




## Securing Smart Vehicles: A Bilateral TARA Approach for ISO 21434 and ASPICE for CS Compliance

Ahmed Adel Mohamed<sup>1,2</sup>, Heba Aslan<sup>2</sup>, Tamer Arafa<sup>2</sup>

<sup>1</sup> UL Solutions, Kornwestheim 70806, Germany

<sup>2</sup> School of Information Technology and Computer Science, Nile University, Giza 12566, Egypt

Corresponding Author Email: [a.adel2179@nu.edu.eg](mailto:a.adel2179@nu.edu.eg)

Copyright: ©2025 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijse.150604>

### ABSTRACT

**Received:** 20 April 2025

**Revised:** 26 May 2025

**Accepted:** 15 June 2025

**Available online:** 30 June 2025

#### **Keywords:**

*automotive cybersecurity, ISO/SAE 21434, ASPICE for CS, risk assessment and threat analysis (TARA), automated tool*

The increasing connectivity in modern vehicles has opened the door to a surge of cyber-attacks, posing significant risks to vehicle safety and potentially leading to substantial financial losses. To address this, our paper introduces an optimized approach to risk assessment and threat analysis (TARA), specifically tailored for secure smart vehicles. We've developed a bilateral model that meticulously adheres to the ISO/SAE 21434 automotive cybersecurity standard and the Automotive SPICE for Cybersecurity (ASPICE for CS) base practices. This unique bilateral model considers both standards simultaneously for each model side, incorporating new requirements to ensure practitioners can achieve full compliance. We've also simplified the categorization of requirements, making them more intuitive and industry-driven. Throughout this paper, we detail the analysis, mapping, and development steps of our proposed model. Our observations and lessons learned from applying this model across various projects have significantly improved its maturity, directly reducing the risks associated with recovery costs and financial losses. To further improve the practical application of this model, we have developed a capable cybersecurity TARA tool based on the model to achieve compliance with both standards. This tool could be used by automotive manufacturers and suppliers during the entire vehicle development lifecycle, from initial design to post-production updates to help identify potential vulnerabilities in electronic control units (ECUs), communication networks, and software, allowing for proactive risk mitigation. The documented and analyzed results from utilizing our model and tool show a remarkable 40% to 60% decrease in operational costs due to the significant reduction in quality and compliance efforts.

## 1. INTRODUCTION

### 1.1 Motivation

The Automotive industry now depends significantly on software operations, over the air and cloud-based communication. Therefore, cybersecurity became a top priority. The vulnerability to cyber-attacks and remote hacking, whether by breaking into electronic systems or networks, poses significant threats to people and their vital assets. Present-day security concerns are different and more complicated than previous times when problems in advanced electronic systems usually came from internal software issues. Now, we need a more comprehensive security approach. As a result, the transport industry has kept pace with these challenges and started developing guidelines that focus on not only safety but also cybersecurity. International standards entities like the International Organization for Standardization (ISO), the German Association for the Automotive Industry (VDA), and SAE International have been at the forefront of these efforts over the last few years. They have introduced standards focused on automotive cybersecurity. For example,

ISO/SAE 21434, "Road Vehicles Cybersecurity Engineering," was published to complement safety standards released earlier as the ISO 26262, "Road Vehicles — Functional Safety" [1, 2]. Additionally, ISO released ISO/TR 4804, "Road Vehicles — Safety and Cybersecurity for Automated Driving Systems — Design, Verification, and Validation," back in 2020 [3]. VDA also created the Automotive SPICE for Cybersecurity, an addition 3 years ago to the ASPICE Process Assessment Model 3.1, that has a novel version, ASPICE Process Assessment Model 4.0. ASPICE is widely recognized and required by vehicle original equipment manufacturers (OEMs) as a process guidance for referencing and assessments of automotive engineering [4-6]. These standards seek to unify cybersecurity engineering efforts by implementing established optimal approaches applied in the industry.

Risk assessment and threat analysis (TARA) is a detailed and systematic process for identifying potential cybersecurity threats and evaluating the related risks. Although ASPICE for Cybersecurity and ISO/SAE 21434 do not specify a strict method for conducting TARA, they provide a framework for the process.

TARA is a comprehensive process that includes several

steps, from pre-analysis to defining cybersecurity goals, requirements and controls. It is guided by structured approaches and methodologies described in the above-mentioned standards. This process ensures a thorough understanding of possible cybersecurity risks and helps develop effective strategies to address them, thereby enhancing the protection and robustness of automotive systems against cyber-attacks.

The ISO/SAE standard 21434 shown in Figure 1 provides requirements and recommendations for ensuring cybersecurity compliant practices in vehicles for road users. It includes requirements for cybersecurity concept, development, and operation phases. It highlights important areas such as risk assessment and threat analysis in clause 15 and conceptual design in clause 9. It also highlights some important concepts such as building security into the design, testing security, managing vulnerabilities, responding to incidents, and continuous monitoring. Using this standard enhances vehicle cybersecurity, protect sensitive information, restrict unapproved access or changes, and make sure the system remains safe and reliable against increasing cyber-risks.

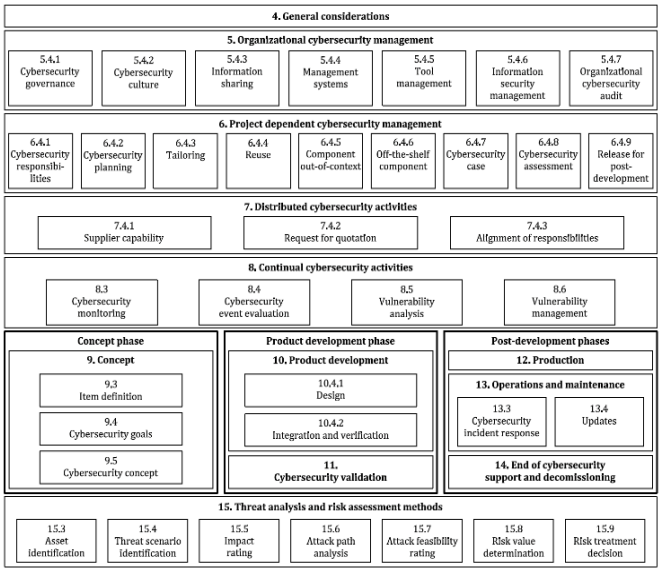


Figure 1. Overall view of the ISO/SAE 21434 [1]

ASPICE was established in 2001 as a variant of ISO/IEC 15504 (SPICE) [7]. Its objective is to measure the development processes performance among automotive industry OEM suppliers. ASPICE defines processes and best practices to ensure vehicle development process quality. ASPICE for Cybersecurity process assessment model (PAM) shown in Figure 2 was released in 2021 as complementary to the ASPICE 3.1 PAM for cybersecurity related automotive development. It introduced 6 new cybersecurity related process areas across 3 process groups. The new process areas Man.7 (Cybersecurity Risk Management), SEC.1 (Cybersecurity Requirements Elicitation), SEC.2 (Cybersecurity Implementation), SEC.3 (Risk Treatment Verification) and SEC.4 (Risk Treatment Validation) address risk assessment and threat analysis practices including verification and validation activities. This standard compliance is highly required by OEMs for tier 1 and subsidiary suppliers.

While ISO/SAE 21434 outlines the broad cybersecurity risk management framework for the entire vehicle lifecycle,

ASPICE for Cybersecurity focuses on the processes for secure automotive software development. Specifically, ISO 21434 defines the "what" of TARA by identifying assets, threats, and impacts across E/E systems, offering flexible methodologies. In contrast, ASPICE for Cybersecurity dictates the "how," focusing on integrating TARA findings into the software development lifecycle through detailed process attributes and measurable characteristics, ensuring threats are systematically addressed in requirements and verified during development.

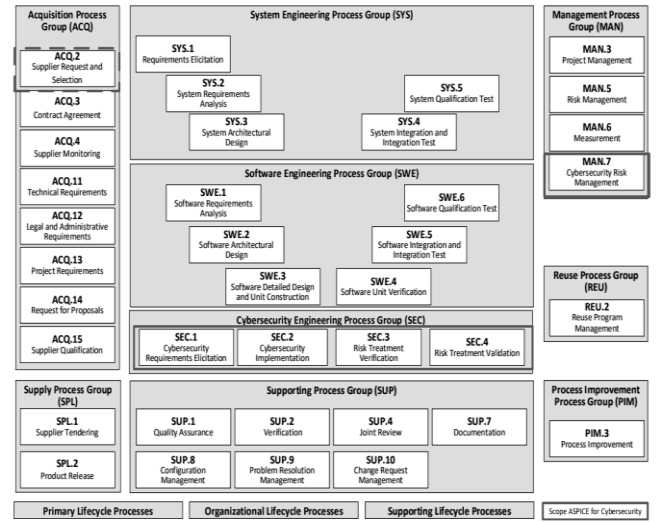


Figure 2. ASPICE for cybersecurity process assessment and reference model scope [4]

## 1.2 Challenge

There are continuous efforts by the industry to standardize their cybersecurity vehicle development activities based on the requirements of those two standards. Consequently, the increased efforts being performed to separately comply with both standards are forming a challenge to OEMs and tier 1 suppliers increasing cost of compliance. The challenges are a result of the lack of connectivity between the two standards. Also, the different requirements structure and content causing confusion to practitioners. One more challenge is the missing requirements between the two standards through the risk assessment and threat analysis activities. Given the mentioned challenges, the need for the optimization of these efforts is highly needed.

## 1.3 Contribution

This paper aims to try to optimize these efforts by developing a bilateral model that can be used by industry practitioners to facilitate both standards compliance and standardization. This model is based on complete and detailed analysis and mapping for the two standards. This mapping can also be used as checklist for cross standards compliance, supporting audits and assessments performed internally by the practitioners. Also, risk assessment and threat analysis tool is proposed to effectively and efficiently perform the TARA activities while conforming to both standards requirements and recommendations. We also tried to include all the experimentation observations and lessons learned from applying the model on different projects and using those outputs to increase the maturity of the model proposed through an empirical process.

The organization of this paper is as follows: Section 2 gives a summary for the previous efforts in standardization of cybersecurity risk assessment and threat analysis. Thereafter the context and relevance of security systems are explained in Section 3. This is followed by section 4, where the initial bilateral model is described. In section 5, the observations of the experimentation of the initial bilateral model are stated and explained. Where, section 6 states the experimentation results conclusion of creating the final bilateral model taking in consideration the lessons learned from applying the initial bilateral model. In section 7, an automated tool is introduced to facilitate and automate the deployment of the model in different projects. Finally, section 8 states the final results and concludes discussion while section 9 states the final conclusion and discusses future work.

## 2. RELATED WORK

The analysis and experimentation of cybersecurity risk assessment and threat analysis approaches have become a main focus of recent research over the past few years. M. Nizam et al. provided an overview of the use of attack graphs in risk assessment and threat analysis in the automotive industry in the studies [8, 9]. The ISO/SAE 21434 standard specifies the technical requirements for cybersecurity management of road vehicles. They proposed a generic model to automate the generation and analysis of attack paths in the risk assessment and threat analysis (TARA) process. R. Schermann et al. provided a proof of concept for a deep learning-based Intrusion Detection System (IDS) for Unmanned Aerial Systems (UAS) in the study [10]. Combining an Intrusion Prevention System (IPS) with IDS using risk assessment and threat analysis from the automotive domain ensures safety of automotive systems even after attacks. The following related works are reviewed to optimize TARA efforts by practitioners aiming to comply with ISO/SAE 21434 and ASPICE for Cybersecurity.

In risk assessment and threat analysis, there are ongoing efforts to improve the effectiveness of detecting possible attacks on vehicle security. P. Das et al. presented a structured approach to cybersecurity threat modelling and risk assessment in their study [11]. Utilizing the STRIDE methodology, they identified and analyzed potential threats targeting an in-vehicle infotainment system. The authors applied both SAHARA and DREAD models to assess and prioritize risks, enabling the formulation of appropriate mitigation strategies. Their work contributes to the development of effective cybersecurity treatments by aligning threat identification with practical, model-based risk evaluation techniques. These efforts were based on multiple studies focused on the release of the ISO/SAE 21434 standard requirements for risk assessment and threat analysis in 2021. Kawanishi et al. [12] published a study on risk assessment and threat analysis based on the asset container method. They focused on a single problem focusing on the insufficient evaluation of attack feasibilities for cyber-physical systems by the Common Vulnerability Scoring System (CVSS)-based approach. Another issue was the finding the relationship between damage factors and the risk assessment and threat analysis process. Kethareswaran et al. [13] provided a detailed summary of the ISO/SAE 21434 standard and analyzed its relevance for automotive architecture development in the study [13].

Mapping the ISO/SAE 21434 requirements to cybersecurity activities was not sufficient. Bridging the gaps in security of automotive systems and the standard requirements was necessary. Siddiqui et al. [14] demonstrated an integrated cybersecurity engineering process as a baseline to map the requirements of ISO/SAE 21434 to traditional system design engineering processes, including risk assessment and threat analysis in the study [13].

Since the release of ASPICE for Cybersecurity in 2021, suppliers and original OEMs have been required to comply with its standards, in addition to the homologation UNECE regulations 155 & 156 [15, 16]. Multiple efforts were made to analyze the requirements and practices of ASPICE for Cybersecurity. R. Messnarz et al. provided a thorough demonstration of the first experiences with ASPICE for Cybersecurity in the study [17]. Furthermore, R. Messnarz et al. outlined the expectations for automotive projects concerning ASPICE for Cybersecurity and provided guidance on creating additional cybersecurity views in system and software architectures in the study [18].

Although the previously mentioned related works highlighted the standard specifications of ISO/SAE 21434 and ASPICE for CS along with compliant risk assessment and threat analysis methods, the efforts made by industry practitioners to standardize their cybersecurity activities and engineering practices—especially the risk assessment and threat analysis activities—to comply with both standards simultaneously were not thoroughly addressed. The challenges of this compliance effort are not yet in focus. Additionally, no detailed cross-analysis and mapping between the two standards have been demonstrated to help practitioners achieve their objectives.

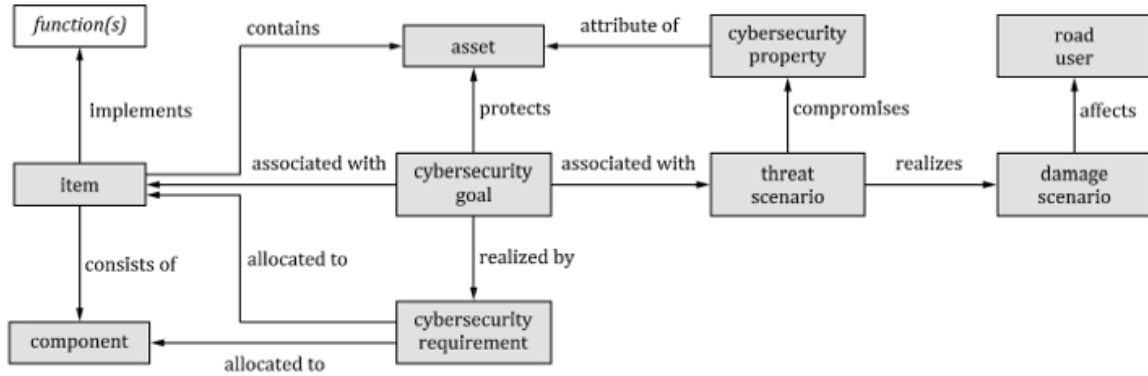
Although the previously mentioned related works, such as those by the studies [8, 9] on attack graph automation and Anand et al. [19] on comprehensive TARA methods, highlighted the specifications of ISO/SAE 21434 and ASPICE for CS along with compliant TARA approaches, a critical gap persists. While studies like Kawanishi et al. [12] refined TARA methodologies and Siddiqui et al. [14] mapped ISO/SAE 21434 to traditional engineering, and the studies [17, 18] provided deep insights into ASPICE for CS implementation, none have thoroughly addressed or demonstrated the practical efforts for industry practitioners to standardize their cybersecurity activities—especially TARA—to comply with *both standards simultaneously*. The inherent challenges of this dual compliance effort, which our work directly confronts, are not yet a primary focus in existing literature. Furthermore, a detailed cross-analysis and explicit, actionable mapping between the distinct requirements of ISO/SAE 21434 and ASPICE for CS, crucial for practitioners to achieve integrated objectives efficiently, remains undemonstrated in prior research.

In the subsequent sections, we will focus on the detailed analysis and mapping of both standards for the risk assessment and threat analysis activities. A bilateral unified process model is developed to cover the requirements of both standards. Additionally, the observations and lessons learned from applying this model to various projects will be shared. These observations and challenges were also used to increase the model's maturity through an empirical process. Furthermore, a risk assessment and threat analysis tool has been created to help practitioners achieve compliance with both standards.

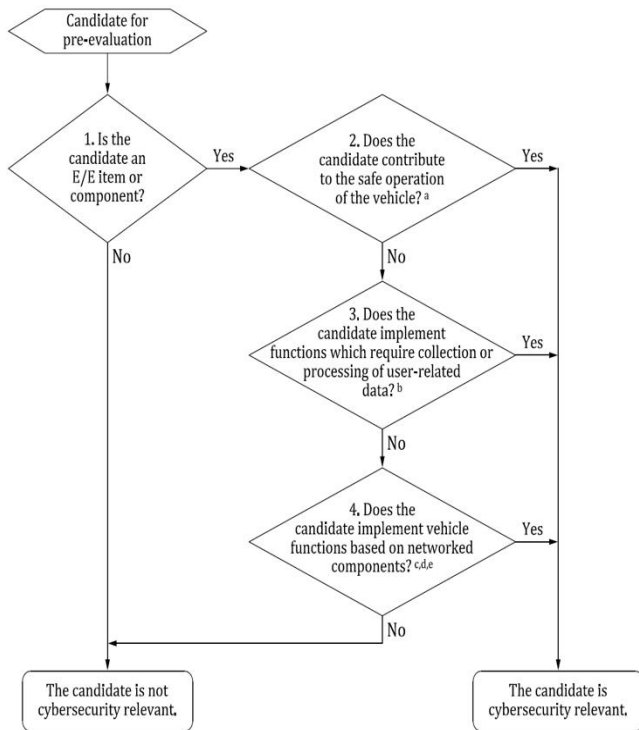
### 3. PRELIMINARIES

#### 3.1 Cybersecurity relevant system decomposition

ISO/SAE 21434 defines systems decomposition and the relationships between item, function, component and related terms shown in Figure 3 While Clause 15 explains modular methods for cybersecurity risk assessments that are invoked in



**Figure 3.** Relationship between function, item, component and related terms – ISO/SAE 21434 [1]



**Figure 4.** Cybersecurity determination criteria decision diagram – ISO/SAE 21434 [1]

### 4. INITIAL BILATERAL MODEL

#### 4.1 Scope

This paper addresses the risk assessment and threat analysis requirements in ISO/SAE 21434:2021, ASPICE for cybersecurity. The model developed focuses on the TARA requirements which is specified in ISO/SAE 21434:2021 Clauses 9, 15 and Annexes H, G and F. Furthermore, on the base practices (BP) defined in MAN.7, SEC.1, SEC.2 and SEC.3 process areas as shown in Table 1.

cybersecurity activities in clause 9 and other clauses.

#### 3.2 Cybersecurity relevance criteria

The ISO/SAE 21434 defines the criteria for determining the cybersecurity relevance for a system item or a component as shown in Figure 4.

**Table 1.** Cross-mapping scope

In-Scope Inputs	ASPICE for CS	ISO/SAE 21434
Phase	Cybersecurity Management & Engineering	Concept/TARA
Capability level (if applicable)	CL 1	NA
Process group/Clause	Cybersecurity Management & Engineering Process Group	Clause 9 – Concept Clause 15 - TARA
Process Areas/Sub-Clauses	MAN.7, SEC1, SEC.2 and SEC.3	9.3.2, 9.4.2 and 9.5.2 15.3.2, 15.4.2, 15.5.2, 15.6.2, 15.7.2, 15.8.2 and 15.9.2
ASPICE Process Attribute/ISO/SAE 21434 Requirement	PA 1.1	RQ-9-1 to RQ-9-11 RQ-15-01 till RQ-15-17

**Table 2.** ISO/SAE 21434 – ASPICE for CS initial phase 1 model [1, 4]

Compliance Model Category	ASPICE for CS	ISO/SAE 21434
Threat analysis and risk assessment	MAN.7.BP1	
	MAN.7.BP2	
	MAN.7.BP3	RQ-09-01
	MAN.7.BP4	RQ-09-02
	MAN.7.BP5	RQ-09-03
	MAN.7.BP6	RQ-09-04
	MAN.7.BP7	RQ-09-05
	MAN.7.BP8	RQ-09-06
Cybersecurity requirements and controls	SEC.1.BP1	RQ-09-07
	SEC.1.BP2	
	SEC.1.BP3	
	SEC.1.BP4	
	SEC.1.BP1	RQ-09-08
	SEC.1.BP2	RQ-09-09
	SEC.1.BP3	RQ-09-10
	SEC.1.BP4	RQ-09-11

**Table 3.** ISO/SAE 21434 – ASPICE for CS initial phase 2 model [1, 4]

Compliance Model Category	ASPICE for CS	ISO/SAE 21434
TARA – Item Definition	NA	[RQ-09-01]
TARA – Operational Environment	MAN.7.BP1	[RQ-09-02]
TARA – Risk Analysis	MAN.7.BP1 MAN.7.BP2 MAN.7.BP3 MAN.7.BP4 MAN.7.BP5	[RQ-09-03]
TARA – Risk Treatment	MAN.7.BP6	[RQ-09-04]
TARA – CS Goals	SEC.1.BP1	[RQ-09-05]
TARA – CS Claims	MAN.7.BP6	[RQ-09-06]
TARA Verification	SEC.1.BP2 SEC.1.BP3	[RC-09-07] [RC-09-11]
TARA – CS Monitoring and Control	MAN.7.BP7 MAN.7.BP8 SEC.1.BP4	[RQ-09-06]
TARA – CS Controls	SEC.2.BP3	[RQ-09-09]
TARA – CS Requirements	SEC.2.BP1	[RQ-09-09]
CS Requirements Allocation	SEC.2.BP2	[RQ-09-10]

#### 4.2 Initial model

An in-depth analysis for the specifications of the ISO/SAE 21434 and ASPICE for Cybersecurity risk assessment and threat analysis requirements have been conducted. Followed by a complete mapping between the ISO/SAE 21434 requirements and ASPICE for CS PA1.1 base practices as indicated in Table 1. In order to simplify the readability for the practitioners, a categorization for the requirements and base practices is used. The initial model was conducted through two

phases. The first phase, the mapping was done based in a wide scope categories which was seen later on that it needed further refinement as seen in Tables 2 and 3. Also in the first mapping effort, Clause 15 was not mapped as clause 9 includes all the TARA process activities which was concluded by experiments on projects that clause 15 is needed by practitioners to implement the standard TARA modular methods. All Automotive Spice for CS base practices for the in-scope process areas along with key ISO/SAE 21434 requirements are briefly explained in the Appendix at the tail of this paper.

In the second phase of the model. We have refined the categorization for better readability and usability for the practitioners.

#### 5. PROJECTS EXPERIMENTATION OBSERVATIONS, CHALLENGES AND MODEL IMPROVEMENT PROPOSALS

A study was performed on four projects from same organization covering various product lines that implemented the proposed model. An ISO/SAE 21434 audit and ASPICE for CS assessments were carried out for these projects. The projects aim to achieve Capability Level 1 (CL 1) in ASPICE and successfully pass the ISO/SAE 21434 audit. To safeguard proprietary information, those projects will be referred to anonymously throughout the paper. The goal was to document observations from the ISO/SAE 21434 audit and the four ASPICE for CS assessments, focusing solely on the shared Merits, challenges, and improvement proposals identified during the audit and assessments after applying the model in the actual project operational settings. The assessment ratings are not discussed here and as found in Tables 4-8.

**Table 4.** Merits, challenges and improvement recommendations - project (A)

ID	A.1	A.2
Compliance Model Category	TARA - Item Definition	TARA Operational Environment
Process Area/Clause	MAN.7.Clause 9	MAN.7.Clause 9
Affected Indicator (BP/RQ)	[RQ-09-01]	[RQ-09-02] MAN.7.BP1
Merits	Item definition is defined with detail in the ISO/SAE 21434 RQ-09-01 where it includes the definition of a) Item boundary b) Item functions c) Preliminary architecture.	The operational Environment is mentioned in both the ASPICE for CS MAN.7.BP1 and ISO/SAE 21434 [RQ-09-02].
Challenges	The item definition while crucial is not defined nor mentioned in the ASPICE for CS. Practitioners was not aware of such definition while using the ASPICE for CS as a reference for implementing the model.	The operational Environment definition and description is clearly required by ISO/SAE 21434 in [RQ-09-02]. While Only mentioned to be considered during the description of the cybersecurity risk management scope in ASPICE for CS MAN.7 BP1. Practitioners using the ASPICE for CS as a reference were didn't have the operational environment defined as required by ISO/SAE 21434 [RQ-09-02].
Model Improvement Recommendations	The Model to include the item definition if ASPICE for CS is to be considered as a reference.	The Model to include the operational Environment definition if ASPICE for CS is to be considered as a reference.

**Table 5.** Merits, challenges and improvement recommendations - project (B)

ID	B.1	B.2
Compliance Model Category	TARA – Risk Analysis	TARA – Risk Treatment
Process Area/Clause	MAN.7.Clause 9	MAN.7.Clause 9
Affected Indicator (BP/RQ)	[RQ-09-03] MAN.7.BP1 MAN.7.BP2	[RQ-09-04] MAN.7.BP6

	MAN.7.BP3 MAN.7.BP4 MAN.7.BP5	
Merits	The ISO/SAE 21434 defines a complete risk analysis criterion for the TARA Model including a process workflow in Figure 3, TARA methods to determine the extent a road user can be influenced by a threat scenario in clause 15 and TARA methods in ANNEX H, G & F in addition to the above mentioned impacted requirement in clause 9. ASPICE for CS mentions some aspects of the Risk Management Scope referring to the TARA practices in the ISO/SAE 21434. Applying the TARA Model through only referring to the ASPICE for CS was not sufficient to practitioners for technical implementation of the TARA. A reference to the ISO/SAE 21434 TARA Model requirements was necessary.	Both requirements for ISO/SAE 21434 [RQ-09-04] and ASPICE for CS MAN.7.BP6 are mapped and were sufficient for compliant implementation by practitioners.
Challenges	The Model to mandate a reference to the ISO/SAE 21434 TARA process requirements in clause 9, specific TARA practices and criteria in clause 15, Process workflow in Figure 3 and ANNEX H, G & F TARA methods.	NA
Model Improvement Recommendations		NA

**Table 6.** Merits, challenges and improvement recommendations - project (C)

ID	C.1	C.2
Compliance Model Category	TARA – CS Goals	TARA – CS Claims
Process Area/Clause	SEC.1/Clause 9	MAN.7.C.9
Affected Indicator (BP/RQ)	[RQ-09-05] SEC.1.BP1	[RQ-09-06] MAN.7.BP6
Merits	Both requirements for ISO/SAE 21434 [RQ-09-05] and ASPICE for CS SEC.1.BP1 are mapped and were sufficient for compliant implementation by practitioners.	Both ISO/SAE 21434 [RQ-09-06] and ASPICE for CS MAN.7.BP6 describes the need for specifying Cybersecurity claims.
Challenges	NA	While ISO/SAE 21434 [RQ-09-06] requires specifying a CS claim. ASPICE for CS in MAN.7.BP6 the word “Typically” in Note 8 Making it as not mandatorily required by the ASPICE for CS. This was a challenge to practitioners using ASPICE for CS as a reference.
Model Improvement Recommendations	NA	The Model to include a mandatory Requirement for the specification of cybersecurity claims in case if the risk treatment decision was to share or retain the risk if the ASPICE for CS is used as reference.

**Table 7.** Merits, challenges and improvement recommendations - project (D)

ID	D.1	D.2
Compliance Model Category	TARA Verification	TARA – CS Monitoring and Control
Process Area/Clause	SEC.1/Clause 9	SEC.1/MAN.7/Clause 9
Affected Indicator (BP/RQ)	[RC-09-07] [RC-09-11] SEC.1.BP2 SEC.1.BP3	MAN.7.BP7 MAN.7.BP8 SEC.1.BP4 (Communication is extra in ASPICE) [RQ-09-06]
Merits	[RC-09-07] [RC-09-11] SEC.1.BP2 SEC.1.BP3	(CS Monitoring is described in detail in clause 8) Both ISO/SAE 21434 and ASPICE for CS focus on cybersecurity monitoring through MAN.7.BP7, MAN.7.BP8 and ISO/SAE 21434 Clause 8. Additionally [RQ-09-06] addresses the consideration of cybersecurity claims in cybersecurity monitoring.
Challenges	ASPICE for CS SEC.1.BP2, SEC.1.BP3 do not address the consistency with respect to cybersecurity claims. Which was neglected by practitioners when considering the reference to be ASPICE for CS.	Communication practices in ASPICE for CS e.g. SEC.1.BP4 are a unique indicator that is not explicitly mentioned by ISO/SAE 21434. Considering ISO/SAE 21434 as a reference, communication was not focused by practitioners which led to the weakness of this indicator compliance in the ASPICE for CS assessment.
Model Improvement Recommendations	Model to include a mandatory requirements to address ensuring consistency with respect to cybersecurity claims when considering the reference to be ASPICE for CS.	Model to include a mandatory requirement for the communication of the cybersecurity goals, requirements and controls to relevant stakeholders if ISO/SAE 21434 is used as reference.

**Table 8.** Merits, challenges and improvement recommendations - project (D)

ID	D.3
Compliance Model Category	TARA – CS Requirements
Process Area/Clause	SEC.2/Clause 9
Affected Indicator (BP/RQ)	SEC.2.BP1 [RQ-09-09]

Merits	Both requirements for ISO/SAE 21434 [RQ-09-09] and ASPICE for CS SEC.2.BP1 are mapped and were sufficient for compliant implementation by practitioners.
Challenges	NA
Model Improvement Recommendations	NA

Insights gained during the implementation of the model showed that practitioners either considered as a reference the base practices of ASPICE for CS or the requirements of ISO/SAE 21434. The improvement proposals for enhancing the model took this insight into account, addressing the cases of reference. Additionally, these improvement proposals were used as a basis for advancing the model's maturity.

## 6. EXPERIMENTATION RESULTS CONCLUSION

After the careful analysis of the project's experimentation observations and challenges. It was concluded that the ISO/SAE 21434 is the most suitable standard to be considered as a default reference for the model. This conclusion was based on the number of gaps and challenges identified during the experimentation. When the ISO/SAE 21434 is used as reference, it had the least number of gaps against ASPICE for CS as shown in Table 9, i.e. the ISO/SAE 21434 requirements

cover most of the ASPICE for CS PA1.1 base practices. Nonetheless, ASPICE for CS can also be used as a reference but considerations for adding new model requirements (MR) to cover both standards requirements were realized.

**Table 9.** ISO/SAE 21434 vs. ASPICE for CS gaps [1, 4]

Model Reference	ISO/SAE 21434	ASPICE for CS
Added requirements (Gaps) Count	2	5

### 6.1 ISO/SAE 21434 referenced bilateral model

A bilateral model is developed based on the ISO/SAE 21434 as a reference as shown in Table 10.

A bilateral new standard model is derived on the basis of the ASPICE for Cybersecurity as a reference as shown in Table 11.

**Table 10.** Bilateral model – referencing ISO/SAE 21434 [1]

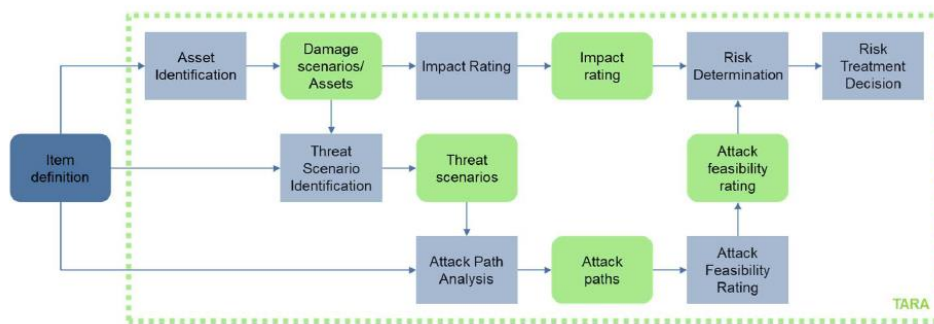
Compliance Model Category	ASPICE for CS	ISO/SAE 21434	Compliance Model Additional Requirements (MR)
TARA – Item Definition	NA	[RQ-09-01]	NA
TARA – Operational Environment	MAN.7.BP1	[RQ-09-02]	NA
TARA – Risk Analysis	MAN.7.BP1 MAN.7.BP2 MAN.7.BP3 MAN.7.BP4 MAN.7.BP5	[RQ-09-03] [RQ-15-01] to [RQ-15-17]	NA
TARA – Risk Treatment	MAN.7.BP6	[RQ-09-04]	NA
TARA – CS Goals	SEC.1.BP1	[RQ-09-05]	NA
TARA – CS Claims	MAN.7.BP6	[RQ-09-06]	NA
TARA Verification	SEC.1.BP2 SEC.1.BP3	[RC-09-07] [RC-09-11]	MR.01 Establish bidirectional traceability between cybersecurity requirements and goals, cybersecurity goals and the threat scenarios, cybersecurity goals and claims to the risk treatment decisions. (add this to project observations)
TARA – CS Monitoring and Control	MAN.7.BP7 MAN.7.BP8 SEC.1.BP4	[RQ-09-06] [RQ-08-01] to [RQ-08-08]	MR.02 Communicate agreed cybersecurity analysis results, risk treatment decisions, goals and requirements to all affected parties continuously through the cybersecurity life cycle.
TARA – CS Controls	SEC.2.BP3	[RQ-09-08]	NA
TARA – CS Requirements	SEC.2.BP1	[RQ-09-09]	NA
CS Requirements Allocation	SEC.2.BP2	[RQ-09-10]	NA

**Table 11.** Bilateral model – referencing ASPICE for CS [4]

Compliance Model Category	ASPICE for CS	ISO/SAE 21434	Compliance Model Additional Requirements (MR)
TARA – Item Definition	NA	[RQ-09-01]	MR.01 Item boundary, Item functions, preliminary architecture shall be identified.
TARA – Operational Environment	MAN.7.BP1	[RQ-09-02]	MR.02 Operational environment of the item relevant to cybersecurity shall be explained.
TARA – Risk Analysis	MAN.7.BP1 MAN.7.BP2	[RQ-09-03] [RQ-15-01] to	MR.03 Analysis approaches to be used shall conform to the specified methods and recommendations described in ISO/SAE 21434 requirements in Clause 15



	MAN.7.BP3 MAN.7.BP4 MAN.7.BP5	[RQ-15-17]	and ANNEX H, G & F.
TARA – Risk Treatment	MAN.7.BP6	[RQ-09-04]	NA
TARA – CS Goals	SEC.1.BP1	[RQ-09-05]	NA
TARA – CS Claims	MAN.7.BP6	[RQ-09-06]	MR.04 Cybersecurity claims shall be specified in case if the risk treatment decision was to share or retain the risk.
TARA Verification	SEC.1.BP2 SEC.1.BP3	[RC-09-07] [RC-09-11]	MR.05 Ensure consistency with respect to cybersecurity claims as specified in ISO/SAE 21434 [RC-09-07] and [RC-09-11].
TARA – CS Monitoring and Control	MAN.7.BP7 MAN.7.BP8	[RQ-09-06] [RQ-08-01] to	NA
TARA – CS Controls	SEC.1.BP4	[RQ-08-08]	NA
TARA – CS Requirements	SEC.2.BP1	[RQ-09-09]	NA
CS Requirements Allocation	SEC.2.BP2	[RQ-09-10]	NA



**Figure 5.** TARA process

## 7. CYBERSECURITY RISK ASSESSMENT AND THREAT ANALYSIS AUTOMATED COMPLIANCE TOOL

A risk assessment and threat analysis automated tool is developed based on the proposed model to include a data set of defined TARA methods described in the ISO/SAE 21434 Clause 9, Clause 15, Annex F (Guidelines for impact rating), Annex G (Guidelines for attack feasibility rating) and Annex H (Examples of application of TARA Methods). This tool is also developed to ensure implicit compliance the ASPICE for CS Practices required to achieve PA1.1 base practices. Applying this tool would be sufficient to conduct the risk assessment and threat analysis activities in an automated compliant approach for the two standards: ISO/SAE 21434 and ASPICE for CS. The detailed TARA process is described in Figure 5.

### 7.1 Impact rating input data and coding

Impact rating criteria is defined explicitly in the ISO/SAE 21434 as shown in Figures 6-9.

Impact rating	Criteria for safety impact rating
Severe	S3: Life-threatening injuries (survival uncertain), fatal injuries
Major	S2: Severe and life-threatening injuries (survival probable)
Moderate	S1: Light and moderate injuries
Negligible	S0: No injuries a

**Figure 6.** Cybersecurity determination criteria decision diagram – ISO/SAE 21434 [1]

Impact rating	Criteria for financial impact rating
Severe	The financial damage leads to catastrophic consequences which the affected road user might not overcome.
Major	The financial damage leads to substantial consequences which the affected road user will be able to overcome.
Moderate	The financial damage leads to inconvenient consequences which the affected road user will be able to overcome with limited resources.
Negligible	The financial damage leads to no effect, negligible consequences or is irrelevant to the road user.

**Figure 7.** Operational impact rating criteria – ISO/SAE 21434 [1]

Impact rating	Criteria for operational impact rating
Severe	The operational damage leads to the loss or impairment of a core vehicle function. EXAMPLE 1 Vehicle not working or showing unexpected behavior of core functions such as enabling of limp home mode or autonomous driving to an unintended location.
Major	The operational damage leads to the loss or impairment of an important vehicle function. EXAMPLE 2 Significant annoyance of the driver.
Moderate	The operational damage leads to partial degradation of a vehicle function. EXAMPLE 3 User satisfaction negatively affected.
Negligible	The operational damage leads to no impairment or non-perceivable impairment of a vehicle

**Figure 8.** Financial impact rating criteria – ISO/SAE 21434 [1]



Impact rating	Criteria for privacy impact rating
Severe	The privacy damage leads to significant or even irreversible impact to the road user. The information regarding the road user is highly sensitive and easy to link to a PII principal.
Major	The privacy damage leads to serious impact to the road user. The information regarding the road user is: a) highly sensitive and difficult to link to a PII principal; or b) sensitive and easy to link to a PII principal.
Moderate	The privacy damage leads to inconvenient consequences to the road user. The information regarding the road user is: a) sensitive but difficult to link to a PII principal; or b) not sensitive but easy to link to a PII principal.
Negligible	The privacy damage leads to no effect or, negligible consequences or is irrelevant to the road user. The information regarding the road user is not sensitive and difficult to link to a PII principal.

**Figure 9.** Privacy impact rating criteria – ISO/SAE 21434 [1]

Equations for mapping impact categories to numerical values are embedded in the tool using Visual Basic for

applications (VBA) language as indicated in Algorithm 1.

**Algorithm 1.** Impact category text value to impact rating numerical value

**Safety S3 value conversion:**

=IF(E11="";"";VALUE(MID(E11;2;1)))

**Financial F0 value conversion:**

=IF(F11="";"";VALUE(MID(F11;2;1)))

An example of the user-interface for the impact analysis and rating can be shown in Figures 10 and 11.

## 7.2 Attack feasibility rating input data and coding

Attack feasibility criteria is defined in the ISO/SAE 21434 as shown in Tables 12 and 13. Those methods and approaches are the references values considered while developing the proposed model tool.

Asset	Security Property	Damage Scenario	Stakeholder: Road User/ driver			
			Criteria for Safety Impact rating	Criteria for Financial Impact rating	Criteria for Operational Impact rating	Criteria for Privacy Impact rating
Communication Channel to the Internet	Authenticity	<i>physical inconveniences due to unexpected movement of the seat to secure position while driving caused by a spoofed message</i>	S3: Life-threatening injuries (survival uncertain), fatal injuries	F0: The financial damage leads to no effect, negligible consequences or is irrelevant to the road user.	O3: The operational damage leads to a vehicle not working, from non-intended operation up to the vehicle being non-operational.	P0: The privacy damage leads to no effect or can create few inconveniences to the road user. In this case, the information regarding the road user is not sensitive and difficult to link to a PII principal.
	Integrity	<i>physical inconveniences due to unexpected movement of the seat to secure position while driving caused by a tampered message</i>	S3: Life-threatening injuries (survival uncertain), fatal injuries	F0: The financial damage leads to no effect, negligible consequences or is irrelevant to the road user.	O3: The operational damage leads to a vehicle not working, from non-intended operation up to the vehicle being non-operational.	P0: The privacy damage leads to no effect or can create few inconveniences to the road user. In this case, the information regarding the road user is not sensitive and difficult to link to a PII principal.
	Non-repudiation	<i>physical inconveniences due to unexpected movement of the seat to secure position while driving caused by a delayed repeated message</i>	S3: Life-threatening injuries (survival uncertain), fatal injuries	F0: The financial damage leads to no effect, negligible consequences or is irrelevant to the road user.	O3: The operational damage leads to a vehicle not working, from non-intended operation up to the vehicle being non-operational.	P0: The privacy damage leads to no effect or can create few inconveniences to the road user. In this case, the information regarding the road user is not sensitive and difficult to link to a PII principal.

**Figure 10.** Impact analysis example from the model tool

Stakeholder OEM/ service provider			Stakeholder: Road User				Stakeholder: OEM			Justification
Criteria for Financial Impact rating	Criteria for Operational Impact rating	Criteria for Privacy Impact rating	S	F	O	P	F <sub>OEM</sub>	O <sub>OEM</sub>	P <sub>OEM</sub>	
F1: The financial damage leads to inconvenient consequences which the affected stakeholder will be able to overcome with limited resources.	O3: The operational damage leads to a service not working, from non-intended operation up to the service being non-operational.	P0: The privacy damage leads to no effect or can create few inconveniences to the service user AND the number of affected PII principals is very limited. In this case, the information regarding the service users is not sensitive and difficult to link to a PII principal.	3	0	3	0	1	3	0	- severe safety impact if seat will move while driving - severe operational impact for the service provider of a fleet

**Figure 11.** Impact rating example from the model tool

**Table 12.** Aggregated attack feasibility rating criteria – ISO/SAE 21434 [1]

Attack Feasibility - Definitions and Values			
Attack Feasibility Category	Definition	Enumerate	Value
Elapsed Time	The time taken by an attacker to identify potential vulnerability, to develop a method to attack and to mount the attack.	≤ 1 day	0
		≤ 1 week	1
		≤ 1 month	4

Specialist Expertise	The required level of generic knowledge of the underlying principles, product types or attack methods.	≤ 6 months	17
		> 6 months	19
		Layman	0
		Proficient	3
		Expert	6
Knowledge of the item	Expertise of the item under investigation. This is distinct from generic expertise, but not unrelated to it.	Multiple experts	8
		Public information	0
		Restricted information	3
		Confidential information	7
		Strictly confidential information	11
Window of opportunity	Related to the Elapsed time. Identification and exploitation of a vulnerability may require considerable amounts of access to a system that may increase the probability of detection of the attack. Some attack methods might require considerable effort off-line, and brief access to the target to exploit. Access may also need to be continuous or over multiple sessions.	Unlimited	0
		Easy	1
		Moderate	4
		Difficult	10
		Standard	0
Equipment	This refers to the equipment required for identifying and exploiting a vulnerability.	Specialized	4
		Bespoke	7
		Multiple bespoke	9

**Table 13.** Attack potential mapping – ISO/SAE 21434 [1]

Values	Attack Potential Required to Exploit Scenario	Attack Feasibility
0 - 9	Basic	High
10 - 13	Enhanced-basic	
14 - 19	Moderate	Medium
20 - 24	High	Low
=> 25	Beyond high	Very low

According to ISO/IEC 18045, attack potential corresponds to the addition of all parameters.

where,

$$\text{Attack Potential (AP)} = \sum P$$

Equations for mapping parameter categories to numerical values and Attack Potential (AP) calculation are embedded in the tool using Visual Basic for applications (VBA) coding language as indicated in Algorithms 2 and 3.

An example of the user-interface for the feasibility analysis and attack potential calculation can be shown in Figures 12 and 13.

**Algorithm 2.** Parameter Category Conversion to Numerical Value

**Elapsed time conversion:**

```
=IF (ISERROR (VLOOKUP (@I:I;'reference values'!$J:$K;2;0)));""; VLOOKUP (@I:I;'reference values'!$J:$K;2;0))
```

**Specialized expertise conversion:**

```
=IF (ISERROR (VLOOKUP (@J:J;'reference values'!$J:$K;2;0)));""; VLOOKUP (@J:J;'reference values'!$J:$K;2;0))
```

**Algorithm 3.** Attack Potential (AP) Calculation

**Attack Potential (AP) numerical aggregation:**

```
=IF (SUM(N7:R7) =0;""; SUM(N7:R7))
```

**Attack Potential (AP) mapping:**

```
=IF (S7="";""; VLOOKUP (@S$4:S974;'reference values'!M$3:P$7;4))
```

Asset	Threat Scenario	Attack Path Analysis
Communication Channel to the Internet	spoofed messages may lead to messages at the wrong time	- get access to the communication channel (back-end, ...) - trigger spoofed (valid) messages which will realize a spoofed communication
	tampered messages may lead to messages at the wrong time	- gets access to the communication channel - intercept message flow - performs a MITM attack to tamper the communication
	replay of messages (jammer) which were intercepted before leads to messages at the wrong time	- intercept the communication - sent a replayed message

**Figure 12.** Attack feasibility analysis example from the

model tool										Total Value	Attack feasibility Value
Elapsed Time	Specialist Expertise	Knowledge of the item	Window of opportunity	IT hardware/ software or other equipment required	Elapsed Time	Specialist Expertise	Knowledge of the item	Window of opportunity	IT hardware/ software or other equipment required		
> 6 months	Expert	Confidential information	Moderate	Specialised	19	6	7	4	4	40	Very low
≤ 6 months	Proficient	Restricted information	Moderate	Specialised	17	3	3	4	4	31	Very low
≤ 6 months	Proficient	Confidential information	Moderate	Standard	17	3	7	4	0	31	Very low
> 6 months	Proficient	Confidential information	Easy	Standard	19	3	7	1	0	30	Very low
> 6 months	Proficient	Restricted information	Moderate	Specialised	19	3	3	4	4	33	Very low
≤ 1 month	Proficient	Restricted information	Moderate	Standard	4	3	3	4	0	14	Medium

**Figure 13.** Attack feasibility analysis example from the model tool

### 7.3 Risk rating and assessment

Risk rating and assessment criteria is defined in the ISO/SAE 21434 as shown in Figure 14.

		Attack Feasibility			
		very low	low	medium	high
impact	severe	2	3	4	5
	serious	1	2	3	4
	moderate	1	2	2	3
	negligible	1	1	1	1

**Figure 14.** Risk matrix – ISO/SAE 21434 [1]

Equations for calculating risk value based on attack feasibility and impact ISO/SAE 21434 risk matrix is embedded in the tool using Visual Basic for applications (VBA) coding language as indicated in Algorithm 4.

**Algorithm 4.** Risk Determination

```
=IF ($N10=0;"I missing";VLOOKUP(AC10;'reference values'!$Y$3:$Z$18;2;0))
```

An example of the user-interface for the risk assessment can be shown in Figures 15 and 16.

7.4 Cybersecurity goals, claims, requirements and controls

Traceability and communication for cybersecurity goals, claims, requirements, and controls are ensured through the mandatory attribute insertion for each risk treatment decision which fulfils the ASPICE for Cybersecurity additional bilateral model requirements as shown in Figure 17.

Asset	Security Property	Damage Scenario	Threat Scenario	Attack Path Analysis	Stakeholder: Road User				Stakeholder: OEM			Value	Attack feasibility
					S	F	O	P	FOOM	OOOM	POOM		
Communication Channel to the Internet	Authenticity	physical inconveniences due to unexpected movement of the seat to secure position while driving caused by a spoofed message	spoofed messages may lead to messages at the wrong time	- get access to the communication channel (back-end, ...) - trigger spoofed (valid) messages which will realize a spoofed communication	3	0	3	0	1	3	0	40	Very low

Figure 15. Risk assessment example from the model tool

Stakeholder: Road User				Stakeholder: OEM				Risk Treatment decision		Cybersecurity Goal/ Controls/ Remarks	Cybersecurity Claim	status of controls
S	F	O	P	FOOM	OOOM	POOM		Option taken				
2	1	2	1	1	2	1		accepting or retaining the risk	risk is very low, can be accepted			open

Figure 16. Risk treatment example from the model tool

Cybersecurity Goal/ Controls/ Remarks	Cybersecurity Claim	status of controls	Cybersecurity Requirements	Relevant Stakeholders	Communication Status	Change Request Number/TARA Version

Figure 17. Traceability and communication attributes defined in the model tool

8. FINAL RESULTS AND DISCUSSION

The interest in standardizing and optimizing cybersecurity engineering in the automotive industry has increased significantly through the past few years. 50% of all cyber incidents in 2023 had high or massive impact. Also, 95% of attacks are executed remotely, of which 85% are long range. Furthermore, 37% of threat actor activities in the deep and dark web target multiple OEMs simultaneously [20]. This translates to severe financial and safety losses. The cost of cyberattacks on vehicles and the broader automotive industry has been escalating in recent years. In 2023, the global automotive sector faced significant financial losses due to cyberattacks, with estimates suggesting that recovery costs per incident range from \$17 million to nearly \$50 million [21, 22]. Risk assessment and threat analysis activities constitutes the major and critical part of cybersecurity engineering activities. Furthermore, it represents the basis on which all cybersecurity activities are built upon. During the implementation, we tried to contribute to the optimization of risk assessment and threat analysis activities referenced in the ISO/SAE 21434 and Automotive SPICE for Cybersecurity. This contribution was by creating a bilateral integrated model and tool which were

experimented on projects that have completely or partially successfully achieved compliance with ISO/SAE 21434 and ASPICE for Cybersecurity. This adherence significantly reduced the risks which are associated with recovery costs and financial damage endured due to escalating cyberattacks. The usage of the model and the TARA automated too also resulted in significant reduction of quality and compliance costs during development.

Although this research didn't directly test how the model performs at different project sizes, it was built with scalability in mind. For smaller projects, the model offers a simple but thorough approach that helps teams apply essential cybersecurity practices without adding unnecessary complexity. Even limited projects can use it to effectively spot and handle risks. On the other hand, for larger and more complex systems, the model is designed to scale up—offering the structure and depth needed for in-depth threat analysis and risk management. It's also built to align with both ISO/SAE 21434 and ASPICE for Cybersecurity, making it suitable for a wide range of automotive development needs.

8.1 Time-effort and cost reduction analysis for automotive cybersecurity projects using our proposed bilateral model

This analysis tracks the time effort spent by teams of 13-20 automotive cybersecurity developers working on an advanced software project. The automotive system integrates multiple sensors, including LiDAR, radar, and cameras, with real-time processing units and AI-based decision-making algorithms. Ensuring cybersecurity in such systems requires rigorous implementation of security measures across multiple software and hardware components.

Project A: ADAS cybersecurity optimization analysis

The bar chart in Figure 18 provides a comparative analysis of the initial and optimized hours required for different cybersecurity tasks within Project A: ADAS Cybersecurity Optimization. The x-axis represents the number of hours allocated for each activity, while the y-axis lists various cybersecurity processes involved in securing Advanced Driver Assistance Systems (ADAS).

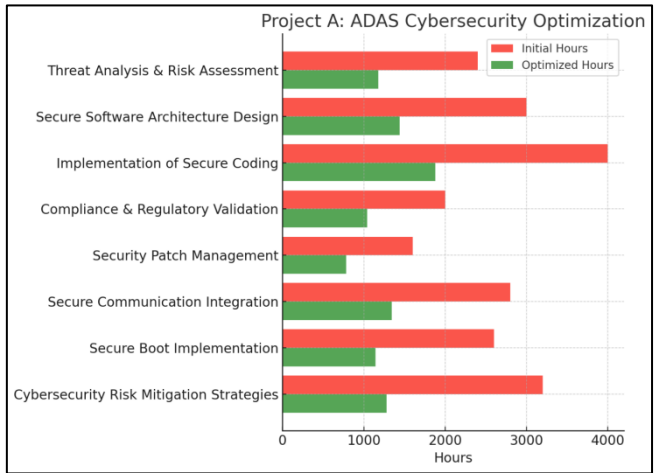


Figure 18. Project A: ADAS cybersecurity optimization data analysis

Project B: Electric vehicle (EV) security implementation analysis

The bar chart in Figure 19 illustrates a comparison between the initial and optimized hours required for various

cybersecurity tasks in Project B: Electric Vehicle (EV) Security Implementation. The x-axis represents the number of hours, while the y-axis lists the security activities necessary for ensuring the protection of EV systems.

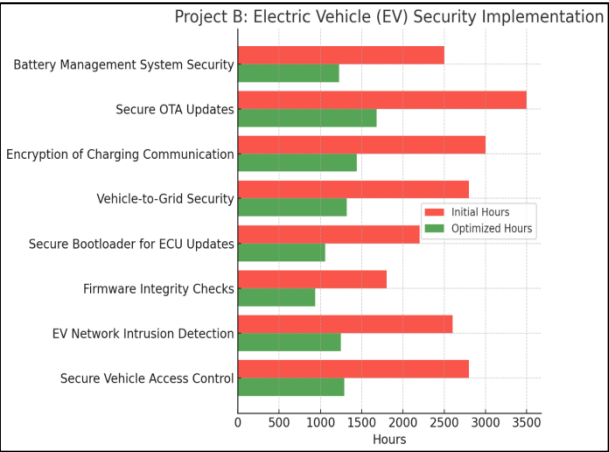


Figure 19. Project B: electric vehicle (EV) security implementation data analysis

Project C: Connected car cybersecurity enhancement

The bar chart in Figure 20 visualizes a comparison between the initial and optimized hours required for various cybersecurity tasks in Project C: Connected Car Cybersecurity Enhancement. The x-axis represents the number of hours, while the y-axis lists the critical security activities necessary to protect connected vehicle ecosystems.

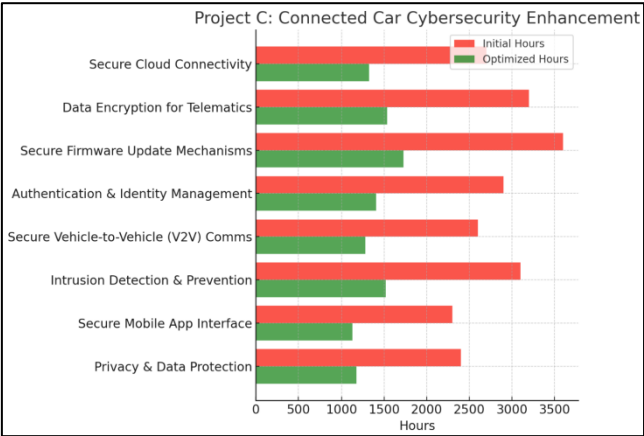


Figure 20. Project C: connected car cybersecurity enhancement data analysis

Project D: Autonomous vehicle security measures

The bar chart in Figure 21 illustrates a comparison between the initial and optimized hours required for various cybersecurity tasks in Project D: Autonomous Vehicle Security Measures. The x-axis represents the number of hours, while the y-axis lists essential security measures for autonomous vehicle (AV) systems.

Initially, development hours were spent on individual, isolated components of the automotive system, where security aspects were addressed separately for different assets such as sensor firmware, communication protocols, and real-time decision-making software. This fragmented approach resulted in higher overall effort and redundancy across tasks.

After implementing the proposed bilateral standard model and the TARA automated tool, which both introduced a structured and unified cybersecurity framework, the development efficiency was improved significantly. This approach centralized security implementations, leveraged reusable security modules, and streamlined testing methodologies. As a result, the effort per task was reduced by 40-60%, leading to enhanced efficiency, reduced costs, and improved security compliance. The following figures represent the initial and optimized development hours, percentage reduction, and corresponding cost savings in percentage for 13-20 developers collectively working on key cybersecurity development tasks.

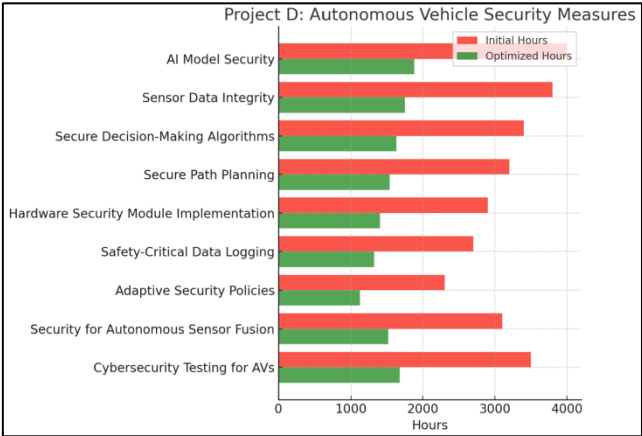


Figure 21. Project D: autonomous vehicle security measures data analysis

8.2 Overall results analysis

Figure 22 illustrates a comparative analysis of the initial and optimized hours required for the different 4 cybersecurity projects. The x-axis represents the stages of evaluation, categorized as "Initial Hours" and "Optimized Hours," while the y-axis quantifies the average hours allocated for each project. Four cybersecurity initiatives are analyzed in this study: Project A: ADAS Cybersecurity Optimization, Project B: Electric Vehicle (EV) Security Implementation, Project C: Connected Car Cybersecurity Enhancement and Project D: Autonomous Vehicle Security Measures.

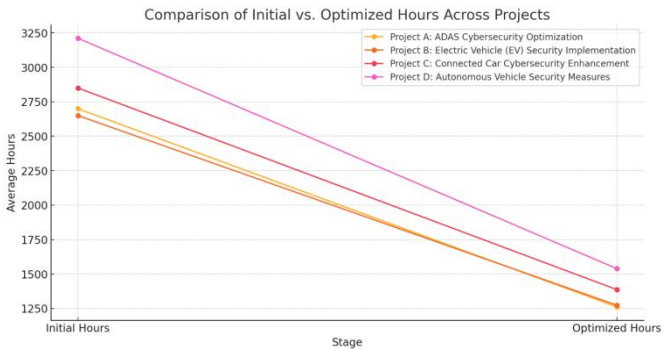


Figure 22. Projects cost reduction projection analysis

The results indicate a significant reduction in the required hours for each project after implementing the proposed bilateral model which is the basis for optimization efforts. Initially, all projects had higher time allocations, but the optimized phase demonstrates substantial efficiency

improvements. The trend lines clearly depict a downward trajectory, highlighting the impact of process enhancements, automation, and refined security methodologies -due to the use of the proposed bilateral model- in reducing effort while maintaining compliance and effectiveness.

This reduction in effort underscores the effectiveness of structured cybersecurity frameworks, process standardization, and automation in minimizing resource utilization without compromising security robustness. The proposed bilateral model has achieved significant cost reductions and enhanced the cybersecurity compliance which in return reduce the future recovery costs and attacks losses.

### 8.3 Limitations

While the proposed bilateral model and tool effectively optimize TARA and ensure compliance with ISO/SAE 21434 and ASPICE for Cybersecurity, some limitations are worth noting for future refinement. The primary limitations of the current model and its application are as follows:

1. Scope of Standardization: The model primarily integrates ISO/SAE 21434 and ASPICE for CS but doesn't yet fully encompass other critical regulations like UNECE WP.29 R155/R156 or regional data privacy laws.

2. Dynamic Threat Landscape: The model's reliance on historical data may struggle to proactively address novel attack vectors, zero-day vulnerabilities, and emerging AI-driven threats.

3. Scalability and Complexity: Performing granular TARA on highly complex, interconnected vehicle systems remains challenging regarding data volume and expert human interpretation.

4. Supply Chain Integration: The model's current depth in assessing cybersecurity risks from third-party components and suppliers across the automotive supply chain is limited.

## 9. CONCLUSIONS AND FUTURE WORK

Developing a secure product nowadays requires additional considerations, practices and efforts. Risk assessment and threat analysis activities play the critical and base role of those considerations. If we add the effort and cost needed to optimize those tasks for compliance, the overhead on projects and organizations becomes a heavy financial and technical debt. Standards complexity, contradictions, gaps and interactions across those standards pose as a new challenge to practitioners. Integration of standards' requirements and approaches in deployed processes is a key factor to optimize compliance cost for secure development. We studied the risk assessment and threat analysis efforts optimization from standards compliance point of view, where we presented a detailed analysis of the two standards. A detailed mapping between the ISO/SAE 21434 requirements and ASPICE for CS base practices. We have also experimented this model on ongoing projects, and we then utilized the outputs of these experiments to enhance the model maturity and derive additional model requirements to ensure both standards compliance in an empirical approach. This model is developed based on market driven categories and bilateral views where it can be utilized according to organizational and project industry demands. We also developed and proposed an automated tool based on the proposed model that takes into account the risk assessment and threat analysis modular

approaches and defined criteria in the ISO/SAE 21434 with an automated calculation and aggregation of impact, feasibility and risk assessment determination. We also added to this tool the necessary additional model requirements to ensure ASPICE for Cybersecurity compliance. Using this model and tool have optimized efforts and costs of secure development compliance from 40% to 60% in all cases providing practitioners with a simplified target-oriented method of compliance to needed standards.

Future work will be focused on integrating an open-source attack scenarios database where it can go through the automated tool without human intervention. This updated database is continuously monitoring manufacturers' cybersecurity management systems. The Meta-data of those attack scenarios will also be migrated to the tool in order to ensure the complete automated TARA process through the tool. Future work will also focus on a more in-depth analysis of the model's performance, specifically quantifying time cost and quality improvements across various TARA tasks. We'll conduct detailed comparative studies to measure efficiency gains and enhanced output quality against traditional methods. This includes evaluating the time for threat identification, risk assessment, and compliance, plus the completeness and accuracy of TARA artifacts. We also plan to explore the model's adaptability and scalability across diverse project sizes, providing concrete performance comparisons.

## REFERENCES

- [1] ISO/SAE. (2021). 21434, Road vehicles – Cybersecurity engineering. <https://www.iso.org/standard/70918.html>.
- [2] ISO. (2018). 26262-1:2018, Road vehicles – Functional safety. <https://www.iso.org/standard/68383.html>.
- [3] ISO. (2020). TR 4804:2020, Road vehicles – Safety and cybersecurity for automated driving systems – Design, verification and validation. <https://www.iso.org/standard/75156.html>.
- [4] VDA QMC. (2021). Automotive SPICE® for cybersecurity version 1.0. [https://www.automotivespice.com/fileadmin/software-downloads/Cybersecurity\\_PAM\\_v1.0.pdf](https://www.automotivespice.com/fileadmin/software-downloads/Cybersecurity_PAM_v1.0.pdf).
- [5] VDA QMC. (2017). Automotive SPICE® 3.1. [https://www.automotivespice.com/fileadmin/software-downloads/Automotive\\_SPICE\\_PAM\\_3\\_1\\_EN.pdf](https://www.automotivespice.com/fileadmin/software-downloads/Automotive_SPICE_PAM_3_1_EN.pdf).
- [6] VDA QMC. (2023). Automotive SPICE® 4.0. [https://www.automotivespice.com/fileadmin/software-downloads/Automotive\\_SPICE\\_PAM\\_4\\_0\\_EN.pdf](https://www.automotivespice.com/fileadmin/software-downloads/Automotive_SPICE_PAM_4_0_EN.pdf).
- [7] ISO/IEC. (2012). 15504-5:2012, Information technology – Process assessment. <https://www.iso.org/standard/53396.html>.
- [8] Saulaiman, M.N.E., Kozlovsky, M., Csilling, A. (2023). Leveraging attack graphs in automotive threat analysis and risk assessment. In the Seventeenth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2023), Valencia, Spain, 70-75. [https://personales.upv.es/thinkmind/dl/conferences/securware/securware\\_2023/securware\\_2023\\_1\\_140\\_30089.pdf](https://personales.upv.es/thinkmind/dl/conferences/securware/securware_2023/securware_2023_1_140_30089.pdf).
- [9] Saulaiman, M.N.E., Csilling, Á., Kozlovsky, M. (2025). Integrated automation for threat analysis and risk assessment in automotive cybersecurity through attack graphs. *Acta Polytechnica Hungarica*, 22(2): 149-168.



- <https://doi.org/10.12700/APH.22.2.2025.2.8>
- [10] Schermann, R., Ammerer, T., Stelzer, P., Macher, G., Steger, C. (2023). Risk-aware intrusion detection and prevention system for automated UAS. In 2023 IEEE 34th International Symposium on Software Reliability Engineering Workshops (ISSREW), Florence, Italy, pp. 148-153. <https://doi.org/10.1109/ISSREW60843.2023.00065>
- [11] Das, P., Panda, A. K., Biswas, S., Kumar, P., Ahmed, S. (2024). STRIDE-based cybersecurity threat modeling, risk assessment and treatment of an in-vehicle infotainment system. *Vehicles*, 6(3): 684-703. <https://doi.org/10.3390/vehicles6030054>
- [12] Kawanishi, Y., Nishihara, H., Yoshida, H., Yamamoto, H., Inoue, H. (2023). A study on threat analysis and risk assessment based on the “asset container” method and CWSS. *IEEE Access*, 11: 18148-18156. <https://doi.org/10.1109/ACCESS.2023.3246497>
- [13] Kethareswaran, V., Padmanaban, S., Ramani, S. (2023). Relevance of ISO/SAE 21434 in vehicular architecture development. *International Journal of Engineering Research & Technology (IJERT)*, 12(12): 1-5. <https://doi.org/10.1109/SMC53992.2023.10394532>
- [14] Siddiqui, F., Khan, R., Tasdemir, S.Y., Hui, H., Sonigara, B., Sezer, S., McLaughlin, K. (2023). Cybersecurity engineering: Bridging the security gaps in advanced automotive systems and ISO/SAE 21434. In 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), Florence, Italy, pp. 1-6 <https://doi.org/10.1109/VTC2023Spring57618.2023.10200490>
- [15] UNECE. (2021). UN regulation No. 155 - Cyber security and cybersecurity management system. <https://unece.org/transport/documents/2021/03/standard/s/un-regulation-no-155-cyber-security-and-cyber-security>.
- [16] UNECE. (2021). UN regulation No. 156 – Software update and software update management system. <https://unece.org/transport/documents/2021/03/standard/s/un-regulation-no-156-software-update-and-software-update>.
- [17] Messnarz, R., Norimatsu, S., Dobaj, J., Ekert, D., Macher, G., Zehetner, T., Aschbacher, L. (2021). First experiences with the automotive SPICE for cybersecurity assessment model. In *Systems, Software and Services Process Improvement: 28th European Conference, EuroSPI 2021, Krems, Austria*. [https://doi.org/10.1007/978-3-030-85521-5\\_35](https://doi.org/10.1007/978-3-030-85521-5_35)
- [18] Liedtke, T., Messnarz, R., Ekert, D., Much, A. (2023). The new cybersecurity challenges and demands for automotive organisations and projects-an insight view. In *European Conference on Software Process Improvement*. [https://doi.org/10.1007/978-3-031-42307-9\\_21](https://doi.org/10.1007/978-3-031-42307-9_21)
- [19] Anand, S.S., Vijayaraghavan, S., Abhi, S. (2023). Enhancing the Connected Vehicle Security Using the SecureAuto Tool. In 2023 International Conference on Computational Intelligence for Information, Security and Communication Applications (CIISCA), Bengaluru, India.
- [20] Upstream, A. (2022). Upstream’s 2022 global automotive cybersecurity report. <https://upstream.auto/resources/upstreams-2022-global-automotive-cybersecurity-report/>.
- [21] VicOne (2023). VicOne automotive cybersecurity report 2023. <https://vicone.com/de-reports/automotive-cybersecurity-report-2023>.
- [22] Tripwire (2023). A look at the 2023 global automotive cybersecurity report. <https://www.tripwire.com/state-of-security/global-automotive-cybersecurity-report>.

## APPENDIX

MAN.7.BP1	determine cybersecurity risk management scope.
MAN.7.BP2	define cybersecurity risk management
MAN.7.BP3	identify potential risks
MAN.7.BP4	prioritize potential risks initially for damage
MAN.7.BP5	analyze potential risks and evaluate risks
MAN.7.BP6	define risk treatment option
MAN.7.BP7	monitor risks.
MAN.7.BP8	take corrective action
SEC.1.BP1	derive cybersecurity goals and cybersecurity
SEC.1.BP2	establish bidirectional traceability
SEC.1.BP3	ensure consistency
SEC.1.BP4	communicate agreed cybersecurity
SEC.2.BP1	refine the details of the architectural design
SEC.2.BP2	allocate cybersecurity requirements
SEC.2.BP3	select cybersecurity controls
SEC.2.BP4	refine interfaces
SEC.2.BP5	analyze architectural design
SEC.2.BP6	refine the details of the detailed design.
SEC.2.BP7	develop software units.
SEC.2.BP8	establish bidirectional traceability
EC.2.BP9	ensure consistency
SEC.2.BP10	communicate agreed results of cybersecurity implementation
SEC.3.BP1	develop a risk treatment verification and integration strategy
SEC.3.BP2	develop specification for risk treatment verification
SEC.3.BP3	perform verification activities
SEC.3.BP4	establish bidirectional traceability
SEC.3.BP5	ensure consistency.
SEC.3.BP6	summarize and communicate results
[RQ-09-01]	identification of item boundary, item functions and preliminary architecture
[RQ-09-02]	description of information about the operational environment of the item
[RQ-09-03]	analysis based on the item definition that can involve e.g. asset identification, impact rating, etc.,
[RQ-09-04]	determination of risk treatment options
[RQ-09-05]	cybersecurity goals definition
[RQ-09-06]	cybersecurity claims definition
[RQ-09-07]	verification activities
[RQ-09-08]	cybersecurity controls definition
[RQ-09-09]	cybersecurity requirements definition
[RQ-09-10]	allocation of cybersecurity requirements
[RQ-09-11]	verification of rq-09-08, rq-09-09, rq-09-10
[RQ-15-01]	damage scenarios definition
[RQ-15-02]	assets with cybersecurity properties definition
[RQ-15-03]	threat scenarios definition
[RQ-15-04]	damage scenarios refinement and assessment
[RQ-15-05]	impact rating determination

[RQ-15-06]	safety related impact ratings derivation	[RQ-09-03]	analysis based on the item definition that can involve e.g. asset identification, impact rating, etc.,
[RQ-15-07]	analysis criteria for impact analysis	[RQ-09-04]	determination of risk treatment options
[RQ-15-08]	attack paths determination	[RQ-09-05]	cybersecurity goals definition
[RQ-15-09]	threat scenarios determination	[RQ-09-06]	cybersecurity claims definition
[RQ-15-10]	attack feasibility determination	[RQ-09-07]	verification activities
[RQ-15-11]	attack feasibility rating method definition	[RQ-09-08]	cybersecurity controls definition
[RQ-15-12]	attack potential based method criteria	[RQ-09-09]	cybersecurity requirements definition
[RQ-15-13]	cvss based approach criteria	[RQ-09-10]	allocation of cybersecurity requirements
[RQ-15-14]	attack vector approach criteria	[RQ-09-11]	verification of rq-09-08, rq-09-09, rq-09-10
[RQ-15-15]	risk value determination	[RQ-15-01]	damage scenarios definition
[RQ-15-16]	risk value determination guideline	[RQ-15-02]	assets with cybersecurity properties definition
[RQ-15-17]	risk treatment options determination	[RQ-15-03]	threat scenarios definition
ISO/SAE 21434 Annex F	guidelines for impact rating	[RQ-15-04]	damage scenarios refinement and assessment
ISO/SAE 21434 Annex G	guidelines for attack feasibility rating	[RQ-15-05]	impact rating determination
ISO/SAE 21434 Annex H	examples of application of tara methods – headlamp system	[RQ-15-06]	safety related impact ratings derivation
MR	model requirement	[RQ-15-07]	analysis criteria for impact analysis
MAN.7.BP1	determine cybersecurity risk management scope.	[RQ-15-08]	attack paths determination
MAN.7.BP2	define cybersecurity risk management	[RQ-15-09]	threat scenarios determination
MAN.7.BP3	identify potential risks	[RQ-15-10]	attack feasibility determination
MAN.7.BP4	prioritize potential risks initially for damage	[RQ-15-11]	attack feasibility rating method definition
MAN.7.BP5	analyze potential risks and evaluate risks	[RQ-15-12]	attack potential based method criteria
MAN.7.BP6	define risk treatment option	[RQ-15-13]	cvss based approach criteria
MAN.7.BP7	monitor risks.	[RQ-15-14]	attack vector approach criteria
MAN.7.BP8	take corrective action	[RQ-15-15]	risk value determination
MAN.7.BP8	take corrective action	[RQ-15-16]	risk value determination guideline
SEC.1.BP1	derive cybersecurity goals and cybersecurity	[RQ-15-17]	risk treatment options determination
SEC.1.BP2	establish bidirectional traceability	ISO/SAE 21434 Annex F	guidelines for impact rating
SEC.1.BP3	ensure consistency	ISO/SAE 21434 Annex G	guidelines for attack feasibility rating
SEC.1.BP4	communicate agreed cybersecurity	ISO/SAE 21434 Annex H	examples of application of tara methods – headlamp system
SEC.2.BP1	refine the details of the architectural design	MR	model requirement
SEC.2.BP2	allocate cybersecurity requirements	[RQ-15-09]	threat scenarios determination
SEC.2.BP3	select cybersecurity controls	[RQ-15-10]	attack feasibility determination
SEC.2.BP4	refine interfaces	[RQ-15-11]	attack feasibility rating method definition
SEC.2.BP5	analyze architectural design	[RQ-15-12]	attack potential based method criteria
SEC.2.BP6	refine the details of the detailed design.	[RQ-15-13]	cvss based approach criteria
SEC.2.BP7	develop software units.	[RQ-15-14]	attack vector approach criteria
SEC.2.BP8	establish bidirectional traceability	[RQ-15-15]	risk value determination
EC.2.BP9	ensure consistency	[RQ-15-16]	risk value determination guideline
SEC.2.BP10	communicate agreed results of cybersecurity implementation	[RQ-15-17]	risk treatment options determination
SEC.3.BP1	develop a risk treatment verification and integration strategy	ISO/SAE 21434 Annex F	guidelines for impact rating
SEC.3.BP2	develop specification for risk treatment verification	ISO/SAE 21434 Annex G	guidelines for attack feasibility rating
SEC.3.BP3	perform verification activities	ISO/SAE 21434 Annex H	examples of application of tara methods – headlamp system
SEC.3.BP4	establish bidirectional traceability	MR	model requirement
SEC.3.BP5	ensure consistency.		
SEC.3.BP6	summarize and communicate results		
[RQ-09-01]	identification of item boundary, item functions and preliminary architecture		
[RQ-09-02]	description of information about the operational environment of the item		