International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
https://ijcjournal.org/index.php/InternationalJournalOfComputer/index

Cloud Security Architecture for the Automotive Industry: A Framework for Secure Multi-Cloud Deployment

Geol Kang*

Hyundai Autoever America, Senior Security Architect,Fountain Valley, California, USA
Email:ggang@autoeveramerica.com

Abstract

This paper examines the automotive industry since it fundamentally transforms toward Software-Defined Vehicles (SDV) and exponentially increases the reliance on cloud and multi-cloud infrastructures. The attack surface expands in a dramatic way because of a shift to this model. Today cyber risks target centralized cloud backends managing entire fleets not individual vehicles. A comprehensive security architecture should be developed proactively and without delay, as potential threats may escalate, and stringent regulatory frameworks such as UNECE R155 and ISO/SAE 21434 are anticipated to come into effect. In this paper, the Automotive Multi-Cloud Security Framework (AMCSF), which is a conceptual cloud security architecture model for the automotive industry, is proposed based on a systematic literature review as well as comparative analysis of industry practices. ISO/SAE 21434 describes vehicle cybersecurity lifecycle processes the five-layer model would integrate. It works also with modern cloud-oriented technologies like Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP). The study primarily concludes that risk can be effectively managed in modern automotive ecosystems only if protections are applied synergistically and include both the vehicle itself and its cloud infrastructure. This paper will be helpful to cybersecurity and cloud solution engineers and architects in automotive (OEM, Tier-1/Tier-2), vSOC/DevSecOps teams, cybersecurity and compliance management specialists (CSMS/UNECE R155, ISO/SAE 21434), as well as consultants and executives responsible for designing and operating secure multi-cloud backends.

Keywords: cloud security; automotive industry; multi-cloud environment; ISO/SAE 21434; UNECE R155.

Received: 7/9/2025
Accepted: 9/9/2025
Published: 11/19/2025

---

* *Corresponding author.*

1. Introduction

The modern automotive industry is changing, shifting from conventional vehicles to more complex cyber-physical systems known as Software-Defined Vehicles (SDVs). The vehicle is now more than just an isolated mechanical device, according to source [1]. Instead, it acts as a mobile data center fully part of the worldwide digital network. This has changed since customers want better connections, which are now basic instead of special. Innovating with Over-the-Air (OTA) updates, Advanced Driver-Assistance Systems (ADAS), and personalized infotainment services shapes new business models and differentiates brands to a large degree [2].

Cloud infrastructure remains a critical element in this new ecosystem. Automakers are adopting multi-cloud strategies now to optimize costs and avoid vendor lock-in. They utilize effective solutions for tasks through services like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP) for IoT platforms, integrations, and analytics. That this approach has become an industry standard is demonstrated through partnerships between leading OEMs such as Volkswagen with AWS, General Motors with Google Cloud, and Toyota with Microsoft Azure [3].

Yet, a key issue exists since it works closely with clouds: cyber threat increases cause the attack surface to grow. Cloud infrastructure reliance makes a huge, attractive, and vulnerable target for attackers that extends far beyond the vehicle itself. Statistics confirm the severity of this issue: in recent years, the number of cyberattacks in the automotive sector has increased by 225%, with 85% of them being remote in nature [4]. There is a clear shift in the attack vector from in-vehicle systems to the vehicle's cloud backend [5]. Such attacks result in significant financial losses and substantial operational disruptions, affecting thousands of dealerships and disrupting production chains [6].

This shift in the threat landscape means that the center of gravity for the most destructive attacks has moved. While early high-profile hacks, such as the compromise of the Jeep Cherokee [7], focused on direct vehicle impact, modern threats are systemic. An attack on a single software supplier can halt factory production or paralyze dealership operations [8], demonstrating a one-to-many effect. Thus, the greatest operational and financial risk now rests with systemic failures of cloud services that support the entire fleet, rather than the compromise of a single vehicle. A security architecture only on in-vehicle systems protection is fundamentally incomplete.

Requirements of a regulatory nature were made strict. Over 50 countries now require UNECE WP.29 R155 regulation for type approval. Throughout the vehicle lifecycle, automakers must implement a Cybersecurity Management System (CSMS) and certify it [7]. ISO/SAE 21434 does explicitly refer to Cybersecurity Engineering. It is the primary technical standard for implementing R155 requirements specifically for Road vehicles.

Accordingly, this study seeks for a thorough, multi-layer security architecture (AMCSF) that aligns with the realities of modern multi-cloud environments and automotive standards (ISO/SAE 21434). The following tasks were those that were set for achieving this goal: (1) regulatory requirements and also the current threat landscape were analyzed; (2) a systematic review of cloud-oriented technologies together with existing security models was

conducted; (3) all findings were synthesized into the AMCSF architecture that was proposed; (4) all risks and all the practical challenges its implementation entails were discussed.

This work is novel because it integrates a conceptual model with closing explicitly the divide between vehicle lifecycle security (as per ISO/SAE 21434). The model attends to the dynamic and ephemeral nature of cloud infrastructure. The proposed architecture formally defines as well as integrates the distinct yet complementary roles of Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP), and they found the elements for regulatory compliance and make the automotive cloud ecosystem resilient.

2. Research Method

The methodological basis of this study combines approaches that ensure both academic rigor and practical relevance of the conclusions. The primary method used to form the theoretical foundation is a Systematic Literature Review (SLR). This structured and reproducible approach allows for the thorough assessment and synthesis of existing scholarly work on the topic. For construction of a new conceptual model, the method choice is driven by the need to generalize a broad spectrum of academic and technical sources.

The data was collected from peer-reviewed articles. They have published both since 2021 to the present day. Searches in leading scholarly databases and digital libraries were conducted, which include IEEE Xplore, the ACM Digital Library, SpringerLink, and Elsevier (ScienceDirect). Keywords combined formed the search strategy and involved “automotive cybersecurity,” “connected vehicle security,” “cloud security architecture,” “multi-cloud security,” “ISO/SAE 21434,” “UNECE R155,” “CSPM,” “CWPP.”

A content analysis method was applied so it could analyze academic publications along with technological solutions and the state of practice. This analysis included objects such as technical documentation from leading cloud providers (AWS, Azure, GCP), materials from security vendors, together with authoritative consulting and research firms such as Upstream Security and Future Market Perceptions (FMI) reported analytical reports. The academic literature often lags behind within the rapidly changing threat landscape. This approach is indeed important because of the technologies emerging now in the cloud security market. Scholarly articles ground standards then analyze them deeply however, industry reports offer threat statistics updated recently, for example, 2024 data, while describing new attack vectors. Vendor technical documentation in turn details the functionality of CSPM as well as CWPP. Also, that documentation describes complex instruments. Thus, combining these sources enables the creation of a model that is both theoretically grounded and practically applicable to current industry challenges.

The analytical part of the study included the following approaches.

Comparative analysis. A detailed comparison of the regulatory requirements of UNECE R155 and the provisions of ISO/SAE 21434 was conducted to identify key security processes that must be extrapolated to the cloud domain.

Thematic synthesis. The results obtained from the SLR and content analysis were grouped into thematic blocks corresponding to architectural layers, control mechanisms, and operational processes. This method enabled the

structuring of heterogeneous information and the identification of key patterns.

Conceptual model development. At the final stage, an inductive method was used to develop the AMCSF architecture. This process involved synthesizing the identified requirements, best practices, and technological solutions into a single, logically coherent, and original model.

Building on prior work, this study aligns with survey-driven syntheses that map the connected-vehicle threat and assurance landscape and emphasize lifecycle governance and monitoring in modern E/E architectures, as shown by Kifor and Popescu and by Rathore and his colleagues. It also resonates with comparative analyses of UNECE WP.29 R155 and ISO/SAE 21434, such as Costantino and his colleagues and Grimm and his colleagues, that clarify process integration, and with safety–security co-analysis approaches exemplified by Li and his colleagues. Architecture-oriented proposals for cloud-connected autonomous systems, including Sebastian, further motivate layered defenses and runtime assurance. Complementary industry perspectives from EY and BCG underscore the systemic, cloud-mediated risks and supplier dynamics that the framework addresses, while software supply-chain and incident-focused studies by Moore and his colleagues and Bhunia and his colleagues substantiate the need for controls at the build, registry, and API frontiers. The AMCSF consolidates these strands into an automotive-specific, multi-cloud model that operationalizes standard-aligned governance, posture management, and workload protection within a coherent vSOC-centric operating construct.

3. Results and Discussion

The modern automotive ecosystem faces a range of cyber threats that have evolved from targeting individual vehicle components to more complex attacks on the entire associated infrastructure. To systematize the threat analysis, it is appropriate to use the structure proposed in Annex 5 of the UNECE R155 regulation, as it represents a regulator-approved list of attack vectors [7]. Threats can be grouped into the following categories.

Threats related to backend servers. This category is the most critical in the context of cloud architectures. It includes ransomware attacks that paralyze operations, leaks, and unauthorized access to confidential data (such as telemetry and customer personal information), as well as the compromise of fleet management systems.

Threats related to communication channels. These include Man-in-the-Middle attacks on V2X communications, manipulation of APIs to gain unauthorized control over vehicle functions (e.g., unlocking doors, starting the engine), and distributed Denial-of-Service (DDoS) attacks on cloud endpoints that provide connectivity to vehicles.

Threats related to software update procedures. Compromise of the OTA delivery pipeline represents a serious threat, as it allows attackers to inject malicious software into a large number of vehicles simultaneously, potentially leading to mass failures or thefts.

Threats related to the supply chain. Attacks may target not the automaker itself, but its suppliers (Tier 1, Tier 2) or software developers. The incident in which production at Toyota plants was halted due to a cyberattack on a supplier clearly demonstrates the vulnerability of the entire ecosystem [4].

In this context, the key processes of ISO/SAE 21434, initially developed for a vehicle's electronic and electrical systems, require rethinking and extension to the cloud environment. Threat Analysis and Risk Assessment (TARA) must cover not only in-vehicle components but also all cloud assets, including virtual machines, containers, databases, API gateways, and data stores. This raises the complex task of applying TARA at different levels of abstraction, from the entire vehicle to an individual cloud microservice [9]. Similarly, the standard's requirement for continuous cybersecurity activities in the post-production phase (monitoring, incident response) directly implies the creation and operation of a specialized Vehicle Security Operations Center (vSOC) with full visibility into the cloud infrastructure.

To address the above challenges, it is proposed the Automotive Multi-Cloud Security Framework (AMCSF). This conceptual model is a multi-layer structure based on the principle of defense-in-depth and synthesizes approaches from automotive and cloud security domains [10]. The architecture consists of five interrelated layers shown in Figure 1.

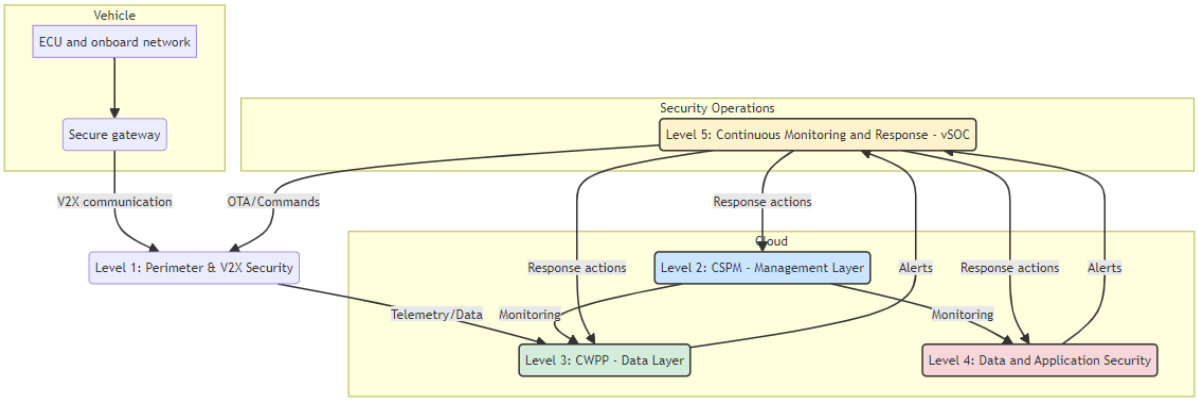

Figure 1: AMCSF architecture conceptual diagram

Layer 1 concerns vehicle and perimeter security. This layer forms the interface between the vehicle and the cloud. Its primary task is to protect V2X communication channels and harden the cloud endpoints with which the vehicle interacts. Key technologies include mutual TLS (mTLS) for strict authentication of both parties, multi-tier VPN architectures to create secure tunnels, and the use of cryptographically strong communication protocols.

Layer 2 concerns Cloud Security Posture Management (CSPM). This is a foundational layer ensuring the security of the entire cloud infrastructure. Its function is to automatically discover and continuously monitor all cloud assets (virtual networks, storage, and databases) and their configurations in a multi-cloud environment. The main goal is proactive prevention and detection of insecure configurations such as public S3 buckets, overly broad network access rules, or weak Identity and Access Management (IAM) policies. In the automotive sector, the application directly maps CSPM policies with ISO/SAE 21434 requirements. CSPM can automatically check servers cut off from the internet, providing OTA updates or IAM roles, using telemetry data, that adhere to least privilege.

Layer four is for protecting applications. Protected services mean executed. It works to safeguard workloads such

as virtual machines, containers, or serverless functions. This covers scanning container images before deployment occurs. It also includes detection of runtime threats like malware as well as memory protection. CWPP is important for securing the microservices of modern automotive backends in the automotive sector. For example, it can detect in real time the compromise of the container since it is responsible for processing remote vehicle-unlock commands or it can identify a vulnerability in a service that streams infotainment content.

Layer three concerns the granular controls that the foundational CSPM and CWPP layers are improved by. A Web Application Firewall (WAF) protects public-facing APIs and web portals against common attacks, such as SQL injection and cross-site scripting, by filtering traffic and blocking any malicious requests. Privileged Access Management (PAM) controls and monitors developer and administrator access to mission-critical backend systems, reducing insider-related risks. End-to-end data encryption protects telemetry and personal data both in transit (using TLS) and at rest (using the AES-256 algorithm).

Layer 5 concerns continuous monitoring and response. This is the operational layer embodied in the Vehicle Security Operations Center (vSOC). Its function is to aggregate alerts from all other layers (CSPM, CWPP, WAF), correlate them with external threat intelligence, and coordinate incident response. This may include automated playbooks, for example, isolating a compromised workload, as well as manual incident analysis by security experts. In the automotive sector, the vSOC is responsible for the full incident management lifecycle: from detecting a cloud-based threat to assessing its potential impact on the fleet and coordinating remediation measures, which may include emergency deployment of a security patch via OTA. This layer also manages protection against DDoS attacks and large-scale threats.

Understanding the synergy between CWPP and CSPM technologies is a key aspect of AMCSF implementation. These two tools address different tasks that complement each other in providing thorough protection for the cloud environment. CSPM protects at the control plane through ensuring of correctness. CSPM also secures the infrastructure configuration itself. Conversely, CWPP protects the data plane by ensuring code executes securely within workloads that keep data secure.

A real instance may show their connection. An automaker may develop a fully secured container for OTA-update commands processing that contains no known vulnerabilities (a task handled by CWPP). An attacker can replace the legitimate container image with a malicious one when a cloud administrator configures the container registry, such as Amazon ECR, to make it publicly accessible. This misconfiguration exists due to CSPM. CSPM must address this single misconfiguration. Thus, even the most robust workload-level protection (CWPP) can be nullified by a vulnerability at the infrastructure level (CSPM). A secure infrastructure posture is a prerequisite for adequate workload protection. Table 1 provides a detailed comparison of their functions in the automotive context.

Table 1: Functional comparison and synergy of CSPM and CWPP in the automotive context

Characteristic	Cloud Security Posture Management (CSPM)	Cloud Workload Protection (CWPP)	Synergy within AMCSF Platform
Primary focus	Cloud infrastructure (control plane)	Cloud workloads (data plane)	CSPM is cloud configuration security. CWPP is runtime workload protection.
Type of protection	Proactive prevention of insecure configurations	Real-time detection and response to threats	CSPM reduces the attack surface; CWPP detects and blocks attacks that manage to bypass it.
Example use cases	- Checking S3 bucket privacy for OTA firmware. - Auditing IAM policies for least-privilege. - Validating firewall/network ACL rules.	- Scanning container images carrying OTA firmware for vulnerabilities. - Detecting malware on remote-diagnostics VMs. - Blocking anomalous API calls inside a microservice.	An alert from CSPM about an overly permissive IAM role can trigger targeted CWPP scanning of the related workloads to check for active exploitation.
Compliance with ISO 21434	Supports organizational cybersecurity governance and continuous monitoring of the environment's security posture.	Supports vulnerability management, incident response, and runtime security during the operational phase of the software lifecycle.	Together, they provide auditable evidence for a comprehensive CSMS covering the entire cloud-connected ecosystem.

Effective incident response is a key element of operational resilience. Figure 2 presents a schematic of the incident response process related to the detection of anomalous activity in the OTA-update service.

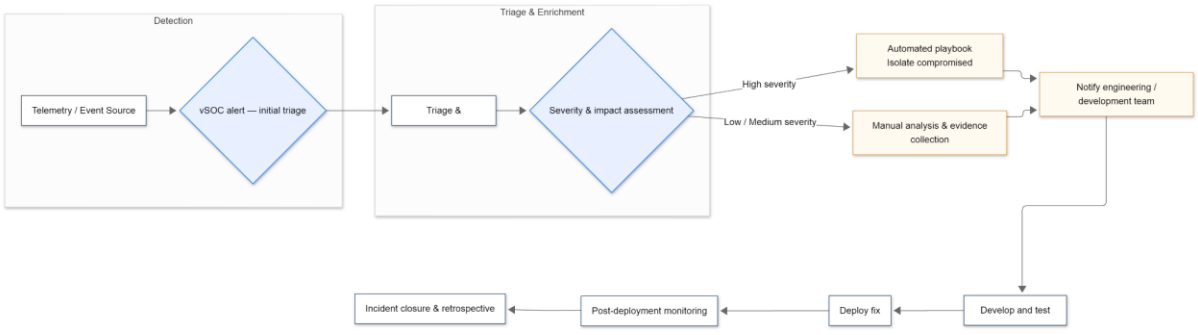

Figure 2: AMCSF Security Incident Response Process Flowchart

Despite the obvious advantages, implementing a thorough security architecture, such as AMCSF, also presents some challenges, both technical and organizational in nature.

A main problem is with established, often legacy, development processes and production systems within the automotive industry. For these systems, integrating modern cloud security practices can be a challenging task. Legacy systems, along with architectures, may be incompatible with new approaches, and this requires substantial investments in modernization. ISO/SAE 21434 is detailed, though it contains certain formulations. These formulations may produce vague interpretations. Implementing the standard requires that they maintain many documents, which creates a significant burden for engineering teams [11].

The automotive industry features a highly complex, multi-tier supply chain. It is a task that is not trivial for ensuring all of the suppliers comply with security, and these suppliers may have different cybersecurity maturity levels. A single supplier vulnerability can jeopardize the entire ecosystem. There is a rather acute shortage of specialists because competencies can span from automotive engineering to cloud security. This complicates the formation of teams that turn out capable of effectively designing, implementing, as well as operating secure cloud systems [12].

These issues create a cyber gap. Formal regulatory compliance often falls short of achieving genuine operational resilience. Simply ticking the boxes for UNECE R155 compliance is insufficient to protect against sophisticated and constantly evolving attacks. The proposed AMCSF architecture is a tool for bridging this gap, as it shifts the emphasis from static compliance to a model of continuous, dynamic monitoring and active threat response.

Building on these results, several clarifications explain more precisely how AMCSF translates into observable security outcomes in multi-cloud automotive backends. First, the framework operationalizes ISO/SAE 21434 processes across the cloud control and data planes by assigning concrete ownership and telemetry requirements at each layer: CSPM establishes configuration baselines and evidence artifacts for governance and assurance, while CWPP provides runtime indicators of compromise and workload provenance for post-production monitoring. This alignment resolves a common ambiguity in extending TARA to cloud systems: risk items identified at the vehicle or feature level are decomposed into cloud assets, attack paths, and guardrails with traceable controls and auditable outputs. Second, AMCSF narrows the dominant one-to-many risk modes by introducing choke points where detection has the greatest systemic payoff. In particular, WAF- and API-gateway-level controls reduce the blast radius of credential-stuffing and injection attacks on public endpoints. At the same time, registry immutability and image signing in the CWPP path constrain supply-chain substitution attacks that could otherwise propagate to the fleet via OTA.

The framework also yields testable propositions for engineering validation. Suppose CSPM policy-as-code is applied to network egress, public storage exposure, and privilege boundaries before workload onboarding. In that case, the rate of high-severity misconfigurations per account should decline monotonically across successive release cycles. If CWPP enforces pre-deployment image attestation and runtime kernel-level telemetry for processes that gate vehicle-command APIs, then the mean time to detect anomalous command flows and container drift should shorten relative to baselines without these controls. Finally, if vSOC correlates CSPM and CWPP alerts with CI/CD metadata, rollback and key rotation playbooks can be triggered deterministically, reducing recovery time for OTA-pipeline incidents. These hypotheses can be evaluated with a minimal, reproducible measurement set: misconfiguration density per cloud account and per project, vulnerable-image prevalence per

release, drift events per workload, detection and recovery latencies per incident class, and coverage of evidentiary artifacts mapped to ISO/SAE 21434 work products.

Essential boundary conditions and trade-offs should be acknowledged. AMCSF presumes disciplined identity partitioning and environment segregation; without these, CSPM findings accumulate faster than they can be remediated, and CWPP signals become noisy. Runtime enforcement introduces overhead that, if not tuned, may affect latency-sensitive services such as remote unlock; therefore, rate-limiting, circuit-breaking, and canarying should be applied to command-path microservices to preserve functional safety. The framework further assumes that suppliers can publish signed artifacts and SBOMs; where suppliers lack that capability, the OEM must compensate with proxy attestations and enhanced ingress controls, raising operational cost. Lastly, while the focus case is OTA, the same control interplay generalizes to other high-risk domains—such as charging-infrastructure backends and telematics ingestion—provided that per-domain data classification and trust boundary definitions are incorporated into CSPM policies and vSOC analytics.

4. Conclusion

The study established that in the threat landscape, changes have been undergone in the automotive industry due to a shift in the primary attack vector from in-vehicle systems to infrastructure in the cloud. These developments — notably the adoption of more stringent international regulations — necessitate a systematic revision of conventional cybersecurity approaches and the extension of existing standards (e.g., ISO/SAE 21434) to cover cloud computing environments.

In this work, researchers address this challenge by proposing a thorough multi-layered approach. It is actually namely the automotive industry AMCSF conceptual cloud security architecture model. It functions as both a practical instrument and a conceptual framework for automakers and their suppliers. It enables secure multi-cloud backends to be designed, implemented, and operated. The key contribution of AMCSF is the formal integration of automotive cybersecurity management processes with modern cloud-oriented technologies such as CSPM and CWPP, and the definition of their synergistic role in providing defense-in-depth.

The practical importance of the proposed architecture is found in its potential to offer a solid guide to meet two aims: adhering to rules needed by UNECE R155, and truly opposing cyberattacks. Protecting customer safety also brand reputation plus revenue, this approach protects data with systems.

Future research should explore several promising aspects. In particular, artificial intelligence can be employed for predictive threat analytics within a virtual Security Operations Center (vSOC); machine-learning techniques are likewise applicable to these tasks. They can also automate the incident response processes. Second, developing and integrating post-quantum cryptography (PQC) remains a current task to ensure long-term vehicle data protection over its lifecycle. Finally, as the electric-vehicle fleet grows, special attention should be paid to standardizing security protocols for the rapidly expanding charging-station infrastructure, which represents a new, critical attack vector.

Within this context, it is useful to articulate the study’s intended scope to ensure the applicability of the proposed

AMCSF is correctly understood. The contribution advances a conceptual, architecture-level model synthesized from a systematic literature review and an analysis of current industry practices as of 2025. The emphasis is on principled layering, control interplay, and governance alignment with ISO/SAE 21434 and UNECE R155, rather than on prescriptive, provider-specific configuration catalogs or organization-specific deployment playbooks. This abstraction is deliberate, supporting portability across multi-cloud environments and enabling flexible mappings to diverse enterprise and regulatory settings.

The analysis focuses on cloud backends that support passenger-vehicle SDV ecosystems, with particular attention to OTA, telematics, and public API command paths that exhibit one-to-many risk propagation. Adjacent domains—such as heavy-duty and off-highway platforms, and regional infrastructures with bespoke compliance regimes—are acknowledged but not modeled in detail. Similarly, charging-infrastructure security, supply-chain attestation processes, and post-quantum cryptographic transitions are identified as forward-looking vectors and framed for subsequent inquiry rather than fully decomposed here.

The framework assumes access to widely available capability classes—CSPM for control-plane governance, CWPP for workload runtime assurance, and vSOC processes for continuous monitoring and response—while remaining implementation-agnostic with respect to specific commercial products. Empirical tuning of the proposed control interplay, metrics, and playbooks is most appropriately performed through OEM- and supplier-led pilots, case studies, and red-team exercises tailored to concrete architectures and operational constraints. These boundaries reflect intentional scoping choices that keep the contribution focused and generalizable, and they complement the outlined agenda for future research and industrial maturation.

References

[1] Autosar, “Limited Edition 20th Anniversary Publication,” Autosar, 2023. Accessed: Sep. 01, 2025. [Online]. Available: https://www.autosar.org/fileadmin/user_upload/AUTOSAR_20th-Book_FINAL_WEB_06-OCT-2023.pdf

[2] “Cyber securing connected cars 2.0: navigating opportunities and risks in the digital era,” EY, 2024. Accessed: Sep. 01, 2025. [Online]. Available: https://www.ey.com/content/dam/ey-unified-site/ey-com/en-in/insights/automotive/documents/ey-cyber-securing-connected-cars-2-navigating-opportunities-and-risks-in-the-digital-era.pdf

[3] T. Weber, A. Koster, M. Quinn, A. Arora, and J. Chapot, “As Auto Software Revs Up, Suppliers Need to Switch Gears,” *BCG Global*, Nov. 14, 2024. https://www.bcg.com/publications/2024/auto-software-revs-up-suppliers-switch-gears (accessed Sep. 02, 2025).

[4] Tajammul Pangarkar, “Automotive Cyber Security Statistics 2024 By Secure Drive,” *Market US*, Jan. 2025. https://scoop.market.us/automotive-cyber-security-statistics/ (accessed Sep. 03, 2025).

[5] C. V. Kifor and A. Popescu, “Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies,” *Sensors*, vol. 24, no. 18, p. 6139, Sep. 2024, doi:

https://doi.org/10.3390/s24186139.

[6] R. S. Rathore, C. Hewage, O. Kaiwartya, and J. Lloret, "In-Vehicle Communication Cyber Security: Challenges and Solutions," *Sensors*, vol. 22, no. 17, p. 6679, Sep. 2022, doi: https://doi.org/10.3390/s22176679.

[7] G. Costantino, M. De Vincenzi, and I. Matteucci, "A Comparative Analysis of UNECE WP.29 R155 and ISO/SAE 21434," *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Jun. 2022, doi: https://doi.org/10.1109/eurospw55150.2022.00041.

[8] S. Bhunia, M. Blackert, H. Deal, A. DePero, and A. Patra, "Analyzing the 2021 Kaseya Ransomware Attack: Combined Spearphishing through SonicWall SSLVPN Vulnerability," *IET Information Security*, Jan. 2025, doi: https://doi.org/10.1049/ise2/1655307.

[9] D. Grimm, A. Lautenbach, M. Almgren, T. Olovsson, and E. Sax, "Gap Analysis of ISO/SAE 21434 – Improving the Automotive Cybersecurity Engineering Life Cycle," *2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC)*, Sep. 2023, doi: https://doi.org/10.1109/itsc57777.2023.10422100.

[10] M. Sebastian, "Multi-Layer Security Architecture for Cloud-Connected Autonomous Systems," *Journal of Computer Science and Technology Studies*, vol. 7, no. 3, pp. 798–803, May 2025, doi: https://doi.org/10.32996/jcsts.2025.7.3.87.

[11] Y. Li, W. Liu, Q. Liu, X. Zheng, K. Sun, and C. Huang, "Complying with ISO 26262 and ISO/SAE 21434: A Safety and Security Co-Analysis Method for Intelligent Connected Vehicle," *Sensors*, vol. 24, no. 6, p. 1848, Mar. 2024, doi: https://doi.org/10.3390/s24061848.

[12] M. Moore, A. Sirish, A. Yelgundhalli, and J. Cappos, "Securing Automotive Software Supply Chains," *Symposium on Vehicle Security and Privacy (VehicleSec)*, 2024, doi: https://doi.org/10.14722/vehiclesec.2024.23015.