Automotive Software Security Engineering based on the ISO 21434

Technical Report

Matthias Bergler and Ramin Tavakoli Kolagari

May 6, 2023

1 Introduction

The first chapter of the paper provides an overview of the importance of automotive security and the increasing threat posed by cyberattacks. It highlights the critical role of ISO 21434, a standard for automotive cybersecurity engineering, in ensuring the security of automotive systems throughout their lifecycle. The chapter also introduces the Security Abstraction Model (SAM), a framework for automotive system design and development, and discusses the need to integrate ISO 21434 with SAM to enable effective implementation of cybersecurity measures. Finally, the chapter outlines the goals and structure of this work, which aims to explore the practical application of integrating ISO 21434 into SAM and provide insights into the benefits and challenges of this approach.

1.1 Motivation Security and Automotive

The automotive industry has been rapidly evolving with the advent of connected and autonomous vehicles. While this has brought about many benefits, such as improved safety features and enhanced driving experiences, it has also raised concerns about the security of these advanced vehicles. The increasing reliance on software, communication networks, and data exchange in modern cars has made them vulnerable to various cybersecurity threats, including unauthorized access, data breaches, and remote manipulation Wang et al. (2021); Luo et al. (2021). As a result, the motivation for security in the automotive industry has become a critical concern for automakers, regulators, and consumers alike.

One of the primary motivations for security in the automotive industry is to protect the safety and privacy of vehicle owners and passengers. As connected vehicles collect and transmit large amounts of data, including personal information, location data, and driving behavior, there is a heightened risk of data breaches and privacy violations. Malicious actors could exploit vulnerabilities in the vehicle's software or communication networks to gain unauthorized access to sensitive data, leading to identity theft, financial fraud, and other serious consequences. Ensuring the security of connected vehicles is crucial to safeguard the privacy and personal safety of the users Schoettle and Sivak (2014).

Another motivation for security in the automotive industry is to prevent unauthorized access and tampering of the vehicle's critical systems, such as the engine, brakes, and steering. As connected vehicles are equipped with multiple electronic control units (ECUs) that communicate with each other, there is a risk of cyber attacks that could compromise the integrity and functionality of these systems. For example, hackers could remotely manipulate the vehicle's controls, leading to potential accidents or even life-threatening situations. Therefore, robust security measures are needed to prevent unauthorized access and tampering of critical systems in connected vehicles, ensuring their safe operation Guan et al. (2022).

Furthermore, protecting the reputation and brand image of automakers is another motivation for security in the automotive industry. A successful cyber attack on a connected vehicle could not only result

in financial losses due to recalls, lawsuits, and damages but also have long-term consequences for the automaker's reputation. Consumers trust that their vehicles are secure and safe to use, and any breach of that trust could significantly impact the brand's image and customer loyalty. Therefore, automakers have a strong motivation to invest in robust security measures to protect their reputation and brand image Turel et al. (2007).

Moreover, regulatory requirements and industry standards also serve as a motivation for security in the automotive industry. Governments and regulatory bodies around the world are increasingly enacting laws and regulations to address the cybersecurity risks associated with connected vehicles. For instance, the European Union's General Data Protection Regulation (GDPR) includes provisions for data protection and privacy in connected vehicles Andraško et al. (2021); Hamulák et al. (2021), and the United States' National Highway Traffic Safety Administration (NHTSA) has issued guidelines for cybersecurity in vehicles Park and Choi (2020); Das et al. (2019). Additionally, industry organizations, such as the Society of Automotive Engineers (SAE) and the Automotive Information Sharing and Analysis Center (Auto-ISAC), have developed cybersecurity best practices and standards for the automotive industry Al-Jarrah et al. (2019). Compliance with these regulations and standards is essential for automakers to meet legal requirements and demonstrate their commitment to security.

The increasing connectivity and autonomy of vehicles have brought about a growing motivation for security in the automotive industry. Protecting the safety and privacy of vehicle users, preventing unauthorized access and tampering of critical systems, safeguarding the reputation of automakers, and ensuring compliance with regulatory requirements and industry standards are all key motivations for enhancing security in the automotive industry. As the reliance on software, communication networks, and data exchange in vehicles continues to grow, it is imperative for automakers to prioritize cybersecurity measures to mitigate potential risks and protect the integrity, safety, and privacy of connected vehicles and their users.

1.2 Importance of integrating ISO 21434 into SAM

The Security Abstraction Model (SAM) is a comprehensive approach used by the automotive industry to manage cybersecurity risks in vehicles. It provides a structured framework for identifying, assessing, and mitigating cybersecurity threats throughout the vehicle's lifecycle. With the emergence of ISO 21434 Macher et al. (2020), a standard specifically focused on cybersecurity engineering in road vehicles, integrating ISO 21434 into SAM becomes crucial for ensuring robust cybersecurity practices in the automotive industry for the following reasons:

1. Standardization and Consistency: ISO 21434 provides a globally recognized standard for managing cybersecurity risks in the automotive industry. By integrating ISO 21434 into SAM, automakers can ensure that their cybersecurity practices are standardized and consistent across the organization. This promotes uniformity in cybersecurity processes, methodologies, and documentation, making it easier to manage and assess cybersecurity risks consistently throughout the vehicle's lifecycle Macher et al. (2020).

2. Comprehensive Risk Management: ISO 21434 emphasizes the importance of identifying, assessing, and mitigating cybersecurity risks throughout the entire development and operational lifecycle of vehicles. By integrating ISO 21434 into SAM, automakers can establish a comprehensive risk management approach that covers all stages of the vehicle's lifecycle, from design and development to production, operation, and maintenance. This ensures that cybersecurity risks are effectively managed at every stage, reducing the likelihood of potential cybersecurity incidents Macher et al. (2020).

3. Secure Development Practices: ISO 21434 promotes the integration of cybersecurity into the entire development process of automotive systems. By integrating ISO 21434 into SAM, automakers can ensure that secure development practices are followed consistently across all stages of the vehicle's lifecycle. This includes secure coding, secure configuration management, and secure

software supply chain management, ensuring that cybersecurity is considered at every step of the development process Macher et al. (2020).

4. Testing and Validation: ISO 21434 emphasizes the importance of rigorous testing and validation of automotive systems to identify and fix potential cybersecurity vulnerabilities. By integrating ISO 21434 into SAM, automakers can establish a robust testing and validation process that includes vulnerability scanning, penetration testing, and security assessments. This helps in identifying and fixing cybersecurity vulnerabilities before the vehicles are deployed, reducing the risk of potential cyber attacks Macher et al. (2020).

5. Conformance to Regulations and Standards: ISO 21434 is gaining increasing recognition and adoption by regulatory bodies and industry organizations as a standard for managing cybersecurity risks in the automotive industry. By integrating ISO 21434 into SAM, automakers can ensure compliance with industry regulations and standards related to automotive cybersecurity. This includes requirements such as the UN Regulation No. 155 Cybersecurity and Software Updates, which mandates compliance with ISO 21434. Compliance with industry regulations and standards helps automakers demonstrate their commitment to cybersecurity and enhances the overall cybersecurity posture of the vehicles Macher et al. (2020).

Integrating ISO 21434 into the Security Abstraction Model (SAM) is essential for the automotive industry to ensure robust and consistent cybersecurity practices. It promotes standardization, comprehensive risk management, secure development practices, testing and validation, and compliance with industry regulations and standards. By incorporating the guidelines outlined in ISO 21434 into SAM, automakers can strengthen their cybersecurity posture and mitigate cybersecurity risks effectively in vehicles Macher et al. (2020).

1.3 Study Contributions

The goal of this paper is to provide an overview of the benefits, considerations, challenges, and practical applications of integrating the ISO 21434 standard into the existing Security Abstraction Model (SAM) processes for the automotive industry. Specifically, our research aims to:

1. Explain relevance and necessities of integrating ISO 21434 into SAM: Our efforts will provide an overview of the benefits of integrating ISO 21434 into SAM, which include improving the quality and safety of software in vehicles, increasing customer satisfaction, and reducing costs associated with software defects and security breaches.

2. Provide an overview of the key considerations and challenges of the full support of ISO 21434 by SAM: We will discuss the scope of ISO 21434 and how it fits within the SAM framework. It will also provide an overview of the key processes and activities in SAM that need to be adapted or augmented to integrate ISO 21434 effectively. Additionally, we will examine the specific challenges involved in integrating ISO 21434 into SAM, such as resistance to change, lack of resources, and the need to train personnel on new processes and tools.

3. Demonstrate the applicability of SAM that fully supports the ISO 21434: We will provide an automotive system model (the braking system) together with an attack model based on the latest SAM version reflecting various aspects of the standard considering nine process steps (of a total of eleven process steps defined by the standard).

2 Background

The second chapter discusses the growing importance of automotive cybersecurity in the context of the increasing use of software and connectivity in modern vehicles. The chapter introduces ISO 21434,

a standard for automotive cybersecurity engineering that provides guidelines for the development and validation of secure automotive systems and the Security Abstraction Modell (SAM) and its role in facilitating the integration of various components and systems within a vehicle. The chapter concludes by emphasizing the need for integrating ISO 21434 with SAM to ensure the security of automotive systems throughout their lifecycle and to enable effective implementation of cybersecurity measures.

2.1 ISO 21434

ISO 21434 is a standard that specifically focuses on cybersecurity engineering in road vehicles. It was published in 2020 by the International Organization for Standardization (ISO) as ISO 21434:2020 - "Road vehicles – Cybersecurity engineering"Macher et al. (2020). This standard provides a comprehensive framework for managing cybersecurity risks in the automotive industry, with the ultimate goal of ensuring the security and integrity of vehicles and protecting them from cyber threats.

The objectives of ISO 21434 are to provide guidance and requirements for integrating cybersecurity engineering practices into the entire lifecycle of road vehicles. The standard aims to establish a systematic and proactive approach to cybersecurity, covering all stages of vehicle development, production, operation, and maintenance. ISO 21434 provides guidelines for managing cybersecurity risks, establishing secure development practices, conducting testing and validation, and ensuring compliance with regulations and standards.

The main objectives of ISO 21434 can be summarized as follows:

1. Cybersecurity Risk Management: ISO 21434 emphasizes the importance of identifying, assessing, and mitigating cybersecurity risks throughout the entire lifecycle of road vehicles. It provides guidance on establishing a systematic and proactive approach to cybersecurity risk management, including risk identification, risk assessment, risk mitigation, and risk monitoring. The objective is to ensure that cybersecurity risks are effectively managed throughout the entire lifecycle of the vehicle, reducing the likelihood of potential cybersecurity incidents.

2. Secure Development Practices: ISO 21434 promotes the integration of cybersecurity into the entire development process of automotive systems. It provides guidelines for establishing secure development practices, including secure coding, secure configuration management, and secure software supply chain management. The objective is to ensure that cybersecurity is considered at every step of the development process, reducing the risk of potential cybersecurity vulnerabilities in the final product.

3. Testing and Validation: ISO 21434 emphasizes the importance of rigorous testing and validation of automotive systems to identify and fix potential cybersecurity vulnerabilities. It provides guidance on conducting vulnerability scanning, penetration testing, and security assessments to identify and address potential cybersecurity risks. The objective is to ensure that vehicles are thoroughly tested and validated for cybersecurity before they are deployed, reducing the risk of potential cyber attacks.

4. Compliance with Regulations and Standards: ISO 21434 recognizes the importance of compliance with industry regulations and standards related to automotive cybersecurity. It provides guidance on ensuring compliance with applicable regulations and standards, such as UN Regulation No. 155 Cybersecurity and Software UpdatesUNECE (2021a). The objective is to ensure that vehicles meet the requirements of relevant regulations and standards, demonstrating the commitment to cybersecurity and enhancing the overall cybersecurity posture of the vehicles.

ISO 21434 is a standard that aims to provide a comprehensive framework for managing cybersecurity risks in the automotive industry. Its objectives include cybersecurity risk management, integration of secure development practices, testing and validation, and compliance with regulations and standards. By following the guidelines outlined in ISO 21434, the automotive industry can establish robust cybersecurity practices and ensure the security and integrity of vehicles in the face of evolving cyber threats.

2.2 Relationship between ISO 21434 and Vehicle Automation

As vehicle automation continues to advance, with the development of autonomous and semi-autonomous vehicles, the need for robust cybersecurity measures becomes increasingly critical. Vehicle automation relies heavily on software, connectivity, and data processing capabilities, which can be vulnerable to cyber threats. Therefore, integrating cybersecurity into vehicle automation systems is crucial to ensure the safety, security, and reliability of these vehicles Macher et al. (2020).

ISO 21434:2020, titled "Road vehicles – Cybersecurity engineering," is a standard that provides guidance for managing cybersecurity risks in the automotive industry, including vehicles with automation capabilities. This standard is designed to address the unique cybersecurity challenges associated with vehicle automation and provides a framework for incorporating cybersecurity into the development, production, operation, and maintenance of these vehicles.

The relationship between ISO 21434 and vehicle automation can be understood in the following key aspects:

1. Cybersecurity Risk Management for Vehicle Automation: ISO 21434 emphasizes the need for a systematic approach to managing cybersecurity risks throughout the entire lifecycle of road vehicles, including those with automation capabilities. This involves identifying and assessing potential cybersecurity risks associated with vehicle automation, such as unauthorized access, data tampering, and remote manipulation of vehicle functions. It also requires developing appropriate mitigation measures to minimize the risk of cybersecurity threats impacting the safe operation of automated vehicles.

2. Secure Development Practices for Vehicle Automation: ISO 21434 provides guidelines for establishing secure development practices for automotive systems, including those related to vehicle automation. It emphasizes the importance of integrating cybersecurity into the entire development process, including secure coding practices, secure configuration management, and secure software supply chain management. This involves implementing secure coding standards and best practices specifically tailored for vehicle automation, securing communication channels between vehicle automation components, and ensuring the integrity and security of software components and updates used in automated systems.

3. Testing and Validation for Vehicle Automation: ISO 21434 highlights the need for rigorous testing and validation of automotive systems, including those related to vehicle automation. It provides guidelines for conducting vulnerability scanning, penetration testing, and security assessments to assess the security of automated systems. This involves testing the functionality and security of automated features, identifying potential vulnerabilities and weaknesses, and validating the effectiveness of cybersecurity mitigation measures in automated systems before deployment.

4. Compliance with Regulations and Standards for Vehicle Automation: ISO 21434 emphasizes the importance of complying with relevant regulations and standards related to automotive cybersecurity, including those that apply to vehicle automation. This involves understanding and adhering to regulations and standards that specifically address cybersecurity in automated vehicles, such as UN Regulation No. 156 Software Update Processes and Management Systems UNECE (2021b). Compliance with these regulations and standards can help ensure that automated vehicles meet the required cybersecurity requirements and operate securely and safely.

5. Documentation and Traceability for Vehicle Automation: ISO 21434 underscores the need for comprehensive documentation and traceability of cybersecurity-related activities, including those associated with vehicle automation. This involves maintaining clear and traceable records of risk assessments, development practices, testing results, and compliance evidence specifically related to vehicle automation. Documentation and traceability are essential for audit and review purposes, as they provide evidence of compliance and accountability in ensuring the cybersecurity of automated vehicles.

ISO 21434 provides guidance for integrating cybersecurity into the development, production, operation, and maintenance of vehicles with automation capabilities. It emphasizes the importance of cybersecurity risk management, secure development practices, testing and validation, compliance with regulations and standards, and documentation and traceability, specifically tailored for vehicle automation. By following the guidelines provided by ISO 21434, automotive stakeholders can enhance the cybersecurity posture of automated vehicles and ensure their safe and secure operation.

2.3 EAST-ADL

The Architecture Analysis and Design Language (EAST-ADL) is a modeling language used in the automotive and embedded systems domain for describing the architecture and design of complex automotive systems. It provides a comprehensive and systematic approach for modeling the software and hardware components, their interactions, and their relationships with the environment in which they operate. EAST-ADL enables engineers to capture the architectural design decisions, analyze the system's behavior, and support the development of automotive systems with higher quality, safety, and efficiency Cuenot et al. (2010).

EAST-ADL was developed by a consortium of European automotive manufacturers, suppliers, and research institutes as part of the European research project "Model-Based Analysis and Design of Novel Architectures for Dependable Electric Vehicles" (MAENAD) Manead (2021). The project aimed to develop a modeling language and associated analysis techniques to support the design of advanced embedded control systems, particularly in the automotive domain.

Some key features of EAST-ADL include:

1. Comprehensive Modeling Capabilities: EAST-ADL provides a rich set of modeling concepts and notations for describing the architecture and design of automotive systems. It allows engineers to model the system's structure, behavior, and interactions, including the software and hardware components, their interfaces, their connections, their modes of operation, and their communication and data exchange mechanisms Cuenot et al. (2010).

2. Support for Functional and Non-functional Requirements: EAST-ADL allows engineers to capture both functional and non-functional requirements of automotive systems. This includes modeling the system's functionality, performance, safety, reliability, and other quality attributes. EAST-ADL also supports the modeling of timing, resource allocation, and other system-level constraints Cuenot et al. (2010).

3. Analysis and Simulation Capabilities: EAST-ADL provides analysis and simulation capabilities that enable engineers to evaluate the behavior and performance of the system at the architectural level. This includes support for model checking, simulation, and other analysis techniques to detect potential design flaws, performance bottlenecks, and other issues early in the development process Cuenot et al. (2010).

4. Integration with Other Modeling Languages: EAST-ADL is designed to be compatible and interoperable with other modeling languages commonly used in the automotive domain, such as the AUTOSAR (AUTomotive Open System ARchitecture) standard. This allows engineers to integrate EAST-ADL models with models developed in other modeling languages, facilitating system-level analysis and simulation Cuenot et al. (2010).

5. Tool Support: Several modeling tools and frameworks are available that support the use of EAST-ADL, providing engineers with a graphical user interface and automated analysis capabilities. These tools help streamline the modeling and analysis process, making it more efficient and effective Cuenot et al. (2010). The modeling tool MetaEdit+ Tolvanen and Rossi (2003) has a full integration of the EAST-ADL as well as a full integration of SAM. So a wholesome modeling process is ensured.

EAST-ADL is a powerful modeling language used in the automotive and embedded systems domain for describing the architecture and design of complex systems. It provides comprehensive modeling capabilities, supports functional and non-functional requirements, offers analysis and simulation capabilities, integrates with other modeling languages, and has tool support, making it a valuable tool for automotive system design Cuenot et al. (2010).

2.4 SAM

The automotive industry is undergoing a significant transformation with the rapid advancement of software-intensive technologies, such as connected cars, autonomous driving, and electric vehicles. However, this increasing complexity and connectivity also bring about new challenges in terms of cybersecurity, as vehicles become vulnerable to various cyber threats, including hacking, data breaches, and remote manipulation.

In response to these challenges, the Security Abstraction Model (SAM) Zoppelt and Tavakoli Kolagari (2019); Bergler et al. (2021); Bergler, Tolvanen, and Kolagari (Bergler et al.) has emerged as a significant concept in the automotive industry. SAM provides a structured approach to model, analyze, and enforce security aspects in the development of automotive software systems. It aims to improve the security assurance, streamline the development process, and enhance the resilience of vehicles against security threats.

The importance of SAM in the automotive industry can be highlighted in several key aspects:

1. Comprehensive Security Management: SAM offers a comprehensive framework for managing security concerns in automotive software development. It provides a systematic approach to identify, analyze, and mitigate security risks throughout the entire development lifecycle of vehicles, from design and implementation to testing and deployment. SAM helps automotive manufacturers and suppliers to effectively manage security aspects in their software systems, ensuring that the vehicles are protected against potential cyber threats.

2. Standardization and Consistency: SAM provides a standardized and consistent approach to modeling and analyzing security aspects in automotive software systems. It offers a common language and methodology for describing security threats, security architectures, and security analysis techniques. This standardization enables better collaboration among different stakeholders in the automotive industry, such as automakers, suppliers, and security experts, and helps to ensure a consistent and unified approach to security across different automotive systems.

3. Enhanced Security Assurance: SAM supports the development of more secure software systems by providing a structured approach to security assurance. It enables the identification of potential security risks early in the development process, allowing for timely mitigation measures to be implemented. SAM also provides a way to systematically verify and validate the security measures in place, improving the overall security assurance of automotive software systems.

4. Improved Efficiency and Resilience: SAM helps streamline the development process of automotive software systems by providing a structured approach to security. It reduces the complexity and ambiguity of security considerations, making it easier for developers to integrate security measures into their software designs. This improved efficiency allows for more effective development of secure software systems, reducing the risk of security breaches and enhancing the resilience of vehicles against threats.

5. Compliance with Industry Standards: SAM aligns with industry standards and guidelines for automotive security, such as ISO 21434, AUTOSAR, and EAST-ADL, which are widely adopted in the automotive industry. By incorporating SAM into the development process, automotive manufacturers and suppliers can ensure compliance with these standards and guidelines, demonstrating their commitment to security best practices.

SAM plays a crucial role in addressing the security challenges faced by the automotive industry. It provides a structured approach to model, analyze, and enforce security aspects in the development of automotive software systems, leading to improved security assurance, streamlined development process, and enhanced resilience against threats.

3 Case Study Braking System

The following scenario is described as an example of the use of SAM and the new features of ISO 21434: Imagine a situation where a hacker gains unauthorized access to the data communication network of a car's braking system. The hacker then intentionally interferes with the communication signals between the car's brake control module and the wheel speed sensors. As a result, the brake system receives incorrect information about the speed of the wheels and the car's braking distance. This causes the brake system to malfunction and fail to engage, even when the driver presses the brake pedal. Consequently, the car is unable to slow down or stop in time, and it collides with another vehicle or object, causing an accident. In this scenario, the hacker's malicious actions disrupt the normal operation of the car's braking system, creating a dangerous situation that puts the driver, passengers, and other road users at risk of injury or death.

3.1 EAST-ADL System Model of the Braking System

The EAST-ADL is an architecture description language that models the core of a system and has manifold complementary models that capture additional information, such as timing, variability, dependability and so on. The modeling of the core has two main and widely appreciated features in practice: first, the system model is described on predefined abstraction levels, starting with an abstract feature modeling as well as two architecture description levels, where the analysis level is a purely functional logical description and the design level already includes a description of hardware and software; second, the component-oriented approach to architecture description is based on a type/prototype concept, which allows for the reuse of components from a component library.

In this Figure 1 we see a small excerpt from the abstract level (the Vehicle Level) and the first architecture description level (the Analysis Level). The item "BrakeByWire", which is to be understood in accordance with the item definition from the standard ISO 26262, refers in this case to the vehicle feature "BrakeByWire" from the Vehicle Level and is realized by the function "BBW_FAA" from the Analysis Level. We can see the internal components of the function "BBW_FAA" in the lower part of the figure, consisting of a sensor "BrakePedal" and four actuators "ABS" (one actuator for each wheel) and a control unit.

3.2 Security Model of the Braking System

As previously discussed, the integration of the ISO 21434 standard into the Security Abstraction Model SAM has many advantages for the automotive industry. The integration of the ISO made some demands on the meta model. The following addressed points from the ISO therefore had to be checked or integrated to complete SAM:

1. Item Definition (ISO 21434 Section 9.3): The item definition is a central component of ISO 21434 and describes the definition and specification of safety-critical elements in a vehicle. It is about gaining a comprehensive understanding of the functions and characteristics of these elements in order to identify and eliminate potential vulnerabilities in the system. The item definition includes a comprehensive analysis of the safety-critical elements, including their functions, interfaces, data flows, requirements, and risks. It also considers the interaction of the elements with each other and with other systems. The item definition is a crucial step in the process of automotive cybersecurity development, ensuring that the systems meet the security requirements and are protected against potential threats.

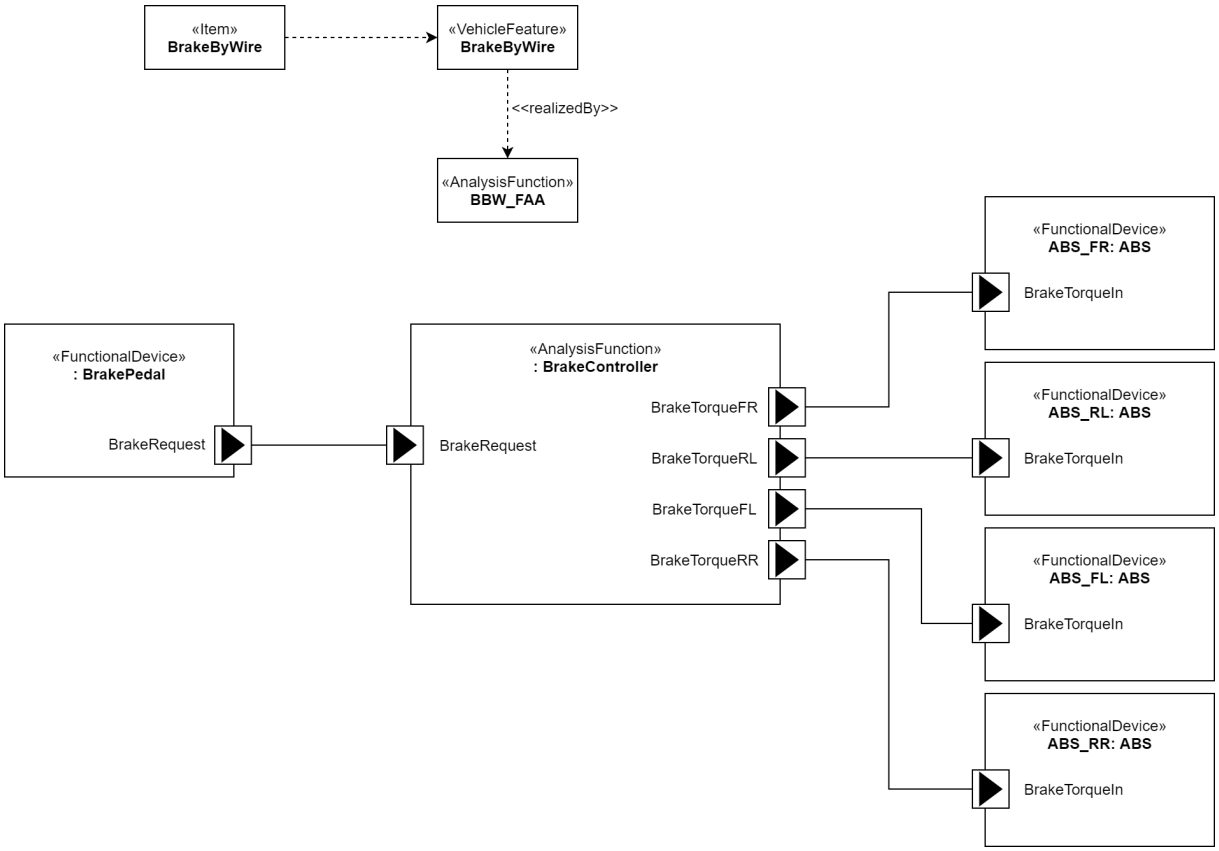

Figure 1: This figure shows the Analysis Architecture of the braking function based on EAST-ADL.

2. Asset Identification (ISO 21434 Section 15.3): Asset Identification is another critical component of ISO 21434 that plays a crucial role in the development of secure automotive systems. Asset Identification refers to the process of identifying the assets that need to be protected within the system. These assets may include hardware, software, data, or other resources that are critical to the proper functioning of the system. The goal of Asset Identification is to gain a comprehensive understanding of the assets and their characteristics in order to properly assess the risks associated with each asset and develop effective security measures. This process involves a detailed inventory of all assets and their associated risks, as well as the establishment of asset classifications and their criticality levels. By properly identifying and classifying assets, the development team can better understand the security requirements of the system and ensure that adequate security measures are implemented to protect the system against potential cyber threats.

3. Identification of Threat Scenarios (ISO 21434 Section 15.4): Threat scenarios are a critical part of ISO 21434 and involve identifying potential cybersecurity threats that could impact automotive systems. This includes identifying potential attack vectors and the potential impacts of a successful cyberattack. By using threat scenarios, the development team can develop more effective security measures and reduce the risk of a successful cyberattack. They are an essential part of ensuring the safety and security of automotive systems.

4. Impact Rating (ISO 21434 Section 15.5): Impact Rating is a process in ISO 21434 used to evaluate the potential impact of a cybersecurity threat on the system by assigning a severity level to each potential threat based on its potential harm and feasibility of mitigation. This helps prioritize security efforts and allocate resources accordingly to ensure the safety and security of automotive systems.

5. Attack Path Analysis (ISO 21434 Section 15.6): In the context of ISO 21434, Attack Path Anal-

ysis is an important tool for identifying potential cybersecurity threats to automotive systems and developing appropriate security measures to mitigate those threats. It is a critical component of the risk management process outlined in the standard and is used to help ensure the safety and security of automotive systems throughout their lifecycle.

6. Attack Feasibility Rating (ISO 21434 Section 15.7): The Attack Feasibility Rating is a process within ISO 21434 that evaluates the likelihood of a successful cybersecurity attack by assessing the attacker's resources and access to information. It helps prioritize security measures and allocate resources accordingly, based on the most significant threats to the system. This process helps to ensure the safety and security of automotive systems.

7. Risk Value Determination (ISO 21434 Section 15.8): ISO 21434 includes a process called risk value determination, which is used to evaluate the level of risk posed by cybersecurity threats to automotive systems. This process assigns a numerical value to each threat and helps the development team prioritize security measures and allocate resources effectively. By using risk value determination, the development team can identify and address the most significant threats to the system's safety and security, ensuring appropriate security measures are implemented. Overall, risk value determination is a vital aspect of ISO 21434, supporting the safe and secure development of automotive systems.

8. Risk Treatment Decision (ISO 21434 Section 15.9): The ISO 21434 standard outlines a process for making decisions about how to treat cybersecurity risks in automotive systems. This involves selecting and implementing security measures to reduce the risks to an acceptable level. The purpose of this process is to prioritize security measures and allocate resources effectively.

9. Cybersecurity Goals (ISO 21434 Section 9.4) [WP-09-03 & RQ-09-07]: The ISO 21434 standard defines cybersecurity goals for automotive systems. These goals help ensure that the system is secure against potential threats and that any vulnerabilities are identified and addressed appropriately. The cybersecurity goals specified in the standard are designed to be flexible and adaptable to different use cases and system architectures. By setting clear goals for cybersecurity, the standard aims to promote a more systematic and comprehensive approach to cybersecurity in the automotive industry.

10. Cybersecurity Claims (ISO 21434 Section 9.4) [WP-09-04 & RQ-09-06]: The cybersecurity claims defined in the ISO 21434 standard refer to the features and functions of automotive systems that provide cybersecurity protection. These claims serve as a means of communicating the level of cybersecurity protection to customers and stakeholders. To ensure that cybersecurity claims are accurate and reliable, the standard requires that they be based on evidence and that they are verifiable. This helps ensure that customers and stakeholders can make informed decisions about the security of the system. The standard also provides guidance on how to test and verify cybersecurity claims to ensure that they are accurate and reliable.

11. Cybersecurity Concept (ISO 21434 Section 9.5): The Cyber Security Concept is a description of the security objectives and measures that apply to an automotive system, as defined in the ISO 21434 standard. It serves as a high-level guide for the development of effective cybersecurity measures and is regularly reviewed and updated throughout the development process.

After making adjustments to the meta model, the previously created scenario has now been replicated as a security model (see Figure 2. This security model focuses on the "BrakeByWire" feature, which interfaces with the EAST-ADL in a vehicle. With the integration of ISO 21434 in SAM, new scores such as "AttackFeasibility", "ImpactRating", and "RiskValue" can now be calculated in addition to the Common Vulnerability Scoring Systems (CVSS) Mell et al. (2006) Base and Temporal score. These scores are essential for assessing the level of risk posed by potential security threats and vulnerabilities in the system. With the ability to calculate these scores in SAM, the system can be analyzed comprehensively

and appropriate security measures can be implemented to mitigate potential risks and ensure the safety and security of the system and its users.

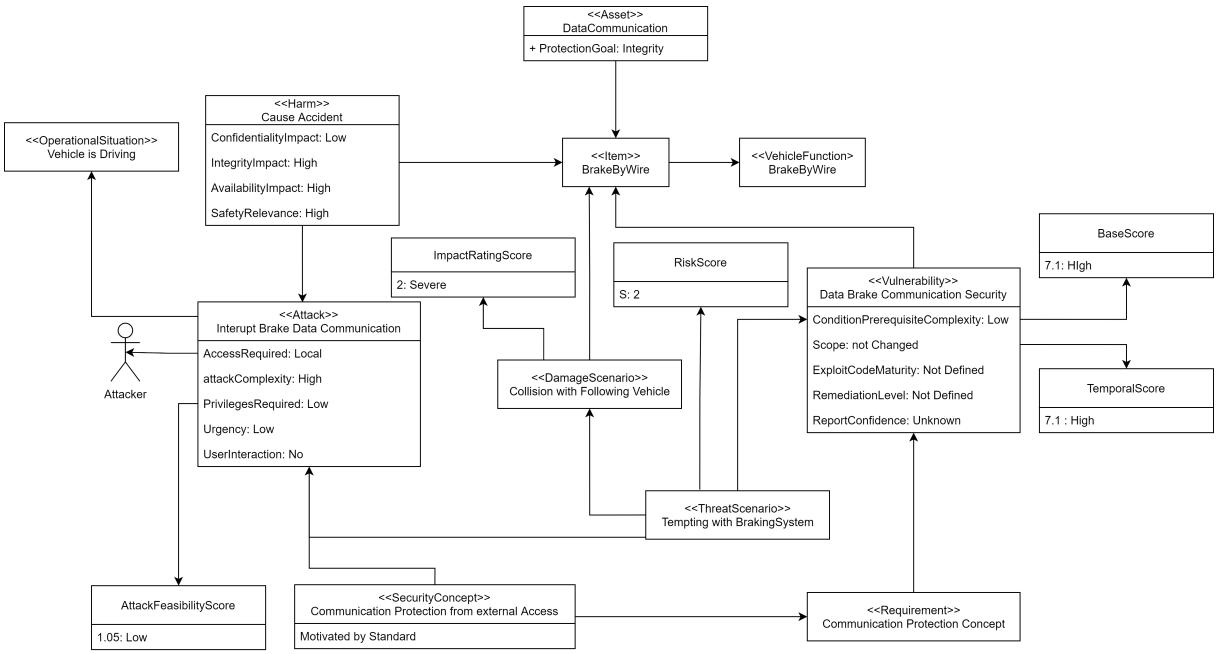

Figure 2: This figure shows the Security Model of the braking system based on SAM.

3.3 Scoring Calculation

Thanks to the successful integration of ISO 21434, it is not only possible to evaluate vulnerabilities, but also attacks and their impact on a system. For this purpose, new scores are introduced in the metamodel based on the ISO 21434 standard:

1. The Common Vulnerability Scoring System (CVSS) is a framework used to evaluate and measure the severity of security vulnerabilities. It provides a consistent and standardized way to assess the potential impact of a vulnerability and assign a score, which can be used to prioritize and plan security measures. CVSS was developed by the Forum of Incident Response and Security Teams (FIRST) and is widely used by security professionals and organizations to evaluate and communicate the severity of security vulnerabilities. This score is already integrated into SAM Bergler, Tolvanen, and Kolagari (Bergler et al.).

2. AttackFeasibilityScore: The AttackFeasibilityScore refers to the attack feasibility rating from the standard. This describes the feasibility of an attack on our system. The calculation basis for this is the already implemented CVSS score. According to CVSS, the ratings are mapped to numbers and used in the corresponding formula from the standard. The new formula is ($E = 8.22xVxCxPxU$) Macher et al. (2020) where E is the exploitability value; V for the value of the attack vector; C for the attack complexity value; P for the value of the privileges required and U for the value of the user interaction. This value can then be mapped back to a textual evaluation based on the standard.

3. ImpactRatingScore: The ImpactRatingScore refers to the impact rating from ISO 21434. This value describes the severity of the consequences of a damage scenario. The impact rating can have the values Negligible (0), Moderate (1), Major (1.5) and Severe (2).

4. RiskScore: The RiskScore refers to the risk value determination from the standard. This value describes the risk that a threat scenario will occur. According to ISO 21434, this value can be determined either using a matrix or using your own calculation formulas. In both cases, the Impact

Rating and the Attack Feasibility Rating are used. In our example, we use the risk matrix provided in the standard.

In our example, the following values result for the respective scores:

- BaseScore: 7.1 High
- TemporalScore: 7.1 High
- AttackFeasibilityScore: 1.05 Low ($E = 8.22x0.55x0.44x0.62x0.85$)
- ImpactRatingScore: 2: Severe (based on the definition in the standard)
- RiskScore: S: 2 (based on the evaluation matrix in the standard)

4 Integrating ISO 21434 into SAM

The integration of the standard into SAM has changed the metamodel and the items Asset, Damage Scenario, Threat Scenario, ImpactRatingScore, RiskScore, AttackFeasibilityRating and AttackFeasibilityScore needed to be added as seen in the Figure 2. The current meta model can be viewed online [1]. The new item asset complements the existing target in the metamodel, which can be both a "Human-Actor" and an "Item" in the sense of ISO 26262. According to ISO 21434, a damage scenario refers to a hypothetical event or sequence of events that could lead to harm to the vehicle, its occupants, or its surroundings. It takes into account the potential sources of harm, the likelihood of the harm occurring, and the severity of the harm that could result. The purpose of defining damage scenarios is to identify the risks associated with the use of the vehicle and to establish measures to prevent or mitigate the effects of those risks. With the introduction of the new item "DamageScenario", the consequences of a successful attack can now be modeled and additionally evaluated by the "ImpactRatingScore". A threat scenario, according to ISO 21434, is a hypothetical situation or sequence of events that could lead to a security threat to a vehicle's functions, components, or data. It includes the potential sources of the threat, the probability of the threat occurring, and the severity of the consequences that could result. The goal of defining threat scenarios is to identify potential security risks and vulnerabilities and to establish measures to prevent or mitigate the effects of those risks. Threat scenarios are an essential part of the risk analysis process in the development of secure vehicles. By integrating the item "ThreatScenario" it is now possible to describe the attack scenario more precisely. In addition, in combination with the other newly introduced scores, an assessment of the risk for such a scenario can be given using the "RiskScore" item. Based on these scores, a strategy can now be developed as to which measures are to be taken to avoid them. The already existing item "Attack" was supplemented by the "AttackFeasibilityScore", whereby the feasibility of an attack can be better assessed. Since CVSS is already integrated into SAM, this can be used as a basis for calculations. The new scores are currently calculated manually because there is no tool support for the new SAM version. Thanks to the successful integration, the following points can now be reliably modeled with SAM:

1. Item Definition
2. Asset Identification
3. Identification of Threat Scenarios
4. Impact Rating
5. Attack Path Analysis
6. Attack Feasibility Rating

[1] https://www.in.th-nuernberg.de/professors/BerglerMa/SAM/

7. Risk Value Determination
8. Risk Treatment Decision
9. Cybersecurity Concept

As far as our research suggests, the two outstanding points Cybersecurity Goals and Cybersecurity Claims are already covered via SAM. However, the standard is not clear here and further research is therefore required to confirm the thesis with certainty.

5 Conclusion

By providing a structured approach for cybersecurity management of road vehicles, ISO 21434 can help ensure that cybersecurity considerations are integrated into the development process for automotive software. However, the process of integrating ISO 21434 into SAM also required adjustments to the existing meta model.

This paper has provided an overview of the key considerations when integrating ISO 21434 into SAM, including the benefits and challenges of the integration as well as the practical application of the integration. The paper has highlighted the importance of adapting or augmenting SAM processes and activities to integrate ISO 21434 effectively.

By preparing an example, the paper has demonstrated how integrating ISO 21434 into SAM may improve the quality and security of software in vehicles, which has the potential to result in increased customer satisfaction, improved brand reputation, and reduced costs associated with software defects and security breaches.

Next steps in development include a comprehensive evaluation study, as well as providing appropriate tool support with the new functionality to enable easier use.

The next development steps include both the provision of suitable tool support and an evaluation study with which the use of SAM in the development process is to be evaluated.

MetaEdit+ will continue to be used for tool support, as good experiences have already been made here in advance. Thanks to the integration in MetaEdit+, there is not only complete access to the contents of the EAST-ADL and thus ISO 26262 for functional safety, but also to the security supplement via SAM. In addition, the newly integrated scores from ISO 21434 can be calculated automatically with MetaEdit+, as has already been done with CVSS.

The evaluation study is to be carried out in cooperation with representatives from the industry. The development process of a vehicle component is to be exercised as an example by using the EAST-ADL and SAM using tool support through MetaEdit+. The representatives from the industry should then give an assessment and feedback on the usability and benefits of SAM.

References

Al-Jarrah, O. Y., C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis (2019). Intrusion detection systems for intra-vehicle networks: A review. *IEEE Access 7*, 21266–21289.

Andraško, J., O. Hamul'ák, M. Mesarčík, T. Kerikmäe, and A. Kajander (2021). Sustainable data governance for cooperative, connected and automated mobility in the european union. *Sustainability 13*(19), 10610.

Bergler, M., J.-P. Tolvanen, and R. T. Kolagari. Integrating security and safety with systems engineering: a model-based approach.

Bergler, M., J.-P. Tolvanen, M. Zoppelt, and R. T. Kolagari (2021). Social engineering exploits in automotive software security: Modeling human-targeted attacks with sam. In *31st European Safety and Reliability Conference, ESREL 2021*, pp. 2502–2509.

Cuenot, P., P. Frey, R. Johansson, H. Lönn, Y. Papadopoulos, M.-O. Reiser, A. Sandberg, D. Servat, R. Tavakoli Kolagari, M. Törngren, et al. (2010). The east-adl architecture description language for automotive embedded software. In *Model-Based Engineering of Embedded Real-Time Systems: International Dagstuhl Workshop, Dagstuhl Castle, Germany, November 4-9, 2007. Revised Selected Papers*, pp. 297–307. Springer.

Das, S., S. R. Geedipally, K. Dixon, X. Sun, and C. Ma (2019). Measuring the effectiveness of vehicle inspection regulations in different states of the us. *Transportation research record 2673*(5), 208–219.

Guan, T., Y. Han, N. Kang, N. Tang, X. Chen, and S. Wang (2022). An overview of vehicular cybersecurity for intelligent connected vehicles. *Sustainability 14*(9), 5211.

Hamulák, O., J. Andraško, and M. Mesarcik (2021). The digital development of the european union: data governance aspects of cooperative, connected and automated mobility. *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política* (34), 7.

Luo, F., Y. Jiang, Z. Zhang, Y. Ren, and S. Hou (2021). Threat analysis and risk assessment for connected vehicles: A survey. *Security and Communication Networks 2021*, 1–19.

Macher, G., C. Schmittner, O. Veledar, and E. Brenner (2020). Iso/sae dis 21434 automotive cybersecurity standard-in a nutshell. In *Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops: DECSoS 2020, DepDevOps 2020, USDAI 2020, and WAISE 2020, Lisbon, Portugal, September 15, 2020, Proceedings 39*, pp. 123–135. Springer.

Manead, M. (2021). About.

Mell, P., K. Scarfone, and S. Romanosky (2006). Common vulnerability scoring system. *IEEE Security & Privacy 4*(6), 85–89.

Park, S. and J.-Y. Choi (2020). Malware detection in self-driving vehicles using machine learning algorithms. *Journal of advanced transportation 2020*, 1–9.

Schoettle, B. and M. Sivak (2014). A survey of public opinion about connected vehicles in the us, the uk, and australia. In *2014 International Conference on Connected Vehicles and Expo (ICCVE)*, pp. 687–692. IEEE.

Tolvanen, J.-P. and M. Rossi (2003). Metaedit+ defining and using domain-specific modeling languages and code generators. In *Companion of the 18th annual ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications*, pp. 92–93.

Turel, H. S., E. M. Yigit, and I. Altug (2007). Evaluation of elderly people's requirements in public open spaces: A case study in bornova district (izmir, turkey). *Building and Environment 42*(5), 2035–2045.

UNECE, U. (2021a, Apr). Un regulation no. 155 - cyber security and cyber security management system.

UNECE, U. (2021b, Apr). Un regulation no. 156 - software update and software update management system.

Wang, Y., Y. Wang, H. Qin, H. Ji, Y. Zhang, and J. Wang (2021). A systematic risk assessment framework of automotive cybersecurity. *Automotive Innovation 4*, 253–261.

Zoppelt, M. and R. Tavakoli Kolagari (2019). Sam: a security abstraction model for automotive software systems. In *Security and Safety Interplay of Intelligent Software Systems: ESORICS 2018 International Workshops, ISSA 2018 and CSITS 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers*, pp. 59–74. Springer.