COMPLIANCE

A Cybersecurity Guide to Automotive Compliance: Understanding ISO/SAE 24089 and UNR156

July 21, 2025

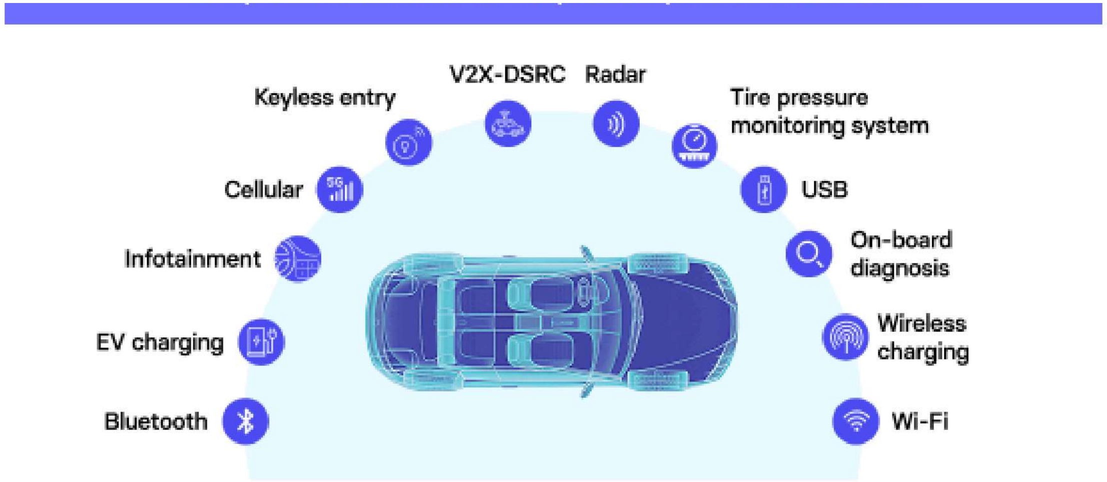
The automotive sector is undergoing a profound transformation. Vehicles today are increasingly defined by their software; connected cars, over-the-air (OTA) updates, and software-defined vehicles (SDVs) are becoming the norm rather than the exception.

These innovations create new functionality and user experiences, but they also expand the overall attack surface. This shift brings complex challenges securing dynamic codebases, maintaining update integrity across global supply chains, and ensuring resilience against evolving threats. Alongside technical change, of course, comes regulatory pressure. Governments and international bodies are mandating higher cybersecurity standards for automakers and suppliers. Regulations like UNR156 require clear proof that vehicles are being updated securely, while standards such as ISO/SAE 24089 set the bar for software update engineering.

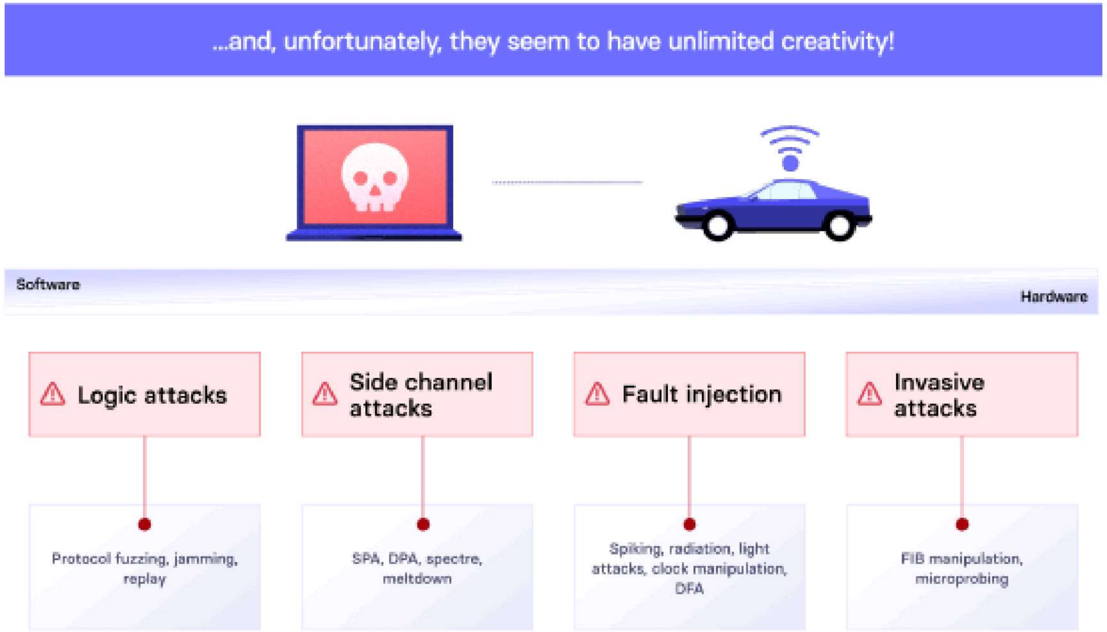
Cybersecurity standards in automotive matter

A structured software update process is no longer optional; it is integral to risk management. Updates must be planned, validated, deployed, and monitored with precision. This mirrors best practices in IT security management, where patch management and vulnerability remediation are foundational controls. Modern automotive supply chains introduce additional complexity, though. Vehicles often incorporate code and hardware from dozens of suppliers, including third-party libraries and modules. This makes comprehensive oversight challenging, as each component could introduce risk or complicate compliance obligations.

The consequences of vulnerabilities in automotive software are severe. Unlike in traditional IT systems, failures can affect safety-critical functions such as braking, steering, or autonomous driving features. Servers, at least, *tend* not to be cruising at highway speeds when they crash. A successful cyberattack could therefore have life-threatening consequences, placing even greater emphasis on rigorous update processes and secure engineering.



Attack scenarios



...and, unfortunately, they seem to have unlimited creativity!

Software

Hardware

Logic attacks	Side channel attacks	Fault injection	Invasive attacks
Protocol fuzzing, jamming, replay	SPA, DPA, spectre, meltdown	Spiking, radiation, light attacks, clock manipulation, DFA	FIB manipulation, microprobing

ISO/SAE 24089 is an international standard developed to provide a comprehensive framework for software update engineering in road vehicles. It serves as guidance to help organizations implement secure, reliable, and traceable software update practices. Unlike regulations that mandate outcomes, ISO/SAE 24089 focuses on defining processes and technical practices that contribute to a robust update management capability.

The scope of ISO/SAE 24089 covers the full lifecycle of software updates: planning, development, validation, execution, and post-deployment monitoring. This lifecycle approach ensures updates are not treated as isolated events but as part of a controlled, repeatable process. For MSPs and developers, this means integrating software update practices into existing secure development and operations pipelines, rather than bolting them on as an afterthought.

Among its key requirements are:

- **Software update management systems (SUMS):** ISO/SAE 24089 defines the structural elements of SUMS, including policies, roles, technical controls, and monitoring mechanisms that collectively govern the update process. SUMS must ensure updates are secure, reliable, and auditable.
- **Risk assessment and validation of update packages:** Before deployment, updates must undergo risk-based evaluation to determine their potential impact. This includes validating that the update achieves its intended function, does not introduce regressions or vulnerabilities, and meets safety requirements.

- **Secure delivery pipelines and update integrity protection:** ISO/SAE 24089 mandates cryptographic measures to protect update packages during delivery, ensuring authenticity and integrity. This typically involves signing update binaries and using secure communication channels for distribution.

ISO/SAE 24089 is closely related to ISO/SAE 21434, the automotive standard for cybersecurity risk management. While ISO/SAE 21434 focuses on identifying and managing risks across the vehicle lifecycle, ISO/SAE 24089 zooms in on the software update process as a critical control within that broader cybersecurity program.

What is UNR156 (UN Regulation No. 156)?

UNR156, issued by the UNECE, is a regulation that requires the implementation of Software Update Management Systems for all new vehicle types in markets that adopt UN vehicle regulations. Unlike ISO/SAE 24089, UNR156 is legally binding in these jurisdictions, and compliance is mandatory for type approval.

UNR156 applies globally wherever UN vehicle regulations are adopted, including the EU and many other regions. For automotive manufacturers and their IT and security partners, this means that non-compliance can directly block market access.

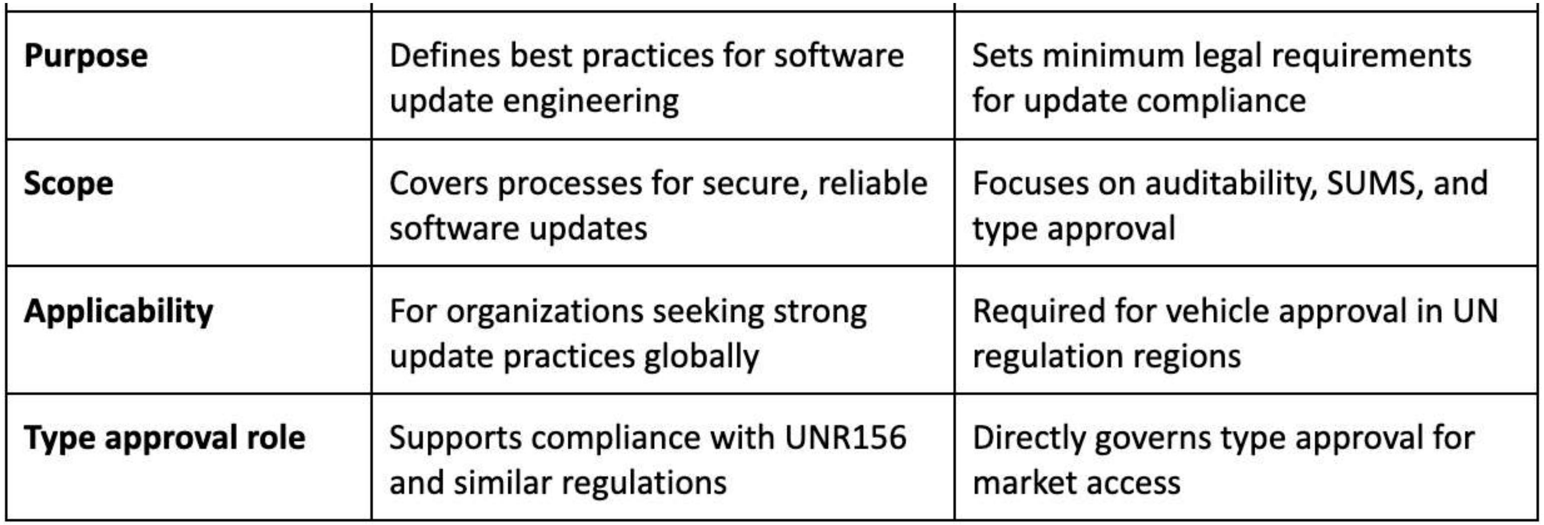
The core elements of UNR156 include:

- **Software update policies and procedures:** Organizations must establish formal documentation describing how updates are planned, approved, delivered, and monitored.

- **Vehicle-level and ECU-level update management:** UNR156 requires that updates be managed both at the level of the entire vehicle and at the level of individual electronic control units (ECUs), including ensuring compatibility and safety after updates.
- **Periodic compliance verification and type approval renewal:** Compliance with UNR156 is not a one-time event; manufacturers must demonstrate ongoing adherence to SUMS requirements to maintain type approval for their vehicles.

ISO 24089 vs. UNR156: Key differences and overlaps

ISO/SAE 24089 and UNR156 address the same goal – secure, reliable automotive software updates – but differ in purpose and application. While UNR156 sets legal requirements for type approval, ISO/SAE 24089 provides best practices to help meet these obligations. Both are essential for teams building compliant and resilient update processes.



Purpose	Defines best practices for software update engineering	Sets minimum legal requirements for update compliance
Scope	Covers processes for secure, reliable software updates	Focuses on auditability, SUMS, and type approval
Applicability	For organizations seeking strong update practices globally	Required for vehicle approval in UN regulation regions
Type approval role	Supports compliance with UNR156 and similar regulations	Directly governs type approval for market access

Together, these standards provide both the regulatory baseline (UNR156) and the technical framework (ISO/SAE 24089) needed to manage automotive software updates securely and effectively across complex supply chains.

Cybersecurity best practices: Here to help overcome ALL the challenges!

Defining secure software delivery pipelines is key to ensuring that updates remain tamper-proof. This involves embedding cryptographic signing, secure transport protocols, and validation checks at every stage of the delivery process. Cybersecurity teams can align their between security, legal, product, and operational teams ensures regulatory alignment and risk-informed decision-making throughout the update lifecycle.

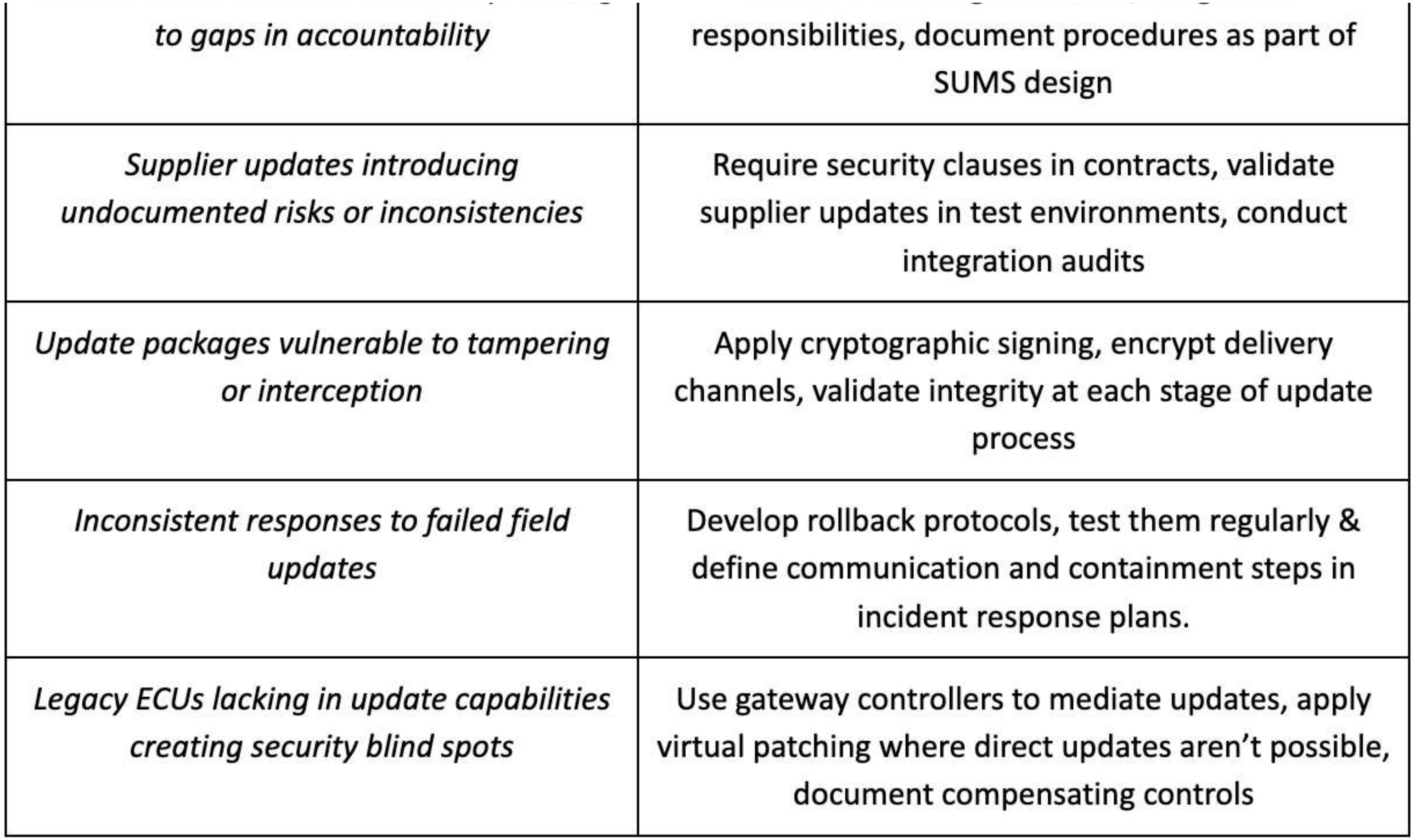
Compliance with ISO/SAE 21434 is foundational to these efforts. Threat modeling, risk assessments, and penetration testing should be applied not only to the base software but to the update mechanisms themselves, helping ensure updates do not inadvertently introduce vulnerabilities.

Important aspects to consider include:

- **Update validation and rollback testing:** Should be integral to the lifecycle, allowing organizations to detect failures quickly and restore systems to a known good state with minimal disruption.
- **Secure OTA infrastructure and resilient in-vehicle update logic:** Technical cornerstones for modern update programs. This includes layered protections such as trusted execution environments, encrypted storage, and runtime checks.
- **Audit-ready logging and lifecycle documentation:** Essential for both internal governance and external regulatory reviews. Security teams should ensure logs cover update approval, distribution, installation, and monitoring phases.

Ultimately, managing supplier updates and third-party code requires strong contractual controls, validated integration processes, and ongoing monitoring to ensure external components continue to meet the rigorous security and compliance expectations of the automotive industry.

operational, and organizational challenges. These obstacles can complicate compliance with standards like ISO/SAE 24089 and UNR156, and increase risk if left unaddressed. The table below illustrates how well-aligned cybersecurity best practices can help overcome each key challenge in a structured, effective way.



to gaps in accountability	responsibilities, document procedures as part of SUMS design
Supplier updates introducing undocumented risks or inconsistencies	Require security clauses in contracts, validate supplier updates in test environments, conduct integration audits
Update packages vulnerable to tampering or interception	Apply cryptographic signing, encrypt delivery channels, validate integrity at each stage of update process
Inconsistent responses to failed field updates	Develop rollback protocols, test them regularly & define communication and containment steps in incident response plans.
Legacy ECUs lacking in update capabilities creating security blind spots	Use gateway controllers to mediate updates, apply virtual patching where direct updates aren't possible, document compensating controls

These approaches not only mitigate risks but also support long-term resilience across complex automotive ecosystems.

Continuous monitoring, frequent updates, and an active security posture are essential to maintaining long-term trust in connected and autonomous vehicles. Organizations must integrate these practices into their operational rhythms rather than treating them as compliance checkboxes. Compliance with standards like ISO/SAE 24089 and regulations like UNR156 delivers long-term value: improved safety, uninterrupted market access, and strengthened brand reputation.

Achieving sustainable compliance and robust cybersecurity requires collaboration across disciplines. Security, legal, engineering, and operations must work together to maintain and evolve secure update practices. vRx by Vicarius can help you overcome these challenges by enabling and supporting teams as they build secure, compliant software update programs for modern vehicles - software that will have automated risk assessment, patch management, and virtual remediation fundamentally baked in.

Book a demo today to find out how we can keep you on track!

Sr. Product Marketing Manager

Share Articles

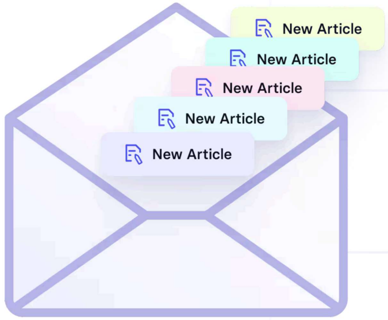
Subscribe for more

Get more infosec news and insights.

EMAIL*

SUBSCRIBE

By submitting this form, you agree that Vicarius will save your contact information to contact you about our products and services. Check out our Privacy Policy to learn about our privacy practices, commitments and how to unsubscribe.



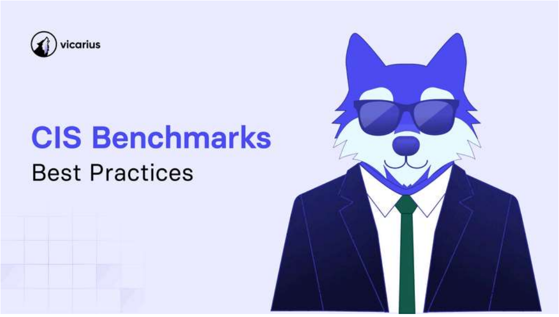
Related Posts

COMPLIANCE

Essential System Hardening Standards Ever...

System hardening may seem like a simple practice, but many neglect it...

May 20, 2025



COMPLIANCE

The CIS Benchmarking Best Practices: Turning...

Incorporating CIS Benchmarks offers more than a path to compliance; it...

May 15, 2025

COMPLIANCE

From Vulnerability Management to...

The Vicarius vRx Maturity Model helps you evolve from reactive...

May 13, 2025

vicarius SOLUTION CUSTOMERS PARTNERS PRICING RESOURCES COMPANY LOGIN REQUEST A DEMO

1000+ members

Turn security converstains into remediation actions

REQUEST A DEMO →

vicarius

AICPA SOC

GO TO

- PRICING
- CASE STUDIES
- SUPPORT
- COMPARE
- SITEMAP

COMPANY

- ABOUT US
- CAREER
- PARTNER PROGRAM

SOLUTION

- VULNERABILITY REMEDIATION
- VULNERABILITY MANAGEMENT

FEATURES

- VRX ANALYSIS
- ASSET MANAGEMENT
- SCRIPTING
- PATCHLESS PROTECTION
- AUTOMATION
- XTAGS
- APPS & OS COVERAGE
- PATCH MANAGEMENT

INDUSTRIES

- MANUFACTURING
- FINANCE
- GOVERNMENT
- SMALL BUSINESS
- HEALTHCARE
- EDUCATION

RESOURCES

- CVE RESEARCH
- APPS & OS PATCH CATALOG
- ARTICLES
- VICARIUS STUDIOS

VANALYZER

USER MANAGEMENT & TEAMS

COMPLIANCE ENGINE