Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.083267

ARTICLE

An Orchestration Model for TARA across Vehicle Manufacturers and Suppliers in Software-Defined Vehicles

Yunkeun Song[1], Samuel Woo[2], Suji Lee[3] and Yousik Lee[3,*]

[1]Department of Computer Science, Dankook University, Yongin, Republic of Korea
[2]Department of Software Science, Dankook University, Yongin, Republic of Korea
[3]Department of Information Security, Soonchunhyang University, Asan, Republic of Korea

*Corresponding Author: Yousik Lee. Email: yousik.lee@sch.ac.kr

Received: 31 March 2026; Accepted: 11 May 2026; Published: 15 June 2026

ABSTRACT: Software-Defined Vehicles (SDVs) increase cybersecurity complexity through the combination of external connectivity, software-intensive functions, and distributed development across vehicle manufacturers and suppliers. Although United Nations (UN) Regulation No. 155 and ISO/SAE 21434 require Threat Analysis and Risk Assessment (TARA) throughout the vehicle lifecycle, conventional TARA methodologies remain largely system-focused and often provide limited procedural guidance for coordinating supplier-derived TARA results at the vehicle level. This paper proposes an orchestration model for TARA across vehicle manufacturers and suppliers that structures TARA activities into the concept phase and the product development phases. The model defines interactions between the vehicle and system perspectives throughout the TARA process. In particular, it supports vehicle-perspective re-rating of system-perspective impact ratings, integration of electrical/electronic (E/E)-architecture-based and technical attack paths, signal-level asset refinement, and asset clustering. The feasibility and industrial applicability of the proposed approach are demonstrated through its application to the Driving Control Unit (DCU): Rear in a virtual SDV model using a commercial TARA tool. In addition, an expert-based qualitative evaluation indicates that the model improves the precision, consistency, traceability, and practical applicability of TARA activities in vehicle manufacturer–supplier collaboration. The results suggest that the proposed orchestration model provides a structured and industry-applicable mechanism for lifecycle-aware and vehicle-level TARA.

KEYWORDS: Threat analysis and risk assessment (TARA); vehicle security; software-defined vehicle (SDV)

1 Introduction

The automotive industry is undergoing a broad digital transformation, driven by the widespread adoption of connectivity features, the advancement of driver assistance systems and the introduction of charging and payment infrastructures following the proliferation of electric vehicles [1,2]. These developments have accelerated the transition from hardware-centric to software-centric vehicle functions, giving rise to the Software-Defined Vehicle (SDV). The shift toward SDVs enables improved technical flexibility and convenience by allowing vehicle functions to be improved or extended through software updates without hardware modifications. However, it also significantly expands the vehicle attack surface due to increased external connectivity and increasing software complexity, thus increasing exposure to cybersecurity threats [3,4].

In practice, an increasing number of cyberattacks have demonstrated the exploitation of vehicle software vulnerabilities to remotely and illicitly control critical vehicle functions such as driving behavior, door locks,

and charging operations, prompting the introduction of regulatory frameworks such as UN Regulation No. 155 and ISO/SAE 21434 to address these growing cybersecurity concerns [3,5–7].

With the establishment of UN Regulation No. 155 and ISO/SAE 21434, TARA has been recognized as a fundamental cybersecurity activity in the automotive industry. Consequently, many vehicle manufacturers and suppliers have adopted TARA methodologies tailored to their organizational contexts, often based on prior research. However, most existing approaches remain system-focused and lack a lifecycle perspective. As a result, they often fail to provide hierarchical analysis from the vehicle perspective, such as evaluating interactions among electronic control units (ECUs) based on the vehicle's electrical/electronic (E/E) architecture and assessing cascading effects across systems. Furthermore, since suppliers may adopt different TARA methodologies, vehicle manufacturers frequently face challenges in achieving consistent and unified assessments from the vehicle perspective [8,9].

TARA should be conducted not only during the initial concept phase of the system but also continuously throughout the development phase, as the system becomes progressively detailed with the selection of hardware components, software platforms, and libraries. Through this iterative process, both vehicle manufacturers and suppliers can assess the introduction of known vulnerabilities, identify emerging attack paths, and improve the accuracy of attack feasibility evaluations. In the era of SDVs, where various hardware and software suppliers collaborate under the coordination of the vehicle manufacturer's E/E architecture, TARA should be performed collaboratively by all stakeholders and integrated consistently from the vehicle manufacturer's perspective.

To overcome the limitations of the aforementioned conventional TARA methodologies and to facilitate integration across the lifecycle and vehicle levels, we propose an orchestration model that reflects the structural characteristics of the automotive ecosystem. It performs TARA iteratively throughout the development lifecycle, offering the following contributions.

1. Compliance with UN Regulation No. 155 and ISO/SAE 21434 is achieved by orchestrating the system perspective TARA results provided by suppliers within a vehicle perspective.
2. Guaranteeing precision, consistency, traceability, and efficiency in TARA activities.
    - Precision: Lifecycle-aware TARA enables the identification of detailed information available at each development stage, which helps detect asset omissions and incorporate newly emerging cybersecurity threats.
    - Consistency and traceability: Vehicle manufacturers orchestrate the results of multiple system-perspective TARA activities based on the E/E architecture and regulatory requirements specific to each target market, thus ensuring consistency and coherence at the vehicle perspective in terms of asset identification, impact rating, attack path analysis, and risk treatment decisions.
    - Efficiency: Clustering the large number of signal-based assets identified during the development phase minimizes redundant analysis.
3. The industrial applicability of the proposed orchestration model is demonstrated through its application to a virtual vehicle using a commercial TARA tool.

This paper is structured as follows. Section 2 provides an overview of the essential background on UN Regulation No. 155, the TARA methodology, and cybersecurity engineering. Section 3 discusses the characteristics and limitations of existing approaches. Section 4 provides a detailed description of the proposed orchestration model. Section 5 presents a case study conducted on a virtual vehicle to evaluate the industrial applicability of the proposed model. Section 6 presents the organizational and technical prerequisites that may arise among stakeholders during the implementation of the proposed mechanism. Finally, Section 7 summarizes the contributions and concludes the paper.

2 Background

2.1 UN Regulation No. 155: Cybersecurity and Cybersecurity Management System

This regulation was developed by the Cybersecurity and Software Updates Taskforce (CS/OTA TF) under WP.29, the Working Party on Automated/Autonomous and Connected Vehicles of the United Nations Economic Commission for Europe (UNECE). It specifies cybersecurity requirements to protect vehicles against cyber threats. Under this regulation, vehicle manufacturers are required to establish a Cybersecurity Management System (CSMS) and obtain vehicle type approval (VTA) from an approval authority for each vehicle type. CSMS must include processes for assessing, categorizing, and treating cybersecurity risks throughout the vehicle lifecycle. The approval authority reviews whether risk assessment activities have been conducted adequately for the vehicle type by the CSMS during the VTA process.

2.2 ISO/SAE 21434: Road Vehicles—Cybersecurity Engineering

ISO/SAE 21434 is an international standard for cybersecurity engineering in road vehicles. It outlines systematic procedures to ensure cybersecurity throughout the entire vehicle lifecycle. The standard specifies detailed requirements and work products that support compliance with the abstract-level requirements of UN Regulation No. 155, making it a practical guideline for both vehicle manufacturers and suppliers. In particular, clause 15 defines the TARA method, which can be applied at any stage of the development lifecycle.

2.3 Threat Analysis and Risk Assessment (TARA)

TARA is a risk-based cybersecurity analysis method that identifies and evaluates potential threats to protected assets, quantifies associated risks, and derives appropriate mitigation strategies. Although various TARA methodologies, such as E-safety Vehicle Intrusion Protected Applications (EVITA) and HEAling Vulnerabilities to ENhance Software Security and Safety (HEAVENS), have been proposed in both academia and industry, the publication of ISO/SAE 21434 has shifted the focus toward approaches that comply with its specified TARA requirements. The standard defines a TARA method consisting of seven modules. Upon completion of the TARA, all identified cybersecurity threats and their corresponding risk values are produced, along with traceable risk treatment decisions. Table 1 presents the TARA methods as specified in ISO/SAE 21434.

Table 1: TARA methods in ISO/SAE 21434.

Modules	Description
Asset identification	Based on the system functions and interfaces defined in the item definition, assets that require protection and their associated cybersecurity properties are identified. From this, potential damage scenarios—representing all possible negative consequences resulting from asset compromise—are derived.
Threat scenarios identification	Threat scenarios, which describe how an attacker could cause the identified damage scenarios, are identified through expert group discussions or by applying systematic approaches such as EVITA and Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE).
Impact rating	The severity of a damage scenario is rated based on four categories: Safety, Financial, Operational, and Privacy.

(Continued)

Table 1 (continued)

Modules	Description
Attack path analysis	Various methods and procedures for realizing the identified threat scenarios are organized, which can be structured using either a top-down or bottom-up approach.
Attack feasibility rating	The attack feasibility of each identified attack path is evaluated using one of the following methods: the attack potential-based approach based on the Common Evaluation Methodology (CEM), the Common Vulnerability Scoring System (CVSS) based approach, or the attack vector-based approach, which is one of the base metrics defined in CVSS.
Risk value determination	The risk value for each threat scenario is calculated based on the results of the impact rating and attack feasibility rating. The risk value serves as a quantitative indicator of risk severity, expressed as a numerical score ranging from 1 to 5, where higher values indicate greater risk levels.
Risk treatment decision	For each identified threat, a risk treatment decision is made based on the calculated risk value. The decision is classified into one of four categories: avoiding the risk, reducing the risk, sharing the risk, or retaining the risk.

3 Related Work

This section reviews early TARA research on automotive cybersecurity, followed by studies that expanded on it. The characteristics and limitations of each approach are discussed. Pioneering models such as EVITA and HEAVENS established foundational risk assessment procedures that are widely adopted across the field. Later studies broadened the scope by targeting autonomous vehicles and introducing evaluation dimensions such as post-attack resilience and privacy.

3.1 Pioneering Research on TARA

Early research on vehicle TARA in the field of automotive cybersecurity was based on global initiatives, particularly EU-led projects such as EVITA [10] and HEAVENS [11], which laid the foundational methodologies for assessing cybersecurity risks in vehicles.

Henniger et al. [12] proposed a model to systematically analyze cybersecurity threats in vehicle networks (IVN) as part of the EVITA project. In this model, system assets are first identified based on representative use cases such as vehicle-to-everything (V2X), diagnostics, and eCall, and subsequently, as described in Section 2, the model executes only a subset of the TARA process to derive the final security risk value. This procedure has since been widely adopted in most subsequent studies on automotive risk assessment. In this paper, the authors aimed to align the impact rating with the international functional safety standard in the automotive industry [13]. However, the proposed model does not define weighted criteria for impact categories, assuming that safety, privacy, operational, and financial impacts are of equal importance.

Wolf and Scheibel [14] proposed a risk assessment model that assigns category-specific weights to impact categories, enabling the cost-effective implementation of security countermeasures based on a

quantitative evaluation. In this model, potential security threats and high-level security objectives are derived from misuse cases that describe scenarios in which security assets can be exploited. A potential security threat refers to a method by which an attacker can intentionally trigger a misuse case. In contrast, a high-level security objective denotes the intended security goal that mitigates such threats. According to ISO/SAE 21434, these elements are defined as threat scenarios and security goals, respectively. The model utilizes the Common Evaluation Methodology (CEM) [15] to assess the attack potential of each identified potential security threat. Simultaneously, the damage potential is assessed in terms of safety, financial, and operational categories and the final risk value is derived accordingly. Although this model is considered well suited for automotive systems where safety is the primary concern, it exhibits a significant limitation in that it does not explicitly account for privacy-related impacts, which are explicitly required by the ISO/SAE 21434 standard.

Islam et al. [16] proposed HEAVENS 1.0, a risk assessment model developed as part of the HEAVENS Project, which incorporates Microsoft's STRIDE [17] for threat modeling and considers multiple impact dimensions, including safety, financial, operational, privacy, and legislation, during impact assessment; however, since this methodology was developed before the standards and regulations discussed in Section 2, it does not align with these current standards. To address this, Lautenbach et al. [18] introduced HEAVENS 2.0 by updating 17 elements—including the removal of legislative impact parameters and the addition of damage scenario identification and attack path analysis—to ensure full compliance with UN Regulation No. 155 and ISO/SAE 21434. However, it still lacks integrated procedures that reflect stakeholder-specific characteristics (e.g., vehicle manufacturers and suppliers) and ensure consistency in the vehicle perspective during the execution of TARA.

3.2 Novel TARA Methodology via Modified Evaluation Categories

Recent follow-up studies have extended early TARA frameworks by narrowing their scope to specific application areas, such as vehicle ad hoc networks (VANETs) or autonomous driving systems, or by focusing on the evaluation of particular impact dimensions, most notably privacy-related risks.

Ren et al. [19] proposed a risk assessment approach designed to protect location privacy within a defined system model for VANET. In this study, threats related to location privacy leakage were analyzed using a top-down attack tree approach, which enabled the derivation of specific attack scenarios. Then each scenario was evaluated based on three criteria proposed by the authors: attack cost, technical difficulty, and probability of detection. This paper provides a detailed analysis of attack paths and the feasibility of attacks related to location information leakage. However, it focuses solely on attack path analysis and attack feasibility rating modules among the various components of TARA. Thus, it does not fully satisfy all TARA requirements as defined in ISO/SAE 21434.

Chah et al. [20] proposed a privacy threat modeling approach for autonomous vehicle systems by applying the Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance (LINDDUN) framework [21]. In this study, a data flow diagram (DFD) was constructed based on the network architecture of a Connected and Autonomous Vehicle (CAV), followed by the identification of privacy-related threat scenarios and the mapping of corresponding Privacy Enhancing Technologies (PETs) to mitigate those threats. However, the analysis is narrowly focused on privacy within autonomous vehicles and does not include evaluations of damage scenarios resulting from threats or the feasibility of attack realization, thereby falling short of meeting the comprehensive requirements of threat and risk assessment as defined in standards such as ISO/SAE 21434.

Park and Park [22] proposed a cyber-resilient risk assessment model tailored for autonomous vehicles by extending traditional risk assessment factors—Probability and Impact—with two additional dimensions: Exposure and Recovery. Exposure was introduced to assess how accessible the vehicle is and how well-known

its vulnerabilities are, while Recovery was added to evaluate how quickly a compromised system can return to normal operation. This includes factors such as real-time detection and response capabilities, patching ability, and response time across the supply chain. This methodology differentiates itself from other TARA approaches by incorporating post-attack resilience into risk assessment, potentially altering the prioritization of risk treatment decisions. However, it presents certain limitations: Although recovery-related factors such as patch-ability and supply chain responsiveness require close collaboration between vehicle manufacturers and suppliers, the model does not provide detailed procedures to support such coordination. In addition, it does not account for threats that can only be identified by suppliers, leaving potential gaps in the risk evaluation process.

3.3 TARA Orchestration

Kiening and Angermeier [23] analyzed which TARA elements should be shared when TARA is performed across different organizations and proposed a method for defining responsibilities in distributed engineering contexts. This approach applies the concept of the Cybersecurity Interface Agreement in ISO/SAE 21434 to TARA, allowing each organization to perform a partial TARA within its own engineering scope while sharing only the information required for cross-organizational integration. It also considers intellectual property protection by limiting the scope of information exchanged between organizations. However, this approach does not provide detailed criteria for reconciling stakeholder-dependent differences in impact ratings, integrating newly identified assets with existing assets, or incorporating implementation-level design information into attack paths as development progresses.

4 Proposed Mechanism: Orchestration Model across Vehicle Manufacturers and Suppliers

This section introduces an orchestration model developed to overcome the limitations of existing methodologies. The proposed model does not redefine the TARA activities specified in ISO/SAE 21434. Rather, ISO/SAE 21434 defines TARA activities and expected work products from a "what-to-do" perspective while leaving room for detailed "how-to-do" procedures for determining in which development lifecycle phases TARA should be performed, at which level it should be conducted, and how vehicle-level and system-level analyzes should be coordinated across those activities. Accordingly, the core contribution of this study is a lifecycle-aware TARA orchestration mechanism that structures the interaction between the vehicle perspective and the system perspective across the concept and product development phases. The model structures the vehicle development lifecycle into two layers: Layer 1 for the concept phase and Layer 2 for the product development phase. It performs an integrated analysis from both vehicle and system perspectives at each layer, going beyond simple role definitions to specify stakeholder interactions for systematic collaboration. In most practical cases, the vehicle perspective is represented by the vehicle manufacturer, which has overall responsibility for the vehicle-level E/E architecture and cross-system consistency, whereas the system perspective is represented by the supplier or the organization responsible for the corresponding system, which has detailed knowledge of system functions, interfaces, and implementation details. This approach complies with ISO/SAE 21434 and ensures consistency in impact ratings, attack feasibility, and the traceability of communication data across all vehicle systems. Furthermore, Layer 2 expands the analysis scope to include threats from hardware and software components, enabling a more precise TARA.

4.1 Overview of the Mechanism

The proposed orchestration model has been developed by considering two key perspectives: the stakeholder perspective and the system lifecycle perspective.

The first perspective considered in the proposed mechanism is that of the stakeholders, primarily vehicle manufacturers and suppliers. Vehicle manufacturers possess a comprehensive understanding of the vehicle's E/E architecture and the interactions among multiple systems, while suppliers have deep expertise in the detailed design of hardware and software components within individual systems. The proposed orchestration model considers these characteristics and facilitates close collaboration between stakeholders at each stage of the TARA process.

The second perspective focuses on the vehicle development lifecycle. Vehicle manufacturers typically perform TARA during the concept phase, where the analysis is performed based on system functions, preliminary architectures, and various assumptions. As a result, a gap arises between the concept phase assessment and the series of production vehicles or systems. To bridge this gap, suppliers should share information about cybersecurity vulnerabilities related to selected hardware and software components with vehicle manufacturers during the product development phase. This enables the identification of new assets, the clustering of assets with similar characteristics and damage scenarios, and the bottom-up derivation of attack paths.

To obtain VTA, vehicle manufacturers must ensure not only consistent evaluations across all systems from the vehicle perspective but also detailed analyses of each system. The proposed orchestration model addresses this need by considering both the distribution of expertise throughout the automotive supply chain and the structure of the vehicle development lifecycle, supporting a more comprehensive and detailed approach to regulatory readiness.

4.2 Layer 1: Concept Phase

In the concept phase, TARA is carried out in close collaboration between the vehicle's perspective and the system's perspective, based on limited design information such as system functions, a preliminary architecture, and a reference system model. From the vehicle perspective, the analysis focuses on impact rating by striving to ensure consistency and traceability from system to system, identifying attack paths based on vehicle E/E architecture, and considering regulatory and market-specific constraints. In contrast, the system perspective focuses on identifying system-specific functions, associated assets, and damage scenarios, with a particular emphasis on impact rating and analyzing technical attack paths. Fig. 1 presents the interactions between the vehicle and system perspectives for each TARA activity in layer 1.

L1-1 Asset identification: From the perspective of the system, all assets required to perform the functions of a given system are identified, and potential damages resulting from the compromise of the cybersecurity properties of each asset are evaluated. Each asset is described in detail—covering its functional role, associated components, creation timing, originator, and any stored or transmitted data—to facilitate a shared understanding among stakeholders.

From the vehicle perspective, the vehicle manufacturer receives asset identification results from all vehicle systems and compiles a list of transmitted and received assets, along with potential damage scenarios for each asset. This holistic review enables the assessment of consistency at the vehicle level and helps identify assets that are missing or no longer in use. It also enables the identification of missing assets in individual systems by comparing commonly implemented functions, such as diagnostics, between systems.

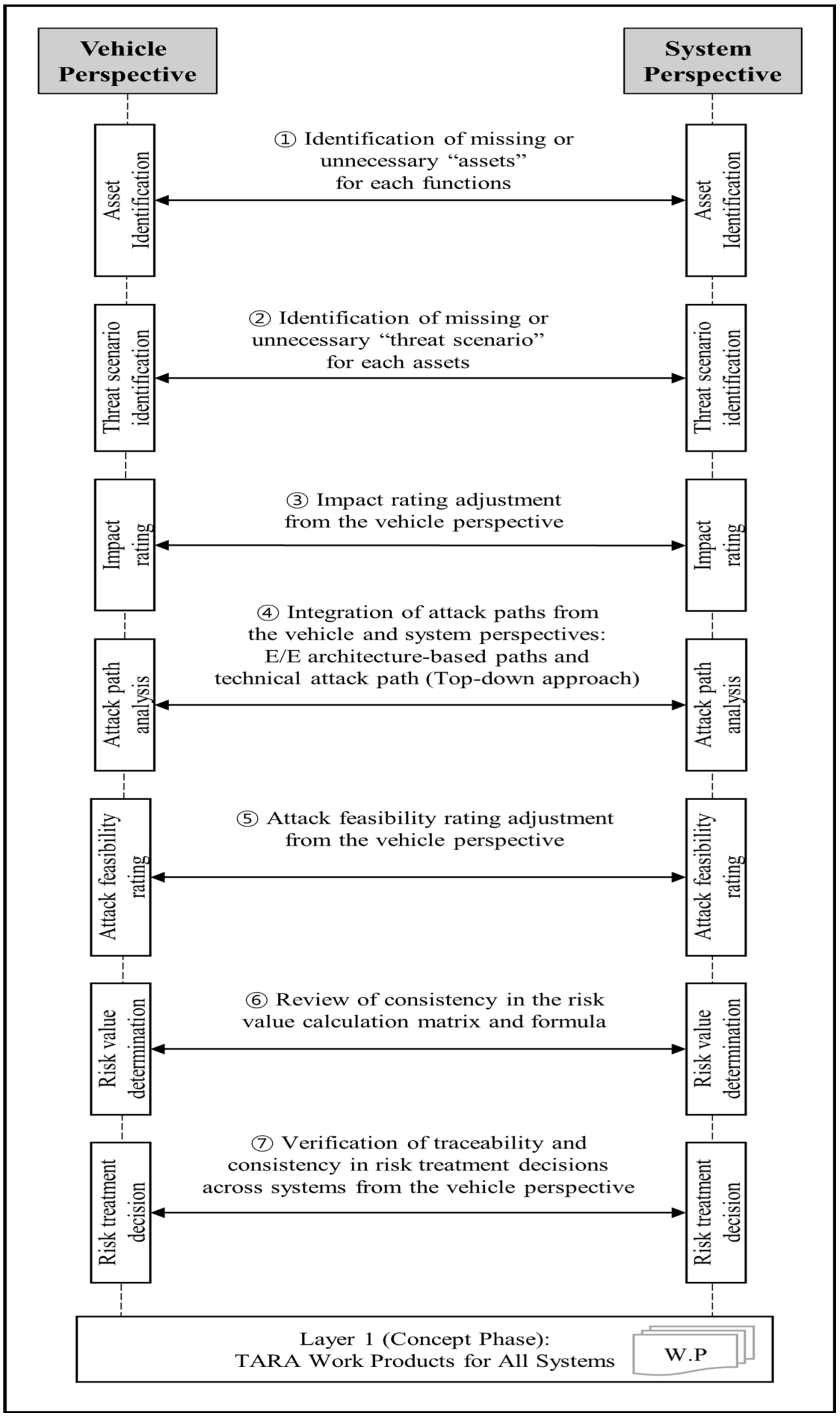

Figure 1: Layer 1—interaction between vehicle and system perspectives.

L1-2 Threat scenario identification: From the perspective of the system, threat scenarios are determined that could compromise the cybersecurity properties of the identified assets. Where applicable, each threat scenario can also include descriptions of the attack surface utilized, the potential attacker, and the tools used. Subsequently, from the vehicle perspective, threat scenarios collected from all constituent systems are

reviewed to ensure consistency across the vehicle. Detailed threat scenario information is then shared with other systems to support the development of consistent technical attack paths during attack path analysis.

L1-3 Impact rating: From the system perspective, the impact of the identified damage scenarios is rated across four categories: Safety, Financial, Operational, and Privacy. However, because suppliers conduct system-perspective impact ratings based on the functionality and assumptions of individual systems, the results may not fully reflect vehicle-level contextual factors, such as legal and regulatory requirements applicable in the target market, the vehicle E/E architecture, and the degree of functional redundancy within the vehicle. Moreover, the same system may be deployed in different vehicle types and sold in different countries or regions, which makes vehicle-perspective evaluation necessary. For this reason, the system-perspective results are re-rated from the vehicle perspective by incorporating these factors. This re-rating step enables the vehicle manufacturer to review supplier-derived impact ratings consistently, rather than merely aggregating system-level results produced under different assumptions. It helps ensure that the assessments of all in-vehicle systems are reflected as consistent impact ratings at the level of the target vehicle.

Eqs. (1) and (2) present a formulation that takes the system-perspective impact rating (denoted as IR_{IC}^{sys}) as input and applies a vehicle-perspective coefficient to re-rate it into the vehicle-perspective impact rating (denoted as IR_{IC}^{veh}).

$$IR_{\text{IC}}^{\text{veh}} = \log_b\left(IR_{\text{IC}}^{\text{sys}} + \varepsilon\right) \gamma_{\text{adj}}^{\text{veh}} \tag{1}$$

$$\gamma_{\text{adj}}^{\text{veh}} = \begin{cases} C_{\text{veh\_type}} + C_{\text{backup}}, & \text{if IC = Safety,} \\ C_{\text{veh\_type}} + C_{\text{reg}}, & \text{if IC = Financial,} \\ C_{\text{veh\_type}} + C_{\text{backup}}, & \text{if IC = Operational,} \\ C_{\text{reg}}, & \text{if IC = Privacy.} \end{cases} \tag{2}$$

In (1), IR_{IC}^{veh} represents the result of the impact rating from the vehicle's perspective for a given impact category IC ($IC \in \{\text{Safety, Financial, Operational, Privacy}\}$). IR_{IC}^{sys} represents the corresponding result of the impact rating from the system perspective. The base b in $\log_b\left(IR_{IC}^{\text{sys}} + \epsilon\right)$ determines how sensitively IR_{IC}^{sys} is reflected in the computation of IR_{IC}^{veh}; a smaller b causes changes in IR_{IC}^{sys} to have a larger influence on the resulting IR_{IC}^{veh}. The constant ϵ is a small positive value added to ensure positive arguments for the logarithmic transformation. Finally, $\gamma_{\text{adj}}^{\text{veh}}$ is the vehicle-perspective coefficient that accounts for vehicle-perspective factors such as vehicle type, target-market regulatory requirements, and functional redundancy. The logarithmic transformation is used to moderate excessive linear amplification when vehicle-level contextual factors are applied to system-perspective impact ratings. Because TARA impact ratings are ordinal in nature, the numerical result of Eq. (1) should not be interpreted as an interval-scale measurement. Instead, it is used as an intermediate value to support consistent vehicle-perspective re-rating and should be mapped back to the predefined impact rating mapping table.

In (2), $\gamma_{\text{adj}}^{\text{veh}}$ is defined such that different coefficients are applied depending on the impact category. $C_{\text{veh\_type}}$ reflects the relative risk associated with the vehicle category (e.g., passenger car, bus, truck); C_{backup} reflects the impact associated with the number of backup systems in the vehicles, including the target system itself and its backup systems; and C_{reg} reflects the impact associated with the country-specific regulatory requirements.

In the Safety category, it is determined by $C_{\text{veh\_type}}$ and C_{backup} because safety severity depends on the vehicle's size and purpose, as well as the redundant systems that can mitigate failures. In the Financial category, it is calculated using $C_{\text{veh\_type}}$ and C_{reg} as financial impacts are influenced by the vehicle's market

segment and the stringency of country-specific regulatory requirements. In the Operational category, it is determined by $C_{\text{veh\_type}}$ and C_{backup} because operational continuity depends on the vehicle's usage context and the availability of backup functions. In the Privacy category, it is determined by C_{reg} because privacy impacts can be evaluated differently depending on target-market regulatory requirements.

Table 2 summarizes the ranges and descriptions of the coefficients used to compute $\gamma_{\text{adj}}^{\text{veh}}$. To ensure consistent scaling across impact categories, each coefficient is mapped to a bounded range of $[1.0, 3.0]$. This range should be interpreted as a relative weighting scale for vehicle-level contextual factors, rather than as an absolute or statistically calibrated measurement. A value of 1.0 represents a neutral or lower contextual influence, while larger values represent stronger vehicle-level influence. For example, a passenger car may be assigned a higher coefficient than a quadricycle because it typically operates at higher speeds and in broader traffic conditions, whereas a truck or bus may receive a higher coefficient because a cybersecurity incident may affect more passengers or surrounding road users. $C_{\text{veh\_type}}$ categorizes vehicles into three types and assigns a corresponding coefficient value. C_{reg} differentiates the coefficient value based on the presence and stringency of regulatory requirements in the target market; for instance, privacy regulations vary across regions such as the EU, Asia, and South America, which can lead to distinct assessments. Finally, C_{backup} reflects functional redundancy by assigning the coefficient value as a function of the number of in-vehicle systems capable of providing the target function, including the assessed system itself and its backup systems. The specific values of the b, ϵ, and the coefficients should therefore be regarded as configurable parameters that may be calibrated according to project-specific assessment criteria, expert judgment, and organizational risk tolerance.

Table 2: Definition of the range of the $\gamma_{\text{adj}}^{\text{veh}}$ coefficient.

Coefficient	Range	Description
$C_{\text{veh\_type}}$	1.0–3.0	1.0: Quadricycle, 2.0: Passenger car, 3.0: Truck/Bus
C_{reg}	1.0–3.0	1.0: None, 2.0: Weak, 3.0: Strong
C_{backup}	1.0–3.0	$(\frac{3}{\min(n,3)})$, $n \in \mathbb{Z}$, $n \geq 1$. n means the number of backup systems in the vehicles, including the target system itself and its backup systems.

L1-4 Attack path analysis: From the system perspective, the analysis focuses solely on technical aspects. Using a top-down approach, the system examines various technical methods and procedures that an attacker might use to realize a given threat scenario. For instance, if an attacker aims to tamper with configuration data stored within the system, they might exploit available wired or wireless interfaces or physically dismantle the device to gain access. The analysis may also involve distinguishing between wireless communication protocols, such as Bluetooth and Wi-Fi, identifying known vulnerabilities for each, and specifying the corresponding exploitation techniques. The comprehensive enumeration of such methods constitutes the technical attack path from the system perspective.

From the vehicle perspective, potential attack paths that an attacker should traverse to access a target system are analyzed based on the vehicle's E/E architecture. For instance, if an attacker intends to influence the driving behavior of a vehicle remotely, the attack path would sequentially involve external communication systems, gateway system, and ultimately reach the driving-related system. This ordered sequence of systems that an attacker should pass through to perform a malicious action is referred to as the E/E architecture-based attack path.

The vehicle perspective ultimately consolidates the E/E architecture-based attack paths and the technical attack paths of each system to construct a unified attack path that represents how a specific asset can be compromised in the context of the entire vehicle.

L1-5 Attack feasibility rating: From the system perspective, the attack feasibility of each identified technical attack path is evaluated. However, since this evaluation is limited to individual systems, an integrated analysis is subsequently conducted from the vehicle perspective. The vehicle perspective collects the attack feasibility ratings for all technical attack paths from the constituent systems and integrates them with the E/E architecture-based attack paths. Based on this integration, vehicle-level attack feasibility ratings are adjusted and shared with each corresponding system. These results are then used in the subsequent step to determine the risk values of the threat scenarios from the system's perspective. For example, if an attacker seeks to remotely influence the vehicle's driving system, the identified attack path may involve sequentially compromising external interfaces, a gateway controller, and ultimately the driving system. In such a case, the final attack feasibility rating for the threat scenario is determined by a dependency-aware aggregation method that evaluates feasibility along the identified attack path, propagating the highest feasibility value among child nodes to their parent nodes. From the attacker's perspective, achieving the root node of the attack path requires traversing both the technical attack path and the E/E architecture-based attack path. In an E/E architecture-based attack path, the parent node typically represents another system, whereas in a technical attack path, it corresponds to a specific technical method or procedure. The attack feasibility rating therefore identifies the most exploitable route among the possible attack paths. The most critical aspect of this evaluation lies in the logical AND/OR relationships between the parent and child nodes. In an AND relationship, the aggregated feasibility of all child nodes defines the parent node's feasibility rating; hence, as the number of AND nodes increases, the overall difficulty of the attack also increases. In contrast, in an OR relationship, only the child node with the highest attack feasibility rating, representing the easiest route, is propagated upward as the feasible attack path. This approach inherently accounts for path interdependencies and ensures that shared components across multiple paths have consistent feasibility ratings.

L1-6 Risk value determination: From the system perspective, the risk values of all identified threat scenarios are calculated using predefined risk matrices or risk formulas. From the vehicle perspective, the consistency of the calculated risk values across all systems is reviewed to ensure that they have been derived using the correct, predefined matrices or formulas.

L1-7 Risk treatment decision: From a system perspective, risk treatment decisions are made based on predefined criteria. Each risk is treated through one of the following strategies: reducing the risk, avoiding the risk, sharing the risk, or retaining the risk. From the vehicle perspective, the outcomes of these risk treatment decisions across all systems are reviewed to ensure consistency and traceability throughout the vehicle. For example, if the mitigation decision for a threat identified in system A involves sharing responsibility with system B, vehicle-level analysis verifies whether the corresponding threat has been appropriately addressed in system B. Furthermore, when threats are treated through reduction, avoidance, or retention strategies, the vehicle perspective checks whether consistent criteria have been applied across all vehicle systems to ensure a uniform level of cybersecurity throughout the vehicle.

4.3 Layer 2: Product Development Phase

In the product development phase, the focus shifts to incorporating additional or modified elements into existing TARA results based on changes identified after the concept phase, as well as detailed information that can only be obtained during the development process. From the system perspective, emphasis is placed on refining asset identification by detailing previously identified assets down to the signal level and performing asset clustering, as well as on analyzing attack paths by identifying vulnerabilities introduced by the selected

hardware and software stacks. Similarly to Layer 1, the perspective of the vehicle involves checking the consistency and alignment of TARA results across multiple systems from the perspective of the vehicle's E/E architecture.

Fig. 2 presents the interactions between the vehicle and system perspectives for each TARA activity in Layer 2.

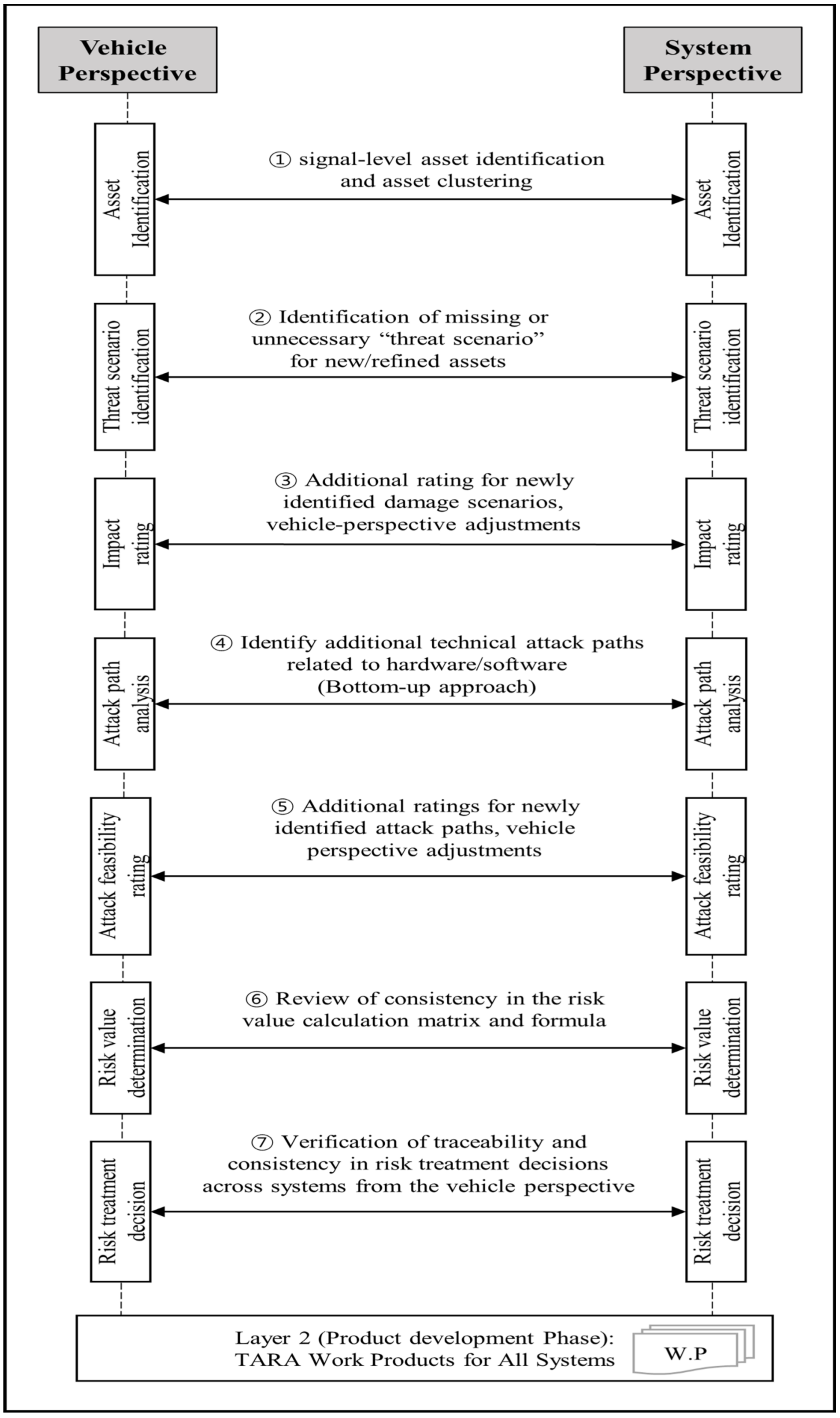

Figure 2: Layer 2—interaction between vehicle and system perspectives.

L2-1 Asset identification: In Layer 2, asset identification is performed under the assumption that the security goals, as determined through the Layer 1 TARA, have already been incorporated into the system. From the system perspective, if new security mechanisms have been implemented to meet these goals, additional assets—such as cryptographic keys or freshness counters—may be identified. Alternatively, abstract assets defined in Layer 1 may be further refined and decomposed to the signal level, significantly enhancing the precision of the TARA. As a result, dozens or even hundreds of assets may be newly identified. However, this increase in asset count can lead to substantial resource consumption in subsequent TARA activities.

To address this issue, asset clustering is performed to group assets that are expected to produce the same risk level into a single representative asset. A risk outcome is considered equivalent when the anticipated impact rating and attack feasibility rating for the assets are identical, indicating that the assets are expected to share the same damage and threat scenarios.

As such, asset clustering can be applied when all of the following conditions are satisfied:

1. Operational context: The assets exist in the same operational context. Stored data shall reside in the same type of memory (e.g., volatile or non-volatile) and be placed at an equivalent physical location on the printed circuit board (PCB). Communication data must be transmitted using the same method (e.g., wired or wireless) and protocol (e.g., CAN, Automotive Ethernet).
2. Functional equivalence: The functions associated with the assets are intended to serve the same operational purpose, such as vehicle acceleration or over-the-air (OTA) updates.
3. Identical damage scenario: When the cybersecurity properties of the assets are compromised, the resulting damage scenarios are expected to be of the same type.

Eq. (3) presents the preliminary clustering condition under which two assets are regarded as equivalent. Two assets a and b are regarded as equivalent if and only if they are deployed in the same operational context, serve the same operational purpose, and lead to the same damage-scenario type when compromised:

$$a \sim b \iff (O(a), F(a), D(a)) = (O(b), F(b), D(b)) \tag{3}$$

Once assets are clustered according to these criteria, a mapping table should be maintained to ensure traceability between individual assets and their corresponding representative asset throughout the TARA process. The table should include fields such as asset ID, representative asset ID, asset type, memory or protocol attributes, functional role, and rationale for clustering, thereby enabling consistent traceability and transparency in asset management.

L2-2 Threat scenario identification: Similar to Layer 1, the system perspective in Layer 2 focuses on identifying threat scenarios associated with newly identified or refined assets. Subsequently, from the vehicle perspective, threat scenarios from all constituent systems are collected and examined for consistency across the vehicle architecture. The results of this consistency check are then communicated to each system to ensure alignment and coherence within the overall TARA process.

L2-3 Impact rating: The detailed activities and procedures from both the system and vehicle perspectives in Layer 2 are identical to those in Layer 1. The only distinction lies in the additional evaluation of newly identified damage scenarios, for which new impact ratings are assigned accordingly.

L2-4 Attack path analysis: From the perspective of the vehicle, the activities of Layer 2 remain consistent with those of Layer 1. However, the system perspective introduces a bottom-up approach to derive additional technical attack paths. During the product development phase, the specific hardware and software stacks required to implement the functionalities of the system are determined through detailed design processes.

In this context, the bottom-up approach extends the attack paths identified in Layer 1 by incorporating new technical attack paths resulting from the selection of microcontroller units (MCUs), application processor (AP) chipsets, printed circuit board (PCB) structures, and software stacks. To support this analysis, various information sources can be leveraged, including system-level penetration testing results, known vulnerabilities from the Common Vulnerabilities and Exposures (CVE) and National Vulnerability Database (NVD) databases, as well as academic papers and conference materials.

To enhance the efficiency of repeated attack path analyses, common elements can be categorized based on chipsets, software components, or communication protocols and managed as a structured database. This database can also be reused in the post-production stages to support incident response and vulnerability management.

L2-5 Attack feasibility rating: The activities and procedures conducted from both the vehicle and system perspectives in this phase are identical to those in Layer 1. However, the only distinction is that, if new technical attack paths are identified from the system perspective using a bottom-up approach, additional evaluations are performed for those paths. Furthermore, the feasibility ratings of the corresponding higher-level nodes should also be updated accordingly. It enables the determination of whether the path represents the most exploitable attack path.

L2-6 Risk value determination: Based on newly identified assets in Layer 2, new threat scenarios can be derived and new risk values may also be calculated due to vulnerabilities arising from selected hardware and software.

L2-7 Risk treatment decision: A new risk treatment decision is made based on this series of processes. The method for selecting treatment options is the same as in Layer 1. When a new security goal is identified as a result of risk mitigation in Layer 2, a comprehensive review of all Layer 2 is required to verify whether additional assets or threats must be considered.

5 Demonstration of the Applicability and Feasibility of the Orchestration Model

In this section, the applicability of the proposed model is demonstrated through a case study based on a virtual vehicle model. The analysis was performed using CycurRISK, an industry-recognized commercial TARA tool [24], to demonstrate the applicability of the orchestration model; however, it should be noted that the proposed model does not depend on any specific tool. The selected target for TARA is the `driving control unit (DCU): Rear`. The case study illustrates how the interactions between the vehicle and system perspectives are implemented in both the concept phase and the product development phase. Through this analysis, it is confirmed that the proposed orchestration model satisfies both the practical applicability and operational effectiveness required in real-world automotive industry settings.

5.1 Vehicle Concept & E/E Architecture

The virtual vehicle used in this analysis is a high performance electric vehicle (EV) equipped with Level 3 autonomous driving capabilities. It is designed as an SDV, enabling dynamic updates and modifications of vehicle functions via OTA updates. The E/E architecture of the vehicle is based on a two-layer control structure that integrates both zonal and function-based architectures. The Base Layer is responsible for defining the overall control strategy and monitoring vehicle operations. It includes the Vehicle Computer (VC), which manages functional safety and cybersecurity across the vehicle, and multiple Zonal Controllers (ZCs), each assigned to a specific physical zone of the vehicle. Based on the base layer, the adaptive layer supports vehicle-specific features such as autonomous driving and external communications. The target system for analysis, the Driving Control Unit (DCU): Rear, is located under the ZC: Rear in the vehicle's E/E

architecture. It controls the rear section of the vehicle by acceleration, deceleration, and steering. In addition, it supports driver-personalized functions such as rear wheel steering angle adjustment, suspension height and stiffness control, and software update capabilities.

Fig. 3 presents the E/E architecture of the target vehicle along with the functional overview of the system selected for analysis.

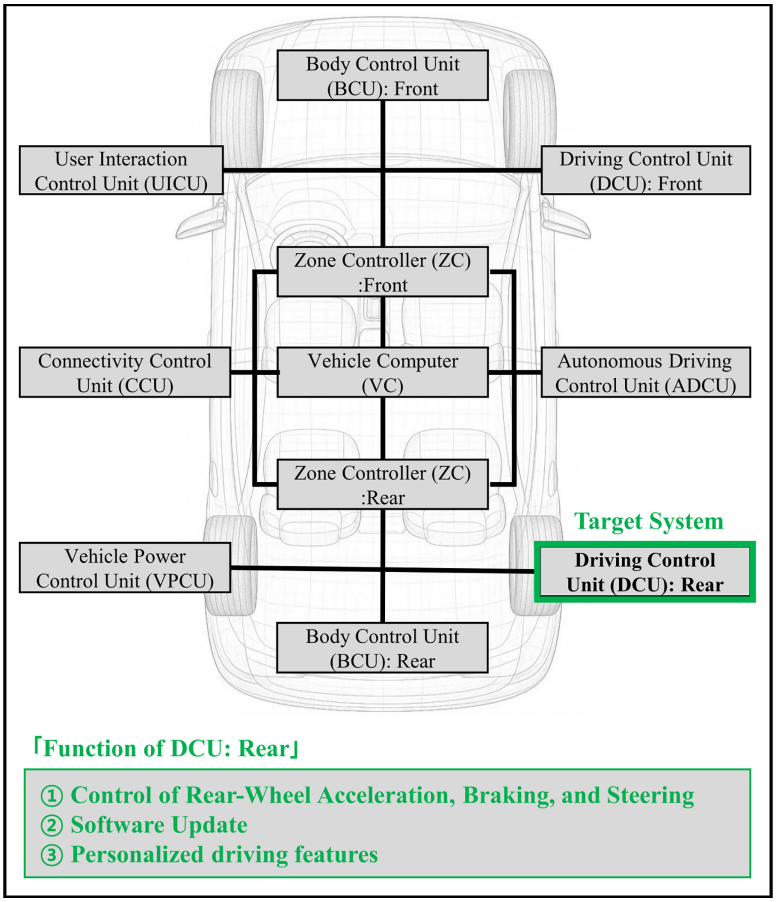

Figure 3: Target vehicle's E/E architecture and the selected system for analysis.

5.2 Interaction between Vehicle and System Perspectives

Through a progressively detailed analysis across development phases, we structurally identified the differences between the system and vehicle perspectives and examined how these differences are harmonized and integrated from the vehicle perspectives.

5.2.1 Asset Identification (L1-1, L2-1) & Impact Rating (L1-3)

In Layer 1 asset identification (L1-1), asset identification is performed to determine the elements that should be protected to ensure the intended functionality of the system. The message `Ast-1. [COMMUNICATION_DATA] vehicle_status`, received from ZC: Rear, is considered an asset because it contains the information necessary for the status of the vehicle for DCU: Rear to perform rear wheel control. Fig. 4 presents the asset `Ast-2` identified for the software update functionality and the asset `Ast-3` identified for the personalized driving features.

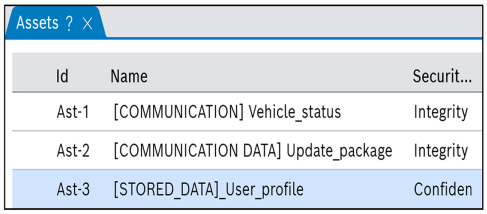

Figure 4: Asset identification (L1-1)—identified assets and their cybersecurity properties.

In Layer 1 impact rating (L1-3), once the function-specific assets have been identified, threat scenarios resulting from the compromise of their cybersecurity properties are derived, followed by an impact rating. In this context, the compromise of cybersecurity properties typically refers to violations of confidentiality, integrity, or availability.

In this impact rating, ε for the vehicle-perspective impact rating was set to 0.1, and the logarithmic base was set to 1.5. Based on these settings, the mapping criteria for the impact rating results are given in Table 3. Each range is defined as one quarter of the value interval that the vehicle-perspective impact rating result can take.

Table 3: Vehicle-level impact rating mapping table.

Range	Impact Level
<4.43	Negligible
4.44~6.69	Moderate
6.70~7.52	Major
≥7.53	Severe

Fig. 5 presents the interaction between the vehicle and system perspectives during the impact rating process. If the integrity of the `Ast-1` asset is compromised, unintended acceleration can occur while driving, which is evaluated as having a severe impact on safety from the system perspective. However, if control mechanisms in other systems can mitigate unintended vehicle behavior, the impact rating may be reduced from the vehicle perspective. In this case, even if DCU: Rear malfunctions, the VC can detect abnormal acceleration patterns that deviate from normal driving behavior and regulate the vehicle within a safe operating range. Therefore, the impact level is re-rated to the major level from the vehicle perspective. Similarly, in the cases of `DS-2: The intended software update has not been performed` and `DS-3: Leakage of personal information stored in the vehicle`, impact levels were re-rated from the vehicle perspective. These scenarios were initially rated as “Negligible” and “Moderate”, respectively, but were re-rated as “Major” and “Moderate” from the vehicle perspective.

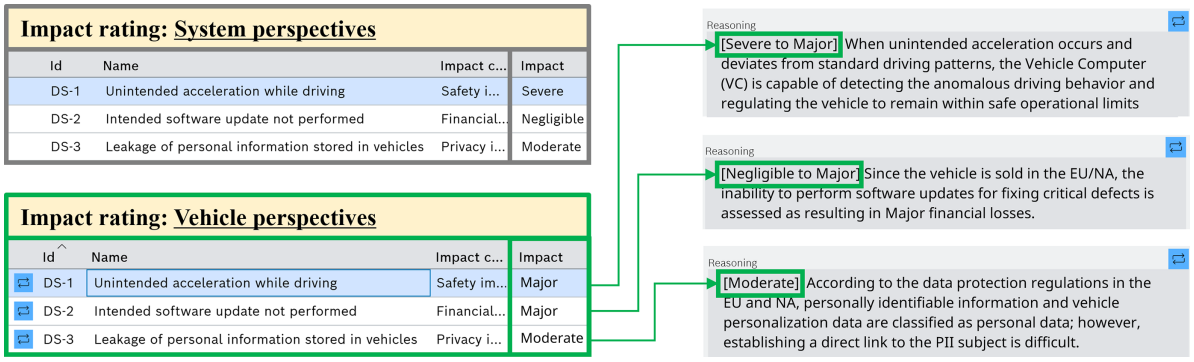

Figure 5: Impact rating (L1-3)—adjusted based on the vehicle perspective.

In Layer 2 asset identification (L2-1), the asset `Ast-1. [COMMUNICATION_DATA] vehicle_status` was further refined based on the finalized development specifications. `Ast-4. [CAN_SIGNAL] Driver_acc_req` represents the driver's acceleration request signal, `Ast-5. [CAN_SIGNAL] ADS_acc_req` corresponds to the acceleration request signal from the autonomous driving system, and `Ast-6. [CAN_SIGNAL] Gear_status` indicates the gear position signal that determines the driving direction of the vehicle, such as forward or reverse. Among them, `Ast-4` and `Ast-5` are communication signals transmitted by the same protocol and can lead to identical damage scenarios. Therefore, they are clustered into a single asset named `Ast-12. [CAN_SIGNAL] acceleration request` To ensure traceability at the signal level, the new asset Ast-12 is added, while the original assets are retained in the TARA records for documentation and reference purposes. This is a simplified example, and in real-world cases, dozens of signal assets may be clustered into a single asset. Fig. 6 presents the signal-level asset refinement and clustering performed during asset identification in Layer 2.

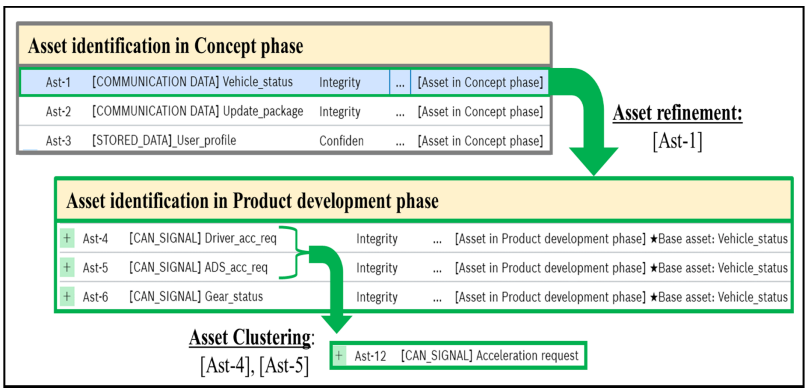

Figure 6: Asset identification (L2-1)—refinement and clustering of signal-level assets.

5.2.2 Threat Scenario Identification (L1-2) & Attack Path Analysis (L1-4) & Attack Feasibility Rating (L1-5)

In Layer 1 threat scenario identification (L1-2), threat scenarios are identified that may compromise the cybersecurity properties of each asset. Furthermore, in Layer 1 attack path analysis (L1-4), the methods and procedures that an attacker may use to achieve these scenarios are analyzed. From the vehicle perspective, these scenarios are mapped onto the E/E architecture to determine which systems should be traversed, while from the system perspective, the corresponding technical attack methods and procedures are specified in detail based on the derived attack paths.

From the vehicle perspective, the asset `Ast-12. [CAN_SIGNAL] acceleration_request` represents communication data received by DCU: Rear. This asset can be spoofed or tampered with by compromising components such as the Connectivity Control Unit (CCU), VC, or Autonomous Driving Control Unit (ADCU). For instance, an attacker may spoof a malicious message via the CCU, which serves as a primary attack surface, and induce ZC: Rear to forward the message unfiltered to DCU: Rear, thereby causing unintended acceleration.

Fig. 7 presents the attack paths based on the E/E architecture identified from the perspective of the vehicle. The threat scenario `Th-13` can be realized through one of five possible attack paths. From the system perspective, each system derives its corresponding technical attack path by analyzing the sub-nodes within each attack path. For example, in `Nd 2-1 of attack path 2`, the attacker attempts to compromise the CCU of the target vehicle by gathering configuration details such as the access point name (APN), embedded or physical SIM card information, the mobile network operator (MNO), and the operating frequency band. The attacker may then capture and analyze communication traffic between the CCU and external servers to identify weaknesses in authentication mechanisms, data formats, or message structures. Using this information, the attacker sets up a fake base station to deceive the vehicle into connecting to it, enabling spoofing of the `acceleration_request` message transmitted to ZC: Rear.

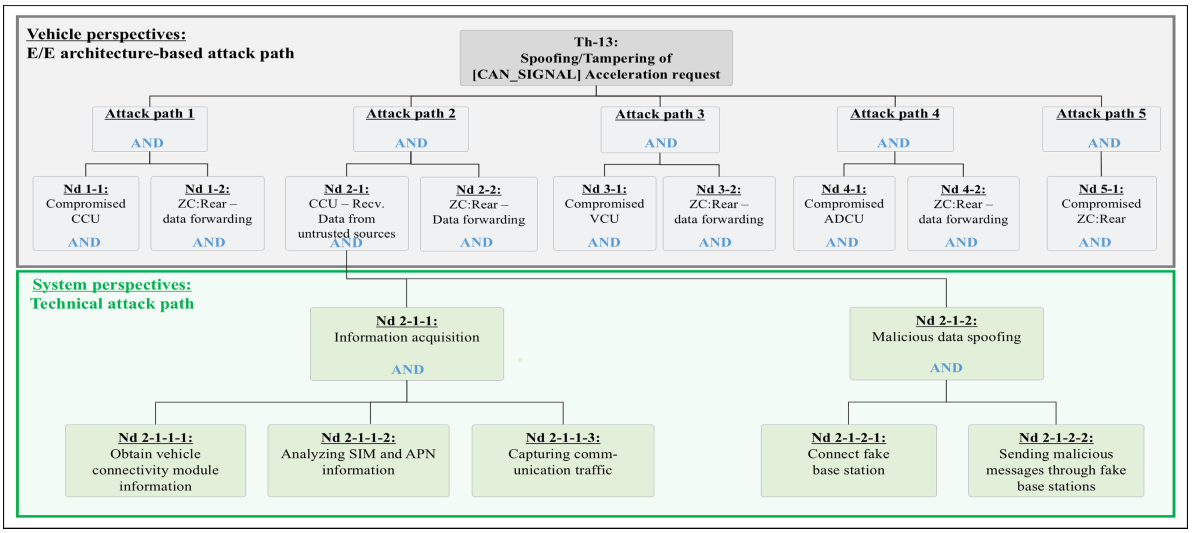

Figure 7: Integration of E/E architecture-based and technical attack paths.

Thus, the complete attack path required to realize a threat scenario is composed of both the vehicle-level E/E architecture-based attack path and the system-specific technical attack path. By consolidating the technical analyzes provided by the system supplier, the vehicle manufacturer can perform cross-system comparisons among similar attack paths. This approach enables the development of more precise and realistic threat scenarios that reflect the complexity of modern software-defined vehicles.

In the product development phase, new vulnerabilities that were not identified during the concept phase can emerge in attack paths, depending on the specific hardware or software selected during development. For example, certain cellular communication chipsets used in vehicles have been reported to contain vulnerabilities such as “buffer copy without checking size [25]”, which may allow remote code execution, and “reachable assertion while processing message [26]” or “improper authorization while error handling [27]”, which may compromise communication availability. These vulnerabilities have been publicly disclosed through Common Vulnerabilities and Exposures (CVE).

Based on this information, Nd 2-1-1 of Fig. 7 can include a new node that represents the identification of known vulnerabilities in the cellular chipset as part of the attack procedure. Similarly, in Nd 2-1-2, an additional attack node can be introduced to demonstrate how these vulnerabilities can be practically exploited. This reflects that newly discovered weaknesses can be integrated into the attack path.

This example highlights that TARA is not a static, one-time output, but a dynamic and iterative cybersecurity activity that should continuously incorporate threat elements emerging from development and implementation decisions. In doing so, the precision and realism of attack path analysis are significantly enhanced.

5.2.3 Risk Value Determination (L1-6 & L2-6) & Risk Treatment Decision (L1-7 & L2-7)

In the concept phase, the integrity compromise of Ast-1. [COMMUNICATION_DATA] vehicle_status was assessed to have a moderate impact, and the attack feasibility for the corresponding threat scenario was rated as medium. As a result, the calculated risk value was 2, and the selected risk treatment strategy was risk transfer to the CCU and ZC: Rear controllers. Consequently, from the vehicle's perspective, the threat identified through the attack path analysis is mitigated at both ZC: Rear and CCU. When the risk is not mitigated within the assessed system itself but is instead transferred to other systems, vehicle-perspective analysis is required to trace and verify whether the countermeasures for the corresponding threat scenario are effectively implemented in those other systems and whether the risk is actually mitigated at the vehicle level. It helps ensure traceability and consistency of risk treatment across systems and layers, thereby maintaining overall vehicle-level consistency.

In the product development phase, the focus is on evaluating changes in attack feasibility caused by newly added attack paths. In the presented example, the additional nodes—one that identifies known vulnerabilities in the cellular chipset and another that exploits these vulnerabilities—do not significantly affect the overall feasibility of the threat scenario. As a result, the risk value remains unchanged.

However, during a future iteration of TARA, a previously identified attack path that was initially deemed difficult to realize may require re-evaluation if newly discovered vulnerabilities significantly increase its feasibility. It highlights that TARA is not a static, one-time output, but a dynamic and iterative cybersecurity activity that should continuously incorporate threat elements emerging from development and implementation decisions. In doing so, the precision and realism of attack path analysis are significantly enhanced.

5.3 Comparative Analysis

Prior TARA studies have typically demonstrated the applicability of their proposed methodologies by focusing on a specific system or function and presenting results within that limited context. This evaluation approach reflects the inherent limitation of methodology proposals, where case-based demonstrations are often used. In this study, we conducted a comparative analysis between the proposed model and previous TARA studies. The analysis was organized around four key criteria: (1) Coverage of ISO/SAE 21434 TARA Activities, (2) lifecycle-specific TARA procedures, (3) system-vehicle orchestration, and (4) applicability and scalability. The results of the analysis are presented in Table 4.

Table 4: Comparative analysis of TARA approaches.

Prior TARA Studies	Coverage of ISO/SAE 21434 TARA Activities	Lifecycle-Specific TARA Procedures	System–Vehicle Orchestration	Demonstration Method: Case Study	Applicability & Scalability
Henniger et al. [12]	Partial (6/7)	Not supported	Not supported	V2X communication, use of nomadic devices	Scalable to other systems, but not vehicle level
Wolf and Scheibel [14]	Partial (5/7)	Not supported	Not supported	None	Scalable to other systems, but not vehicle level
Islam et al. [16]	Partial (4/7)	Not supported	Not supported	On-board diagnostics (OBD) & road speed limit (RSL)	Scalable to other systems, but not vehicle level
Lautenbach et al. [18]	Full (7/7)	Not supported	Not supported	Road speed limit (RSL)	Scalable to other systems, but not vehicle level
Ren et al. [19]	Partial (1/7)	Not supported	Not supported	Road Side Unit (RSU)	Designed solely for VANETs, not scalable to other systems or vehicle levels
Chah et al. [20]	Partial (1/7)	Not supported	Not supported	Autonomous driving data sharing, infotainment services, and OTA updates	Scalability is limited to systems handling privacy-related information
Park and Park [22]	Partial (2/7)	Not supported	Not supported	OTA updates, vehicle collision-avoidance	Scalability is limited to systems handling privacy-related information
Proposed Model	Full (7/7)	Supported	Supported	DCU: Rear of SDV vehicle model	Scalable to other systems and vehicle levels

Coverage of ISO/SAE 21434 TARA activities refers to the extent to which each study explicitly addresses the seven TARA activities defined in ISO/SAE 21434. Several prior studies were developed before the publication of ISO/SAE 21434, while others were intentionally designed to address selected aspects of TARA, such as privacy protection, resilience-oriented evaluation, or specific attack analysis procedures. Therefore, studies with narrower coverage should be interpreted as focused contributions within their intended scope. In this comparison, Lautenbach et al. [18] and the proposed model cover all seven TARA activities, whereas the other studies explicitly address selected parts of the TARA process according to their research objectives.

In the automotive industry, lifecycle-based TARA procedures are often regarded as self-evident. However, most existing methodologies are limited to the concept phase or do not clearly articulate how TARA should differ between lifecycle stages. The proposed model overcomes these limitations by covering both the concept and product development phases, thereby incorporating new emerging threats and detailed design

assets. In particular, during the development phase, the proposed model captures a large number of signal-level assets and consolidates them through asset clustering, which significantly enhances the precision of asset identification.

Orchestration between system- and vehicle-level analyses is indispensable to ensure consistency and coherence between distributed TARA activities, particularly to meet regulatory compliance requirements. From the perspective of vehicle manufacturers, consistency must be guaranteed in all in-vehicle systems. However, except for the proposed model, most existing approaches remain predominantly system-centric or fail to address how system-level results should be integrated at the vehicle level. the proposed model closed this gap by introducing an interaction mechanism that incorporated analysis information verified by relevant stakeholders at each stage of TARA, thus achieving seamless integration between system- and vehicle-level analyses.

From the perspective of applicability and scalability, most prior TARA methodologies could only be extended or applied to specific domains or system-level analyses. The approaches proposed by Ren et al. [19], Chah et al. [20] and Park and Park [22] demonstrated certain advances within limited contexts such as VANETs, privacy-related systems, or automated attack path generation, yet their applicability remained confined to specific environments without extending to other systems or lifecycle phases. In contrast, the proposed orchestration model demonstrates scalability not only across different systems but also at the vehicle level, confirming that it can be effectively extended to the vehicle level.

5.4 Expert-Based Qualitative Evaluation

TARA activities inherently rely on expert-driven qualitative assessment, particularly in impact rating, attack feasibility rating, and risk treatment decision-making, where analysts should interpret damage scenarios, attack conditions, and acceptable risk levels based on domain knowledge and organizational policies. Therefore, an expert evaluation was conducted to assess whether the proposed orchestration model provides practical support for TARA activities from the perspective of automotive cybersecurity practitioners and researchers. This evaluation was not intended to provide comprehensive validation using industrial project data. Instead, it evaluated whether the proposed model provides structural support for more precise, consistent, traceable, and efficient TARA activities. The experts reviewed the proposed workflow, with particular attention to how vehicle-level and system-level TARA results are coordinated across the concept and product development phases.

The expert panel consisted of 12 participants from suppliers, TARA consulting companies, and research institutes, all of whom had experience in conducting or evaluating TARA activities. To reflect different perspectives in the automotive cybersecurity ecosystem, the panel included seven supplier experts, three TARA consulting experts, and two research institute experts. Each expert was provided with a summary of the proposed orchestration model, the virtual SDV case, and the evaluation questionnaire, and was asked to assess the model from the perspectives of precision, consistency, traceability, efficiency, and practical applicability.

The evaluation was conducted using an 11-item questionnaire based on a five-point Likert scale, where 1 indicated “strongly disagree” and 5 indicated “strongly agree.” The questionnaire was organized into five evaluation categories: precision, consistency, traceability, efficiency, and practical applicability. These categories were selected to reflect the main claims of the proposed model and to assess whether the model can support more systematic TARA activities in a vehicle manufacturer–supplier collaboration context. The detailed questionnaire items are summarized in Table 5. Precision was evaluated in terms of omitted asset identification, development-stage information, and attack path refinement. Consistency focused on the alignment of supplier-derived system-level TARA results with the vehicle-level assessment and the use of

consistent criteria across in-vehicle systems. Traceability examined whether assets and TARA artifacts could be linked from the concept phase to the product development phase. Efficiency was assessed in terms of the potential reduction of duplicated analysis through asset clustering, while practical applicability considered the feasibility of applying the model to vehicle manufacturer–supplier collaboration and VTA-oriented evidence preparation.

Table 5: Questionnaire items for expert-based qualitative evaluation.

Category	Questionnaire Item
Precision	Q1. The proposed model helps identify assets that may be overlooked in a system-focused TARA workflow.
Precision	Q2. The proposed model helps reflect development-stage information, such as hardware, software, interfaces, and communication data, in TARA activities.
Precision	Q3. The integration of E/E-architecture-based and technical attack paths helps identify more detailed attack paths.
Consistency	Q4. The proposed model helps align supplier-derived system-level TARA results with the vehicle-level assessment.
Consistency	Q5. The vehicle-perspective impact re-rating step helps reduce differences caused by supplier-specific assumptions.
Consistency	Q6. The proposed model helps apply consistent criteria across multiple in-vehicle systems.
Traceability	Q7. The proposed model helps trace assets from abstract assets identified in the concept phase to detailed signal-level assets defined in the product development phase.
Traceability	Q8. The proposed model helps trace how supplier-derived TARA results are reflected in the vehicle-level assessment.
Efficiency	Q9. Asset clustering can reduce duplicated analysis of similar or repeated signal-based assets.
Practical applicability	Q10. The proposed model is applicable to practical TARA collaboration between vehicle manufacturers and suppliers.
Practical applicability	Q11. The proposed model can support preparation of TARA evidence for Vehicle Type Approval under UN Regulation No. 155.

Fig. 8 presents the expert-based qualitative evaluation results. The results by expert group show that the proposed orchestration model was evaluated positively across all groups, although the emphasis varied depending on the experts' organizational backgrounds. Supplier experts provided the most conservative ratings, with an overall mean score of 3.87. Their lowest score was observed for efficiency, with a mean score of 3.43. However, this value remains above the neutral point of the five-point Likert scale, suggesting that the proposed model was still perceived as more effective than applying no structured orchestration approach. The relatively lower efficiency score may reflect the initial burden of adopting a new methodology, including learning the procedure, preparing structured TARA artifacts, and coordinating information across

organizations. In contrast, TARA consulting experts gave the highest overall rating, with a mean score of 4.69. They rated consistency, traceability, and practical applicability particularly highly, with mean scores of 4.78, 4.83, and 4.83, respectively. This suggests that experts who frequently support cross-organizational TARA activities may recognize the value of harmonizing supplier-derived TARA results at the vehicle level. Research institute experts also evaluated the model positively, with an overall mean score of 4.40, and gave especially high ratings for precision and traceability, with mean scores of 4.67 and 4.75, respectively. This indicates that the lifecycle-aware linkage between concept-phase artifacts and product-development-phase details was considered methodologically useful. Overall, the results suggest that the proposed model was perceived as more useful than a conventional system-focused TARA approach across all evaluation categories, particularly in traceability and vehicle-level consistency.

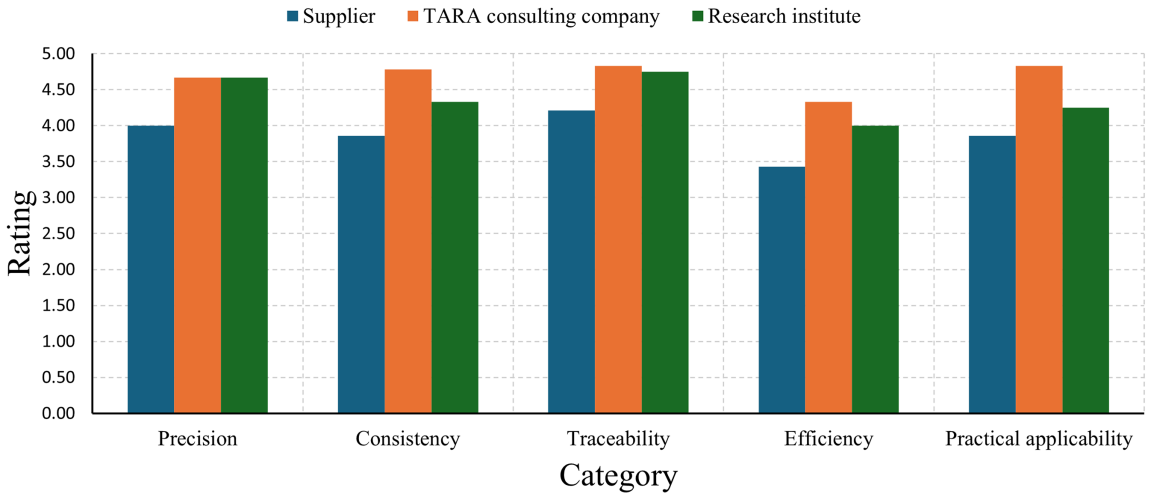

Figure 8: Expert-based qualitative evaluation results.

6 Organizational and Technical Prerequisites for Successful Implementation of the Proposed Orchestration Model

To successfully implement the proposed orchestration model in the automotive industry, the following two practical prerequisites must be addressed. By establishing these two prerequisites, organizations can implement the proposed orchestration model more efficiently while enhancing regulatory readiness.

First, to enable seamless coordination between vehicle manufacturers and suppliers, it is essential to establish a cybersecurity interface agreement (CIA) as required by ISO/SAE 21434. The CIA shall specify the roles, interactions, and data-exchange formats for each detailed TARA activity defined in the proposed model across both the concept phase and the product development phase. Stakeholder consensus on these elements is essential to effectively apply the interaction mechanisms tailored to the lifecycle and the detailed TARA activities.

Second, manufacturers and suppliers often use different tools or data structures, making it difficult to consolidate the TARA results. To address this, a mutually agreed upon data exchange format should be established between stakeholders, and open and standardized formats such as OpenXSAM may be considered. OpenXSAM facilitates consistent, tool-agnostic data sharing and improves traceability and comparability.

7 Conclusion

TARA is a key cybersecurity activity that provides a systematic approach to identifying assets and threats, enabling the implementation of effective countermeasures. In this paper, we propose an orchestration model across vehicle manufacturers and suppliers aligned with ISO/SAE 21434 and tailored to the automotive ecosystem for more detailed and practical execution. The proposed orchestration model was applied in both the concept phase and the product development phase of the vehicle development lifecycle. In each phase, the roles of vehicle manufacturers and suppliers were clearly defined for every detailed TARA activity.

Conventional TARA methods often focus on specific systems or environments, resulting in limited coverage of the full set of ISO/SAE 21434 TARA activities and insufficient consideration of the vehicle manufacturer's perspective required for VTA. For example, identical systems may be evaluated differently across countries due to regulatory differences, and E/E architecture configurations can affect attack path identification. To address these issues, the proposed orchestration model assigns stakeholder responsibilities, fosters integration across TARA activities, and supports iterative execution as designs evolve. Its applicability was demonstrated using the DCU: Rear system in a virtual SDV model.

Future work will focus on validating the security goals identified during the TARA process and advancing automated testing techniques capable of uncovering previously unidentified vulnerabilities and overlooked attack paths. In addition, we plan to integrate standardized and automated vulnerability management flows, using the Software Bill of Materials (SBOM) and Vulnerability Exploitability eXchange (VEX), into the proposed orchestration model to enhance the timeliness and scalability of vulnerability integration throughout the vehicle development lifecycle. Once ISO/SAE PAS 8475 [28] on Cybersecurity Assurance Levels (CAL) and Targeted Attack Feasibility (TAF) is officially published, we will examine how the proposed orchestration model can be extended in line with its guidance, particularly with respect to coordinating TARA outcomes, risk treatment decisions, and the expected strength of cybersecurity controls between vehicle manufacturers and suppliers. We will also consider extending the model to post-development lifecycle phases, including production, operation and maintenance, and decommissioning, by linking TARA outcomes with vulnerability monitoring and field feedback. These initiatives aim to improve the robustness and credibility of TARA outcomes across the vehicle lifecycle. Ultimately, the goal is to establish an open TARA database, rooted in the findings of this research, to foster a collaborative ecosystem accessible to academic and industrial stakeholders.

Acknowledgement: The authors thank K. Choi of ETAS Korea for his technical support with CycurRISK.

Funding Statement: This work was supported by the Technology development Program (RS-2024-00402427) funded the Korea Planning & Evaluation of Industrial Technology (KEIT, Korea).

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Yunkeun Song; methodology, Yunkeun Song and Yousik Lee; validation, Yunkeun Song; investigation, Yunkeun Song; writing—original draft preparation, Yunkeun Song; writing—review and editing, Samuel Woo, Suji Lee and Yousik Lee; visualization, Yunkeun Song; supervision, Yousik Lee; funding acquisition, Yousik Lee. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. PwC Strategy&. Digital auto report 2023 (volume 2): assessing global mobility market dynamics [Internet]. 2023 [cited 2026 Mar 28]. Available from: https://www.strategyand.pwc.com/tr/digital-auto-report-2023-volume-2.
2. Deloitte. Software-defined vehicles: engineering the mobility revolution [Internet]. 2023 [cited 2026 Mar 28]. Available from: https://www.deloitte.com/content/dam/assets-zone3/us/en/docs/industries/consumer/2023/us-deloitte-automotive-software-defined-vehicles-september-2023.pdf.
3. VicOne. The state of SDV cybersecurity: navigating innovation and risk [Internet]. 2025 [cited 2026 Mar 28]. Available from: https://cdn.vicone.com/archives/vicone/reports/the-state-of-sdv-cybersecurity.pdf.
4. McKinsey & Company. Automotive software and electronics 2030: mapping the sector's future landscape [Internet]. 2019 [cited 2026 Mar 28]. Available from: https://www.mckinsey.org/.
5. Upstream Security. Global automotive cybersecurity report 2025 [Internet]. 2025 [cited 2026 Mar 28]. Available from: https://upstream.auto/reports/global-automotive-cybersecurity-report-2025/.
6. United Nations Economic Commission for Europe. UN regulation No. 155: cyber security and cyber security management system [Internet]. 2021 [cited 2026 Mar 28]. Available from: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security.
7. International Organization for Standardization, SAE International. ISO/SAE 21434:2021. Road vehicles—cybersecurity engineering [Internet]. International Standard. Geneva, Switzerland: International Organization for Standardization; 2021 [cited 2026 Mar 28]. Available from: https://www.iso.org/standard/70918.html.
8. Tuma K, Widman M. Seven pain points of threat analysis and risk assessment in the automotive domain. IEEE Secur Privacy. 2021;19(5):78–82. doi:10.1109/MSEC.2021.3093137.
9. Greiner S, Massierer M, Loderhose C, Lutz B, Stumpf F, Wiemer F. A supplier's perspective on threat analysis and risk assessment according to ISO/SAE 21434. In: 20th Escar Europe: The World's Leading Automotive Cyber Security Conference; 2022 Nov 15–16; Berlin, Germany.
10. EVITA Project Consortium. E-safety vehicle intrusion protected applications (bib10) [Internet]. 2008 [cited 2026 Mar 28]. Available from: https://www.evita-project.org.
11. HEAVENS Consortium. Security models [Internet]. Deliverable D2. 2016 [cited 2026 Mar 28]. Available from: https://autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf.
12. Henniger O, Apvrille L, Fuchs A, Roudier Y, Ruddle A, Weyl B. Security requirements for automotive on-board networks. In: Proceedings of the 2009 9th International Conference on Intelligent Transport Systems Telecommunications (ITST); 2009 Oct 20–22; Lille, France. New York, NY, USA: IEEE. p. 641–6. doi:10.1109/ITST.2009.5399279.
13. International Organization for Standardization. ISO 26262-3:2018. Road vehicles—functional safety—part 3: concept phase [Internet]. International Standard. Geneva, Switzerland: International Organization for Standardization; 2018 [cited 2026 Mar 28]. Available from: https://www.iso.org/standard/68385.html.
14. Wolf M, Scheibel M. A systematic approach to a qualified security risk analysis for vehicular IT systems. In: Automotive-safety & security 2012. Karlsruhe, Germany: Gesellschaft für Informatik e.V; 2012. p. 195–210.
15. International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 18045:2022. Information security, cybersecurity and privacy protection—evaluation criteria for IT security—Methodology for IT security evaluation [Internet]. International Standard. Geneva, Switzerland: International Organization for Standardization; 2022 [cited 2026 Mar 28]. Available from: https://www.iso.org/standard/72889.html.
16. Islam MM, Sandberg C, Lautenbach A, Olovsson T. A risk assessment framework for automotive embedded systems. In: Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security; 2016 May 30; Xi'an, China. New York, NY, USA: ACM. p. 3–14. doi:10.1145/2899015.2899018.
17. Swiderski F, Snyder W. Threat modeling. Redmond, WA, USA: Microsoft Press; 2004.
18. Lautenbach A, Almgren M, Olovsson T. Proposing bib11 2.0—an automotive risk assessment model. In: CSCS'21: Proceedings of the 5th ACM Computer Science in Cars Symposium. New York, NY, USA: ACM; 2021. p. 1–12. doi:10.1145/3488904.3493378.

19. Ren D, Du S, Zhu H. A novel attack tree based risk assessment approach for location privacy preservation in the VANETs. In: Proceedings of the 2011 IEEE International Conference on Communications (ICC); 2011 Jun 5–9; Kyoto, Japan. New York, NY, USA: IEEE. p. 1–5. doi:10.1109/ICC.2011.5962947.
20. Chah B, Lombard A, Bkakria A, Yaich R, Abbas-Turki A, Galland S. Privacy threat analysis for connected and autonomous vehicles. Procedia Comput Sci. 2022;210(4):36–44. doi:10.1016/j.procs.2022.10.117.
21. Deng M, Wuyts K, Scandariato R, Preneel B, Joosen W. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requir Eng. 2011;16(1):3–32. doi:10.1007/s00766-010-0115-7.
22. Park S, Park H. PIER: cyber-resilient risk assessment model for connected and autonomous vehicles. Wirel Netw. 2024;30(5):4591–605. doi:10.1007/s11276-022-03084-9.
23. Kiening A, Angermeier D. TRADE—threat and risk assessment for automotive distributed engineering. In: Proceedings of the 19th escar Europe: The World's Leading Automotive Cyber Security Conference; 2021 Nov 9–11; Frankfurt am Main, Germany. p. 116–30.
24. ETAS GmbH. ESCRYPT CycurRISK: software tool for threat analysis and risk assessment [Internet]. [cited 2026 Mar 28]. Available from: https://www.etas.com/ww/en/products-services/cybersecurity-products/escrypt-cycurrisk/.
25. CVE Program. CVE-2023-47610 [Internet]. 2023 [cited 2026 Mar 28]. Available from: https://www.cve.org/CVERecord?id=CVE-2023-47610.
26. CVE Program. CVE-2022-25702 [Internet]. 2022 [cited 2026 Mar 28]. Available from: https://www.cve.org/CVERecord?id=CVE-2022-25702.
27. CVE Program. CVE-2022-25685 [Internet]. 2022 [cited 2026 Mar 28]. Available from: https://www.cve.org/CVERecord?id=CVE-2022-25685.
28. International Organization for Standardization, SAE International. ISO/SAE DPAS 8475. Road vehicles—cybersecurity assurance levels (CAL) and targeted attack feasibility (TAF) [Internet]. International Standard. Geneva, Switzerland: International Organization for Standardization; 2026 [cited 2026 Apr 28]. Available from: https://www.iso.org/standard/83187.html.