2018.

F Nasser Nowdehi, **Aljoscha Lautenbach** and Tomas Olovsson. "In-vehicle CAN Message Authentication: An Evaluation Based on Industrial Criteria". In *2017 IEEE 86th Vehicular Technology Conference (VTC2017-Fall)*. Pages 1–7. IEEE. 2017.

G **Aljoscha Lautenbach**, Nasser Nowdehi, Tomas Olovsson and Romi Zaragatzky. "A preliminary security assessment of 5G V2X". In *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*. Pages 1–7. IEEE. 2019.

[1] This paper received the best-paper award at CPSS 2016

Acknowledgments

First of all, I owe a debt of gratitude to my supervisors Prof. Tomas Olovsson and Prof. Magnus Almgren for their advise, insights, support and patience over many years. For ensuring the proper process and quality of my PhD studies, I am also grateful to my examiner Prof. Johan Karlsson and the various directors of graduate studies who have chaired my "follow-up meetings": Prof. Gerardo Schneider, Prof. Jan Jonsson, Prof. Agneta Nilsson, Prof. Wolfgang Ahrendt, and Prof. Nir Piterman. I would also like to thank my defense opponent Prof. Panagiotis Papadimitratos and my grading committee consisting of Prof. Maria Kihl, Prof. Nele Mentens and Prof. Alexandre Bartel for generously giving their time, carefully reading my work, and offering valuable feedback and suggestions.

During my time at Chalmers, I had the pleasure of meeting many brilliant people who made it an enjoyable place to study and work. I have lost touch with many of them by now, but I am still grateful for the good times that we have shared. A special thanks to my master thesis supervisor Risat, without whom I may not have started my PhD studies. To the automotive security research group, Pierre, Nasser, Boel, Thomas R and Kim, thank you for the many interesting discussions and being good colleagues! My office mates from three different offices Jochen, Michal, Nick, Anton, Beshr, Nasser and Thomas R also helped immensely in creating a welcoming working environment. During my year in the board of Doktorandsektionen, I especially appreciated the friendship and guidance of Linnea, Maria, Anna K, Elke, Onur, Cristina, Silvia and Oskar. I have similarly good memories of my time in the CSE PhD Council with Elena, Nadja, Jeff, Herbert and Grischa. In the network and systems division, I am happy to have met Valentin, Bapi, Nhan, Yiannis, Iosif, Thomas P, Aras, Ivan, Wissam, Carlo, Hannah, Fazeleh, Babis, Christos, Dimitris, Amir, Bastian, Laura, Georgia, Klondike, Vincenzo, Ali, Romaric, Elad, Tomas, Magnus, Marina, Olaf, Phillipas, Peter, and finally Erland, who sadly is no longer with us. I was also fortunate to enjoy a good conversation, board games, cultural exchanges or the occasional beer with Pablo,

Bart, Luciano, Daniel Ha, Daniel S, Alexander, Per, Hamid, Raul, Evgeny, Marco, Steven, Musard, Andrei, Alejandro, Dave, Wolfgang, Gerardo, Behrooz, Fatemeh, Dmitry, Stavros, Nicole and Hedy.

Furthermore, I am thankful for my current colleagues at Evidente who provide a great place to work.

It was a also true pleasure to organize the PhD pubs with Elke, Isabel, Iosif, Sigrid, Siavash, Alla, Paulo, Aykut, Monika and Ali! Unfortunately, it seems the PhD pubs died of COVID. I am also grateful for the fun I have had playing Skat and Doppelkopf with Thomas, Eike, Herbert, Daniel and Charlotte, playing Badminton with Anna, Aidin, Justin, Melinda, Brian, Anja and Ben, and discussing politically or morally interesting questions with the "Rumble in the pub" crew, including Edit, Brian, Farzaneh, Nicole, and Piotr.

I would also like to take this opportunity to thank the members of my old badminton club HEEP for having been an integral part of my life back then, with special mention of my fellow board members Marjan, Ellen and Eddy, and my fellow Thembi connoisseurs David and Reinier. Similarly, my academic life in Maastricht would not have been half as fun without Roland, Bart, Anna, Daan, Irmin, Max, Bene, and finally Kalle, who died much too young. I miss you my friend. Special thanks also to Sascha, Christoph and Freddy, who have stuck with me for close to 25 years.

I will inevitably have forgotten to mention someone important: my apologies to you.

I am lucky to have a loving family who has supported me in all my endeavors. Vielen lieben Dank, Walter, Frauke und Sina: ich weiß eure Unterstützung sehr zu schätzen, auch wenn ich es eventuell nicht oft genug sage. I would also like to acknowledge the memory of my uncle Jörg, who always inspired me.

Finally, I would like to thank my wonderful wife Melisa for her patience, love and support throughout this long journey. Ti si nevjerovatna, na dobar način. Volim te!

Aljoscha Lautenbach
Göteborg, 30th of September, 2025

Contents

List of Figures

List of Tables

Part I

Thesis overview

Introduction

"Cars are just computers with four wheels and an engine. It's no surprise that the software is vulnerable, and that everything is connected."

– Bruce Schneier,
December 2022

As technology continues to advance — becoming smaller, faster and more energy efficient — a growing number of devices and machines, including vehicles and their environments, are being connected. Modern drivers expect their vehicles to provide time-efficient routes, real-time updates on traffic and weather, and access to news and entertainment. Seamless smart-phone integration is a given [93], as are advanced driver-assistance systems (ADAS) like traffic sign recognition and hazard detection [27, 73], while intelligent transportation systems (ITS) optimize traffic safety and flow. These advancements demand high connectivity and increase system complexity [93] through the use of emerging technologies such as artificial intelligence and the growing use of sensors and actuators for environmental interaction. These innovations, however, bring heightened cybersecurity risks [15, 52, 77, 93], which we explore in this thesis.

It may be noteworthy that cybersecurity is distinct from safety. While the goals of cybersecurity and safety are the same, namely the protection of the system and the humans operating in the system's environment, their underlying fault model is different: cybersecurity is generally concerned with protection against intentional malicious manipulation, whereas safety is primarily concerned with protection against random faults [5, 33, 78].

Thesis structure. Part I introduces the overall challenges addressed in this thesis and places the work in its context. In section 1, we present the motivation for the thesis, including the challenges of automotive system development, the need for cybersecurity, and the knowledge gap regarding

automotive cybersecurity. In section 2, the necessary background is introduced, including the legal context, standardization, the automotive life-cycle, and automotive technology with a focus on electronic control units and communication systems. In section 3, we outline the objectives of the thesis, the research questions that have driven the work and how the different papers address the research questions. In section 4, we present the problem statement and contributions for each paper. In section 5, we provide a brief summary of our contributions and concluding remarks.

Parts II and III contain the papers which constitute the main part of this thesis: In part II, we address aspects of risk assessment and standardization, covering papers A to C, and in part III, we investigate automotive cybersecurity measures, covering papers D to G.

1 Motivation

Automotive systems, as almost all embedded systems, were traditionally designed without cybersecurity concerns in mind. One obvious reason is that when electronic control units (ECUs) first started to appear in vehicle design over 40 years ago, they had no or very limited connectivity and cybersecurity was of little concern in general [52, 85]. In the 1990s, ECUs started to supplant mechanical controls in vehicle functions and the in-vehicle network grew in complexity [52, 83, 85]. At this point, it may have been prudent to start considering cybersecurity, but in the early 2000s when the first research papers started to appear on the topic, most vehicles still had no protection against malicious manipulation [53, 62, 103]. Consequently, it became clear that more research on this topic was needed in order to understand the risks involved, as well as to propose strategies and processes to protect vehicles against malicious manipulation [15, 52, 103].

1.1 Challenges in automotive system development

The automotive industry faces challenges that set it apart from many other industries and which make software development and cybersecurity difficult. Some of these challenges are shared across embedded systems industries, while others are specific to the transportation sector and the automotive industry in particular. In the context of this work, the most important challenges that automotive systems face are:

- **Long product life-times** (10 - 20 years). This implies that chosen cybersecurity measures must work for up to 20 years. New hardware and software vulnerabilities are found regularly,

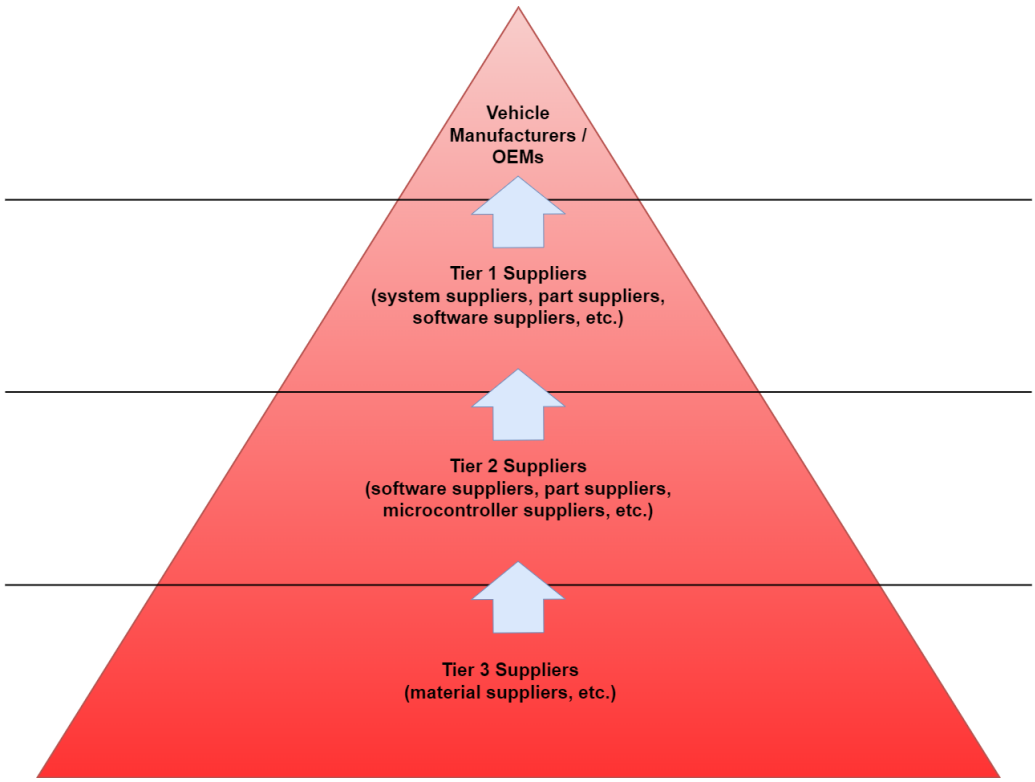


Figure 1: Automotive supplier relationships

which necessitates secure software updates so the vulnerabilities can be addressed in a timely manner [19, 23].

- **Long development lead times** (~5 years), and thus slow adoption of new technology [24]. Old electronic control units (ECUs) that do not support remote software updates are replaced slowly so that remote software updates are still not available for every piece of software in a vehicle since.

- **High cost pressure** to stay competitive with small profit margins [8, 9], in particular for passenger cars. This leads to **resource-constrained systems** that are minimal and efficient. Automotive systems used to be highly heterogeneous with specifically tailored hardware of

different processor architectures which only had as much computing power and memory as absolutely necessary. A more recent trend is to reduce the number of physical ECUs by replacing them with virtual ECUs that run on more powerful hardware, but there is still a strong need for efficiency due to market pressures.

- **Energy efficiency requirements** to save fuel and electricity, avoid cooling problems and stay competitive [16].

- **Different legal requirements** across regions that vehicle manufacturers must conform to in order to maintain access to those markets [23, 63, 81].

- **Low latency real-time requirements** and performance demands, alongside **high reliability and safety requirements**.

- **Multi-tiered supply chains** with dozens or hundreds of suppliers. Vehicles have thousands of physical and digital components, and many companies are involved in producing and assembling them [13, 14]. Not only are there many different suppliers for components, there are also *multiple tiers* to the supply chain [70, 72] (cf. figure 1). Tier 1 suppliers sell directly to the vehicle manufacturer, whereas tier 2 suppliers produce parts that are sold to tier 1 or other tier 2 suppliers. Tier 3 suppliers are typically considered to be the suppliers of the raw materials for the parts. For example, a vehicle manufacturer might purchase a complete braking subsystem from a tier-1 supplier. That supplier may, in turn, procure some of the ECUs from a tier-2 supplier, who might further source components, such as specific hardware or software, from other tier-2 or tier-3 suppliers.

  From a security point of view, this layered complexity introduces several technical and organizational challenges [9, 90]. During the development phase, security requirements need to be clearly communicated to all involved parties, which has the potential for misunderstandings and misaligned responsibilities [90]. Furthermore, security risks need to be adequately assessed, but each of the companies may only have a partial system view, and different concerns such as intellectual property and confidentiality concerns may hinder a clear, unimpeded information exchange on the topic. Similarly, if a vulnerability is discovered during the operational phase, it is important that the details are communicated to all relevant parties. Moreover, there must be clear responsibility for addressing the vulnerability, along with a defined timeline for its resolution [17, 45].

These challenges indicate why many of the cybersecurity solutions from the IT domain are not directly applicable in an automotive setting. It is necessary to first understand the automotive context in which the solutions are to be applied, and then to adapt the cybersecurity solutions to the concrete context.

1.2 The need for automotive cybersecurity

Several factors have contributed to the sharp rise in importance of cybersecurity in the automotive industry over the last two decades. One of the factors is that many automotive systems have transitioned from being mechanical or analog to digital, including safety-critical functions such as steering and braking [24]. This lowers production costs, simplifies maintenance and enables advanced signal processing on relatively simple hardware. However, it also enables malicious manipulation since most functions are configurable and controlled by software [11, 15, 52, 97].

Another factor for the increased interest in cybersecurity is that there is a larger trend in society and across all industries to interconnect devices to enable new types of services. The automotive industry is no exception: vehicles connect to cloud services, for instance for remote diagnostics and remote software updates [49, 50, 51], and user expectations are that devices, such as smartphones, integrate seamlessly into the vehicle [93]. As a consequence, attackers have a significantly larger attack surface [15], and the need for cybersecurity rises [15, 52, 77, 93].

Moreover, intelligent transport systems (ITS) are being developed in an effort to increase road safety and traffic flow and they introduce completely new communication channels such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication [20]. This, in turn, poses risks if the communication infrastructure and participating systems are not sufficiently protected [76].

Over the last 20 years, attacks on automotive systems have been demonstrated in theory and practice (cf. fig. 2). In 2004, Wolf et al. [103] were among the first to discuss the lack of cybersecurity features in vehicular networks in a scientific context. Larson and Nilsson highlighted several cybersecurity issues, such as threats emanating from wireless networks in cars [53], and they simulated attacks on the CAN bus [74]. Nilsson et al. [75] conducted similar simulations on the FlexRay bus, and Larson et al. [54] also offered pioneering insights into the potential application of Intrusion Detection Systems (IDS) in vehicular networks. In 2010, Koscher et al. [52] provided an experimental analysis of a vehicular network, and demonstrated practically that once an attacker gains access to the in-vehicle network (for instance via the On-Board Diagnostics, OBD, port),

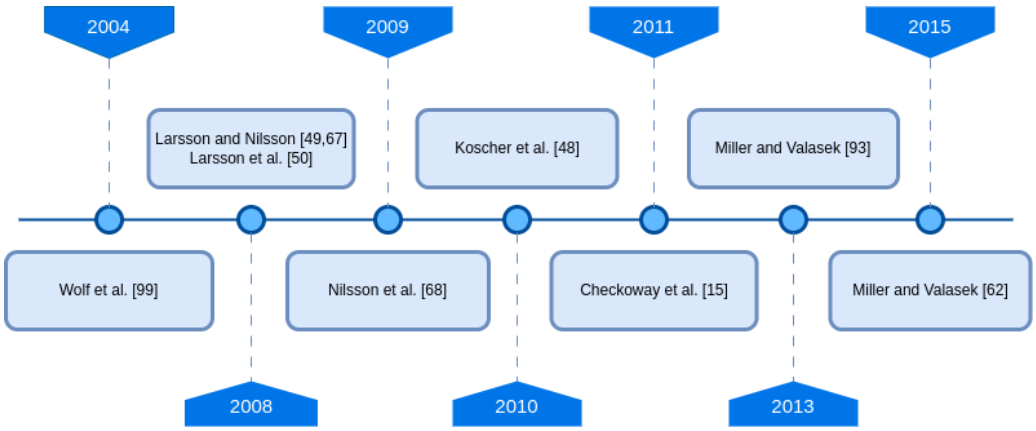


Figure 2: A timeline of selected pioneering research on automotive cybersecurity

it is easy to disrupt and manipulate the vehicle's operations. However, the attacks demonstrated by Koscher et al. still require physical access, which is why Checkoway et al. [15] investigated a vehicle's external attack surfaces to find that many of the communication channels are unprotected. In 2013, Miller and Valasek [97] presented a media effective hack of a Ford Escape and a Toyota Prius via the OBD port. Since then, they have presented new vehicle related cybersecurity issues several years in a row: in 2015, they hacked a Jeep Cherokee remotely with a reporter in it [68]. As a result, public awareness that cybersecurity is needed has risen steadily, and customers start to demand basic cybersecurity and privacy features in vehicles [93].

1.3 The knowledge gap

As previous research has demonstrated, cybersecurity is essential to safeguard automotive systems from malicious manipulation. However, determining the appropriate level of protection requires a thorough understanding of the risks. This enables prioritization, mitigation of the most significant threats, and identification of a threshold where further efforts no longer justify the returns. Additionally, risk assessment helps pinpoint risks that require ongoing monitoring for potential changes. When the research presented in this thesis began in 2013, a flexible framework for automotive risk assessment was still missing.

Some of automotive industry's unique challenges, such as real-time requirements, cost constraints and specialized hardware, demand the use of technologies decidedly different from those in modern information technology. Therefore, to effectively mitigate identified risks, it is crucial to understand how current automotive technologies affect the implementation of cybersecurity measures, and how emerging technologies can be used to their best effect.

Although risk mitigation is important, it is equally valuable to plan for cybersecurity issues such as vulnerability discovery and incident management to ensure operational security and safety. Achieving this requires well-defined and efficient processes—an area that remains underexplored in the context of the automotive industry.

Therefore, the work presented in this thesis is primarily motivated by the need for:

1. Understanding cybersecurity risks of connected vehicles.
2. Effective mitigation of these identified cybersecurity risks by implementing
   (a) cybersecurity measures and
   (b) efficient cybersecurity processes to respond to discovered vulnerabilities and incidents.

2 Background

To gain deeper insight into the needs described in section 1.3 above, this section introduces the legal context and key standards, alongside the automotive life-cycle and technology that shape the implementation of effective cybersecurity measures.

2.1 Legal context, standardization and the automotive life-cycle

As a recent addendum to the 1958 "Agreement Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts [...]"[2] [95], *UNECE Regulation 155 (UNR 155)* [96] requires vehicle manufacturers to fulfill certain cybersecurity requirements in order to get type approval for new vehicles. Among others, these cybersecurity requirements include:

- A documented cybersecurity risk assessment for the entire vehicle and supply-chain

[2] see the citation for the full title

- Implementation of appropriate cybersecurity measures
- The capability to detect and respond to possible cybersecurity attacks
- Log data to support the detection of cyber-attacks and to provide data forensic capability for cyber-attack analysis

UNR 155 is in full effect since July 2024 and is binding in at least 54 countries, including all countries in the European Union (EU), Japan, Australia and the Korean Republic. In other words, all major vehicle manufacturers are required to follow UNR 155 if they want to stay competitive in the global market. Note also that the supply-chain is explicitly included, so although the legal requirements only apply to the vehicle manufacturers, they in turn must push cybersecurity requirements to their suppliers to get type approval in accordance with the 1958 agreement.

Many industries that use embedded systems, in particular in domains with safety-critical applications, have similar legislation already in place. In the EU, the *Medical Device Regulation 2017/745* [25] and the *In-Vitro Medical Device Regulation 2017/746* [26] mandate cybersecurity for certain types of medical devices, as does *section 524B of the Food, Drug and Cosmetics act* in the USA. The *Machinery Regulation 2023/1230* [29] recently adopted in the EU, which specifies essential health and safety requirements for machinery products, also introduces requirements on cybersecurity. Certain types of embedded systems can also fall under *EU directive 2022/2555* [28] *on measures for a high common level of cybersecurity across the Union (NIS2)*, which mandates cybersecurity for critical entities that provide essential services, such as those in banking, transportation, energy and other critical sectors. Even more broadly, *Cyber Resilience Act, EU regulation 2024/2847* [30], which entered into force in December 2024, mandates cybersecurity for all products with digital components. In other words, cybersecurity is no longer optional and heavy fines await companies that do not fulfill the legislative cybersecurity requirements.

The two most influential automotive cybersecurity standards are SAE J3061 and ISO/SAE 21434. In 2016, the SAE International *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061* [84] became the first international standard on automotive cybersecurity. This SAE standard includes an appendix with exemplary risk assessment methods, and one of those is the risk assessment framework presented in paper A, known as the HEAVENS model [1, 42]. SAE J3061 had the crucial role of introducing a larger audience in the automotive domain to cybersecurity engineering, and in 2021 it was superseded by the joint ISO/SAE standard *ISO/SAE 21434 – Road Vehicles – Cybersecurity Engineering* [46]. It describes an overall framework for cybersecurity

engineering, with particular emphasis on threat analysis and risk assessment, and it specifies which work products need to be developed for specific life-cycle phases. Since its initial publication, ISO/SAE 21434 has seen rapid and broad adoption, in large part due to UNECE Regulation 155. Several publications discuss specific aspects of the implications of the ISO/SAE standard and UNR 155, for example Macher et al. [60], Schmittner et al. [88], Gierl, Kristen and Sax [35], Constantino, De Vincenzi, and Matteucci [18], and Greiner et al. [36]. In addition to the HEAVENS model, we also contribute by extending it to fit the requirements in ISO/SAE 21434 in paper B, and by analyzing the standard for potential improvements in paper C.

The automotive life-cycle is an important concept to structure the various life-cycle phases of a vehicle. Different standards and research publications provide slightly different descriptions of the automotive life-cycle, but since the automotive cybersecurity engineering standard ISO/SAE 21434 is directly relevant for this thesis and features prominently in part II, we present the life-cycle described there. The main life-cycle phases are *concept phase*, *product development phase* and *post development phases*, with the post-development phases consisting further of *production*, *operations*, *maintenance* and *decommissioning*. Understanding these automotive life-cycle phases is necessary for the context of part II, specifically papers A, B and C. In the following sub-sections, we describe the concept phase, the product development phase and the post-development phases in some more detail.

Concept and product development

On a high level, the *concept phase* in ISO/SAE 21434 includes the creation of an *item definition*, a *threat analysis and risk assessment* (TARA) and a *cybersecurity concept*, i.e., system requirements for technical and operational controls to mitigate the identified cybersecurity risks. The item definition is a system definition that provides an understanding of the planned functionality, the environment, how the system interacts with its environment and a preliminary architecture.

For threat analysis and risk assessment, the standard defines a framework that follows the workflow depicted in figure 3. Note that the framework only defines the activities that must be completed for the TARA, but the methodology to achieve the required results is almost entirely left to the implementer, although the standard includes a few mandatory aspects and some recommendations. The benefits of systematization of threat analysis and risk assessment are further explored in RQ1 (cf. the thesis objectives in section 3), and a detailed description of each step of the ISO/SAE 21434 TARA framework can be found in paper B.

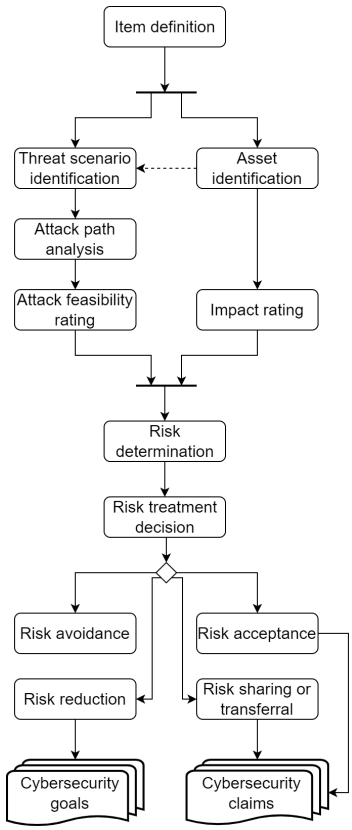


Figure 3: TARA workflow indirectly defined in ISO/SAE 21434

Risk assessment is an essential tool to guide and accompany the development process: An estimated risk rating of a threat helps to determine which threats require cybersecurity measures to mitigate the risk and how stringently the measure must be implemented and verified. Risk is commonly estimated to be the product or a combination of the likelihood and the impact of the threat [43]. There are many risk assessment frameworks, but few were developed specifically for the automotive industry, which was the motivation for paper A. For additional background on different risk assessment frameworks refer to the related work of papers A and B (A.2 and B.6). While paper A describes a risk assessment methodology that predates and has influenced ISO/SAE 21434, paper B aligns the methodology with the standard, and paper C proposes modifications to improve the risk assessment framework in the standard.

An important outcome of the TARA are so called *cybersecurity goals*, which are high-level system requirements, and if appropriate, these goals can be broken down into specific technical and operational cybersecurity requirements. These define the cybersecurity measures that mitigate the corresponding risks, and cybersecurity measures are discussed in part III of this thesis. The goals, requirements and measures are described in the *cybersecurity concept*, including an allocation of measures to components.

The *product development phase* includes activities for *design*, *integration and verification* and *cybersecurity validation*, with implementation being covered implicitly. During product development, the risk assessment needs to be updated regularly. RQ3 (cf. section 3) investigates how automotive technology influences the implementation of cybersecurity controls, which is further explored in part III and papers D, E, F, and G.

Post-development: production, operations, maintenance and decommissioning

In the *post-development phase*, *production* concerns the actual product assembly, including hardware and software installation and configuration. The provisioning of cryptographic keys and certificates happens in production, and it is therefore critical that the cybersecurity requirements are clearly specified in the production control plan and that all involved parties have committed to uphold them. These often include requirements on the production process itself to ensure the integrity of the root of trust and cryptographic materials.

During *operations and maintenance*, the main concerns are secure updates and incident response. For effective and efficient incident response, plans for cybersecurity monitoring and incident handling must be developed in advance, so that related requirements can be taken into

account during the earlier development phase. RQ2 (cf. section 3) delves deeper into the question of how to manage vulnerabilities and incidents effectively, which is explored in paper C.

Finally, cybersecurity concerns during *decommissioning* revolve around secure deletion of sensitive material, such as privacy related data or private cryptographic keys, based on the previously developed post-development requirements.

2.2 Automotive technology: embedded systems and communications

A thorough understanding of automotive technology is required to assess its influence on the design and implementation of cybersecurity measures[3] (cf. RQ3 in section 3). In this section, we therefore discuss *software defined vehicles* and *in-vehicle architectures*, including in-vehicle networks and electronic control units, as well as *intelligent transportation systems*.

Software defined vehicles

The software for modern vehicles contains millions of lines of code, adding significant development costs, while also acting as a value differentiator [13]. In recent years, the idea of *software-defined vehicles* has started to emerge, in reference to concepts such as *software-defined networking* or *software-defined radio*, where previously hardware-controlled behavior is now configured in software. Likewise, the main operations and features of software-defined vehicles are software-controlled, so a vehicle that is equipped with appropriate hardware may receive functional improvements or additional features through software updates. For example, if sufficiently advanced external sensors and computing resources are available, a software update may introduce additional automated driving features through interpreting and acting on the collected sensor data in new ways.

However, the explosion of software in vehicles may also have detrimental effects on cybersecurity. Since software development is a complex activity, it often introduces bugs which may be security relevant [66]. An obvious conclusion is that more software may lead to more cybersecurity vulnerabilities.

[3] We use cybersecurity measures and cybersecurity controls synonymously.

In-vehicle architectures

There are two main types of in-vehicle architectures: *centralized* and *de-centralized* network architectures. For several decades, de-centralized network architectures were most common in vehicle designs, with tight resource-constraints on the hardware. However, recent technical advancements have shifted new designs towards centralized architectures. This change is largely driven by an increasing demand for automated driving solutions, which rely on machine learning algorithms to process large data sets. Such systems require significantly more memory and processing power than was traditionally available in vehicles [6, 64]. Moreover, advances in virtualization technology have provided solutions to ensure the strict separation required for safety-critical systems [6, 64]. However, since this is a relatively recent development, the work in this thesis presupposes de-centralized network architectures and resource-constrained electronic control units (ECUs).

De-centralized in-vehicle networks. In a modern vehicle, most functions are controlled by ECUs: adaptive cruise control, airbag deployment, anti-lock braking system, engine control, interior lighting, remote key-less entry, seat position control, telecommunication, etc. The ECUs which control these functions are interconnected.

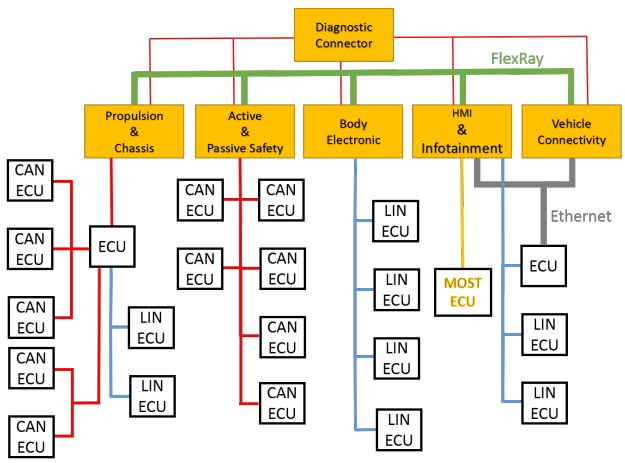


Figure 4: An example of an in-vehicle network with a FlexRay backbone

The communication infrastructure of a vehicle can be divided into its internal communication and its external communication. Internal communication includes signals, i.e., messages, between sensors, actuators and control units, for instance from the throttle sensor to the engine control unit to adjust the vehicle speed. External communication includes communication with intelligent transport systems or remote services such as streaming music or diagnostics servers. Most demonstrated attacks require a multi-layered approach: first the outer layers are compromised to serve as entry points to compromise the inner layers. Therefore, automotive security always needs to be holistic.

Depending on the type of vehicle, the brand and the precise model, it typically contains somewhere between 30 and 150 electronic control units. These ECUs form the internal, or in-vehicle, network. This network consists of several different bus technologies. An example of such an in-vehicle network is depicted in figure 4.

Common automotive buses are the *controller area network (CAN)*, *FlexRay*, *automotive Ethernet*, *local interconnect (LIN)* and *media oriented system transport (MOST)* buses, and every vehicle has an *on-board diagnostics port (OBD-II)*. The most prevalent bus is the CAN bus, which is favored because it is cheap and predictable. Even though the technology is old and slow (max. speed 1 Mbit/s), it is still the most used bus for safety-critical automotive applications [92, 103]. An alternative is the faster but more complex and more expensive FlexRay bus (max. speed 10 Mbit/s), but unless a company already uses FlexRay, most new developments favor *automotive Ethernet*, an adaptation of Ethernet for automotive use cases [39, 40, 55], which primarily requires changes to the cabling and physical layer. From a cybersecurity perspective, a clear advantage of automotive Ethernet is that it can re-use existing technology developed for IT networks, such as switches and firewalls. The cheap LIN bus is often the bus of choice for body electronics [92]. Finally, the comparatively expensive MOST bus may still be used for infotainment systems, although FlexRay and automotive Ethernet have become more common.

A combination of the above buses can be found in every vehicle, and yet, surprisingly few of them include security measures on the physical, link or network layer. In paper F of this thesis, we have investigated authentication measures that have been proposed for the CAN bus, identified the criteria they would need to fulfill in order to be used in practice and evaluated the proposed solutions according to those criteria.

Electronic control units. The nodes in in-vehicle networks are so called electronic control units (ECUs). They used to be 16-bit or 32-bit micro-controllers with a limited amount of permanent and

volatile storage, and with several network interfaces. However, as discussed above, more complex micro-controllers with a mix of CPU cores, including 64-bit architectures, and significantly more memory and other advanced features, are increasingly common. In addition to being networked, most ECUs are connected to actuators and sensors to collect, process and act on control information, which is the hallmark of cyber-physical systems. A highly simplified representation of the hardware of an electronic control unit is depicted in figure 5.

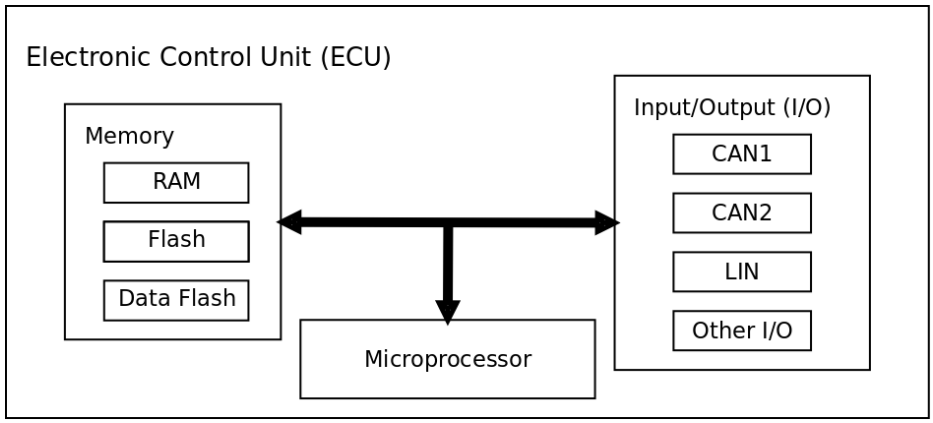


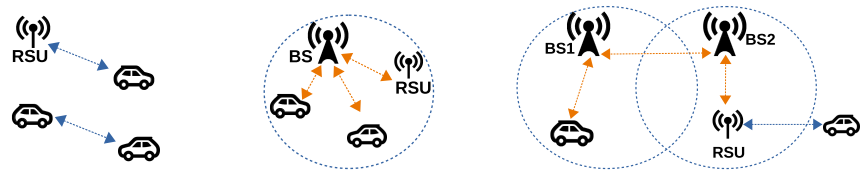
Figure 5: A highly simplified representation of a typical electronic control unit (ECU)

Several CPU architectures are in common use for ECUs, such as instruction sets from Renesas and Tricore, as well as ARM and PowerPC based architectures [4, 24, 34, 65, 71, 80]. Each architecture has its own way of interacting with and controlling its environment, and the corresponding memory architectures can vary widely between the processor families. Nevertheless, the underlying mechanisms are sufficiently similar that their security properties can be analyzed, as we demonstrate in paper E.

Intelligent transportation systems

Intelligent transportation system (ITS) is an umbrella term for interconnected systems that aim to improve road traffic safety, flow and convenience by monitoring and managing traffic. Aside from the necessary back-end systems for analysis and management, ITS introduces new modes of communication for road vehicles, generally known as *vehicle-to-everything (V2X)* communication. This includes direct communication between vehicles (V2V), communication of vehicles with so

called road-side units (RSUs) which are stationary monitoring and communication stations beside the road (V2R), and communication of vehicles with back-end network infrastructure (V2N) using e.g., a base station (BS) (cf. figure 6).



(a) Direct (802.11p or PC5)

(b) Fully network-assisted (4G/5G)

(c) Semi network-assisted (4G/5G + 802.11p or PC5)

Figure 6: Different scenarios for V2V and V2R communications

Figure 6 illustrates the variety of communication modes and technologies underlying intelligent transportation systems, each of which introduces distinct challenges and opportunities. Two distinctions to categorize them are (1) direct communication versus network-assisted communication, and (2) wireless local area networks versus telecommunication networks. Unless industry-wide agreement is reached, ITS may have to support all of them to cover all communication scenarios.

Multiple communication technologies increase system complexity and the potential attack surface for cyber-attacks. The corresponding network stacks vary in security capabilities, and in paper G we explore opportunities and challenges for V2X cybersecurity presented by 5G[4].

3 Objectives

Automotive cybersecurity engineering involves many technical and scientific challenges, and in this thesis we focus on three specific objectives to advance the state of the art. The first objective is to investigate how risk assessment approaches from other domains can be adapted to the automotive domain taking its specific challenges into account. The second objective is to understand how cybersecurity engineering processes need to be adapted for the automotive industry in order to be effective. Finally, the third objective is to study automotive technology in order to understand its

[4] 5th generation of telecommunication technology

impact on the design and implementation of cybersecurity measures. These objectives are reflected in the following research questions:

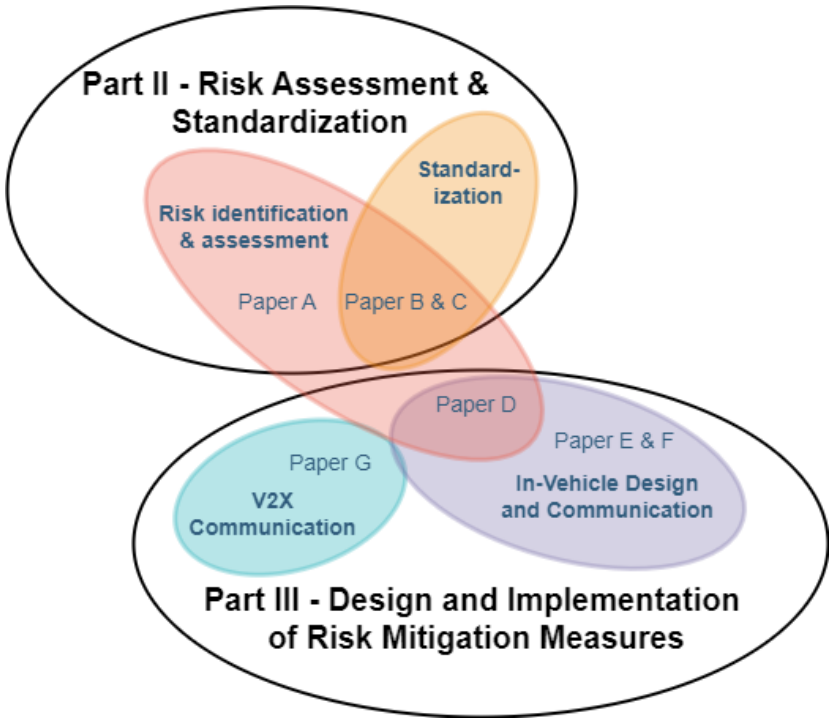


Figure 7: Visualization of the topic categories

RQ1 *How can systematization of threat analysis and risk assessment facilitate cybersecurity requirements engineering in the automotive industry?*

RQ2 *How can cybersecurity engineering processes be implemented or adapted to account for cybersecurity implications in automotive systems?*

RQ3 *How do the design and technology choices in automotive systems influence the development of cybersecurity measures?*

These research questions encompass cybersecurity topics such as risk identification and assessment, standardization, vehicle-to-everything (V2X) communication, in-vehicle communication and design; the relationship of these topics and how the papers relate to them is depicted in figure 7, and table 1 indicates which research question is addressed in which paper.

Motivation for RQ1. Cybersecurity requirements engineering is an important part of automotive projects to ensure that suitable cybersecurity measures are designed and implemented. Threat analysis and risk assessment (TARA) is the most common approach to elicit and prioritize cybersecurity requirements, which is crucial to understand the risks of a specific design to direct efforts and resources appropriately. Therefore, it is important to understand how systematic approaches to threat analysis and risk assessment can support the requirements engineering process, and what the strengths and weaknesses of these approaches are. Whether such approaches are well aligned with automotive standards and processes, and how that alignment can be improved, are also pertinent questions.

We address RQ1 by proposing a framework for threat analysis and risk assessment, also known as the HEAVENS model, that is well aligned with existing automotive processes (**paper A**). Through the preceding standard SAE J3061, this model has influenced the automotive cybersecurity engineering standard ISO/SAE 21434, and we update the proposed framework to better align with it (**paper B**). Moreover, we investigate how the threat analysis and risk assessment processes and terminology in ISO/SAE 21434 can be improved (**paper C**), and we confirm the importance of these processes for industry practitioners (**paper D**).

Motivation for RQ2. While cybersecurity engineering has been a well-established discipline for many decades, its application to the automotive domain is still relatively new. Consequently, it is important to explore how established cybersecurity engineering processes, originally designed for information technology, can be effectively applied to the automotive domain. Additionally, it is necessary to assess whether these processes need to be adapted to address the unique requirements and challenges of automotive systems. This is particularly relevant for vulnerability and incident handling, where automotive practices are still comparatively immature due to their recent emergence. Additionally, it is worth exploring whether standardized automotive cybersecurity processes can be enhanced by leveraging insights from the IT domain.

We address RQ2 by analyzing the processes in ISO/SAE 21434 and compare its vulnerability and incident handling requirements to guidelines from the IT domain (**paper C**), and by exploring

how risk assessment approaches from other domains can be applied to the automotive domain (**paper A**).

Motivation for RQ3. The technology used in automotive systems provides a number of challenges and opportunities for the design of cybersecurity measures. In particular, the resource-constrained nature of the electronic control units and bus systems in use requires careful consideration, and the introduction of new technology, such as 5G telecommunication networks, presents opportunities that are worth investigating.

We address RQ3 by exploring the concrete use of resource-constrained ECUs and how to improve memory safety (**paper E**), by evaluating proposed authentication solutions for the CAN bus, based on identified industrial criteria (**paper F**), and by studying the new features of the 5G New Radio physical layer to investigate if they may have benefits for cybersecurity (**paper G**). To a lesser degree, the technology constraints on common automotive cybersecurity solutions are also discussed in **paper D**.

Table 1: Research questions addressed in each paper

	Risk assessment and standardization			Design and implementation of risk mitigation measures			
	Paper A	Paper B	Paper C	Paper D	Paper E	Paper F	Paper G
RQ1	●	●	◐	◐	○	○	○
RQ2	◐	○	●	○	○	○	○
RQ3	○	○	○	◐	●	●	●

4 Contributions

In the following we summarize the papers included in Part II and Part III of this thesis. We put the papers into context, describe their contributions, and elaborate on how they address the research questions.

4.1 Risk assessment and standardization

In Part II, we study the role of cybersecurity risk assessment in requirements elicitation, evaluate approaches for its effective implementation, and analyze the integration of the new cybersecurity engineering standard, ISO/SAE 21434, with both emerging and established practices.

Paper A - A Risk Assessment Framework for Automotive Embedded Systems

PROBLEM STATEMENT AND RELATED WORK. Risk assessment is an integral part of both safety and cybersecurity engineering, providing guidance for the development and implementation of protective measures. The automotive safety standard, ISO 26262 [44], outlines procedures for the entire safety life-cycle, including hazard analysis and risk assessment (HARA). The outcomes of HARA are high-level safety goals and the assignment of *Automotive Safety Integrity Levels (ASILs)*, which specify the required safety levels. Since ISO 26262 is widely adopted within the automotive industry, aligning new cybersecurity processes with it is advantageous. Furthermore, industry actors frequently prefer methodologies rooted in established standards, raising the question of how cybersecurity risk assessment can be performed in a manner that aligns with ISO 26262 while adhering to widely recognized frameworks.

The pioneering risk rating methodology for automotive electrical and/or electronic (E/E) systems stems from the EVITA project [82]. Wolf and Scheibel [102] further refined the ideas by Henniger et al. [41], and also combine existing techniques into a risk rating framework for automotive systems. Several other security risk assessment approaches have been proposed which integrate directly into existing safety processes [10, 59, 61, 89]. In contrast, we propose a cybersecurity risk assessment which is aligned with, but separate from, the safety processes, because cybersecurity requires a different set of expertise.

CONTRIBUTIONS AND THEIR IMPLICATIONS. We propose a risk assessment framework specifically tailored towards the automotive industry. Its design is guided by the goal of integrating cybersecurity engineering practices into automotive development processes with minimal disruption to existing workflows. To achieve this, the framework is closely aligned with the processes defined in the widely adopted safety standard ISO 26262. A key feature of the framework is the derivation of *security levels*, which provide an indication of a system's security level, analogous to ASILs. Additionally, it offers a systematic approach to cybersecurity requirement elicitation, addressing RQ1. To enhance its practical applicability, the framework combines elements from other

established standards such as Common Criteria [12] and BSI 100-4 [31]. The first international standard to address automotive cybersecurity, SAE standard *J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* [84], recognizes the *HEAVENS* model [42], which forms the basis of this paper, as one of several viable risk assessment frameworks.

STATEMENT OF CONTRIBUTIONS. This paper was co-authored by Mafijul Islam, Aljoscha Lautenbach, Christian Sandberg and Tomas Olovsson. The original idea for the paper came from Mafijul Islam, and the framework was developed in the HEAVENS research project with contributions by many of its members (cf. [42]). The first paper submission was primarily prepared by Mafijul Islam and Aljoscha Lautenbach, with idea and quality contributions from Christian Sandberg and Tomas Olovsson. All revisions and quality improvements based on feedback from subsequent conference submission were prepared by Aljoscha Lautenbach with input and guidance from Tomas Olovsson.

Paper B - Proposing HEAVENS 2.0 – an automotive risk assessment model

PROBLEM STATEMENT AND RELATED WORK. The automotive cybersecurity engineering standard ISO/SAE 21434 outlines a risk assessment framework, but leaves the specific methodology to the implementer. This raises a pertinent question: can previously proposed risk assessment methodologies, such as the HEAVENS model proposed in paper A, be adapted to comply with ISO/SAE 21434? Moreover, the HEAVENS model has been found to exhibit several weaknesses, as identified through both analytical evaluation and practical insights gathered over years of application in the automotive industry. Several other automotive cybersecurity risk assessment approaches have been proposed, which pre-date ISO/SAE 21434 and do not fulfill its requirements [61, 69, 86, 102], whereas some newer works take ISO/SAE 21434 [46] and UNR 155 [96] into account [87, 101].

CONTRIBUTIONS AND THEIR IMPLICATIONS. We perform a comprehensive gap analysis of the original HEAVENS model in relation to ISO/SAE 21434 and identify 12 necessary model updates to ensure standard compliance. These updates primarily address process-related aspects and terminology alignment. Furthermore, we evaluate the HEAVENS model for methodological weaknesses unrelated to standard compliance and identify five additional updates to address them. Applying these 17 updates leads to HEAVENS 2.0, which is compliant with ISO/SAE 21434 while resolving several shortcomings of the original framework. We also demonstrate the viability of HEAVENS 2.0 through an illustrative example. This updated framework can be utilized as a risk

assessment methodology in any automotive project requiring ISO/SAE 21434 compliance. By refining the risk assessment process, we also contribute additional insights to address RQ1.

STATEMENT OF CONTRIBUTIONS. This paper was co-authored by Aljoscha Lautenbach, Magnus Almgren and Tomas Olovsson. The initial concept for the paper was developed by Aljoscha Lautenbach, who also conducted the research and wrote the paper. Magnus Almgren and Tomas Olovsson provided feedback and quality assurance throughout all stages of the project.

Paper C - Gap Analysis of ISO/SAE 21434 – Improving the Automotive Cybersecurity Engineering Life Cycle

PROBLEM STATEMENT AND RELATED WORK. UNECE regulation 155 (UNR 155) and the publication of ISO/SAE 21434 have lead to industry-wide adoption of threat analysis and risk assessment (TARA). However, experiences with TARA applications have revealed challenges in managing the results coherently throughout the supply chain and vehicle life-cycle. Moreover, UNR 155 requires vehicle manufacturers to detect and respond to cybersecurity incidents and provide forensic data for post-incident analysis, but the cybersecurity engineering framework in ISO/SAE 21434 is lacking in this regard. Specifically, the vulnerability and incident handling processes, along with their associated terminology, are not aligned with established standards from the IT domain. Furthermore, the separation of vulnerability and incident handling is unclear, and critical steps, such as post-incident analysis, are absent in the standard. A number of works analyze ISO/SAE 21434 and highlight practical implications [18, 22, 35, 60]. Other publications address the challenges of applying TARA in distributed automotive development projects [21, 48, 56].

CONTRIBUTIONS AND THEIR IMPLICATIONS. To address the issues outlined above, we analyze the TARA processes as well as the vulnerability and incident handling processes to identify potential deficiencies. Based on this analysis, we propose modifications and augmentations to ISO/SAE 21434 that aim to mitigate or resolve these shortcomings. Our proposed improvements include a new TARA management process designed to enhance information handling and coordination among stakeholders, as well as refinements to the vulnerability and incident handling processes and related terminology. If adopted, these enhancements are expected to further increase applicability of ISO/SAE 21434 to demonstrate compliance with UNR 155. Finally, the process improvements proposed in this paper contribute to addressing RQ2.

STATEMENT OF CONTRIBUTIONS. This paper was co-authored by Daniel Grimm, Aljoscha Lautenbach, Magnus Almgren, Tomas Olovsson and Eric Sax. The original idea for the paper

emerged from a collaboration between Daniel Grimm and Aljoscha Lautenbach. The writing was carried out in equal measures by Daniel Grimm and Aljoscha Lautenbach, with feedback and quality assurance provided by Magnus Almgren, Tomas Olovsson and Erik Sax during the later stages of the project.

4.2 Design and implementation of risk mitigation measures

In Part III, we investigate the influence of automotive technology on cybersecurity measures, and how automotive cybersecurity experts evaluate different design and implementation issues.

Paper D - Understanding Common Automotive Security Issues and Their Implications

PROBLEM STATEMENT AND RELATED WORK. Developing secure software is a challenging task that requires specialized training or tools to recognize patterns that lead to code vulnerabilities [38, 57, 67]. Historically, cybersecurity received little attention in the context of vehicular software. While many automotive software developers are trained in adhering to safety regulations, they often lack equivalent security training. To effectively design and deliver such training, it is essential to identify the specific challenges developers are likely to encounter and to explore strategies for addressing them. Extensive research has been conducted to identify automotive cybersecurity issues [52, 92, 103], demonstrate practical attacks [15, 68] and explore the interaction between automotive cybersecurity and safety [5, 33, 47, 58, 79, 104].

CONTRIBUTIONS AND THEIR IMPLICATIONS. Using a straightforward example application, we identify eight cybersecurity issues of broad relevance, ranging from early design considerations to implementation decisions. For each issue, we propose recommendations aimed at providing at least partial resolutions. To validate the significance of these issues and the suitability of the proposed solutions, we surveyed automotive cybersecurity experts to gather their perceptions and insights. The findings confirm that the identified issues are regarded as problematic, with the engineering challenges associated with key distribution emerging as particularly difficult to address. Additionally, the results indicate that many of these issues can be mitigated through improved documentation and enhanced access to cybersecurity expertise.

STATEMENT OF CONTRIBUTIONS. This paper was co-authored by Aljoscha Lautenbach, Magnus Almgren, and Tomas Olovsson. The original concept for the paper was developed by Aljoscha Lautenbach, who also designed, conducted, and analyzed the survey, with some input on survey design provided by Grischa Liebel. Aljoscha Lautenbach wrote the paper, while Magnus

Almgren and Tomas Olovsson contributed ideas, feedback, and quality assurance throughout all stages of the project.

Paper E - What the stack? On Memory Exploitation and Protection in Resource Constrained Automotive Systems

PROBLEM STATEMENT AND RELATED WORK. Memory corruption bugs are arguably among the most dangerous kinds of software bugs, since their exploitation can grant the attacker a large degree of control [98]. In traditional IT systems, such as desktops and servers, a continuous "arms race" has unfolded between increasingly sophisticated attack techniques and the defensive measures to protect system memory. However, this dynamic has largely bypassed resource-constrained embedded automotive systems. With the growing connectivity of vehicles, it has become increasingly important to investigate the potential exploitation of memory corruption vulnerabilities in automotive contexts. Van der Veen et al. [98] and Szekeres et al. [94] independently provided a historic overview and a classification of different types of memory corruption bugs. We are not aware of any work that specifically discusses memory corruption bugs in the context of constrained automotive systems.

CONTRIBUTIONS AND THEIR IMPLICATIONS. We present an analysis of the typical hardware architecture of an electrical control unit (ECU) and examine how this architecture affects memory exploitation and protection techniques. In particular, we discuss that some deployed systems lack robust memory protection, making them vulnerable to stack-based memory corruption exploits. However, established mitigation techniques, such as stack canaries and non-executable RAM, can considerably reduce the risk of successful exploitation. This work directly addresses an aspect of RQ3 by exploring the architecture of resource-constrained ECUs and its impact on the implementation of memory protection cybersecurity measures.

STATEMENT OF CONTRIBUTIONS. This paper was co-authored by Aljoscha Lautenbach, Magnus Almgren and Tomas Olovsson. The initial concept was developed by Aljoscha Lautenbach, who also wrote the paper. Magnus Almgren and Tomas Olovsson contributed by providing feedback and ensuring quality at every stage of the project.

Paper F - In-vehicle CAN Message Authentication: An Evaluation Based on Industrial Criteria

PROBLEM STATEMENT AND RELATED WORK. The controller area network (CAN) bus remains the most prevalent bus in in-vehicle networks. However, the underlying technology and protocols, developed over 3 decades ago, were not designed with security in mind. Many solutions have been proposed to add authentication to the CAN bus, but few, if any, have been implemented in real vehicles. The security problems of the CAN bus have been highlighted in many publications, for instance in [11, 52, 92, 103] to name but a few. Vasile et al. [99] evaluated the performance of several proposed CAN message authentication solutions on CAN-FD and FlexRay.

CONTRIBUTIONS AND THEIR IMPLICATIONS. With help from industry experts, we identified five requirements that a CAN bus authentication solution would have to fulfill in order to be a viable option for practical use. We provide a comprehensive overview of the most promising CAN authentication solutions, and evaluate them according to five industrial criteria: *cost-effectiveness*, *backward compatibility*, *support for vehicle repair and maintenance*, *sufficient implementation details* and *acceptable overhead*. We find that no solution meets all five criteria, with backward compatibility and acceptable overhead being the biggest adoption hurdles for the proposed CAN authentication schemes. We therefore conclude that the wide-spread use of CAN is questionable from a cybersecurity point of view. By investigating how the attributes of the CAN bus influence the implementation of message authentication, we contribute further insights to RQ3.

STATEMENT OF CONTRIBUTIONS. This paper was co-authored by Nasser Nowdehi, Aljoscha Lautenbach and Tomas Olovsson. The original idea for the paper was born from discussions between Nasser Nowdehi and Aljoscha Lautenbach, and the paper was written in equal measures by Nasser Nowdehi and Aljoscha Lautenbach, with feedback and quality assurance from Tomas Olovsson throughout all stages of the project.

Paper G - A preliminary security assessment of 5G V2X

PROBLEM STATEMENT AND RELATED WORK. Intelligent transportation systems (ITS) play an increasingly important role in modern traffic and automotive applications. Given that some of ITS functions are safety-critical, ensuring the security of ITS communications is paramount. The *European Telecommunication Standards Institute (ETSI)* has defined standards for all network layers of ITS, ranging from application to access and physical layers. The ETSI access

layer standard, ITS G5, is based on IEEE 802.11p, which lacks inherent cybersecurity features, requiring such protections to be provided by higher layers. Alternatively, the access layer can employ LTE-V2X, 3GPP standard for cellular-based *vehicle-to-everything (V2X)* communication, which offers basic security through the telecommunication network. With the advent of the 5G telecommunication standard and its associated New Radio (NR) technology, which is compatible with C-V2X, it is worth investigating whether 5G technology can offer enhanced cybersecurity capabilities at the lower layers of the protocol stack, thereby surpassing the security provided by existing technologies. Previous research has investigated V2X and C-V2X with a focus on safety and performance [32, 100], as well as emerging 5G technologies [2, 37, 91] and security [3, 7].

CONTRIBUTIONS AND THEIR IMPLICATIONS. We analyze the ETSI ITS use cases for *Active Road Safety*, *Cooperative Traffic Efficiency*, *Cooperative Local Services* and *Global Internet Services* with regards to their required cybersecurity attributes. Additionally, we review existing research on the properties of 5G New Radio technology and evaluate its applicability to these use cases. The inherent features of 5G New Radio are expected to enhance confidentiality and privacy, while potentially reducing authentication times in specific scenarios. By investigating how this emerging technology impacts potential cybersecurity measures, this work contributes to the broader understanding of its impact and provides partial insights into addressing RQ3.

STATEMENT OF CONTRIBUTIONS. This paper was co-authored by Aljoscha Lautenbach, Nasser Nowdehi, Tomas Olovsson and Romi Zaragatzky. The initial research, forming the foundation of the paper, was conducted by Romi Zaragatzky as part of her master's thesis [105], which was partially supervised by Nasser Nowdehi and Aljoscha Lautenbach. The paper was collaboratively written and prepared for conference submission by Nasser Nowdehi and Aljoscha Lautenbach, with the consent of Romi Zaragatzky. Tomas Olovsson provided feedback and quality assurance throughout all stages of the paper.

5 Summary and concluding remarks

This thesis covers different aspects of automotive cybersecurity risk management, from risk assessments to the appropriate mitigation and management of these risks. This includes questions on requirements engineering, vulnerability and incident handling, the influence of automotive technology on cybersecurity measures and the perception of cybersecurity issues.

We make several contributions to improve the state of automotive cybersecurity. The first three papers address issues around risk assessment and standardization. In **paper A**, we propose a risk assessment framework to identify and rate threats to automotive systems with a *security level*, known as the HEAVENS model. Alignment with the functional safety standard ISO 26262 was a design goal of the framework, and the security levels can guide the development process of security-relevant functions similar to how automotive safety integrity levels (ASILs) guide the development process for safety-critical functions. Through its inclusion in the first automotive cybersecurity standard SAE J3061, the HEAVENS model has influenced the risk assessment framework in the succeeding automotive cybersecurity engineering standard ISO/SAE 21434. In **paper B**, we present HEAVENS 2.0 which further refines the approach of paper A by making it compliant with the ISO/SAE standard and by incorporating insights gained from practical application in industry. This results in higher utility and usability of the framework. In **paper C**, we analyze ISO/SAE 21434 for weaknesses in the requirements of the threat analysis and risk assessment processes, as well as regarding vulnerability and incident handling. We propose enhancements for future versions of the standard, which have been submitted for consideration to the relevant ISO committee, *ISO/TC 22/SC 32/WG11 Cybersecurity*.

The remaining four papers provide insights into the design and implementation of cybersecurity risk mitigation measures. In **paper D**, we investigate cybersecurity practitioners' perception of various issues and demonstrate that comprehensive documentation and access to cybersecurity expertise is crucial for successful development projects. In **paper E**, we examine the architecture of a resource-constrained electronic control unit for its susceptibility to exploitation through memory corruption vulnerabilities. Our analysis confirms that stack-based buffer overflow vulnerabilities are exploitable; however, this risk can be mitigated using protective measures such as stack canaries and non-executable RAM, which are commonly employed in desktop and server systems. In **paper F**, we explore authentication solutions for the most prevalent automotive bus, the CAN bus, and examine the reasons behind the industry's slow adoption of such measures. Discussions with industry experts identified five criteria that authentication solutions must meet to be viable for practical application: cost-effectiveness, backward compatibility, support for repair and maintenance, sufficient implementation detail and acceptable overhead. Our evaluation of ten proposed authentication solutions reveals that none fully satisfy all these criteria. Finally, in **paper G**, we conduct a preliminary cybersecurity assessment of 5G telecommunication technology, specifically New Radio (NR), in its role within the physical and access layers of intelligent transport systems.

Our findings suggest that NR possesses characteristics that could inherently enhance confidentiality and privacy while also offering potential advantages for authentication.

As cybersecurity risk assessment is now legally mandated in many countries, and since the HEAVENS model has impacted the widely used standard ISO/SAE 21434, the related contributions of papers A, B and C in Part II should remain relevant for a long time to come. Moreover, certain aspects in Part III such as the identification of requirements for industrial applicability of cybersecurity measures in paper F should retain long-term usefulness.

Although this thesis primarily focuses on automotive systems, many of its findings are applicable to embedded systems across other domains that face similar challenges, including certain industrial systems, medical systems, and other forms of transport such as marine transport. The risk assessment methodology, in particular, is well-suited for domains that utilize safety-critical systems. Additionally, the insights on the influence of automotive technology on cybersecurity measures are equally relevant to other sectors employing comparable technologies.

References

[1] HEAVENS: HEAling Vulnerabilities to ENhance Software Security and Safety – End-of-Project Report, December 2012. https://www.vinnova.se/en/p/heavens-healing-vulnerabilities-to-enhance-software-security-and-safety/.

[2] M. Agiwal, A. Roy, and N. Saxena. Next generation 5G wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 18(3):1617–1655, 2016.

[3] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov. 5G security: Analysis of threats and solutions. *2017 IEEE Conference on Standards for Communications and Networking, CSCN 2017*, pages 193–199, 2017.

[4] ARM. *ARMv7-M Architecture Reference Manual*, December 2014. https://developer.arm.com/docs/ddi0403/e/armv7-m-architecture-reference-manual.

[5] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1):11–33, 2004.

[6] V. Bandur, G. Selim, V. Pantelic, and M. Lawford. Making the case for centralized automotive e/e architectures. *IEEE Transactions on Vehicular Technology*, 70(2):1230–1245, 2021.

[7] K. Bian, G. Zhang, and L. Song. Toward Secure Crowd Sensing in Vehicle-to-Everything Networks. *IEEE Network*, pages 1–6, 2017.

[8] S. Biller, L. M. A. Chan, D. Simchi-Levi, and J. Swann. Dynamic pricing and the direct-to-customer model in the automotive industry. *Electronic Commerce Research*, 5(2):309–334, 2005.

[9] M. Broy. Challenges in automotive software engineering. In *Proceedings of the 28th International Conference on Software Engineering*, ICSE '06, page 33–42, New York, NY, USA, 2006. Association for Computing Machinery.

[10] S. Burton, J. Likkei, P. Vembar, and M. Wolf. Automotive functional safety = safety + security. In *Proceedings of the First International Conference on Security of Internet of Things*, SecurIT '12, pages 150–159, New York, NY, USA, 2012. ACM.

[11] P. Carsten, T. R. Andel, M. Yampolskiy, and J. T. McDonald. In-vehicle networks: Attacks, vulnerabilities, and proposed solutions. In *Proceedings of the 10th Annual Cyber and Information Security Research Conference*, pages 1–8. ACM, 2015.

[12] CCRA Members. *Common Criteria for Information Technology Security Evaluation*. CCMB-2012-09-00X, Version 3.1, Revision 4.

[13] R. N. Charette. This car runs on code. *IEEE Spectrum*, February 2009. https://spectrum.ieee.org/this-car-runs-on-code.

[14] R. N. Charette. Software is eating the car. *IEEE Spectrum*, June 2021. https://spectrum.ieee.org/software-eating-car.

[15] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of the 20th USENIX Security Symposium*, pages 77–92, San Francisco, CA, USA, Aug. 2011.

[16] F. Chiara and M. Canova. A review of energy consumption, management, and recovery in automotive systems, with considerations of future trends. *Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering*, 227(6):914–936, 2013.

[17] P. Cichonski, T. Millar, T. Grance, and K. Scarfone. Computer security incident handling guide, 8 2012.

[18] G. Costantino, M. De Vincenzi, and I. Matteucci. In-Depth Exploration of ISO/SAE 21434 and Its Correlations with Existing Standards. *IEEE Communications Standards Magazine*, 6(1):84–92, 2022.

[19] A. Costin, J. Zaddach, A. Francillon, D. Balzarotti, and S. Antipolis. A Large-Scale Analysis of the Security of Embedded Firmwares. In *USENIX Security Symposium*, pages 95–110, 2014.

[20] G. Dimitrakopoulos and P. Demestichas. Intelligent Transportation Systems. *IEEE Vehicular Technology Magazine*, 5(1):77–84, March 2010.

[21] J. Dobaj, G. Macher, D. Ekert, A. Riel, and R. Messnarz. Towards a security-driven automotive development lifecycle. *Journal of Software: Evolution and Process*, n/a(n/a):e2407, 2021.

[22] C. Ebert and J. John. Practical Cybersecurity with ISO 21434. *ATZelectronics worldwide*, 17, Mar. 2022.

[23] ENISA. Cyber Security and Resilience of smart cars, January 2017. `https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars`.

[24] J. Erjavec and R. Thompson. *Automotive technology: a systems approach*. Cengage Learning, 2014.

[25] European Union. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance). *Official Journal of the European Union*, 60(L 117):1–175, May 2017. Available online: `http://data.europa.eu/eli/reg/2017/745/oj`.

[26] European Union. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance). *Official Journal of the European Union*, 60(L 117):176–332, May 2017. Available online: `http://data.europa.eu/eli/reg/2017/746/oj`.

[27] European Union. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (Text with EEA relevance). *Official Journal of the European Union*, 62(L 325):1–40, December 2019. Available online: `http://data.europa.eu/eli/reg/2019/2144/oj`.

[28] European Union. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). *Official Journal of the European Union*, 65(L 333):80–152, December 2022. Available online: `http://data.europa.eu/eli/dir/2022/2555/oj`.

[29] European Union. Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council

Directive 73/361/EEC (Text with EEA relevance). *Official Journal of the European Union*, 66(L 165):1–102, June 2023. Available online: http://data.europa.eu/eli/reg/2023/1230/oj.

[30] European Union. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance). *Official Journal of the European Union*, (L):1–81, November 2024. Available online: http://data.europa.eu/eli/reg/2024/2847/oj.

[31] Federal Office for Information Security (BSI), Germany. *BSI-Standard 100-4 – Business Continuity Management*. 2009.

[32] A. Filippi, K. Moerman, V. Martinez, A. Turley, O. Haran, and R. Toledano. IEEE802.11p ahead of LTE-V2V for safety applications. Technical report, 2017.

[33] D. G. Firesmith. Common concepts underlying safety, security, and survivability engineering. Technical Report CMU/SEI-2003-TN-033, Software Engineering Institute - Carnegie Mellon University, Dec 2003. https://kilthub.cmu.edu/ndownloader/files/12057656.

[34] P. Gai and M. Violante. Automotive embedded software architecture in the multi-core age. In *2016 21st IEEE European Test Symposium (ETS)*, pages 1–8, May 2016.

[35] M. Gierl, R. Kriesten, and E. Sax. Security Assessment Prospects as Part of Vehicle Regulations. In M. Trapp, E. Schoitsch, J. Guiochet, and F. Bitsch, editors, *SAFECOMP 2022 Workshops*, pages 97–109, Cham, 2022. Springer International Publishing.

[36] S. Greiner, M. Massierer, C. Loderhose, B. Lutz, F. Stumpf, and F. Wiemer. A supplier's perspective on threat analysis and risk assessment according to ISO/SAE 21434. In *escar 2022 EU*, 2022.

[37] A. Gupta and R. K. Jha. A survey of 5G network: Architecture and emerging technologies. *IEEE Access*, 3:1206–1232, 2015.

[38] H. Hanif, M. H. N. Md Nasir, M. F. Ab Razak, A. Firdaus, and N. B. Anuar. The rise of software vulnerability: Taxonomy of software vulnerabilities detection and machine learning approaches. *Journal of Network and Computer Applications*, 179:103009, 2021.

[39] P. Hank, S. Müller, O. Vermesan, and J. Van Den Keybus. Automotive Ethernet: In-vehicle Networking and Smart Mobility. In *Proceedings of the Conference on Design, Automation and Test in Europe*, DATE '13, pages 1735–1739, San Jose, CA, USA, 2013. EDA Consortium.

[40] P. Hank, T. Suermann, and S. Müller. Automotive Ethernet, a Holistic Approach for a Next Generation In-Vehicle Networking Standard. In G. Meyer, editor, *Advanced Microsystems for Automotive Applications 2012: Smart Systems for Safe, Sustainable and Networked Vehicles*, pages 79–89, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[41] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl. Security requirements for automotive on-board networks. In *Proceedings of the 9th International Conference on Intelligent Transport System Telecommunications (ITST)*, 2009.

[42] M. Islam, C. Sandberg, A. Bokesand, T. Olovsson, H. Broberg, P. Kleberger, A. Lautenbach, A. Hansson, A. Söderberg-Rivkin, and S. P. Kadhirvelan. Deliverable D2 - Security Models. HEAVENS Project, Version 1.0 (Release 1), September 2014.

[43] ISO. ISO/IEC 31000: Risk Management – Principles and guidelines, 2009. ISO/IEC 31000:2009.

[44] ISO. Road vehicles — Functional safety, 2011. ISO 26262:2011.

[45] ISO/IEC. ISO/IEC 30111 Information technology — Security techniques — Vulnerability handling processes, Oct. 2019.

[46] ISO/SAE. ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering, Aug 2021.

[47] E. Jonsson. Towards an integrated conceptual model of security and dependability. In *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, pages 646–653. IEEE, 2006.

[48] A. Kiening and D. Angermeier. TRADE - Threat and Risk Assessment for Automotive Distributed Engineering. In *ESCAR 2021 EU*, 2021.

[49] P. Kleberger and T. Olovsson. Protecting Vehicles Against Unauthorised Diagnostics Sessions Using Trusted Third Parties. In F. Bitsch, J. Guiochet, and M. Kaâniche, editors, *Computer Safety, Reliability, and Security: 32nd International Conference, SAFECOMP 2013, Toulouse, France, September 24-27, 2013. Proceedings*, pages 70–81, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[50] P. Kleberger and T. Olovsson. Securing Vehicle Diagnostics in Repair Shops. In A. Bondavalli and F. Di Giandomenico, editors, *Computer Safety, Reliability, and Security: 33rd International Conference, SAFECOMP 2014, Florence, Italy, September 10-12, 2014. Proceedings*, pages 93–108. Springer International Publishing, 2014.

[51] P. Kleberger, T. Olovsson, and E. Jonsson. An in-depth analysis of the security of the connected repair shop. In *The Seventh International Conference on Systems and Networks Communications (ICSNC), Proceedings. Lisbon, 18-23 November, 2012. IARIA.*, page 99, 2012.

[52] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 447–462, May 2010.

[53] U. E. Larson and D. K. Nilsson. Securing vehicles against cyber attacks. In *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*, CSIIRW '08, pages 30:1–30:3, New York, NY, USA, 2008. ACM.

[54] U. E. Larson, D. K. Nilsson, and E. Jonsson. An approach to specification-based attack detection for in-vehicle networks. In *Intelligent Vehicles Symposium, 2008 IEEE*, pages 220–225. IEEE, 2008.

[55] J. Lastinec and L. Hudec. Approach to securing in-vehicle communication using ethernet/IP. Dec 2014.

[56] A. Lautenbach, M. Almgren, and T. Olovsson. Proposing HEAVENS 2.0 – an Automotive Risk Assessment Model. In *Computer Science in Cars Symposium*, CSCS '21, New York, NY, USA, 2021. ACM.

[57] G. Lin, S. Wen, Q.-L. Han, J. Zhang, and Y. Xiang. Software vulnerability detection using deep neural networks: A survey. *Proceedings of the IEEE*, 108(10):1825–1848, 2020.

[58] M. Line, O. Nordland, L. Røstad, and I. Tøndel. Safety vs. security. In *Probabilistic Safety Assessment and Management (PSAM), Proceedings of the 8th international Conference on*, pages 685–699. IAPSAM, 2006.

[59] G. Macher, A. Höller, H. Sporer, E. Armengaud, and C. Kreiner. A combined safety-hazards and security-threat analysis method for automotive systems. In *Computer Safety, Reliability, and Security*, pages 237–250. Springer, 2015.

[60] G. Macher, C. Schmittner, O. Veledar, and E. Brenner. ISO/SAE DIS 21434 Automotive Cybersecurity Standard - In a Nutshell. In A. Casimiro, F. Ortmeier, E. Schoitsch, F. Bitsch, and P. Ferreira, editors, *SAFECOMP 2020 Workshops*, pages 123–135, Cham, 2020. Springer International Publishing.

[61] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner. SAHARA: A Security-Aware Hazard and Risk Analysis Method. In *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*, DATE '15, pages 621–624, San Jose, CA, USA, 2015. EDA Consortium.

[62] S. M. Mahmud and S. Alles. In-vehicle network architecture for the next-generation vehicles. SAE Technical Paper 2005-01-1531, SAE International, Apr. 2005.

[63] S. E. Markey. Security and Privacy in Your (SPY) Car Act of 2017. Technical report, March 2017. `https://www.congress.gov/bill/115th-congress/senate-bill/680`.

[64] L. Mauser and S. Wagner. Centralization potential of automotive e/e architectures. *Journal of Systems and Software*, 219:112220, 2025.

[65] A. Mayer and F. Hellwig. System Performance Optimization Methodology for Infineon's 32-bit Automotive Microcontroller Architecture. In *Proceedings of the Conference on Design, Automation and Test in Europe*, DATE '08, pages 962–966, New York, NY, USA, 2008. ACM.

[66] G. McGraw. *Software Security: Building Security in*. Addison-Wesley professional computing series. Addison-Wesley, 2006.

[67] N. Meng, S. Nagy, D. D. Yao, W. Zhuang, and G. A. Argoty. Secure coding practices in Java: challenges and vulnerabilities. In *Proceedings of the 40th International Conference on Software Engineering*, ICSE '18, page 372–383, New York, NY, USA, 2018. Association for Computing Machinery.

[68] C. Miller and C. Valasek. Remote Exploitation of an Unaltered Passenger Vehicle. Technical report, Defcon 23, August 2015. `http://illmatics.com/Remote%20Car%20Hacking.pdf`.

[69] J.-P. Monteuuis, A. Boudguiga, J. Zhang, H. Labiod, A. Servel, and P. Urien. SARA: Security Automotive Risk Analysis Method. In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security*, CPSS '18, page 3–14, New York, NY, USA, 2018. Association for Computing Machinery.

[70] S. K. Moore. How to Keep the Automotive Chip Shortage From Happening Again. *IEEE Spectrum*, July 2021. `https://spectrum.ieee.org/automotive-chip-shortage`.

[71] P. S. Murvay, A. Matei, C. Solomon, and B. Groza. Development of an AUTOSAR Compliant Cryptographic Library on State-of-the-Art Automotive Grade Controllers. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*, pages 117–126, Aug 2016.

[72] A. Mutschler. Automotive Complexity, Supply Chain Strength Demands Tech Collaboration. *Semiconductor Engineering*, August 2023. `https://semiengineering.com/automotive-complexity-supply-chain-strength-demands-tech-collaboration/`.

[73] S. Nandavar, S.-A. Kaye, T. Senserrick, and O. Oviedo-Trespalacios. Exploring the factors influencing acquisition and learning experiences of cars fitted with advanced driver assistance systems (adas). *Transportation Research Part F: Traffic Psychology and Behaviour*, 94:341–352, 2023.

[74] D. K. Nilsson and U. E. Larson. Simulated Attacks on CAN Buses: Vehicle Virus. In *IASTED International conference on communication systems and networks (AsiaCSN)*, pages 66–72, 2008.

[75] D. K. Nilsson, U. E. Larson, F. Picasso, and E. Jonsson. A First Simulation of Attacks in the Automotive Network Communications Protocol FlexRay. In *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS'08*, pages 84–91. Springer, 2009.

[76] N. Nowdehi and T. Olovsson. Experiences from implementing the ETSI ITS SecuredMessage service. In *2014 IEEE Intelligent Vehicles Symposium Proceedings*, pages 1055–1060, June 2014.

[77] W. Payre, J. Perelló-March, A. Kanakapura Sriranga, and S. Birrell. The notorious b.i.t: The effects of a ransomware and a screen failure on distraction in automated driving. *Transportation Research Part F: Traffic Psychology and Behaviour*, 94:42–52, 2023.

[78] L. Piètre-Cambacédès and M. Bouissou. Cross-fertilization between safety and security engineering. *Reliability Engineering & System Safety*, 110:110–126, 2013.

[79] L. Piètre-Cambacédès and C. Chaudet. The SEMA referential framework: avoiding ambiguities in the terms "security" and "safety". *International Journal of Critical Infrastructure Protection*, 3(2):55–66, 2010.

[80] C. P. Quigley, R. McMurran, R. P. Jones, and P. T. Faithfull. An Investigation into Cost Modelling for Design of Distributed Automotive Electrical Architectures. In *2007 3rd Institution of Engineering and Technology Conference on Automotive Electronics*, pages 1–9, June 2007.

[81] C. Ratcliff. *Fact Sheets of the European Union - Road traffic and safety provisions*, March 2017. `http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_5.6.5.html`.

[82] A. Ruddle, D. Ward, B. Weyl, S. Idrees, Y. Roudier, M. Friedewald, T. Leimbach, A. Fuchs, S. Gürgens, O. Henniger, R. Rieke, M. Ritscher, H. Broberg, L. Apvrille, R. Pacalet, and G. Pedroza. Security requirements for automotive on-board networks based on dark-side scenarios. EVITA Project, Deliverable D2.3, v1.1., Dec. 2009.

[83] SAAB. *SAAB architecture from 2003 to 2006*, 2003–2006. `http://saabworld.net/f146/bus-diagnostics-communication-saab-9-3-2003-2006-a-25524/`.

[84] SAE International. SAE J3061_201601 - Cybersecurity guidebook for cyber-physical vehicle systems, Jan. 2016.

[85] F. Sagstetter, M. Lukasiewycz, S. Steinhorst, M. Wolf, A. Bouard, W. R. Harris, S. Jha, T. Peyrin, A. Poschmann, and S. Chakraborty. Security challenges in automotive hardware/software architecture design. In *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 458–463, 2013.

[86] K. Schmidt, P. Tröger, H.-M. Kroll, T. Bünger, F. Krueger, and C. Neuhaus. Adapted Development Process for Security in Networked Automotive Systems. *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, 7(2):516–526, 2014.

[87] C. Schmittner, J. Dobaj, G. Macher, and E. Brenner. A Preliminary View on Automotive Cyber Security Management Systems. In *Proceedings of the 23rd Conference on Design, Automation and Test in Europe*, DATE '20, page 1634–1639, San Jose, CA, USA, 2020. EDA Consortium.

[88] C. Schmittner, J. Dobaj, G. Macher, and E. Brenner. A preliminary view on automotive cyber security management systems. In *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1634–1639, 2020.

[89] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch. Security application of failure mode and effect analysis (FMEA). In *Computer Safety, Reliability, and Security*, pages 310–325. Springer, 2014.

[90] S. Serdarasan. A review of supply chain complexity drivers. *Computers & Industrial Engineering*, 66(3):533–540, 2013. Special Issue: The International Conferences on Computers and Industrial Engineering (ICC&IEs) - series 41.

[91] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally. 5G for vehicular communications. *IEEE Communications Magazine*, 56(1):111–117, Jan 2018.

[92] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaaniche, and Y. Laarouchi. Survey on security threats and protection mechanisms in embedded automotive networks. In *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*, pages 1–12, 2013.

[93] M. K. Svangren, M. B. Skov, and J. Kjeldskov. The connected car: An empirical study of electric cars as mobile digital devices. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '17, pages 6:1–6:12, New York, NY, USA, 2017. ACM.

[94] L. Szekeres, M. Payer, T. Wei, and D. Song. SoK: Eternal War in Memory. In *2013 IEEE Symposium on Security and Privacy (SP)*, pages 48–62, May 2013.

[95] UNECE. Agreement Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations, Oct. 2017.

[96] UNECE. Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, Mar. 2021.

[97] C. Valasek and C. Miller. Adventures in Automotive Networks and Control Units. Technical report, Defcon 21, August 2013. `http://www.ioactive.com/pdfs/~IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf`.

[98] V. Van der Veen, N. dutt-Sharma, L. Cavallaro, and H. Bos. Memory errors: the past, the present, and the future. In *Proceedings of the 15th International Symposium on Research in Attacks, Intrusions, and Defenses*, pages 86–106. Springer, 2012.

[99] P. Vasile, B. Groza, and S. Murvay. Performance analysis of broadcast authentication protocols on CAN-FD and FlexRay. In *Proceedings of the WESS'15: Workshop on Embedded Systems Security*, WESS'15, pages 7:1–7:8, New York, NY, USA, 2015. ACM.

[100] V. Vukadinovic, K. Bakowski, P. Marsch, I. D. Garcia, H. Xu, M. Sybis, P. Sroka, K. Wesolowski, D. Lister, and I. Thibault. 3GPP C-V2X and IEEE 802.11p for vehicle-to-vehicle communications in highway platooning scenarios. *Ad Hoc Networks*, 74:17–29, 2018.

[101] Y. Wang, Y. Wang, H. Qin, H. Ji, Y. Zhang, and J. Wang. A Systematic Risk Assessment Framework of Automotive Cybersecurity. *Automotive Innovation*, pages 1–9, 2021.

[102] M. Wolf and M. Scheibel. A systematic approach to a qualified security risk analysis for vehicular IT systems. In E. Plödereder, P. Dencker, H. Klenk, H. B. Keller, and S. Spitzer, editors, *Automotive - Safety & Security 2012*, Lecture Notes in Informatics, pages 195–210. Gesellschaft für Informatik, Bonn, 2012.

[103] M. Wolf, A. Weimerskirch, and C. Paar. Security in automotive bus systems. In *Workshop on Embedded Security in Cars*, 2004.

[104] R. Zalman and A. Mayer. A secure but still safe and low cost automotive communication technique. In *Proceedings of the 51st Annual Design Automation Conference*, DAC '14, pages 1–5, New York, NY, USA, 2014. ACM.

[105] R. Zaragatzky. Master Thesis: Security analysis of introducing 5G in V2X communications. Technical report, Chalmers University of Technology, 2018.