

Original Article

Open Access

The Paradigm Shift in Whole Vehicle Type Approval: Critical Evaluation of UN R155 and R156 in the Era of Software-Defined Vehicles (SDVs)

Majid Nouri ^{1*}

1. Vehicle Engineering Research Group, Research Center of Technology and Engineering, Standard Research Institute, Karaj, Iran

Abstract

The automotive industry is witnessing a profound technological transformation, migrating from traditional hardware-centric engineering to the era of Software-Defined Vehicles (SDVs). In this paradigm, vehicle functionality, performance, and safety attributes are increasingly governed by software that evolves throughout the vehicle's lifecycle. This transition challenges the fundamental tenets of traditional Whole Vehicle Type Approval (WVTA) frameworks, which have historically relied on "frozen" hardware configurations and static validation methodologies. As vehicles transition into dynamic, hyper-connected ecosystems capable of continuous over-the-air (OTA) updates, legacy certification processes face a critical regulatory vacuum. This paper provides a critical evaluation of the recent integration of UN Regulations No. 155 (Cyber Security) and No. 156 (Software Update Management System) into the global regulatory landscape. By examining the tension between the iterative, agile nature of software development cycles and the traditionally sequential timelines of regulatory compliance, this study identifies the operational challenges faced by both Original Equipment Manufacturers (OEMs) and Type Approval Authorities. Furthermore, it analyzes the shift from product-based validation to process-oriented auditing, arguing that contemporary standards must evolve from static point-in-time assessments to continuous, lifecycle-based monitoring. The findings offer strategic insights into harmonizing cybersecurity engineering (ISO/SAE 21434) with regulatory requirements, providing a roadmap for future-proofing automotive standards in an increasingly digitized global market.

Keywords Software-Defined Vehicles (SDVs), Whole Vehicle Type Approval (WVTA), UN R155, UN R156, Cybersecurity, Over-the-Air (OTA) Updates, Regulatory Compliance.

1. Introduction

The global automotive regulatory framework is undergoing a fundamental transformation as vehicles evolve from largely mechanical systems into software-defined, connected, and increasingly autonomous platforms. Historically, vehicle type approval was based on a relatively

stable hardware configuration, where compliance could be assessed through a combination of design review, component testing, and verification against fixed technical prescriptions. In this traditional paradigm, the vehicle was treated as a predominantly static product, and regulatory conformity was established at the point of manufac-



© The Author(s) 2023. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

* Correspondence:
nouri.standard@gmail.com

ture and market entry. However, the rise of connected vehicles, over-the-air (OTA) software deployment, digital control architectures, and lifecycle-based feature updates has rendered this static model increasingly insufficient for ensuring safety, cybersecurity, and regulatory compliance over the full service life of the vehicle [1], [2].

Within this context, the World Forum for Harmonization of Vehicle Regulations (WP.29) under the United Nations Economic Commission for Europe (UNECE) has emerged as the central international body shaping the next generation of vehicle type approval requirements. WP.29 has progressively moved beyond conventional performance-based regulations toward lifecycle-oriented governance mechanisms that address emerging risks associated with cybersecurity and software update management. Two landmark regulations—UN Regulation No. 155 on Cyber Security and Cyber Security Management Systems (CSMS) and UN Regulation No. 156 on Software Update Management Systems (SUMS)—represent a decisive regulatory shift from static product validation to continuous process assurance [1], [2].

UN Regulation No. 155 requires manufacturers to establish and maintain a cyber security management system capable of identifying, assessing, and mitigating cyber risks throughout the vehicle lifecycle, including design, production, operation, maintenance, and decommissioning [1]. This regulation effectively extends regulatory scrutiny from the physical vehicle to the organizational processes that govern cybersecurity governance, threat analysis, vulnerability management, and incident response. In parallel, UN Regulation No. 156 establishes requirements for managing software updates in a controlled, traceable, and secure manner, including updates delivered remotely through OTA mechanisms [2]. The regulation obliges manufacturers to demonstrate that software changes do not compromise vehicle safety, environmental performance, or approval-relevant functions, and that update processes are properly documented, validated, and monitored across the lifecycle [2].

This regulatory shift is particularly significant because it changes the epistemic basis of type approval. Under the traditional model, approval authorities primarily assessed whether a vehicle type conformed to technical requirements at a specific point in time. In contrast, the new framework requires evidence that manufacturers have implemented robust management systems capable of controlling dynamic and evolving risks after approval has been granted. Thus, compliance is no longer limited to product characteristics alone, but increasingly depends on the maturity of organizational processes, software governance, and risk-based lifecycle management [1], [2]. This transformation also implies a deeper integration

between regulatory science and cybersecurity engineering, especially through alignment with ISO/SAE 21434, which provides a structured engineering framework for cybersecurity risk management in road vehicles [3].

The academic literature has begun to address this transition from several perspectives. Recent studies emphasize that UN R155 and UN R156 are not merely new technical regulations, but rather foundational instruments for establishing a regulatory architecture compatible with software-defined vehicles [4], [5]. For example, research on high-assurance software update management systems highlights the challenges of assuring secure update delivery, validation, traceability, and rollback mechanisms in accordance with UN R156 [4]. Other studies have explored how security-by-design approaches can operationalize the combined requirements of ISO/SAE 21434 and WP.29 regulations in OTA update workflows, demonstrating that cybersecurity compliance must be embedded from the earliest development phases rather than added as a post-development control layer [5]. These works collectively show that regulatory compliance in modern automotive systems is increasingly a lifecycle engineering problem rather than a one-time certification exercise.

From a type approval perspective, the implications are profound. Approval authorities and technical services must now evaluate not only whether a vehicle meets prescribed test criteria, but also whether the manufacturer's CSMS and SUMS are effective, auditable, and continuously maintained. This introduces new challenges in terms of assessment scope, organizational competence, evidence collection, and post-approval surveillance. Moreover, because software updates can modify safety-critical and approval-relevant functionality after market entry, regulators must consider how to maintain conformity over time without stifling innovation or slowing the deployment of beneficial digital features [1], [2]. The resulting tension between regulatory stability and software agility is one of the defining challenges of contemporary type approval systems.

Accordingly, the present paper critically examines the role of WP.29 in reshaping global vehicle type approval through UN R155 and UN R156. It argues that these regulations mark a transition from hardware-centric conformity assessment toward a process-oriented, lifecycle-based regulatory paradigm. By synthesizing regulatory texts and recent scholarly studies, the paper identifies key implementation challenges for manufacturers, approval authorities, and technical services, and highlights the need for harmonized methodologies capable of addressing cybersecurity, software updates, and approval continuity in the era of software-defined vehicles.

2. The Technological Gap

The global automotive industry is undergoing a profound technological transition from mechanically dominated and hardware-defined products toward software-defined, connected, and increasingly automated mobility platforms. This transformation is occurring at a pace that challenges the traditional logic of international vehicle regulation and type approval. Historically, vehicle approval systems were designed around the assumption that a vehicle type could be assessed at a defined point in time based on a stable configuration of hardware, components, and control systems. However, this assumption is becoming increasingly fragile as modern vehicles rely on software functions, cloud connectivity, over-the-air updates, data-driven services, and automated driving capabilities that may evolve throughout the vehicle lifecycle [6]–[8]. The resulting technological gap is not merely a delay in updating standards; it is a structural mismatch between two fundamentally different development logics. Vehicle technologies, particularly in the domains of connectivity, automation, cybersecurity, and software updates, are increasingly developed through agile engineering cycles, iterative software deployment, and continuous improvement models. In contrast, international standards and regulatory instruments are typically developed through consensus-based procedures that require extensive technical deliberation, stakeholder negotiation, validation, and formal adoption [9], [10]. This creates a temporal asymmetry: technology evolves in months or even weeks, while international standards and regulations often require several years to be developed, harmonized, and implemented.

2.1. From Static Type Approval to Dynamic Vehicle Configurations

A key source of this gap is the transition from static vehicle approval to dynamic vehicle configuration management. Traditional type approval assumes that the approved vehicle configuration remains materially unchanged after approval, except for controlled modifications that may trigger extensions or amendments to the approval. This model was suitable for conventional vehicles in which safety, emissions, and performance characteristics were primarily defined by mechanical design and embedded electronic control units with limited post-market modification capability.

By contrast, software-defined vehicles can receive post-production software updates that alter diagnostic functions, driver assistance systems, battery management strategies, infotainment services, cybersecurity countermeasures, and, in some cases, safety-relevant operational behavior [11], [12]. Consequently, the approved vehicle is no longer a static product but a continuously evolving

cyber-physical system. This raises an essential regulatory question: how can compliance be maintained when the object of approval changes after the original approval decision?

The contrast between conventional type approval and software-defined vehicle compliance can be conceptualized as a transition from a single-point approval model to a lifecycle-based compliance model. In the traditional model, regulatory conformity is mainly assessed before market entry, based on a stable and production-representative vehicle configuration. In contrast, software-defined vehicles may experience repeated software updates, cybersecurity patches, functional enhancements, and configuration changes after approval. Therefore, compliance must be maintained dynamically across the operational lifecycle of the vehicle.

As illustrated in Figure 1, traditional type approval is based on a relatively linear regulatory pathway in which vehicle design, testing, approval, and market use occur in a sequential manner. The approved vehicle configuration is assumed to remain substantially stable after market entry, and any significant technical change is normally managed through an extension or amendment of the approval. By contrast, the SDV lifecycle compliance model requires a continuous regulatory feedback loop. In this model, software updates, cybersecurity patches, vulnerability responses, and functional modifications may occur after the initial type approval decision. Consequently, the approved vehicle type cannot be understood merely as a fixed technical configuration. Instead, it must be understood as a controlled configuration space governed by software identification, update traceability, impact assessment, validation evidence, and post-deployment monitoring. This shift explains why modern type approval frameworks increasingly depend on management-system requirements such as cybersecurity management systems and software update management systems.

2.2. The Acceleration of Connected and Automated Vehicle Technologies

Connected and automated vehicles intensify this technological gap because they combine multiple fast-moving technology domains. These vehicles rely on sensor fusion, vehicle-to-everything communication, artificial intelligence, high-performance computing platforms, cloud-based services, digital maps, remote diagnostics, and cybersecurity monitoring. Each of these domains evolves at a speed that is difficult to accommodate within traditional international standardization cycles [13], [14]. Automated driving functions, in particular, challenge conventional validation methods. Traditional approval testing has often relied on repeatable physical tests un-

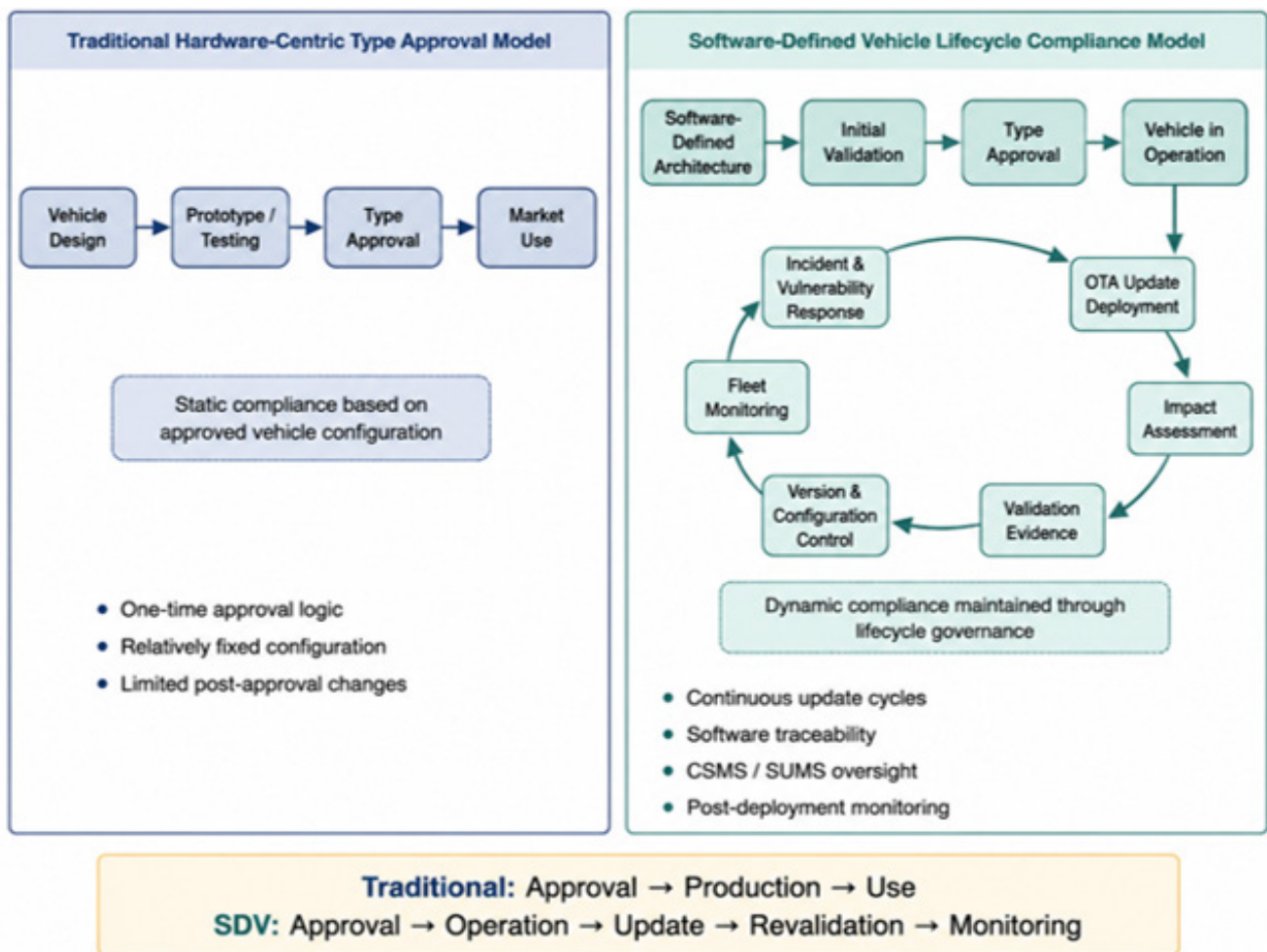


Fig 1. Traditional Type Approval versus SDV Lifecycle Compliance

der controlled conditions. However, automated driving systems must operate within complex and variable operational design domains, where safety depends not only on component reliability but also on perception accuracy, behavioral decision-making, scenario coverage, fallback strategies, and interaction with other road users [15]. This creates a validation challenge that cannot be fully addressed by conventional pass/fail testing alone.

Furthermore, automated driving technologies increasingly depend on machine learning-based perception and decision-support systems. Such systems may exhibit performance characteristics that are difficult to specify exhaustively in advance, especially under rare, uncertain, or edge-case scenarios. As a result, regulatory frameworks must increasingly incorporate simulation, scenario-based testing, real-world monitoring, safety cases, and post-deployment evidence. However, the international harmonization of such methods remains an ongoing and complex process [15], [16].

A defining characteristic of software-defined vehicles is

that they operate not merely as mechanical products, but as complex cyber-physical systems composed of interdependent hardware, software, communication, and data layers. This layered architecture increases functional flexibility, enables remote feature deployment, and supports continuous optimization, but it also expands the scope of compliance-relevant interactions. As a result, regulatory assessment must extend beyond traditional component verification toward a systemic understanding of the vehicle's digital stack, as depicted in Figure 2.

Figure 2. Layered Technology Stack of Connected and Software-Defined Vehicles

As presented in Figure 2, the compliance status of an SDV emerges from the interaction of multiple technological layers rather than from isolated physical subsystems alone. Embedded controllers, operating software, vehicle networks, external connectivity, backend infrastructure, and data governance mechanisms all contribute to the vehicle's safety, security, and update behavior. This

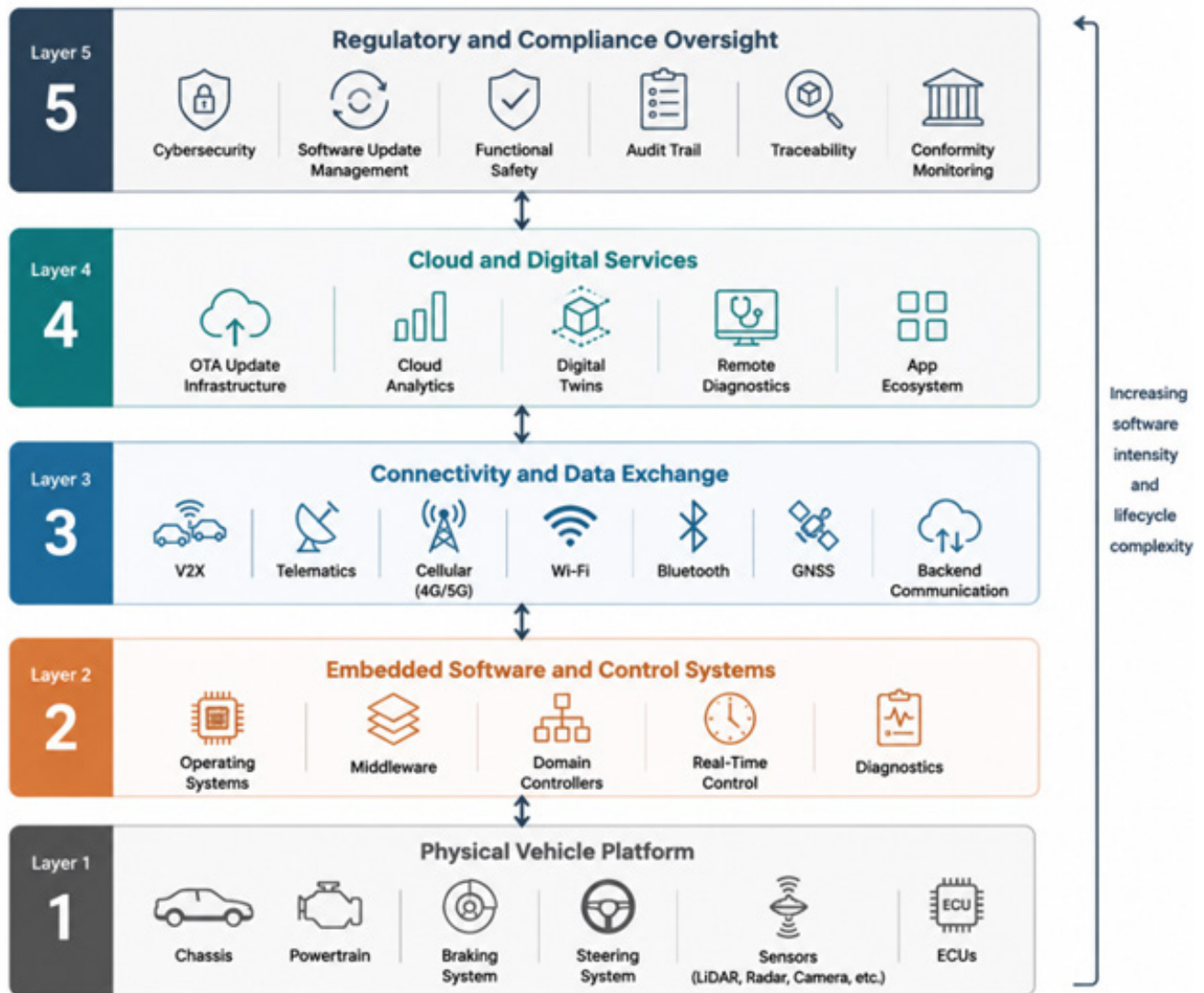


Fig 2. Layered Technology Stack of Connected and Software-Defined Vehicles

layered complexity explains why existing homologation structures face difficulty in addressing software-intensive vehicle evolution through purely product-based assessment methods. 3.3. Functional Safety, Cybersecurity, and Software Updates: A Converging Assurance Problem

The technological gap is further complicated by the convergence of functional safety, cybersecurity, and software update management. Functional safety standards such as ISO 26262 provide a structured approach to hazards arising from malfunctioning behavior of electrical and electronic systems [6]. However, modern connected vehicles face risks that may not originate from random hardware failures or systematic development faults alone. Cybersecurity threats, software vulnerabilities, data corruption, malicious updates, and compromised communication channels can also generate safety-relevant consequences [7], [17].

ISO/SAE 21434 has significantly advanced the automotive cybersecurity engineering framework by introducing lifecycle-based cybersecurity risk management for road vehicle electrical and electronic systems [7]. Nevertheless, implementing cybersecurity assurance in rapidly evolving software-defined architectures remains challenging. Vehicles increasingly incorporate third-party software, open-source components, supplier-developed modules, wireless communication interfaces, and cloud-based services. Each of these elements may change over time, creating a continuously shifting threat landscape. Similarly, ISO 24089 addresses software update engineering and provides a structured framework for managing software updates at organizational and project levels [8]. This is highly relevant to the implementation of software update management systems. Yet, practical challenges remain in determining how to assess the cumulative impact

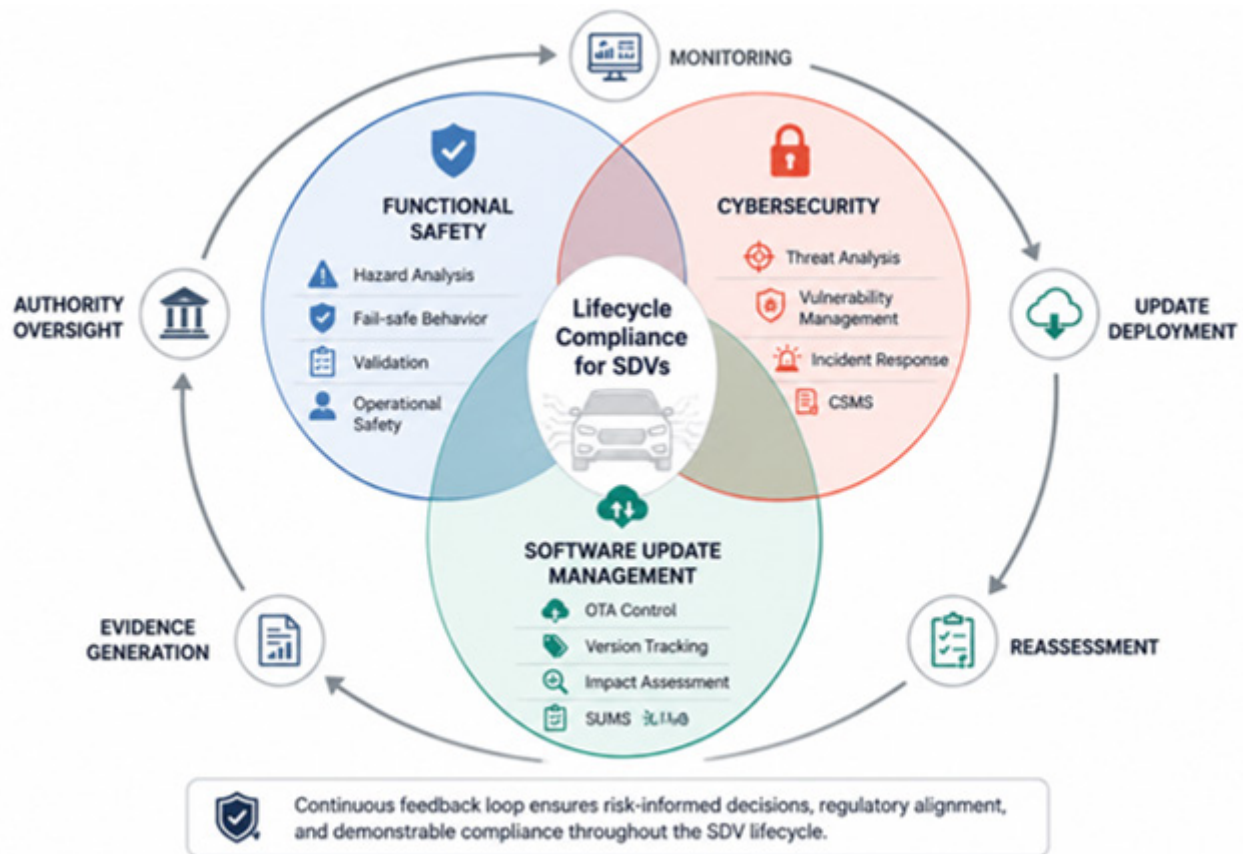


Fig 3. Convergence of Functional Safety, Cybersecurity, and Software Update Governance in SDV Regulation

of frequent updates, how to validate interactions between updated and non-updated systems, how to ensure rollback safety, and how to maintain traceability across fleets with different software configurations [8], [11], [12].

The regulatory challenge posed by software-defined vehicles does not arise from software alone, but from the increasing interdependence between safety-critical functionality, cybersecurity protection, and post-approval software modification. In conventional regulatory practice, these domains were often addressed separately. By contrast, SDVs require an integrated compliance model in which safety assurance, cyber risk management, and software update governance operate in a coordinated manner. This convergence is conceptually illustrated in Figure 3.

Figure 3. Convergence of Functional Safety, Cybersecurity, and Software Update Governance in SDV Regulation
As shown in Figure 3, the governance of SDVs depends on the alignment of three regulatory logics: protection against unsafe behavior, protection against malicious exploitation, and control over software changes introduced during operation. This convergence has major implica-

tions for type approval, as authorities must increasingly evaluate not only the technical performance of the vehicle, but also the manufacturer's capability to manage risk, maintain traceability, and preserve compliance over time. Accordingly, SDV regulation is evolving toward an integrated lifecycle governance model rather than a set of isolated technical checks.

2.3. The Standardization Lag and Its Regulatory Consequences

The delay between technological innovation and regulatory harmonization has several consequences for type approval systems. First, approval authorities may face uncertainty when assessing technologies that are not yet fully covered by existing standards. Second, manufacturers may experience fragmented requirements across jurisdictions, especially where national authorities interpret emerging technologies differently. Third, technical services may need new competencies in software auditing, cybersecurity assessment, data governance, simulation evaluation, and lifecycle compliance monitoring [9], [10], [18].

This standardization lag also affects market access. If standards are too slow to adapt, innovative technologies may enter the market under unclear regulatory expectations, increasing legal and safety uncertainty. Conversely, if regulatory authorities adopt overly conservative interpretations, innovation may be delayed or fragmented. The central regulatory challenge is therefore to create approval systems that are sufficiently robust to protect safety and cybersecurity, yet sufficiently adaptive to accommodate rapid technological change.

One promising direction is the movement from product-only approval toward process-based and lifecycle-based approval. This does not eliminate the need for vehicle-level testing, but it complements it with evidence that the manufacturer has effective management systems for cybersecurity, software updates, configuration control, incident response, and post-deployment monitoring. In this sense, the emerging regulatory model increasingly resembles a hybrid framework: part product certification, part management system audit, and part continuous compliance monitoring.

2.4. Implications for International Type Approval

For international type approval, the technological gap creates a need to redefine the meaning of conformity. In a conventional vehicle, conformity primarily means that production vehicles remain consistent with the approved type. In a software-defined vehicle, conformity must also mean that software versions, update processes, cybersecurity controls, and post-market modifications remain within approved and controlled boundaries.

This requires a more dynamic understanding of type approval. Approval authorities may need access to software identification systems, update histories, change impact assessments, cybersecurity monitoring results, and evidence of continued compliance. Manufacturers, in turn, must maintain stronger internal governance over software configuration, supplier changes, vulnerability management, and update deployment. Technical services must be capable of auditing these processes and assessing whether the manufacturer's controls are sufficient to prevent unsafe or non-compliant vehicle states.

In summary, the technological gap between connected/autonomous vehicle development and international standardization is driven by the divergence between rapid software-based innovation and slower consensus-based regulatory development. This gap manifests in four principal areas: post-production software evolution, automated driving validation, safety–cybersecurity convergence, and lifecycle compliance assurance. Addressing this gap will require a regulatory transition from static type approval toward adaptive, lifecycle-oriented, and soft-

ware-aware approval frameworks.

3. Critical Analysis of SUMS: Implementation Challenges for OEMs and Type Approval Authorities

The Software Update Management System, SUMS, introduced under UN Regulation No. 156, represents a major regulatory response to the increasing role of software in modern vehicles. Its main purpose is to ensure that software updates, including over-the-air updates, are managed in a controlled, traceable, and auditable manner throughout the vehicle lifecycle [19]. This is particularly important for software-defined vehicles, where post-approval updates may affect safety-related functions, cybersecurity controls, emissions performance, driver information systems, or other type approval-relevant characteristics.

Unlike traditional type approval, which is largely based on the assessment of a stable vehicle configuration before market entry, SUMS introduces a lifecycle-oriented compliance model. Under this model, the manufacturer must demonstrate not only that the vehicle complies at the time of approval, but also that it has an effective system for identifying software versions, assessing update impacts, validating changes, recording update history, and ensuring that compliance is not compromised after deployment [19], [20]. This represents a fundamental shift from approving a fixed product toward auditing the manufacturer's capability to manage software evolution.

3.1. Challenges for OEMs

For OEMs, the first major challenge is software configuration management. Modern vehicles contain numerous electronic control units, domain controllers, embedded software modules, calibration datasets, connectivity interfaces, and cloud-dependent services. As a result, identifying the exact software configuration of a vehicle and linking it to the approved type can be technically complex. SUMS requires OEMs to maintain reliable software identifiers and records, but this becomes increasingly difficult as vehicle architectures become more centralized, updateable, and software-intensive.

A second challenge is the impact assessment of software updates. Not all updates have the same regulatory significance. Some updates may only affect infotainment functions, while others may influence braking, steering, automated driving, cybersecurity protection, emissions strategies, or diagnostic functions. The difficulty lies in determining whether a software update affects type approval-relevant parameters. Even apparently minor software modifications may create indirect effects through interactions with other vehicle systems. Therefore, OEMs need robust internal procedures to classify updates, assess

risks, validate changes, and decide whether regulatory notification or approval extension is required.

A third challenge concerns the integration of SUMS with cybersecurity and safety processes. Software updates may be introduced to correct vulnerabilities, but cybersecurity patches can also affect safety-related vehicle behavior. Similarly, updates intended to improve safety functions may introduce new cybersecurity risks. Therefore, SUMS cannot operate separately from the Cybersecurity Management System, CSMS, required under UN Regulation No. 155, or from functional safety and SOTIF processes [22]–[25]. For OEMs, this requires close coordination between software engineering, cybersecurity, homologation, safety, legal, supplier management, and aftersales teams.

Finally, OEMs face a significant burden in evidence generation and audit readiness. They must be able to demonstrate that each relevant update has been properly assessed, validated, approved, deployed, and recorded. This includes maintaining evidence on software versioning, update content, affected systems, validation results, rollback strategies, cybersecurity implications, and post-deployment monitoring. The challenge is not only producing technical evidence, but presenting it in a structured form that type approval authorities can review effectively.

3.2. Challenges for Type Approval Authorities

For type approval authorities, SUMS introduces a different kind of regulatory task. Instead of assessing only a defined vehicle configuration, authorities must evaluate the effectiveness of the manufacturer's software update management processes. This requires capabilities closer to management-system auditing, combined with technical understanding of vehicle software architecture, cybersecurity, functional safety, and update validation.

One of the most difficult issues is defining the boundary between minor updates and approval-relevant updates. If every software update required regulatory intervention, the approval system would become inefficient and slow. However, if too much discretion is left to manufacturers, compliance-relevant changes may escape sufficient oversight. Authorities must therefore develop risk-based criteria for assessing when an update requires notification, documentation review, approval extension, or direct technical assessment.

Another challenge is institutional capacity. Many approval authorities were originally designed to evaluate physical components and vehicle test results, not continuous software lifecycle processes. The rise of OTA updates, cybersecurity patches, cloud-connected functions, and automated driving features requires new expertise, digital reporting tools, and audit methodologies. Without these

capabilities, SUMS may become a formal requirement rather than an effective compliance mechanism.

A further concern is international consistency. Although UN R156 provides a harmonized regulatory basis, different authorities may interpret software update relevance, documentation requirements, and audit depth differently. Such variation can create uncertainty for OEMs operating across multiple markets and may weaken the mutual-recognition logic of the UNECE type approval framework. Therefore, common guidance, standardized templates, and shared audit practices are essential for consistent SUMS implementation.

3.3. Critical Assessment

SUMS is a necessary but not sufficient response to the regulatory challenges created by software-defined vehicles. Its strength lies in recognizing that compliance must be maintained after type approval and that software updates require systematic governance. It shifts the regulatory focus from one-time product conformity toward lifecycle control, traceability, and organizational capability. However, SUMS also creates practical tensions. OEMs must remain agile enough to deploy software improvements and cybersecurity patches quickly, while still producing sufficient evidence for regulatory assurance. Authorities must rely partly on manufacturer self-assessment, while also maintaining independent oversight. At the same time, both sides must manage growing technical complexity without making the approval process excessively slow or burdensome.

Therefore, the effective implementation of SUMS should be based on a risk-based approach. Low-risk updates may only require internal documentation and traceability, while updates affecting safety, cybersecurity, emissions, automated driving, or other regulated functions should trigger stronger validation, reporting, or approval procedures. In this sense, SUMS should be understood as a bridge between traditional type approval and future lifecycle-based regulation for software-defined vehicles.

4. Comparative Study: EU WVTA and U.S. Self-Certification in the Software-Defined Vehicle Era

The regulatory treatment of software-defined vehicles reveals a fundamental divergence between the European Union's Whole Vehicle Type Approval, WVTA, framework and the United States' self-certification model under the Federal Motor Vehicle Safety Standards, FMVSS. The EU framework is based on ex ante regulatory control, where vehicles, systems, components, and separate technical units must obtain approval before market entry. Within this model, the adoption of UN Regulation No. 155 on cybersecurity and UN Regulation No. 156 on

software update management has strengthened the role of pre-market verification, organizational auditing, and lifecycle compliance. Manufacturers must demonstrate that they operate effective Cybersecurity Management Systems, CSMS, and Software Update Management Systems, SUMS, before vehicles can be approved and placed on the market. This makes the European approach more process-oriented and preventive, particularly suitable for addressing over-the-air updates, cybersecurity risks, and post-approval software modifications in software-defined vehicles [26].

By contrast, the U.S. regulatory model relies primarily on manufacturer self-certification. Under the FMVSS framework, manufacturers are responsible for certifying that their vehicles comply with applicable safety standards at the time of sale, while the National Highway Traffic Safety Administration, NHTSA, exercises authority mainly through post-market enforcement, defect investigations, recalls, and civil penalties. This model provides greater flexibility for innovation and faster deployment of software-based functions, since regulatory approval is not generally required before market introduction. However, it also creates challenges for continuous software compliance, especially where OTA updates may alter vehicle behavior after sale. In the SDV context, the EU model emphasizes prior assurance, auditability, and harmonized lifecycle governance, whereas the U.S. model emphasizes manufacturer responsibility, market access flexibility, and reactive enforcement. For global OEMs, this divergence creates a complex compliance environment: the same software update may be subject to structured approval and documentation expectations in Europe, while being managed through internal certification, risk assessment, and potential post-market scrutiny in the United States [27], [28].

5. Conclusion and Recommendations: Embedding Security by Design in Vehicle Development

The transition toward software-defined vehicles has fundamentally changed the regulatory meaning of vehicle compliance. In conventional type approval, compliance was mainly assessed against a relatively stable physical configuration before market entry. However, in SDVs, vehicle functions may evolve continuously through software updates, connectivity features, cloud-based services, data-driven functions, and over-the-air deployment. This makes cybersecurity and software update governance inseparable from vehicle safety, functional performance, and regulatory conformity. UN Regulations No. 155 and No. 156 represent an important step in this transition by requiring manufacturers to establish Cybersecurity Management Systems, CSMS, and Software Up-

date Management Systems, SUMS. Nevertheless, these regulations should be understood not as final solutions, but as the foundation for a broader lifecycle-based compliance model.

A central conclusion of this study is that cybersecurity cannot be treated as an additional verification layer applied at the end of vehicle development. Instead, it must be embedded into the earliest stages of system architecture, software design, supplier selection, validation, production, post-market monitoring, and update management. This requires a clear shift from security as compliance evidence toward security as an engineering principle. In this context, “Security by Design” means that cybersecurity risks are anticipated, modelled, mitigated, validated, and monitored throughout the entire vehicle lifecycle, rather than being addressed only after vulnerabilities or incidents emerge.

To operationalize this approach, OEMs should integrate cybersecurity requirements directly into vehicle concept development and system architecture. Threat analysis and risk assessment should be performed at the design stage, before software modules, communication interfaces, electronic control units, sensors, and backend services are finalized. Security objectives should be traceable to technical controls, validation evidence, supplier requirements, and software update procedures. This traceability is particularly important for SDVs, where a later software update may alter the risk profile of the vehicle even if no physical component has changed.

A second recommendation is to ensure strong integration between CSMS, SUMS, functional safety, and SO-TIF processes. Cybersecurity measures may affect safety behavior, and safety-related software updates may introduce new cybersecurity dependencies. Therefore, risk assessment should not be conducted in isolated organizational silos. Instead, OEMs should establish cross-functional governance involving cybersecurity engineers, software developers, functional safety experts, homologation teams, supplier managers, legal compliance units, and aftersales operations. This integrated model would reduce the risk that software updates are validated only from one technical perspective while creating unintended consequences in another domain.

Third, OEMs should adopt a risk-based software update classification system. Not all updates require the same level of regulatory attention or validation depth. Updates affecting infotainment or user-interface functions may be managed through internal documentation and traceability, provided they do not interact with regulated systems. By contrast, updates affecting braking, steering, automated driving, emissions control, cybersecurity mechanisms, diagnostic functions, or driver warnings should trigger

enhanced impact assessment, validation, documentation, and, where necessary, notification to or approval by the competent authority. Such a risk-based model can preserve innovation speed while maintaining regulatory assurance. Fourth, cybersecurity should be extended to the software supply chain. Since modern vehicles depend on software components, tools, libraries, cloud services, and electronic systems supplied by multiple actors, OEMs must ensure that suppliers comply with compatible cybersecurity and update-management requirements. Contractual obligations should be supported by technical evidence, vulnerability disclosure procedures, software bill of materials, secure development practices, and audit rights. Without supply-chain transparency, Security by Design cannot be effectively implemented at the vehicle level. Finally, type approval authorities should develop stronger technical capacity and harmonized audit methods for assessing cybersecurity and software update governance. The future of vehicle approval will depend less on one-time inspection of physical components and more on the ability to evaluate lifecycle control systems. Authorities should therefore use common guidance, standardized documentation templates, digital reporting tools, and risk-based review criteria. This would reduce regulatory fragmentation and support more consistent implementation of UN R155 and UN R156 across markets. In conclusion, the SDV paradigm requires a regulatory transformation from static product approval toward continuous lifecycle assurance. Security by Design provides the technical and organizational foundation for this transformation. It enables manufacturers to build vehicles that are not only compliant at the moment of approval, but capable of remaining safe, secure, and auditable throughout their operational life. The long-term effectiveness of UN R155 and UN R156 will therefore depend on how deeply cybersecurity is integrated into engineering culture, software governance, supplier management, and regulatory oversight.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Received: Jun. 2026 Accepted: Aug. 2026

Published online: Aug. 2026

DOI: 10.22034/ASAS.2026.586192.1108

References

- [1] UNECE, UN Regulation No. 155: Cyber security and cyber security management system. United Nations Economic Commission for Europe. Available: [https://unece.org/sites/default/files/2023-02/R155e_\(2\).pdf](https://unece.org/sites/default/files/2023-02/R155e_(2).pdf)
- [2] UNECE, UN Regulation No. 156: Software update and software update management system. United Nations Economic Commission for Europe. Available: [https://unece.org/sites/default/files/2024-03/R156e_\(2\).pdf](https://unece.org/sites/default/files/2024-03/R156e_(2).pdf)
- [3] ISO/SAE, ISO/SAE 21434: Road vehicles — Cybersecurity engineering. International Organization for Standardization / SAE International, 2021.
- [4] Development for high-assurance software update management system complying with UN R156. IEEE Xplore. Available: <https://ieeexplore.ieee.org/iel8/6287639/6514899/10595114.pdf>
- [5] An adaptable security-by-design approach for ensuring a ... ScienceDirect. Available: <https://www.sciencedirect.com/science/article/pii/S0167404824005741>
- [6] ISO, ISO 26262: Road vehicles — Functional safety. Geneva, Switzerland: International Organization for Standardization, 2018.
- [7] ISO/SAE, ISO/SAE 21434:2021 — Road vehicles — Cybersecurity engineering. Geneva, Switzerland: International Organization for Standardization / SAE International, 2021.
- [8] ISO, ISO 24089:2023 — Road vehicles — Software update engineering. Geneva, Switzerland: International Organization for Standardization, 2023.
- [9] OECD, The Governance of Regulators: Driving Performance at Regulatory Agencies. Paris, France: OECD Publishing, 2014.
- [10] OECD, International Regulatory Co-operation: The Role of International Organisations in Fostering Better Rules of Globalisation. Paris, France: OECD Publishing, 2016.
- [11] S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces," in Proceedings of the 20th USENIX Security Symposium, San Francisco, CA, USA, 2011.
- [12] K. Koscher et al., "Experimental security analysis of a modern automobile," in Proceedings of the IEEE Sympo-

sium on Security and Privacy, Oakland, CA, USA, 2010, pp. 447–462.

[13] SAE International, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, SAE J3016. Warrendale, PA, USA: SAE International, 2021.

[14] European Commission, Ethics of Connected and Automated Vehicles: Recommendations on Road Safety, Privacy, Fairness, Explainability and Responsibility. Brussels, Belgium: European Commission, 2020.

[15] ISO, ISO 34502:2022 — Road vehicles — Test scenarios for automated driving systems — Scenario-based safety evaluation framework. Geneva, Switzerland: International Organization for Standardization, 2022.

[16] ISO, ISO 21448:2022 — Road vehicles — Safety of the intended functionality. Geneva, Switzerland: International Organization for Standardization, 2022.

[17] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," Black Hat USA, 2015.

[18] OECD, Regulatory Policy Outlook 2021. Paris, France: OECD Publishing, 2021.

[19] United Nations Economic Commission for Europe, UN Regulation No. 156: Uniform provisions concerning the approval of vehicles with regard to software update and software updates management system, UNECE, Geneva.

[20] UNECE World Forum for Harmonization of Vehicle Regulations, Software update and software updates management system: Interpretation and implementation guidance under UN Regulation No. 156, UNECE WP.29 documentation.

[21] International Organization for Standardization, ISO 24089: Road vehicles — Software update engineering, ISO, Geneva.

[22] United Nations Economic Commission for Europe, UN Regulation No. 155: Uniform provisions concerning the approval of vehicles with regard to cyber security and cyber security management system, UNECE, Geneva.

[23] International Organization for Standardization and SAE International, ISO/SAE 21434: Road vehicles — Cybersecurity engineering, ISO/SAE.

[24] International Organization for Standardization, ISO 26262: Road vehicles — Functional safety, ISO, Geneva.

[25] International Organization for Standardization, ISO 21448: Road vehicles — Safety of the intended functionality, ISO, Geneva.

[26] European Parliament and Council of the European Union, Regulation (EU) 2018/858 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, Official Journal of the European Union, 2018.

[27] National Highway Traffic Safety Administration, Fed-

eral Motor Vehicle Safety Standards and Regulations, U.S. Department of Transportation, Washington, DC.

[28] National Highway Traffic Safety Administration, Cybersecurity Best Practices for the Safety of Modern Vehicles, U.S. Department of Transportation, Washington, DC.

Submit your manuscript to Advances in the standards and applied sciences journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Open Access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

**Submit your next manuscript at:
journal.standards.ac.ir**