Industry-Specific Standard Implementation: Challenges, Effectiveness and Automation (ISO/SAE 21434)

Alphonse Joseph
Master in Cybersecurity / University West
alphonse.joseph@student.hv.se

Karine Yassine
Master in Cybersecurity / University West
karine.yassine@student.hv.se

Akshita Jagadeesan
Master in Cybersecurity / University West
akshita.jagadeesan@student.hv.se

Filmon Mehari
Master in Cybersecurity / University West
filmon-mehari.gebrezghi@student.hv.se

***Abstract*—This literature review explains the challenges that automotive organisations face when implementing ISO/SAE 21434, analyzes its effectiveness in real-world applications and examines the role of automation tools in supporting compliance. This study draws on academic research, industry papers and technical reports related to ISO 21434 and its application in engineering environments. Due to unclear requirements varied TARA approaches and lack of coordination between engineering, IT and backend teams companies apply the standard in various ways. Cybersecurity activities remain outdated throughout the vehicle lifecycle weakening the traceability. Additionally, as there is no standardized method to measure the cybersecurity effectiveness which makes it difficult to evaluate whether the standard strengthens the security defenses. Automation tools can support with tasks like documentation, TARA and analyzing systems making workflow faster and more consistent but those tools still need experts to guide them as tools can't make decisions themselves. Most importantly they can't be used alone to prove that a company meets the ISO 21434 standards. Overall review highlights the need for clearer guidance, common measurement methods and smarter tools so companies can apply ISO/SAE 21434 in a consistent and reliable way.**

***Index Terms*—ISO/SAE 21434, automotive cybersecurity, TARA, UNECE R155, implementation challenges, effectiveness measurement, automation tools**

I. Introduction

A. Context and Motivation

Modern vehicles have gone through a profound transformation evolving from mechanical system into highly connected cyber-physical systems incorporating advanced driver assistance, automation and vehicle-to-everything (V2X) communication. This evolution has expanded the automotive attack surface as demonstrated by real-world vehicle cyberattacks [1]. As a result, ISO/SAE 21434 was introduced in 2021 as the first cybersecurity engineering standard for road vehicles [2]. ISO/SAE 21434 establishes a structured framework for identifying, assessing and managing cybersecurity risks across the full vehicle lifecycle - concept, development,production,operation,maintanence and decommissioning.

At the regulatory level, UNECE WP.29 regulation R155 requires manufacturers to prove cybersecurity risk management as a prerequisite for type approval [3]. Since ISO/SAE 21434 is widely adopted as the technical foundation for satisfying R155, implementing it properly is essential for both OEMs and suppliers.However, academic work increasingly shows gaps between the intended use of the standard and real industry practice. Reviews and gap analysis reveal issues such as vague requirement wording, inconsistent interpretation of TARA methods and insufficient lifecycle guidance [1], [4].

The growing complexity of modern vehicle platforms increases the need for automation in cybersecurity engineering. Research proposes advances TARA models, model based system engineering and risk aware intrusion detection to help organisation scale their compliance efforts [5]–[7]. Yet these approaches also reveal fundamental limitation, which include dependency on expert judgement, integration issues of heterogenous data sources and lack of standardised validation metrics.

B. Problem Statement

Even though ISO/SAE 21434 offers a solid framework for automotive cybersecurity engineering, real world use reveals difficulties in uniform adoption across companies. Studies show that:

- TARA is often performed as a one time activity and not continued throughout the lifecycle [4], [8].
- Cybersecurity risk management is split across engineering, production,IT and backend divisions [9].
- Requirement ambiguity and vague definitions lead to inconsistent interpretations [10].
- Existing validation and verification practices lack mature, quantitative effectiveness metrics [1], [5].
- Automation tools show promise but face limitations in data quality,scalability and integration [6], [7].

Both regulatory compliance and organisational cybersecurity assurance depend on consistent and effective imple-

mentation , a consolidated understanding of implementation challenges,effectiveness measurement and automation support is needed. Existing research addresses these aspects separately but no literature review synthesizes them into a total picture. This study addresses that gap.

C. Research Questions

This review is structured around the following research questions:

- RQ1: In practice, how have manufacturers implemented ISO/SAE 21434, and what challenges have emerged?
- RQ2: To what extent can the effectiveness of ISO/SAE 21434 be measured, and what validation and verification methods are currently in use?
- RQ3: What role do automation tools play in achieving compliance with ISO/SAE 21434, and what are their limitations.

II. Background and Related Work

A. Key Definitions

ISO/SAE 21434 defines automotive cybersecurity engineering as the set of processes used to identify, assess and mitigate cybersecurity risks across the entire vehicle lifecycle. This is formally defined in ISO/SAE 21434 [2], which specifies organisational, project-level and product-level cybersecurity requirements covering concept, development, production, operation, maintenance, and decommissioning.

A central concept underpinning the standard is Threat Analysis and Risk Assessment (TARA), which identifies assets, analyses potential threat scenarios, evaluates attack feasibility and impact, and assigns risk values that guide cybersecurity goals and requirements. Multiple studies note that ISO/SAE 21434 leaves flexibility in how TARA is performed leading to diverse interpretations [1], [4].

Additional key terms include: Additional key terms include cybersecurity goals, requirements, Security Relevance Analysis (SRA), and the Cybersecurity Management System [3], which form the core vocabulary of modern automotive cybersecurity engineering.

Together, these concepts form the core vocabulary of modern automotive cybersecurity engineering.

B. Relevant Standards, Frameworks and Regulations

ISO/SAE 21434:2021 is the main international standard governing cybersecurity engineering for road vehicle E/E systems. It provides lifecycle oriented requirements, mandatory work products and expectations for traceability between risks, requirements and their verification. Various studies note that while comprehensive the standard often lacks procedural detail, leading to variation in how organisations apply it [1], [10].

1) UNECE WP.29 Regulation R155: R155 establishes cybersecurity as a regulatory requirement for type approval in many markets. Manufacturers must demonstrate that cybersecurity risks are continuously monitored and mitigated via a CSMS. A comparative study confirms that ISO/SAE 21434 is effectively treated as the engineering foundation to fulfilling R155 obligations [3].

2) ISO 26262 Functional Safety: ISO 26262 governs functional safety for automotive E/E systems. Several papers analyse its relationship with ISO/SAE 21434 highlighting overlap in lifecycle structure but fundamental differences in failure models and verification expectations [1]. Additional work shows that integrating both standards in autonomous and electric vehicles remains challenging and requires coordinated safety-security engineering [11].

3) Other Standards and Frameworks: At the organisational level, standards like ISO/IEC 27001 and industrial frameworks such as IEC 62443 are at times referenced in the automotive domain, but studies indicate they cannot replace ISO/SAE 21434 because they lack road vehicle specific engineering detail [9].

Together, these frameworks create a complex compliance landscape, one in which ISO/SAE 21434 acts as the core engineering reference while R155 provides the regulatory requirement.

C. Prior Work on ISO/SAE 21434 Implementation (RQ1)

Research constantly shows that application of ISO/SAE 21434 in practice introduces significant organisational and methodological challenges.

Gap analysis in detail shows that TARA is mostly done as a one-time activity with limited mechanisms for lifecycle updates. Vulnerability and incident handling are often less developed compared to IT security practices. ISO/SAE 21434 is not significantly guided by multi stakeholder coordination across OEMs and suppliers [4].

Another study shows that cybersecurity responsibilities are distributed across engineering, production, backend operations and IT. These divisions employ inconsistent risk-assessment scales, tools, and terminologies resulting in fragmented risk visibility and reduced traceability. It points out clearly that ISO/SAE 21434 alone does not guarantee coherent enterprise-level cybersecurity governance [9].

Requirement level challenges are prominent too. Research demonstrates that several ISO/SAE 21434 requirements are ambiguously worded which makes experts interpret their obligation strength and scope differently. This ambiguity undermines consistent implementation across projects and suppliers [10].

At the concept phase, studies find that although ISO/SAE 21434 outlines required work products, it does not provide much procedural detail on how to derive them. As such, engineers rely on workshops, templates, or experience-driven heuristics, that vary across organizations.

Finally, scalability challenges arise when applying SRA to complex systems [8].

Across these studies, the literature shows that manufacturers often struggle with ambiguity, scalability, cross-divisional coordination, and lifecycle management collectively shaping the practical implementation challenges addressed by RQ1.

D. Prior Work on Effectiveness, Validation, and Automation (RQ2 & RQ3)

1) Effectiveness and Validation (RQ2): The literature emphasises that evaluating the effectiveness of ISO/SAE 21434 remains an open challenge. Research argues that the standard lacks quantitative criteria for acceptable risk, leaving organisations to define bespoke scoring methods. This reduces comparability and hinders unified effectiveness assessment [1].

To address this, several researchers propose enhanced TARA models:

- **TARA 2.0 for Connected and Automated Vehicles** introduces improved risk scoring that considers three things:
  - How much automation is involved
  - How much privacy is affected
  - How confident experts are in their assessment

  This improves repeatability and expresses uncertain features absent in standard ISO 21434 scoring [5].
- **Cyber Threat Susceptibility Assessment for Heavy-Duty Vehicles** tailors risk assessment to the specific threats faced by highly automated vehicles, demonstrating that ISO 21434's standard metrics don't apply equally across different vehicle types [6].
- **Systematic Risk Analysis of Multi-Stage Attacks in Zonal E/E Architecture** shows that ISO 21434's simple, linear threat models fail to capture lateral movement between system domains. To address this, the authors validate risks using attack-graph modeling, which offers a more detailed and realistic view for modern vehicle architectures [7].

These studies reveal that cybersecurity validation and verification methods are still inconsistent and vary by domain, highlighting the lack of maturity in measuring effectiveness.

2) Automation and Tool Support (RQ3): Automation appears in the literature as both a necessity and a challenge. Several studies demonstrate automation applications:

- **Cyber Threat Susceptibility Assessment for Heavy-Duty Vehicles** includes an automated scoring procedure to prioritise threats [6].
- **TARA 2.0** adds semi-automated reasoning to calculate combined risk scores.
- **Streamlining Security Relevance Analysis** uses automated clustering and decision support to cut down repetitive SRA work [8].
- **Risk-Aware Intrusion Detection and Prevention System for Automated UAS** applies risk-based intrusion detection to adjust mitigation actions dynamically [12].

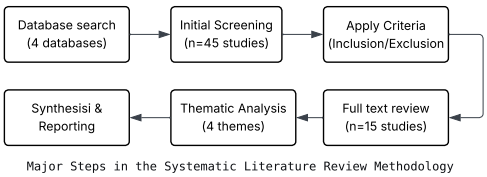
These studies collectively show that automation:

- Improves scalability
- Reduces repetitive manual work
- Increases consistency

However, several limitations remain:

- Heavy reliance on expert-defined weighting factors
- Difficulties integrating automated tools across organisational units
- Limited transparency and explainability especially when ML-based tools are used
- Lack of standardised datasets for validation
- Problems using automated outputs as formal evidence in cybersecurity cases

The literature therefore indicates that even though automation enhances compliance support, however, current tools are fragmented, immature and poorly integrated making it hard to fully operationalise ISO/SAE 21434. These issues form the core focus of RQ3.



Major Steps in the Systematic Literature Review Methodology

TABLE I
SYSTEMATIC LITERATURE REVIEW METHODOLOGY

Component	Description
Time Frame	2020–2025
Databases	IEEE Xplore, Google Scholar, ResearchGate, ISO/SAE/UNECE repositories
Search Terms	"ISO/SAE 21434 implementation challenges"; "UNECE R155 compliance"; "TARA automation"; "automotive cybersecurity effectiveness"
Inclusion Criteria	Explicit reference to ISO/SAE 21434; focus on automotive cybersecurity; peer-reviewed or technical reports; addresses at least one research question
Exclusion Criteria	Opinion pieces, marketing material; non-English publications; duplicate studies
Final Studies	15 studies selected for thematic analysis
Analysis Method	Thematic analysis structured around RQ1, RQ2, and RQ3

III. METHODOLOGY

A. Literature Search and Selection

This literature review follows a systematic approach, gathering literature from 2020 to 2025 via IEEE Xplore, Google Scholar, ResearchGate, and official standards repositories (ISO, SAE, UNECE). Additional sources included white papers, technical reports, and regulatory documents such as the EU NIS2 Directive.

B. Search Strategy

Search terms included:

- "ISO/SAE 21434 implementation challenges"
- "UNECE R155 compliance"
- "TARA automation"
- "automotive cybersecurity effectiveness"

TABLE II
DISTRIBUTION OF THEMES IN REVIEWED LITERATURE

ID	Theme	Studies	%
T1	Interpreting and operationalising ISO/SAE 21434 requirements	12	80%
T2	Organisational misalignment and cross-lifecycle complexity	7	46%
T3	Measuring the effectiveness of ISO/SAE 21434	7	46%
T4	Automation support for ISO/SAE 21434 compliance	8	53%

C. Inclusion and Exclusion

- **Included:** Peer-reviewed articles, conference papers, standards, and technical reports explicitly referencing ISO/SAE 21434 and addressing at least one research question.
- **Excluded:** Opinion pieces, marketing material, and non-English publications.

D. Analysis Approach

Selected literature was analyzed thematically according to the three research questions, identifying recurring challenges, measurement gaps, and automation trends in ISO/SAE 21434 implementation. This version matches the scope, sources, and approach of your full report, not just the earlier draft. Let me know if you'd like to tighten it further or add more detail.

IV. THEMATIC ANALYSIS

This section presents four themes identified through our review of 15 studies. Table II summarizes these themes, their prevalence in the literature, and the number of studies addressing each theme.

A. Theme 1: Interpreting and Operationalising ISO/SAE 21434 Requirements (RQ1)

Various studies indicate that the wording and structure of ISO/SAE 21434 create interpretation challenges which directly impact how manufacturers implement the standard in practice.

The paper *In-Depth Exploration of ISO/SAE 21434 and Its Correlations with Existing Standards* [1] provides a clause by clause analysis and maps the standard to related frameworks such as ISO 26262.It shows that while the overall lifecycle and process structure are clear, many work products and activities are defined only at a high level. The absence of prescriptive guidance allows significant variation in how organisations apply TARA define cybersecurity goals and allocate requirements leading to inconsistent implementation across companies and even within projects of the same organisation.

The study *Towards ISO/SAE 21434 Compliance: Quantifying Ambiguity and Detailing Requirements* [10] measures ambiguity in selected requirements of ISO/SAE 21434. Using requirements engineering techniques, the authors show that key phrases such as 'sufficiently' and 'as appropriate' are interpreted differently by experts. This variation complicates internal alignment and makes it difficult for OEMs and suppliers to agree on what compliance means. While the study's strength lies in its structured approach to ambiguity, it focuses on a limited set of requirements and does not test how clarifications would affect engineering outcomes.

Two other papers examine early-phase application of the standard. *Streamlining Security Relevance Analysis According to ISO 21434* [8] finds that the default SRA process leads to repetitive, component-level decisions that become tedious and error-prone for large architectures.

Likewise *Towards the Development of the Cybersecurity Concept According to ISO/SAE 21434 Using Model-Based Systems Engineering* [13] notes that standard requires a cybersecurity concept but does not explain how to derive it systematically from TARA results and system models. The authors propose an MBSE-based workflow to structure cybersecurity goals and requirements though this approach has only been tested in limited case studies.

When taken together these works show that interpretation and operationalisation of ISO/SAE 21434 are non-trivial engineering problems. The standard leaves many degrees of freedom, which leads to ambiguity, heavy reliance on expert judgement, and inconsistent practices between organisations. This theme directly addresses RQ1, highlighting that the challenges begin not only at the organisational or lifecycle level but already at the level of understanding.

B. Theme 2: Organisational Misalignment and Cross-Lifecycle Complexity (RQ1)

The second major theme concerns organisational and lifecycle issues that arise once companies attempt to operationalise ISO/SAE 21434 across departments and suppliers.

Cross-Divisional Cybersecurity Risk Management in Automotive [9] shows that cybersecurity tasks span product engineering, production, IT and backend services but these divisions use different tools, terminologies, and risk scales. Even when each division claims alignment with ISO/SAE 21434 their processes are incompatible resulting in poor traceability and weak risk visibility across functions.

The Gap Analysis of ISO/SAE 21434 [4] highlights lifecycle issues:

- TARA is often performed only once
- Results are not updated when vehicle functions evolve
- Incident and vulnerability handling are less developed than IT-security standards.

These gaps become more critical in the context of regulation.

UNECE WP.29 R155 vs. ISO/SAE 21434 [3] shows that manufacturers must prove continuous risk management for type approval but without lifecycle TARA updates and structured incident response, traceability to regulatory requirements is weakened.

Finally, the growing use of machine learning and automated functions further complicates organisational workflows. Both *Bridging the Gaps: ISO 21434, ISO 26262 and ML in Autonomous Vehicles* [14] and *Functional Safety and Cybersecurity in AV/EVs* [11] show that existing processes cannot seam-

lessly integrate ML-based components, forcing companies into ad-hoc, manually synchronized workflows.

Overall, the literature shows that ISO/SAE 21434 does not guarantee smooth organisational practice. Implementing the standard is a complex challenge involving both technical and organisational factors, which reinforces RQ1

C. Theme 3: Measuring the Effectiveness of ISO/SAE 21434: Emerging Methods and Limitations (RQ2)

Across the literature, researchers agree that ISO/SAE 21434 does not provide standardised metrics for assessing the effectiveness of cybersecurity engineering activities. This leads to inconsistencies in how organisations verify TARA results, cybersecurity goals and mitigation strategies. Several studies propose improvements to address these gaps.

TARA 2.0 for Connected and Automated Vehicles [5] introduces refined scoring factors—such as privacy impact, system automation level, and confidence weighting—to make risk values more transparent and repeatable. *Cyber Threat Susceptibility Assessment for Heavy-Duty Vehicles* [6] adapts impact and feasibility metrics to the specific architecture and operational context of heavy-duty fleets, showing that generic ISO/SAE 21434 risk scoring can misprioritise threats.

A different perspective is offered by *Systematic Risk Analysis of Multi-Stage Attacks in Zonal E/E Architecture* [7], which shows that traditional single step risk evaluation underestimates lateral movement and multi hop attack paths. By incorporating attack-graph reasoning, this work highlights gaps in ISO/SAE 21434's linear threat-modelling approach.

Put together, the studies show that current validation and verification methods for ISO/SAE 21434 are fragmented with no unified quantitative benchmark for defining effective cybersecurity. The proposed approach improves detail and realism but often rely heavily on expert defined weights and lack broad empirical validation. This shows that effectiveness measurement remains at an early stage of maturity.

D. Theme 4: Automation as a Support Mechanism for ISO/SAE 21434 Compliance (RQ2 & RQ3)

Automation appears continuously in the literature as a practical way to manage the scale and complexity of ISO/SAE 21434 activities but its benefits always comes with limitations.

On the process side, *Streamlining Security Relevance Analysis According to ISO 21434* [8] shows that repetitive SRA tasks can be partially automated to reduce manual effort and improve consistency. *Towards the Development of the Cybersecurity Concept According to ISO/SAE 21434 Using Model-Based Systems Engineering* [13] shows how MBSE tools can help carry cybersecurity goals and requirements through system architectures, improving traceability.

In risk assessment, *TARA 2.0* [5] and the *Heavy-Duty Vehicle Susceptibility Model* [6] use automated scoring logic to prioritise large numbers of threat scenarios more systematically. Runtime automation is explored in *Risk-Aware Intrusion Detection and Prevention System for Automated UAS* [12], which uses risk inputs to adjust intrusion detection and response decisions dynamically.

Despite these advances, several limitations remain across studies:

- Automated scoring still depends on expert-defined parameters
- Tool outputs are difficult to combine across engineering, IT and backend divisions
- ML-based methods lack explainability needed for audits
- Automated results often require manual justification before they can be included in cybersecurity cases

While automation helps ISO/SAE 21434 compliance by improving scalability and reducing manual errors, it does not yet offer a fully reliable or standardised approach. Current tools must be seen as a supportive rather than definitive which addresses the concerns raised in RQ3.

V. Discussion

This section discusses the results in relation to the research questions, focusing on implementation methods, efficiency, automation, and the broader implications for the automotive industry.

A. RQ1 Implementation and challenges

The literature shows that ISO/SAE 21434 is being adopted by many vehicle manufacturers, mainly due to regulatory pressure from frameworks such us UNECE R155 [3]. Most organizations aim to follow a life-cycle approach, where cybersecurity is considered from the concept phase through system development, validation and even after production. However the way this is implemented varies considerably between organizations. Larger manufacturers generally appear to have more structured cybersecurity processes, while smaller suppliers often struggle due to limited resources and a lack of expertise [4].

Several organisational challenges are also highlighted in the literature. Responsibility for cybersecurity is often spread across multiple teams, and coordination between departments and suppliers is not always effective [1]. In addition, the documentation and traceability requirements of ISO/SAE 21434 can be demanding, which sometimes leads to cybersecurity being treated more as a compliance activity than as an engineering process [15].

Differences in how the standard is interpreted further contribute to uneven implementation across manufacturers and suppliers, as shown by studies quantifying requirement ambiguity [10] and analayzing interpretation varations [1]. Furthermore, the lack of continuous TARA updates throughout the vehicle lifecycle—highlighted in gap analyses [4] and comparative studies of R155 compliance [3]—undermines the regulatory requirement for ongoing risk management.

These implementation challenges—spanning from ambiguous requirements [10] to fragmented organizational practices [9] and inconsistent lifecycle management [3], [4] collectively explain why uniform adoption of ISO/SAE 21434 remains difficult despite regulatory pressure.

B. RQ2: Effectiveness and Measurement

Research indicates that assessing the effectiveness of ISO/SAE 21434 remains difficult. Most current evaluation approaches focus on whether processes are being followed, rather than on whether cybersecurity is actually improving in practice [15]. Methods such as threat analysis, penetration testing, and audits are commonly used, but may not reflect real-world protection [12].

Another problem identified in the literature is the lack of standardised metrics and key performance indicators (KPIs) for automotive cybersecurity [4]. Without clear benchmarks, organisations tend to rely on indirect indicators, such as incident response times or the number of identified vulnerabilities. In contrast to functional safety, there are still no widely accepted maturity models or certification schemes in the automotive cybersecurity domain, making it difficult to judge whether ISO/SAE 21434 leads to measurable improvements in cyber resilience in real operating environments [14]. As a result, reported outcomes vary, and effectiveness remains difficult to compare across organisations.

C. RQ3: Automation and Tools

Automation appears to be most useful for supporting structured and repetitive tasks related to ISO/SAE 21434, particularly in areas such as documentation, threat modelling, testing, and traceability. Automated TARA tools help make threat analysis more efficient and consistent [5], and security testing tools also contribute to faster validation process [12]. However, no single tool covers the entire cybersecurity [4], which means organisations often need to combine several tools and still rely on manual work.

Automation also remains limited in areas that require judgement, such as assessing consequences or defining cybersecurity objectives [7]. In addition, tool support for machine learning-based vehicle systems is still relatively immature [14]. Smaller suppliers, in particular, may face both financial and technical challenges when adopting advanced tools. This indicates that ISO/SAE 21434 cannot be implemented in the same way across the entire supply chain, especially among smaller organisations [11]. Overall, while tools are helpful, they cannot substitute for human expertise in decision making.

D. Practical and Policy Implications

From a practical perspective, the automotive industry would benefit from placing greater emphasis on staff training, cross-functional collaboration, and stronger involvement of suppliers [1]. The use of shared tools, standardised templates, and central governance structures could also help make implementation more consistent and manageable [5].

Regulatory bodies could further support industry efforts by offering clearer guidance on how effectiveness should be evaluated and what organisations can expect during audits [2], [15]. This aligns with broader cybersecurity governance trends such as the EU's NIS2 Directive [16], which emphasizes supply-chain security and incident reporting across critical sectors including automotive manufacturing. For tool providers, the focus should be on improving usability, interoperability, and integration with existing development processes [4].

E. Research Gaps and Limitations

The literature points to major gaps in measuring the real impact of cybersecurity [4]. There is a lack of clear quantitative performance measures and maturity models, which makes it difficult to really know how well the standard works in practice [14]. Outcomes remain unpredictable due to the lack of standard metrics, but have no easy method to see if it actually makes the systems more secure [7], [12].

VI. Conclusion

This literature review establishes that although ISO 21434 is widely utilized in the automotive industry, organizations implement the standard in diverse ways. Vague requirements, differing interpretation, and varied TARA methodologies contribute to non-uniform cybersecurity practices which can lead to documentation issues and weak traceability across the vehicle lifecycle. This study emphasizes a very critical problem: that there is no standardized and measurable way to evaluate the cybersecurity effectiveness. ISO 21434 does not give an explicit mechanism to assess the security performance. Due to this, companies must rely on experts judgement, custom scoring systems and process based audits, making it difficult to determine whether the cybersecurity activities truly improving the safety and resilience of the vehicle systems. Overall, this review synthesizes how ISO 21434 is applied, how the effectiveness of cybersecurity activities is evaluated, and the ways automation is leveraged. It highlights industry-wide obstacles, from organizational misalignment, the lack of harmonized measurement methods for cybersecurity performance and the functional gaps in current automation tools. Prospectively, future research should focus on establishing a clear and standard way to measure the effectiveness, developing more efficient automation tools that work in a synchronized way across different department, and methodologies that ensure cybersecurity is integrated across all phases of the vehicle lifecycle.

VII. Academic Integrity

- Brainstorming search terms: ChatGPT
- Improving grammar/clarity: ChatGPT

References

[1] S. C. Board, "In-depth exploration of iso/sae 21434 and its correlations with existing standards," Technical Report, 2023, pDF, 905.63 KB.

[2] *Road vehicles — Cybersecurity engineering — ISO/SAE 21434:2021*, International Organization for Standardization (ISO) and SAE International Std., 2021, pDF, 4.61 MB. [Online]. Available: https://www.iso.org/standard/70918.html

[3] G. Costantino, M. D. Vincenzi, and I. Matteucci. (2022) A comparative analysis of unece wp.29 r155 and iso/sae 21434. in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. Accessed: 2025-12-01. [Online]. Available: https://ieeexplore.ieee.org/document/9799351

[4] D. Grimm, A. Lautenbach, M. Almgren, T. Olovsson, and E. Sax. (2023) Gap analysis of iso/sae 21434 – improving the automotive cybersecurity engineering life cycle. in *2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC)*. Accessed: 2025-12-05. [Online]. Available: https://ieeexplore.ieee.org/document/10422100

[5] V. C. Initiative, “Tara 2.0 for connected and automated vehicles: An enhanced threat analysis and risk assessment methodology,” White Paper, 2024, pDF, 1.98 MB.
[6] N. Rahimi, B.-A. Schuelke-Leech, and M. Mirhassani. (2025) Cyber threat susceptibility assessment for heavy-duty vehicles based on iso/sae 21434. https://ieeexplore.ieee.org/document/10921673. Accessed: 2025-11-28.
[7] R. Pitchaimani, S. Canard, B. Hammi, and A. S. Spornic. (2025) Systematic risk analysis of multi-stage attacks in zonal automotive e/e architecture. in *2025 23rd International Symposium on Network Computing and Applications (NCA)*. Accessed: 2025-12-03. [Online]. Available: https://ieeexplore.ieee.org/document/11261563
[8] C. Jakobs, B. Naumann, M. Werner, K. Schmidt, J. Eichler, and H. Heskamp. (2022) Streamlining security relevance analysis according to iso 21434. https://ieeexplore.ieee.org/document/10085633. Accessed: 2025-12-01.
[9] P. Wagner. (2025) Cross-divisional cybersecurity risk management in automotive: Requirements and current practices. in *2025 IEEE 30th International Conference on Emerging Technologies and Factory Automation (ETFA)*. Accessed: 2025-12-05. [Online]. Available: https://ieeexplore.ieee.org/document/11205792
[10] R. Kurachi, T. Sasaki, and Y. Ujiie. (2024) Towards iso/sae 21434 compliance: Quantifying ambiguity and detailing requirements. https://ieeexplore.ieee.org/document/10757689. Accessed: 2025-12-02.
[11] S. Khokha. (2024) From standards to implementation: Functional safety and cybersecurity in modern autonomous and electric vehicles. in *2024 International Conference on Cybernation and Computation (CYBERCOM)*. Accessed: 2025-12-03. [Online]. Available: https://ieeexplore.ieee.org/document/10803155
[12] R. Schermann, T. Ammerer, P. Stelzer, G. Macher, and C. Steger. (2023) Risk-aware intrusion detection and prevention system for automated uas. in *2023 IEEE 34th International Symposium on Software Reliability Engineering Workshops (ISSREW)*. Accessed: 2025-12-06. [Online]. Available: https://ieeexplore.ieee.org/document/10301336
[13] S. Japs. (2021) Towards the development of the cybersecurity concept according to iso/sae 21434 using model-based systems engineering. https://ieeexplore.ieee.org/document/9604680. Accessed: 2025-12-05.
[14] S. Daiene de Oliveira Bastos, K. Castelo Branco, and A. Luiz de Oliveira. (2025) Bridging the gaps: A comparative analysis of iso 21434, iso 26262 and machine learning in autonomous vehicles. in *2025 Brazilian Symposium on Robotics (SBR) and 2025 Workshop on Robotics in Education (WRE)*. Accessed: 2025-12-06. [Online]. Available: https://ieeexplore.ieee.org/document/11249566
[15] ISO Technical Committee 22/SC 32, “Auditing the iso/sae 21434 standard: Guidance and considerations,” https://www.iso.org/, 2022, pDF, 1.10 MB, Accessed: 2025-11-30.
[16] European Parliament and Council of the European Union, “Directive (eu) 2022/2555 of the european parliament and of the council of 14 december 2022 on measures for a high common level of cybersecurity across the union (nis2 directive),” https://eur-lex.europa.eu/eli/dir/2022/2555/oj, 2022, official Journal of the European Union, L 333, 27/12/2022, p. 80–152.