SmartSuite

Framework / Cybersecurity / ISO Industry Standards

ISO/SAE 21434:2021

ISO/SAE 21434 is a cybersecurity engineering standard that defines processes to manage cyber risks across vehicle lifecycles and supply chains.

What it is

ISO/SAE 21434 is an international cybersecurity engineering standard for road vehicles that establishes requirements and processes to manage cyber risks throughout the lifecycle of automotive systems. Its primary goal is to help organizations identify, assess, and reduce cybersecurity threats that can impact vehicle safety, reliability, and data integrity.

Jointly published by the International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE), ISO/SAE 21434 is adopted by automotive manufacturers, suppliers, and cybersecurity teams. The standard covers the entire vehicle supply chain and lifecycle, focusing on security controls, risk management, vulnerability management, and incident response for both passenger and commercial vehicles.

At a glance

PUBLISHER International Organization for Standardization (ISO)	TYPE Framework	VERSION 2021
EFFECTIVE August 2021	DOMAIN Cybersecurity	FAMILY ISO Industry Standards
REGION International	INDUSTRY Automotive	ADOPTION MODEL Industry Requirement
IMPLEMENTATION COMPLEXITY High		

Source: https://www.iso.org/standard/70918.html

Why it matters

- **Strengthen cybersecurity risk management** Establish consistent processes to identify, evaluate, and mitigate cyber threats impacting vehicle safety and reliability.
- **Enhance regulatory alignment** Support compliance with global automotive regulations, including UNECE WP.29, by aligning internal controls with industry-recognized standards.
- **Improve incident response readiness** Enable structured vulnerability management and faster response to emerging cybersecurity incidents across connected automotive systems.
- **Increase audit readiness** Facilitate easier demonstration of effective cybersecurity controls during external audits and regulatory reviews.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ISO/SAE 21434

AI/Vehicle Cybersecurity Requirements Library

Manage lifecycle requirements, policies, and governance for vehicle cybersecurity.

TARA and Risk Traceability

Connect threats and risks to cybersecurity goals, requirements, and verification.

Supplier Security Oversight

Track supplier requirements, evidence, and ongoing compliance across the chain.

Verification, Validation, and Evidence

Store test plans/results and link evidence to specific security requirements.

Vulnerability and Incident Workflows

Manage disclosures, patches, and incident response processes across products.

Vehicle Program Reporting and Readiness

Report status, open risks, and readiness across vehicle programs and releases.

Common framework mappings

ISO 27001:2022 | ISO 27002:2022 | MITRE ATT&CK | NIST CSF 2.0 | UNECE R155

Official resources

ISO/SAE 21434 Standard

Defines cybersecurity requirements and processes for managing cyber risks in road vehicles.

iso.org/standard/70918.html

Frequently asked questions

What is ISO/SAE 21434 used for?

ISO/SAE 21434 is an international standard that establishes requirements and guidelines for managing cybersecurity risks throughout the lifecycle of road vehicles. Its main goal is to help automotive organizations identify, assess, and mitigate cyber threats that could impact vehicle safety, reliability, or data integrity.

Is compliance with ISO/SAE 21434 mandatory or certifiable?

ISO/SAE 21434 itself is not a mandatory regulatory requirement nor a certifiable standard in the traditional sense. However, aligning with its requirements supports compliance with regulatory obligations like UNECE WP.29 and can be audited to demonstrate due diligence in managing automotive cybersecurity risks.

Who does ISO/SAE 21434 apply to?

ISO/SAE 21434 applies to automotive manufacturers, suppliers, and other stakeholders involved in the design, development, production, operation, and decommissioning of road vehicles and their components. It covers both passenger and commercial vehicles across the supply chain.

What key concepts or artifacts are required by ISO/SAE 21434?

Key artifacts include documented cybersecurity risk assessments, threat and risk analysis (TARA), cybersecurity goals and requirements, evidence of risk treatment, vulnerability management records, and incident response procedures. These support governance, transparency, and traceability throughout the vehicle’s lifecycle.

How does the implementation process work for ISO/SAE 21434?

Implementation involves integrating security controls and risk management activities into each lifecycle phase of the vehicle, conducting continuous threat analysis, validating technical and organizational measures, and maintaining documentation for audit trails. Teams should establish clear processes for collaboration between engineering, IT, and compliance functions.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What is the relationship between ISO/SAE 21434 and other automotive regulations or standards?

ISO/SAE 21434 is closely aligned with regulatory programs such as UNECE WP.29, which mandates automotive cybersecurity management. It complements other standards like ISO 26262 (Functional Safety) by focusing specifically on cyber risk, while ISO/SAE 21434 covers broader system and supply-chain security requirements.

What ongoing compliance activities are required under ISO/SAE 21434?

Organizations must maintain regular risk assessments, update vulnerability management practices, perform compliance reviews, and document incident response actions. Monitoring for emerging threats and continuous improvement of controls are central to sustaining compliance with ISO/SAE 21434.

How would SmartSuite support ISO/SAE 21434?

SmartSuite assists with ISO/SAE 21434 by providing risk tracking, pre-built control management libraries, and streamlined evidence collection tailored to automotive cybersecurity requirements. Its features enable compliance tracking, remediation workflows, audit readiness, and automated reporting to help organizations manage ongoing regulatory compliance and program maturity.

License included / downloadable: No ISO/SAE 21434 must be purchased via the ISO/SAE standards catalog. License not included with platform

Full framework page and mappings: smartsuite.com/frameworks/iso-sae-21434-road-vehicles-cybersecurity-engineering