Tag: #SUMS

27 June, 2025 · 5 mins read

Relationship between UN R155, UN R156 and ISO/SAE 21434, ISO 24089

As autonomous, connected vehicles evolve, so do risks associated with cybersecurity and software update management. Maintaining public safety being a top regulatory priority, certain regions like the European Union have introduced stringent compliance requirements for vehicle manufacturers and suppliers. Most notably, the UNECE Regulation No. 155 and UNECE Regulation No. 156 now mandate that automotive stakeholders demonstrate their ability to manage cyber risks and ensure secure software update processes.

To meet these legally binding requirements, industry players increasingly turn to internationally recognized standards such as ISO/SAE 21434 and ISO 24089 that delineate technical implementation measures. This blog post explores how ISO standards help translate UNECE requirements into actionable steps – focusing on the relationship between UN R155, UN R156 and technical standards, ISO/SAE 21434 and ISO 24089.

UN R155, UN R156 Regulation

As the name denotes, the UN R155, UN R156 “regulations” are legally binding requirements developed by UNECE WP.29, defining what must be done for vehicle type approval for passenger cars (M category), commercial vehicles (N category) and certain trailers (O category).

The foundational requirements for UN R155 and UN R156 differ based on their primary objectives. Under UN R155, vehicles with networked electronic components are required to establish a Cybersecurity Management System (CSMS), an organizational-level risk-management framework designed to maintain vehicle cybersecurity throughout the lifecycle. In contrast, UN R156 mandates the implementation of Software Update Management System (SUMS) for vehicles capable of receiving software updates, ensuring updates are secure, traceable and properly managed.

UN R155, UN R156: SYSTEM REQUIREMENTS

REGULATION	FOCUS	SYSTEM REQUIREMENTS
UN Regulation No. 155 (UN R155)	• Vehicle cybersecurity across the lifecycle	• Cybersecurity Management System (CSMS)
UN Regulation No. 156 (UN R156)	• Secure and auditable vehicle software update management	• Software Update Management System (SUMS)

While these regulations give guidance on what to do, how to execute the guidelines is not provided, which is where technical standards like ISO/SAE 21434 and ISO 24089 come into play as implementation blueprints.

ISO/SAE 21434, ISO 24089 Standard

Unlike “regulations,” ISO/SAE 21434 and ISO 24089 are voluntary “standards” developed by ISO and SAE working groups. While not legally binding, they are widely adopted as technical frameworks to demonstrate compliance with UNECE requirements.

ISO/SAE 21434 focuses on managing cybersecurity risks across the vehicle lifecycle, detailing methods for identifying, evaluating and mitigating threats. Aligned with UN R155 which mandates the establishment of a Cybersecurity Management System (CSMS), the standard outlines core system capabilities, including governance, resource management and organizational responsibility. While the UN R155 regulation defines what must be established for vehicle cybersecurity, the ISO/SAE 21434 standard provides the framework for how to implement it.

Similarly, the ISO 24089 standard centers on the secure management of software updates, ensuring both functional performance and cybersecurity integrity are maintained. Following the mandate of UN R156 to establish a Software Update Management System (SUMS), the standard illustrates methods for software configuration tracking, secure update delivery, and validated installation procedures. Parallel to the relationship between UN R155 and ISO 21434, the UN R156 regulation defines what components are required for secure software updates, while the ISO 24089 standard outlines how to structure it.

ISO/SAE 21434, ISO 24089 ROLE

Regulation	Focus	Certification Required	Main Supporting Standard
UN R155	Vehicle Cybersecurity	Cybersecurity Management System (CSMS)	**ISO/SAE 21434**
UN R156	Software Updates	Software Update Management System (SUMS)	**ISO 24089**

Mapping ISO Standards to Cybersecurity and Software Update Requirements

Although ISO/SAE 21434 and ISO 24089 were not legally derived from UN R155 and UN R156, they share a common foundation. Both the standards and regulations emerged from the same regulatory push to mitigate cybersecurity threats associated with increasingly software-driven vehicles, which explains their current alignment. However, due to natural overlaps between cybersecurity and software update management, it would be an oversimplification to claim that ISO/SAE 21434 solely supports UN R155, or vice-versa.

ISO/SAE 21434 Support for UN R156

While ISO/SAE 21434 is not specifically a software update standard, it addresses cybersecurity considerations that arise in software update processes, particularly where secure deployment and threat mitigation intersect. This can be observed in '*Clause 13. Operations and maintenance*' which covers cybersecurity activities during vehicle operation, including incident response, vulnerability monitoring, and post-production software updates. In this way, ISO/SAE 21434 partially supports components of a Software Update Management System (SUMS) relevant to UN R156, while primarily serving the requirements of UN R155.

ISO 24089 Support for UN R155

Similarly, ISO 24089, though not a cybersecurity standard, acknowledges the critical role of cybersecurity in software update workflows. For example, '*Clause 5. Project level*' outlines roles, responsibilities, and planning processes that overlap with Cybersecurity Management System (CSMS) framework principles. As such, ISO 24089 partially supports operational requirements of the Cybersecurity Management System (CSMS) aligned with UN R155, and cannot be viewed in isolation from cybersecurity needs.

Taken together, while ISO/SAE 21434 is closely aligned with UN R155 for cybersecurity control and ISO 24089 with UN R156 for software updates, the distinction between the two is not clear-cut. Given the interconnected nature of both domains, areas of overlap exist where the two standards work in tandem to support shared regulatory objectives.

Streamlining Automotive Compliance

While the range of standards and regulations in automotive cybersecurity may seem complex, understanding how they interconnect allows stakeholders to navigate compliance with greater clarity and control.

AUTOCRYPT's suite of in-vehicle cybersecurity solutions covering testing and consulting services is designed to align with the requirements of UN R155 and UN R156 and technical guidelines set by ISO/SAE 21434 and ISO 24089 standards. Supporting secure software update processes and cybersecurity control across the vehicle's lifecycle, our services are positioned to help simplify compliance and improve informed decision-making.

Visit our UNECE WP.29 Consulting page to learn more about how OEMs and Tier suppliers can control cybersecurity measures for vehicle type approval.

To contact our team about how your company can get started, contact global@autocrypt.io.

how we can work together.

Contact Us

Sewoo Building 1, 6-8F,
115, Yeouigongwon-ro
Yeongdeungpo-gu
Seoul, Korea

Sales: global@autocrypt.io
HR: info@autocrypt.io

Company

About Us

Careers

Resources

Downloads

Latest News

Blog

Newsletter

Solutions

AutoCrypt® IVS

AutoCrypt® V2X

AutoCrypt® PnC

Demo

SCMS Interoperability Test

PnC Cloud Test

Subscribe To Our Newsletter

Enter your email

Social Links

Terms & Conditions | Privacy Policy

Scroll to top