ENSURING CYBERSECURITY STANDARDS COMPLIANCE BY INTEGRATION OF MULTIPLE STANDARDS IN THE CONTEXT OF AUTOMOTIVE SOFTWARE DEVELOPMENT PROJECTS

Teză de doctorat – Rezumat în engleză

pentru obținerea titlului științific de doctor la

Universitatea Politehnica Timișoara

în domeniul de doctorat ____Inginerie si Management____

autor ing. __Darius Barmayoun__

conducător științific ___ Prof.ing.dr.ec Marian Mocan __

luna_02_ anul_2025_

INTRODUCTION

The automotive industry is undergoing a significant transformation driven by rapid technological advancements and increasing connectivity. This shift is not just about new technologies but a fundamental redefinition of vehicle design, development, and operation. The growing presence of connected vehicles amplifies cybersecurity risks, exposing society to potential cyberattacks (1). Modern vehicles are no longer just transportation devices; they are sophisticated, interconnected systems integrating autonomous driving capabilities, IoT-enabled devices, and complex electronic architectures. This evolution introduces critical cybersecurity challenges, as the likelihood and severity of cyber threats continue to increase (2).

Ensuring cybersecurity in the automotive industry is now an essential priority. As electronic and electrical (E/E) systems advance, traditional communication protocols like the Controller Area Network (CAN) bus are being supplemented or replaced by technologies such as automotive Ethernet (3). These advancements expand the attack surface, making vehicles and their ecosystems vulnerable to cyber threats, which compromise user privacy, safety, and operational integrity. This risk also extends to Original Equipment Manufacturers (OEMs) and their suppliers, necessitating strong cybersecurity measures (4). Cybersecurity in the automotive sector requires a sector-specific approach, considering the industry's unique characteristics, such as long product lifecycles, complex supply chains, and stringent safety requirements. This includes securing Vehicle-to-Everything (V2X) communications, cloud-based services, and the integrity of Electronic Control Units (ECUs). While V2X-related cyberattacks are still in their early stages, they are expected to become increasingly common in the coming years (4).

In response to these risks, regulators and industry bodies have introduced comprehensive cybersecurity standards and frameworks. Among the most significant are ISO/SAE 21434 and ASPICE for Cybersecurity, which establish structured methodologies for managing cybersecurity risks in automotive systems. Additionally, the UNECE WP.29 R155 and R156 regulations, introduced in 2021, mandate cybersecurity compliance for all new vehicles starting in July 2024 (5). These regulations and standards ensure a structured approach to cybersecurity risk management, providing best practices and a common language for industry stakeholders.

Key Standards and Regulations:

1. ISO/SAE 21434 – A fundamental cybersecurity framework that addresses risk management throughout the automotive lifecycle, covering risk assessment, incident response, and recovery (6).

2. ASPICE for Cybersecurity – An adaptation of Automotive SPICE, providing guidelines for the development and assessment of cybersecurity-related automotive projects (7).
3. UNECE WP.29 R155 & R156 – Global regulations requiring cybersecurity measures in vehicle production and mandating compliance audits, with full enforcement beginning in July 2024 (8,9).

While these standards provide structured approaches to cybersecurity, implementation remains a challenge, especially for Tier 1 and Tier 2 suppliers. These suppliers must integrate cybersecurity requirements into their products and development processes, a complex and resource-intensive task. The growing regulatory landscape necessitates efficient compliance mechanisms to reduce resource demands related to audits and assessments.

Therefore, this introduction sets the foundation for understanding cybersecurity in the automotive sector by reviewing UNECE R155 & R156, ISO/SAE 21434, and ASPICE for Cybersecurity. It highlights the necessity of harmonizing these frameworks to simplify compliance and enhance cybersecurity resilience. By addressing these challenges, the industry can establish a more secure and robust automotive ecosystem, ensuring compliance while mitigating evolving cyber threats. This discussion contributes both to academic research and practical industry implementation, reinforcing the critical role of cybersecurity in modern automotive systems.

CYBERSECURITY IN THE AUTOMOTIVE INDUSTRY

Cybersecurity in the automotive industry has evolved significantly, emerging as a critical concern only in recent years. Historically, the industry focused on functional safety, prioritizing the physical integrity and reliability of vehicles to prevent mechanical failures and accidents. Unlike sectors such as finance or healthcare, which integrated cybersecurity early due to their digital nature, the automotive sector lagged behind in cybersecurity adoption (10). With the introduction of CASE (Connected, Automated/Autonomous, Shared/Service, Electrification) technologies and the rise of Industry 4.0, the automotive industry now faces increasing cybersecurity challenges. The transition toward connected and autonomous vehicles has expanded the attack surface, introducing threats that compromise not just physical safety but also data security and privacy (11,12). The rise of IoT, telematics, and autonomous driving has dramatically increased vehicle exposure to cyber risks. Autonomous vehicles, which rely on sensors and data processing, are vulnerable to sensor spoofing, software manipulation, and network breaches (13). Additionally, electric vehicles (EVs) present new cybersecurity challenges related to charging networks, battery management systems, and data privacy (14). For instance, the 2015 Jeep Cherokee hack demonstrated the real-world risks of cyber vulnerabilities, where researchers remotely took control of a vehicle through its entertainment system (15). Similarly, increased integration of sensors in EVs has led to privacy concerns, as they collect and store sensitive driver data that can be exploited for malicious purposes (16,17).

Cybersecurity threats in the automotive sector stem from multiple actors, including:

- State-sponsored hackers targeting infrastructure and public systems (8).
- Black-hat hackers exploiting vehicle vulnerabilities for financial gain, as seen in keyless vehicle thefts (8).
- Hackers for personal gain, manipulating software or hardware for unauthorized modifications (8).

According to the 2022 Upstream Cybersecurity report, 84.5% of cyberattacks in 2021 were remote, demonstrating the shift from physical attacks to long-range hacking methods using cellular networks,

APIs, and internet-based vulnerabilities (8). By 2022, 97% of all attacks were remote, reflecting the growing sophistication of cybercriminals and the broader attack surface of connected vehicles (5).

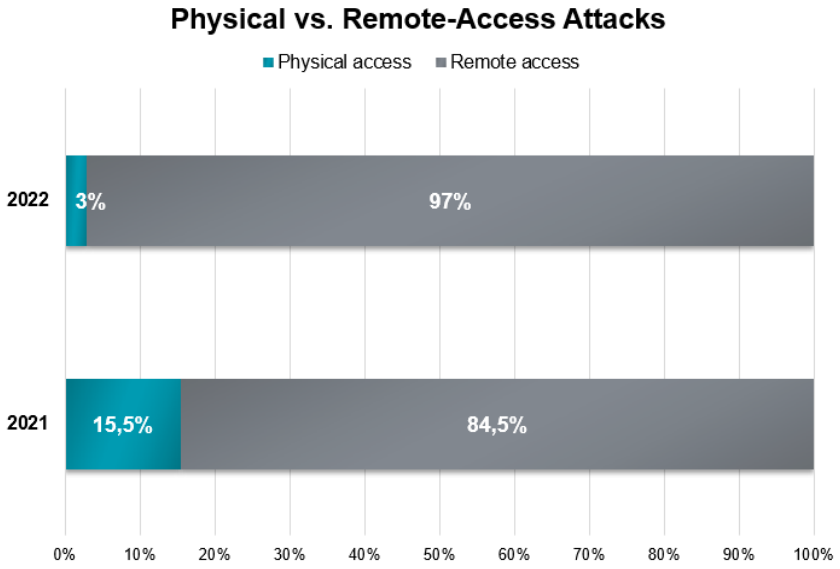

Fig. 1. Physical vs. Remote-Access Attacks 2021 vs.2022
[8][5]

The realization of cybersecurity risks led to the introduction of regulatory standards aimed at securing automotive systems. The UNECE WP.29 regulations, developed by the United Nations Economic Commission for Europe, have been a turning point in automotive cybersecurity (5). These regulations mandate continuous cybersecurity risk management, software updates, and compliance audits throughout a vehicle's lifecycle. WP.29 establishes cybersecurity as a fundamental component of automotive safety, shifting the industry from a reactive approach to a proactive and holistic security strategy.

In addition to WP.29, ISO/SAE 21434 provides a structured approach to cybersecurity risk management, covering risk assessment, mitigation, and incident response (5). Together, these standards ensure that cybersecurity is integrated into the vehicle development and operational lifecycle. The implementation of cybersecurity regulations and standards is reshaping vehicle design, manufacturing, and post-market services. Automotive companies must invest in cyber risk assessment, secure software development, and compliance processes, which introduce financial and operational challenges (5). However, cybersecurity compliance is not just a regulatory requirement; it has become a competitive advantage, influencing consumer trust, legal liabilities, and market differentiation. Looking ahead, emerging technologies such as Artificial Intelligence (AI) and Blockchain are expected to play a crucial role in strengthening cybersecurity frameworks in the automotive sector. AI-driven cybersecurity solutions can detect and respond to threats in real-time, while blockchain technology can enhance data integrity and transparency in vehicle networks (5).

Cybersecurity has become an indispensable element of modern automotive systems, evolving from an overlooked concern to a key pillar of safety and regulatory compliance. The transition to connected and autonomous vehicles has expanded the threat landscape, necessitating advanced security measures, regulatory alignment, and industry-wide cooperation. The UNECE WP.29 regulations and ISO/SAE 21434 standard have set a new foundation for cybersecurity in the automotive industry, ensuring that cybersecurity is not only a technical necessity but a strategic imperative for future mobility.

DEVELOPMENT OF REGULATORY AUTOMOTIVE CYBERSECURITY STANDARDS

The increasing complexity and frequency of cybersecurity threats in the automotive sector have necessitated the development of comprehensive regulatory frameworks and standards to safeguard connected and autonomous vehicles. Historically, the automotive industry primarily focused on functional safety, ensuring the physical integrity and reliability of vehicles. However, with the rapid digital transformation of vehicles, cybersecurity has become an essential pillar of modern automotive safety. The growing reliance on software-driven functionalities, connected services, and over-the-air (OTA) updates has increased the risk of cyber threats, requiring a systematic and proactive approach to cybersecurity compliance (18). In response to these challenges, key regulations and standards such as UNECE WP.29 R155 and R156, ISO/SAE 21434, and ASPICE for Cybersecurity have been introduced to establish uniform security measures across the automotive lifecycle. These frameworks are not merely guidelines but enforceable mandates that require automakers to integrate cybersecurity into vehicle design, development, production, and post-production operations (18).

The UNECE WP.29 regulations, introduced in June 2020, marked a critical turning point in global automotive cybersecurity. The R155 regulation mandates that automakers establish a Cybersecurity Management System (CSMS) to ensure continuous risk management and mitigation across the entire vehicle lifecycle. This regulation compels manufacturers to identify and mitigate cyber threats during development, implement cybersecurity controls in production, and maintain ongoing security protections post-production (19). Additionally, R156 focuses specifically on software update security, requiring manufacturers to secure OTA update mechanisms and reapply for approval when software modifications impact technical performance (20). These regulations ensure that cybersecurity is not limited to pre-market development but remains an ongoing obligation throughout the operational life of a vehicle.

Alongside UNECE regulations, ISO/SAE 21434 has become a cornerstone standard for cybersecurity in the automotive industry. Developed collaboratively by ISO and SAE International, this standard establishes a structured approach for assessing and managing cybersecurity risks across the entire automotive engineering process. Unlike UNECE WP.29, which focuses on regulatory compliance, ISO/SAE 21434 provides a detailed framework for risk assessment, incident response, and cybersecurity governance within automotive organizations. It defines methodologies for calculating risk scores, prioritizing vulnerability management, and integrating cybersecurity practices from conceptualization to decommissioning (4). This standard supports the UNECE WP.29 regulations by offering technical guidance on how cybersecurity requirements should be met, ensuring that cybersecurity becomes an intrinsic part of vehicle engineering rather than an afterthought.

The Upstream Security Global Automotive Cybersecurity Reports (2021 and 2022) highlight the challenges faced by regulatory bodies in keeping pace with rapid technological advancements. The 2021 report emphasizes that the speed of innovation in connected vehicle technologies has often outpaced regulatory development, a trend previously observed with privacy laws such as the General Data Protection Regulation (GDPR), which was implemented after widespread digital adoption (18). Similarly, the automotive industry has seen a gap between the deployment of connected technologies and the introduction of cybersecurity regulations, leading to vulnerabilities that cybercriminals have exploited. Recognizing this urgency, the introduction of UNECE WP.29 regulations and ISO/SAE 21434 in 2020 was a crucial step in addressing these cybersecurity gaps. These frameworks not only ensure compliance but also enable automakers to deploy innovative cybersecurity measures while maintaining regulatory oversight (8).

In addition to UNECE WP.29 and ISO/SAE 21434, ASPICE for Cybersecurity plays a vital role in aligning cybersecurity practices with automotive software development. Automotive SPICE (ASPICE) is a widely recognized framework for process improvement in software engineering, and its

cybersecurity extension ensures that cybersecurity is integrated into software development from the early design stages. ASPICE for Cybersecurity helps automakers and suppliers streamline cybersecurity compliance, improve software security, and establish systematic processes for identifying and mitigating cyber risks. By incorporating cybersecurity into the entire software lifecycle, ASPICE ensures that secure coding, vulnerability testing, and threat modelling are embedded into automotive development practices, reducing the risk of cyber vulnerabilities in production vehicles. The relationship between these regulatory frameworks and standards highlights a shift in the automotive industry from reactive cybersecurity measures to proactive and integrated cybersecurity strategies. UNECE WP.29 provides a regulatory baseline, ISO/SAE 21434 offers technical methodologies, and ASPICE for Cybersecurity ensures that cybersecurity is aligned with software development best practices. This multi-layered approach ensures that cybersecurity risks are addressed at every stage of vehicle production and operation, providing a comprehensive framework for securing connected and autonomous vehicles against evolving cyber threats (4).

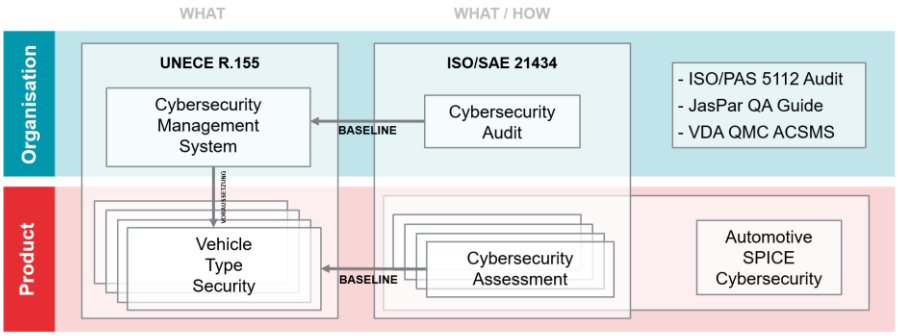

Fig. 2. Relation between regulations, standards, and frameworks

Therefore, the evolution of cybersecurity regulations in the automotive industry reflects a broader transformation in how cybersecurity is perceived and implemented. What was once considered a secondary concern has now become a regulatory necessity and a strategic imperative for automakers. The implementation of UNECE WP.29, ISO/SAE 21434, and ASPICE for Cybersecurity represents a global effort to create a standardized approach to cybersecurity compliance, ensuring that the industry keeps pace with technological advancements and emerging cyber threats. As the automotive sector continues to evolve, the integration of cybersecurity into vehicle design, manufacturing, and post-production services will be crucial in maintaining consumer trust, regulatory compliance, and long-term industry resilience.

ISO/SAE 21434 AND ITS INTEGRATION

ISO/SAE 21434, titled "Road Vehicles – Cybersecurity Engineering," is a crucial standard in the automotive industry that marks a significant evolution in the approach to cybersecurity within automotive software development. Its adoption highlights the increasing recognition of cybersecurity as a fundamental component of automotive safety and reliability. As automotive systems have advanced in functionality and connectivity, they have also become more interconnected and susceptible to cyber threats (12). The standard establishes a comprehensive framework for managing cybersecurity risks throughout the entire vehicle lifecycle, from the concept phase to design, production, operation, maintenance, and decommissioning. Given the complexity of modern vehicles, which are no longer standalone mechanical systems but part of a broader digital ecosystem, cybersecurity must be an integrated engineering principle rather than a project-based concern (21).

ISO/SAE 21434 is distinct from previous standards such as SAE J3061, as it does not follow a strict sequential process but instead outlines a flexible, activity-based cybersecurity risk management

approach. The standard provides clear objectives, practical methodologies, and illustrative examples to help automotive manufacturers and suppliers integrate cybersecurity principles effectively (22). With regulatory bodies increasingly prioritizing automotive cybersecurity, compliance with ISO/SAE 21434 is becoming essential for market access and competitive advantage. The standard provides a common language and structured practices for cybersecurity engineering, fostering collaboration and knowledge sharing across the automotive sector. As a result, it significantly strengthens the overall cybersecurity posture of the industry. However, despite its importance, there remains a lack of frameworks and tools for cybersecurity training and testing within the automotive sector, posing challenges for its widespread implementation (23). The primary objective of ISO/SAE 21434 is to integrate cybersecurity considerations into the engineering processes of electrical and electronic (E/E) systems within road vehicles (6). As modern vehicles increasingly depend on advanced electronic control units (ECUs), embedded software, and networked functionalities, the standard ensures that security principles evolve alongside technological advancements. Extending ISO 26262 (Functional Safety Standard), ISO/SAE 21434 mandates the integration of cybersecurity throughout the vehicle lifecycle, ensuring a risk-based approach to cybersecurity engineering (4).

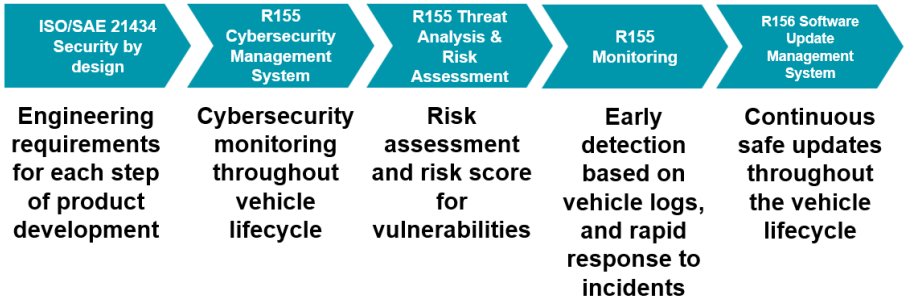

Fig.3. ISO/SAE 21434 and WP.29 collaborate to safeguard vehicles [5]

ISO/SAE 21434 provides organizations with a structured framework for:

- Developing and implementing cybersecurity policies and processes that align with regulatory requirements and industry best practices.
- Effectively managing cybersecurity risks by prioritizing threat assessment, vulnerability mitigation, and proactive security controls.
- Cultivating a strong cybersecurity culture within organizations by promoting awareness, training, and proactive engagement in cybersecurity initiatives.

By integrating these principles, ISO/SAE 21434 enables organizations to establish a Cybersecurity Management System (CSMS). This system ensures a systematic and consistent approach to cybersecurity, covering continuous monitoring, incident response planning, and cybersecurity control implementation throughout the lifecycle of E/E systems. The adoption of CSMS, as guided by ISO/SAE 21434, empowers automotive companies to respond effectively to emerging cyber threats while maintaining compliance with international cybersecurity regulations.

ASPICE FOR CYBERSECURITY AND ITS INTEGRATION

The integration of ASPICE for Cybersecurity into the automotive development framework represents a significant advancement in the industry's approach to cybersecurity. Initially introduced in early 2021 by the German Association of the Automotive Industry (VDA), this add-on module extends the ASPICE process assessment model (PAM) version 3.1 by incorporating cybersecurity-specific considerations.

This development is a strategic response to the growing complexity of cybersecurity threats that OEMs and suppliers must address while ensuring compliance with strict regulatory requirements (24). The module ensures that cybersecurity practices are effectively embedded throughout the entire engineering cycle, covering the development, production, maintenance, and decommissioning phases. Additionally, it aligns cybersecurity processes with organizational policies and project management frameworks, reinforcing a systematic approach to mitigating cyber risks (25).

A notable aspect of this initiative is the introduction of Automotive SPICE for Cybersecurity, which establishes guidelines for cybersecurity implementation in automotive projects. It serves as a reference for process model implementers and assessors, enabling them to evaluate cybersecurity components (systems and software) based on the requirements of ISO/SAE 21434 (26). Despite the release of ASPICE 4.0 (27), ASPICE for Cybersecurity remains an independent add-on module, rather than being fully integrated into the PAM 4.0 process groups mapping. This decision underscores the specialized nature of cybersecurity within automotive development, recognizing that cybersecurity presents distinct challenges that require focused attention. ASPICE for Cybersecurity extends Automotive SPICE by introducing a new process group and modifying existing Acquisition (ACQ) and Management (MAN) process groups (26). This ensures that every ASPICE PAM process is supported by specific outcomes, designated output work products, and foundational base practices, making it more applicable for cybersecurity assessments. Although ASPICE for Cybersecurity follows a formalized evaluation approach, assessing product quality requires technical assessments and work product review checklists (28).

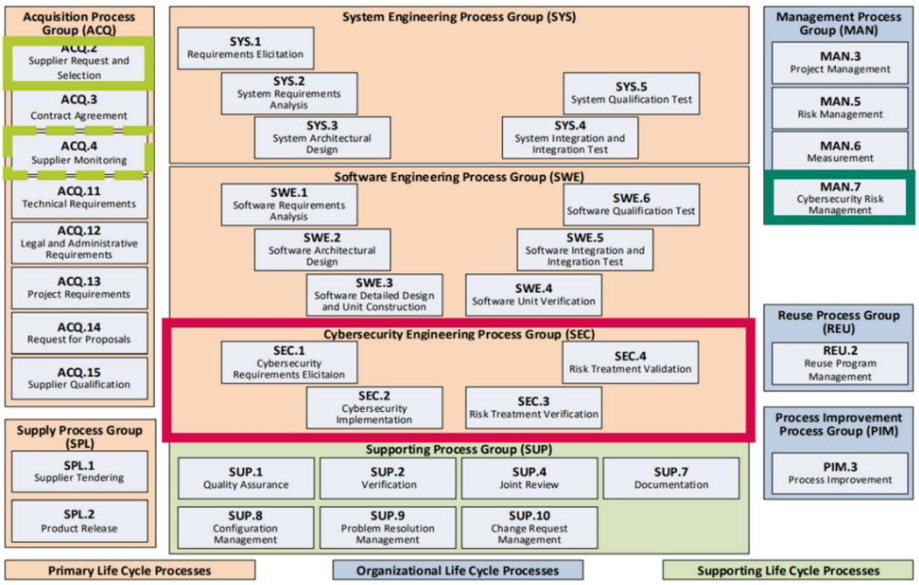

Fig. 1. Overview of ASPICE and ASPICE for Cybersecurity Process Reference Model (PRM) [24]

A major structural change is the introduction of the Cybersecurity Engineering Process Group (SEC), which consists of four key cybersecurity processes: Cybersecurity Requirements Elicitation (SEC.1), Cybersecurity Implementation (SEC.2), Risk Treatment Verification (SEC.3) and Risk Treatment Validation (SEC.4). Each of these processes aligns with overarching cybersecurity objectives, ensuring a systematic approach to identifying and mitigating automotive cybersecurity risks (29). Additionally, the Cybersecurity Risk Management (MAN.7) process is now embedded within the Management Process Group (MAN), emphasizing continuous Threat Analysis and Risk Assessment (TARA) (30). This integration is crucial, as it facilitates risk identification, prioritization, monitoring, and mitigation, while ensuring compliance with global cybersecurity regulations.

By aligning ASPICE for Cybersecurity with UNECE Regulation R155, the framework not only meets regulatory demands but also sets a higher standard for cybersecurity best practices in the automotive industry. Its structured approach ensures that OEMs and suppliers can navigate the complexities of automotive cybersecurity, securing connected vehicles against evolving digital threats while maintaining consumer trust and compliance.

ASPICE for Cybersecurity is closely linked to ISO/SAE 21434, particularly in its role in identifying gaps in lifecycle management, security processes, and risk assessments (31). While Automotive SPICE PAM 3.1 and ASPICE for Cybersecurity primarily address system and software engineering, they do not include indicators for mechanical and hardware engineering disciplines. However, ASPICE PAM 4.0 has introduced a Hardware Engineering Process Group, expanding the framework to address broader automotive security concerns (27). Despite its integration with ISO/SAE 21434, ASPICE for Cybersecurity does not cover all elements of the ISO/SAE 21434 framework. Certain aspects, such as cybersecurity management, ongoing security measures, and post-development lifecycle actions, fall under the Automotive Cybersecurity Management System (ACSMS) and are evaluated separately during an ACSMS audit (7).

ASPICE for Cybersecurity plays a critical role in advancing automotive cybersecurity measures, offering a structured framework for risk management and compliance. By integrating with UNECE WP.29 R155 and aligning with ISO/SAE 21434, it ensures that cybersecurity is systematically incorporated into automotive development processes. The introduction of new cybersecurity-specific processes, assessment models, and work products strengthens OEMs' and suppliers' ability to mitigate cyber threats in an increasingly connected automotive environment. As cybersecurity threats continue to evolve, ASPICE for Cybersecurity is essential for ensuring regulatory compliance, protecting vehicle systems, and maintaining consumer trust. Its structured approach helps automotive companies implement robust cybersecurity measures, fostering long-term resilience against digital threats in the automotive sector.

COMPLIANCE MATRIX DEVELOPMENT

Ensuring compliance with multiple industry standards in automotive cybersecurity is a complex but necessary process. Two key standards, ISO/SAE 21434 (6) and ASPICE for Cybersecurity (7), provide structured frameworks for cybersecurity engineering and process assessment. Given the need for automotive organizations to adhere to both standards, a compliance matrix was developed to systematically align their requirements. This matrix serves as a structured tool to facilitate understanding, implementation, and concurrent compliance with ISO/SAE 21434 and ASPICE for Cybersecurity.

The primary purpose of the compliance matrix is to provide clear mapping between ISO/SAE 21434 requirements and ASPICE base practices. This approach enhances compliance efforts by identifying overlaps and correspondences between the two standards, reducing duplication of work and improving efficiency in audits and assessments. The matrix also offers detailed rationalizations to help practitioners understand how the implementation of one standard aligns with the other, ensuring an integrated cybersecurity approach. Furthermore, it serves as a continuous improvement tool, allowing organizations to refine and enhance their cybersecurity processes based on evolving threats and regulatory expectations. The development of the compliance matrix began with the creation of an Excel-based tool, chosen for its ability to manage large datasets with complex relationships. The process involved listing all relevant requirements from ISO/SAE 21434 along one axis and mapping them to the base practices of ASPICE for Cybersecurity along the other. The mapping relationships varied from one-to-one, one-to-many, many-to-one, and many-to-many, requiring detailed analysis to ensure accuracy and completeness. To strengthen the mapping, each relationship was rationalized by reviewing the intent, scope, and application of requirements from both standards, identifying common themes

such as risk assessment, threat analysis, and verification, and articulating how compliance with one standard contributes to compliance with the other.

Several challenges arose during the development of the compliance matrix. Terminology differences between ISO/SAE 21434 and ASPICE for Cybersecurity sometimes led to misinterpretations, necessitating careful analysis to establish equivalencies. Structural variations posed additional difficulties, as ISO/SAE 21434 follows a requirement-based model, whereas ASPICE is process-centric, requiring a flexible approach in mapping. Some ISO/SAE 21434 requirements overlapped with multiple ASPICE practices, while others had no direct counterpart, demanding thoughtful consideration to address these gaps. To ensure accuracy and practicality, the compliance matrix underwent several iterations of refinement. Subject matter experts in automotive cybersecurity reviewed the mappings and rationalizations, identifying inconsistencies and suggesting improvements. The matrix was then tested in real-world projects, assessing its effectiveness in streamlining compliance efforts. Based on expert feedback and testing outcomes, adjustments were made to improve its usability and accuracy.

Given the limitations of an Excel-based tool, particularly regarding scalability and user experience, the compliance matrix was transitioned into a web application. This transition brought several advantages. A web-based compliance matrix allows real-time access from any device, enabling collaboration among geographically dispersed teams. The application features an intuitive and interactive interface with search functions, filtering options, and hyperlinks, improving usability. Centralized updates ensure that all users access the most current information, avoiding the inefficiencies of manually updating multiple versions of an Excel file. Furthermore, the web application can integrate with project management and documentation tools, further enhancing compliance efficiency. The development of the compliance matrix and its transition into a web-based platform has significant implications for compliance efforts in the automotive industry. Organizations can save time and resources by leveraging the matrix to simultaneously address multiple standards, while the web-based format simplifies navigation, implementation, and documentation retrieval. With a centralized compliance tool, organizations ensure consistent application of cybersecurity standards across different projects and teams, reducing the risk of gaps or inconsistencies. The detailed rationalizations provided in the matrix enhance practitioners' understanding of how different standards interconnect, improving the effectiveness of cybersecurity processes. During audits or regulatory assessments, the compliance matrix serves as concrete evidence of compliance, with the web platform facilitating efficient presentation and review of required documentation.

Overall, the compliance matrix is a transformative tool in automotive cybersecurity, ensuring seamless alignment between ISO/SAE 21434 and ASPICE for Cybersecurity. Its structured approach, expert-reviewed mappings, and web-based implementation enable organizations to navigate complex cybersecurity requirements more efficiently, ultimately strengthening regulatory compliance, cybersecurity risk management, and overall automotive cybersecurity resilience.

MAPPING BETWEEN ISO/SAE 21434 AND ASPICE FOR CYBERSECURITY

The mapping between ISO/SAE 21434 (6) and ASPICE for Cybersecurity (7) aims to align the requirements and processes of these two critical automotive cybersecurity standards, ensuring integrated compliance and efficient implementation in vehicle development. This chapter provides detailed mappings between specific ISO/SAE 21434 clauses (7, 9, 10, 11, and 15) and the corresponding base practices in ASPICE for Cybersecurity.

For each ISO/SAE 21434 clause, the mapping includes explanations of how its specific requirements correspond to ASPICE base practices. Additionally, rationalizations are provided to clarify the relationships between the two standards, ensuring that practitioners understand how compliance with one support adherence to the other.

This comprehensive mapping serves as a practical tool for organizations seeking to integrate compliance efforts efficiently. By identifying alignments and correspondences, practitioners can reduce redundancy, enhance implementation efficiency, and establish a unified approach to cybersecurity. Ultimately, this mapping framework facilitates simultaneous compliance with both standards, promoting a more streamlined and cohesive approach to automotive cybersecurity.

As this is a summary of the PhD thesis, only a selection of mappings between ISO/SAE 21434 and ASPICE for Cybersecurity will be presented. The following example illustrates the alignment between ISO 21434 Requirement RQ-10-01 and ASPICE for Cybersecurity base practices SEC.2.BP1, SEC.2.BP4, and SEC.2.BP6.

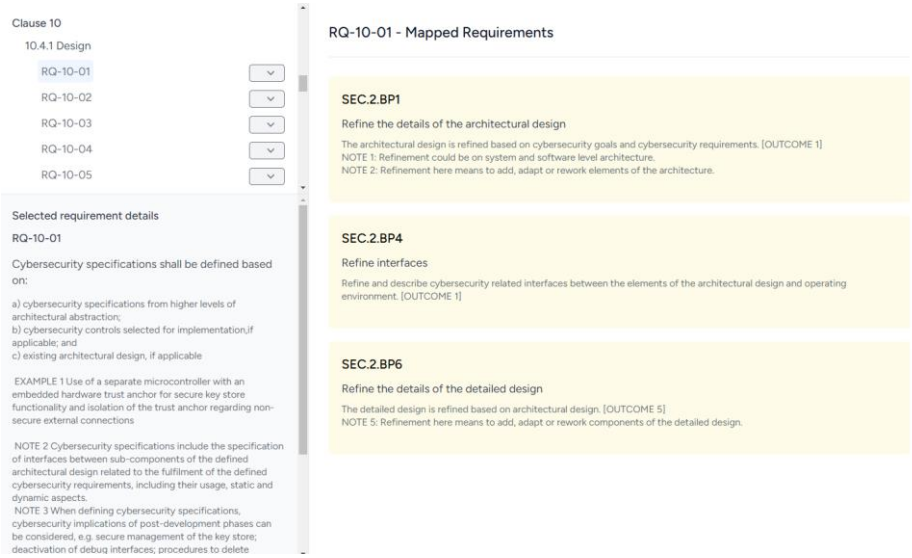

Fig.5. Mapping of ISO 21434 Requirement RQ-10-01

ISO 21434 Requirement RQ-10-01 mandates that cybersecurity specifications must be defined based on key elements, including higher-level cybersecurity specifications, selected cybersecurity controls, and existing architectural designs. This requirement emphasizes early integration of cybersecurity measures into system architecture rather than retrofitting them later in development. It also requires a detailed description of interfaces between sub-components, covering both static and dynamic aspects to ensure secure interactions. Additionally, it considers post-development security measures, such as secure key storage, debug interface deactivation, and protection of personally identifiable information. The requirement further suggests identifying configuration and calibration parameters, such as the correct setup of hardware security modules (HSMs), and evaluating component capabilities, including processor performance and memory resources, to ensure effective implementation of cybersecurity controls.

In ASPICE for Cybersecurity, the base practices SEC.2.BP1, SEC.2.BP4, and SEC.2.BP6 align closely with RQ-10-01 by providing a structured approach to cybersecurity integration within architectural and detailed designs.

- SEC.2.BP1 focuses on refining the architectural design to incorporate cybersecurity goals and requirements at both system and software levels. This ensures that cybersecurity is an integral part of the design process, aligning with ISO 21434's emphasis on utilizing higher-level cybersecurity specifications and existing architectures.
- SEC.2.BP4 addresses the security of interfaces between system elements and their operating environment, ensuring that all interfaces are analyzed and defined concerning their

cybersecurity implications. This directly supports RQ-10-01's requirement for detailed specification of interfaces between sub-components, enabling secure interactions and mitigating potential vulnerabilities.

- SEC.2.BP6 ensures that detailed design refinements incorporate cybersecurity measures, addressing specific implementation aspects such as hardware selection (e.g., processor performance and memory resources) and software configurations. This aligns with RQ-10-01's emphasis on component capabilities and configuration parameters to support effective cybersecurity controls.

Together, these ASPICE practices ensure that cybersecurity considerations are systematically integrated at all levels of design, from high-level architecture to component-level details. This holistic approach ensures that cybersecurity risks identified in threat analysis and risk assessment (TARA) phases are effectively mitigated through comprehensive architectural and design strategies.

ISO/SAE 21434 Requirement RQ-10-02 mandates that cybersecurity requirements must be allocated to specific components of the architectural design. This requirement highlights the importance of embedding security considerations directly into system architecture to ensure that each system component contributes to a comprehensive cybersecurity framework. By assigning cybersecurity requirements to individual components, organizations ensure that security is integrated at every level of the system, creating a layered defense against potential cyber threats. This allocation process is fundamental to building robust cybersecurity defenses, as it ensures that all architectural elements collectively fulfill overarching cybersecurity objectives.

Fig. 62. Mapping of ISO 21434 Requirement RQ-10-02

This ISO requirement aligns closely with ASPICE for Cybersecurity base practice SEC.2.BP2, which focuses on assigning cybersecurity requirements to specific elements of the architectural design. SEC.2.BP2 requires a deliberate and systematic allocation of security requirements to both hardware and software components, ensuring that identified risks are mitigated at all levels of the system. The note accompanying SEC.2.BP2 emphasizes that cybersecurity requirements can be allocated at the system level, addressing hardware and infrastructure security, or at the software level, securing applications and code.

Both ISO RQ-10-02 and ASPICE SEC.2.BP2 emphasize that merely defining cybersecurity requirements is insufficient; these requirements must be thoughtfully distributed across system components to ensure effectiveness. This approach allows security measures to be tailored to the unique functionalities and vulnerabilities of each component, strengthening the overall security posture of the system.

Furthermore, both the ISO requirement and ASPICE practice underscore the necessity of considering all system levels in cybersecurity allocation. Cyber threats can target any layer of the system architecture and allocating cybersecurity requirements at multiple levels ensures comprehensive

protection. This defence-in-depth strategy, widely advocated in cybersecurity best practices, implements multiple security layers to mitigate diverse threats

CASE STUDIES

In Case Study A, the strategic use of the Compliance Matrix led to a 52% cost reduction during the ASPICE assessment. By proactively addressing non-conformances identified in the ISO/SAE 21434 audit and mapping them to ASPICE for Cybersecurity base practices, the project team minimized duplicate efforts and effectively closed gaps before the ASPICE assessment. This streamlined the evaluation process, reducing the time and resources required for compliance. The impact of this approach was evident across multiple audit phases. The Project Audit was reduced from four to three days, the Preparation Phase from three to one day, and the Gap Closure Phase from five to two days. These reductions were achieved by using the compliance matrix to systematically align ISO non-conformances with ASPICE practices, ensuring that many issues were resolved in advance. This reduced the number of new findings during the ASPICE assessment, allowing assessors to focus on specific ASPICE practices that required attention.

Table 1. Efforts reduction in case an ISO/SAE Audit was already conducted (Values expressed as Number of involved Employees x Number of Days)

	ISO 21434	ASPICE	ASPICE Improvemnt
Organizational Audit	5x5		
Project Audit / Assessment	5x5	5x4 ->	5x3
Preparation	6x5	6x3 ->	6x1
Gap closure	10x5	6x5 ->	6x2

Beyond time and resource savings, the compliance matrix improved team preparedness, facilitating better documentation, enhanced communication with assessors, and a clearer understanding of compliance expectations. Although not all ASPICE base practices map directly to ISO/SAE 21434, this proactive approach minimized surprises during the assessment, helping the team address specific ASPICE requirements more effectively. The cost savings extended beyond the immediate assessment, benefiting long-term compliance efficiency. The supplier's reputation for strong cybersecurity management was reinforced, improving trust with OEMs and enhancing business opportunities. By institutionalizing the compliance matrix, the Tier 1 supplier can replicate these benefits across future projects, making compliance more efficient, scalable, and cost-effective.

In Case Study B, the strategic use of the Compliance Matrix Web Tool by a Tier 1 supplier resulted in a 37% cost reduction during the ISO 21434 audit. By leveraging non-conformance mappings from the ASPICE assessment, the supplier streamlined the ISO compliance process, reducing resource allocation and audit-related expenses. The pre-existing work from the ASPICE assessment provided a solid foundation for ISO 21434 compliance, minimizing duplication of effort and optimizing the audit workflow (6,7). While the organizational audit phase remained unchanged, requiring five employees over five days, significant reductions were observed in other audit phases. The project audit/assessment phase was reduced from five days to three, the preparation phase from five days to two, and the gap closure phase from five days to three. These reductions were achieved through pre-emptive identification of cybersecurity gaps using the compliance matrix, allowing for more efficient resource

allocation and minimizing redundant assessments. The cost savings extended beyond man-hour reductions, also impacting external audit fees and project timelines. By shortening audit phases, the supplier minimized potential project delays, ensuring that OEM deliverables remained on schedule, which is crucial in the competitive automotive industry. Furthermore, the compliance matrix improved team readiness, leading to better communication with auditors, fewer misunderstandings, and faster issue resolution.

Table 2. Efforts reduction in case an ASPICE Assessment was already conducted (Values expressed as Number of involved Employees x Number of Days)

	ASPICE	ISO 21434	ISO 21434 Improvemnt
Organizational Audit		5x5 ->	5x5
Project Audit / Assessment	5x4	5x5 ->	5x3
Preparation	6x3	6x5 ->	6x2
Gap closure	6x5	10x5 ->	10x3

This efficiency reinforced the supplier's commitment to cybersecurity, strengthening trust with the OEM and potentially leading to future business opportunities. Institutionalizing the compliance matrix methodology ensures that cost-saving benefits can be replicated across multiple projects, making compliance more efficient and scalable. This case study highlights how proactive planning, strategic resource use, and standards alignment can lead to significant financial and operational advantages in the increasingly regulated automotive cybersecurity landscape.

FINANCIAL ANALYSIS

The cost-benefit analysis of the compliance tool for ASPICE for Cybersecurity assessments demonstrates significant financial and efficiency improvements. By comparing planned vs. actual costs, the study confirms that the tool delivers a high return on investment (ROI), with substantial cost savings driven by effort reduction, streamlined documentation, and accelerated gap closure.

The implementation of the compliance tool led to significant cost savings in conducting the ASPICE for Cybersecurity assessment, primarily by reducing preparation time, streamlining documentation review, and accelerating gap closure. The initial assessment cost of €62,368.94 was reduced to €29,440.91 after using the tool. Factoring in the annual subscription fee of €2,250, the total cost after implementation was €31,690.91, resulting in total savings of €32,928.03.

The financial impact of the compliance tool was assessed using key financial metrics:

- Net Present Value (NPV): €30,678.03, indicating a strong net economic gain after deducting the tool's cost.
- Benefit-Cost Ratio (BCR): 14.65, meaning that for every €1 spent, the organization gained €14.65 in financial benefits, proving the tool's high profitability.

- Return on Investment (ROI): 1367.9%, demonstrating that for every €1 spent, the organization saved €13.68, making the tool an exceptionally valuable investment.

While regional labour costs, particularly in Bavaria, Germany, can influence cost estimations, the tool consistently reduces assessment time and costs. However, factors such as team expertise, unforeseen complexities, and regulatory changes may impact cost projections, requiring organizations to remain adaptable in their financial expectations.

Despite these challenges, the compliance tool optimizes financial resource allocation, enhances compliance efficiency, and accelerates assessment timelines, proving its value in highly regulated industries like automotive cybersecurity. The tool ensures long-term sustainability in compliance efforts, allowing organizations to meet regulatory requirements while maximizing operational performance and cost efficiency.

These metrics confirm that the compliance tool significantly enhances cost efficiency in cybersecurity assessments, offering high returns, rapid cost recovery, and long-term financial benefits. Its implementation not only lowers assessment costs but also improves compliance efficiency, making it a strategic asset for organizations managing regulatory requirements in automotive cybersecurity.

SCIENTIFIC CONTRIBUTION

This research makes several significant contributions to the field of automotive cybersecurity compliance, focusing on improving efficiency, integration, and automation of compliance processes. The key contributions of this work can be summarized as follows:

1. Development of a Compliance Matrix for ASPICE for Cybersecurity and ISO/SAE 21434

- Bridges the gap between ASPICE for Cybersecurity and ISO/SAE 21434, providing a structured mapping of overlapping requirements.
- Eliminates redundant work by identifying common compliance activities, reducing unnecessary effort.
- Improves alignment between software development processes and cybersecurity risk management.
- Enhances audit readiness by offering a clear and structured approach to compliance verification.
- Facilitates continuous compliance, allowing for regular updates and maintenance of cybersecurity documentation.

2. Development of a Web-Based Compliance Tool

- Replaces traditional Excel-based compliance tracking with a dynamic, interactive platform.
- Automates compliance verification, reducing manual effort in assessing standards alignment.
- Provides real-time tracking of cybersecurity compliance, improving project visibility.
- Supports team collaboration, allowing multiple stakeholders to work within a centralized compliance system.

- Enables easy updates and scalability, adapting to changing regulatory requirements without major rework.

3. Integration of Cybersecurity Standards into a Unified Framework

- Presents a methodology for integrating multiple cybersecurity standards within a single compliance framework.
- Reduces complexity in meeting regulatory requirements, making cybersecurity compliance more efficient.
- Ensures a systematic approach to handling cross-framework compliance, making it easier for organizations to manage multiple standards simultaneously.
- Enables organizations to transition to a continuous compliance approach, reducing last-minute certification efforts.

4. Practical Contributions to Industry

- Simplifies compliance processes for OEMs and suppliers, reducing both cost and effort in cybersecurity assessments.
- Optimizes compliance workflows, ensuring that cybersecurity standards are met without disrupting development processes.
- Improves training and knowledge transfer, making cybersecurity compliance easier to understand and implement across engineering teams.
- Addresses the need for a structured compliance methodology, filling an industry gap in aligning ASPICE for Cybersecurity with ISO/SAE 21434.

5. Academic Contributions

- Expands research on cybersecurity standards integration, providing a model for future compliance studies in the automotive industry.
- Introduces a methodology for mapping cross-framework requirements, applicable to other domains such as functional safety (ISO 26262).
- Lays the foundation for further research on automated compliance tools, digitalization, and AI-assisted cybersecurity compliance.
- Contributes to the emerging topic of "continuous compliance", an evolving research area in cybersecurity standardization.

In conclusion, this research introduces both theoretical and practical advancements in automotive cybersecurity compliance, offering structured methodologies, practical tools, and industry-oriented solutions. By aligning ASPICE for Cybersecurity and ISO/SAE 21434, developing a digital compliance platform, and providing a framework for integrated compliance, this work significantly enhances efficiency, reduces redundancy, and sets a new standard for cybersecurity assessments in the automotive sector.

REFERENCES

[1] A. Torok, Z. Szalay, and B. Saghi, "New Aspects of Integrity Levels in Automotive Industry-Cybersecurity of Automated Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 1, pp. 383–391, Jan. 2022, doi: 10.1109/TITS.2020.3011523.

[2] H. Martin *et al.*, "Combined automotive safety and security pattern engineering approach," *Reliab Eng Syst Saf*, vol. 198, 2020, doi: 10.1016/j.ress.2019.106773.

[3] D. Zelle, C. Plappert, R. Rieke, D. Scheuermann, and C. Krauß, "ThreatSurf: A method for automated Threat Surface assessment in automotive cybersecurity engineering," *Microprocess Microsyst*, vol. 90, 2022, doi: 10.1016/j.micpro.2022.104461.

[4] Upstream Security Ltd., *2024 Global Automotive Cybersecurity Report - The automotive cybersecurity inflection point: From experimental hacking to large-scale automotive attacks— the focus shifts to im-pact*. 2024.

[5] Upstream Security Ltd., *2023 Global Automotive Cybersecurity Report - The Automotive industry is rapidly expand-ing into a vast smart mobility ecosystem, introducing new levels of cyber sophistication and attack vectors*. 2023.

[6] ISO/SAE 21434, *ISO/SAE 21434:2021 Road vehicles Cybersecurity engineering*. 2021.

[7] VDA QMC, *Automotive SPICE® Process Reference and Assessment Model for Cybersecurity Engineering*, 1st Edition. VDA QMC, 2021.

[8] Upstream Security Ltd., *2022 Global Automotive Cybersecurity Report - Automotive Cyber Threat Landscape In Light Of New Regulations*. 2022.

[9] L. Rehberg and A. Brem, "Industrial prototyping in the German automotive industry: bridging the gap between physical and virtual prototypes," *Journal of Engineering and Technology Management - JET-M*, vol. 71, 2024, doi: 10.1016/j.jengtecman.2024.101798.

[10] R. Barrios, D. Schippers, C. Heiden, and G. Pappas, "A cybersecurity strategy for Industry 4.0," in *Autonomous Systems: Sensors, Processing, and Security for Vehicles and Infrastructure 2019*, M. C. Dudzik and J. C. Ricklin, Eds., SPIE, May 2019, p. 23. doi: 10.1117/12.2524667.

[11] F. Siddiqui *et al.*, "Cybersecurity Engineering: Bridging the Security Gaps in Advanced Automotive Systems and ISO/SAE 21434," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, IEEE, Jun. 2023, pp. 1–6. doi: 10.1109/VTC2023-Spring57618.2023.10200490.

[12] T. Kaneko, S. Yamashita, A. Takada, and M. Imai, "Triad concurrent approach among functional safety, cybersecurity and SOTIF," *Journal of Space Safety Engineering*, vol. 10, no. 4, 2023, doi: 10.1016/j.jsse.2023.09.001.

[13] G. Baldini, "Detection of cybersecurity spoofing attacks in vehicular networks with recurrence quantification analysis," *Comput Commun*, vol. 191, 2022, doi: 10.1016/j.comcom.2022.05.021.

[14] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and M. Warren, "Cybersecurity Readiness for Automated Vehicles," in *2022 International Conference on Frontiers of Artificial Intelligence and Machine Learning (FAIML)*, IEEE, Jun. 2022, pp. 7–12. doi: 10.1109/FAIML57028.2022.00012.

[15] M. Schellekens, "Car hacking: Navigating the regulatory landscape," *Computer Law and Security Review*, vol. 32, no. 2, 2016, doi: 10.1016/j.clsr.2015.12.019.

[16] Z. Muhammad, Z. Anwar, B. Saleem, and J. Shahid, "Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental Sustainability," *Energies (Basel)*, vol. 16, no. 3, 2023, doi: 10.3390/en16031113.

[17] R. Aghapour, M. Zeraati, F. Jabari, M. Sheibani, and H. Arasteh, "Cybersecurity and Data Privacy Issues of Electric Vehicles Smart Charging in Smart Microgrids," in *Green Energy and Technology*, 2022. doi: 10.1007/978-3-031-05909-4_4.

[18] Upstream Security Ltd., *2021 Global Automotive Cybersecurity Report - Research Into Cyber Attack Trends In Light Of Cybersecurity Standards And Regulations*. 2021.

[19] UNECE R155, *Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system*. 2021.

[20] UNECE R156, *Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system*. 2021.

[21] S. Japs, F. Kargl, H. Anacker, and R. Dumitrescu, "Why make it hard?-Usage of aggregated statistical data for risk assessment of damage scenarios in the context of ISO/SAE 21434," in *Procedia CIRP*, 2022. doi: 10.1016/j.procir.2022.05.252.

[22] C. Schmittner, B. Schrammel, and S. König, "Asset Driven ISO/SAE 21434 Compliant Automotive Cybersecurity Analysis with ThreatGet," in *Communications in Computer and Information Science*, 2021. doi: 10.1007/978-3-030-85521-5_36.

[23] T. Faschang and G. Macher, "An Open Software-Based Framework for Automotive Cybersecurity Testing," in *Communications in Computer and Information Science*, 2023. doi: 10.1007/978-3-031-42307-9_22.
[24] D. Barmayoun, M. Marian, and R. Bogdan, "Automotive Internal Development Process Improvement for Assuring Compliance with the ASPICE for Cybersecurity Extension," in *Communications in Computer and Information Science*, 2022. doi: 10.1007/978-3-031-15559-8_25.
[25] E. Magdy, "A-SPICE for Cybersecurity: Analysis and Enriched Practices," in *Communications in Computer and Information Science*, 2021. doi: 10.1007/978-3-030-85521-5_37.
[26] N. Moselhy, A. Adel, and A. Seddik, "Automotive SPICE Draft PAM V4.0 in Action: BETA Assessment," in *Communications in Computer and Information Science*, 2023. doi: 10.1007/978-3-031-42310-9_7.
[27] VDA QMC, *ASPICE PAM 4.0*. 2023.
[28] C. Schlager *et al.*, "Consistency of Cybersecurity Process and Product Assessments in the Automotive Domain," in *Communications in Computer and Information Science*, 2023. doi: 10.1007/978-3-031-42307-9_24.
[29] VDA QMC, *Automotive SPICE® for Cybersecurity Guidelines*. 2021.
[30] R. Messnarz, D. Ekert, G. Macher, S. Stolfa, J. Stolfa, and A. Much, "Automotive SPICE for Cybersecurity – MAN.7 Cybersecurity Risk Management and TARA," in *Communications in Computer and Information Science*, 2022. doi: 10.1007/978-3-031-15559-8_23.
[31] VDA QMC, *Automotive SPICE® Guidelines*, 2nd Edition. 2023.