SmartSuite

Framework / Cybersecurity / ISO Industry Standards

ISO/SAE 21434:2021

ISO/SAE 21434:2021 specifies engineering requirements for cybersecurity risk management across the life of road vehicle electrical and electronic systems, from concept to decommissioning.



What it is

ISO/SAE 21434:2021 is the international standard that specifies engineering requirements for cybersecurity risk management across the concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces. ISO/TC 22/SC 32 and the SAE Vehicle Cybersecurity Systems Engineering Committee prepared it jointly, and ISO published the first edition on August 31, 2021. It cancels and supersedes SAE J3061:2016.

At a glance

PUBLISHER International Organization for Standardization (ISO) and SAE International	TYPE Framework	VERSION ISO/SAE 21434:2021 (first edition)
EFFECTIVE August 31, 2021	DOMAIN Cybersecurity	FAMILY ISO Industry Standards
REGION International	INDUSTRY Automotive	ADOPTION MODEL Voluntary
IMPLEMENTATION COMPLEXITY High		

Source: iso.org/standard/70918.html

Why it matters

- **One vocabulary across the supply chain** Defined terms such as item, component, asset, damage scenario and cybersecurity goal let a vehicle maker and a supplier describe the same risk the same way.
- **A clear split of responsibility** Clause 7 assigns responsibilities for cybersecurity activities between customer and supplier, recorded in a cybersecurity interface agreement.
- **Risk managed across the whole life** Clauses 9 to 14 run from concept through product development, validation, production and operations to end of cybersecurity support and decommissioning.
- **Traceable evidence** Work products, identified as WP, are the results of cybersecurity activities that fulfill one or more requirements.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ISO/SAE 21434

Requirements by Clause

Hold the provisions and work products of clauses 5 to 15 in Compliance Management as requirements with owners, status and linked evidence.

Threat and Risk Register

Record threats and risks for each item in Cyber & IT Risk with the treatment decision and the controls that modify the risk (clause 15).

Vulnerability Tracking

Track vulnerabilities and their remediation in Cyber & IT Risk through to end of cybersecurity support (clause 8).

Supplier Oversight

Assess and monitor suppliers in Third Party Risk Management and keep each cybersecurity interface agreement on record (clause 7).

Verification and Validation Evidence

Attach test results to the requirements they verify or validate, so the evidence behind a cybersecurity case stays linked (clauses 10 and 11).

Audits and Remediation

Plan and run audits of cybersecurity processes in Internal Audit Management and track remediation to closure.

Common framework mappings

IEC 62443 | 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 and when was it published?

ISO/SAE 21434:2021 is the international standard for road vehicle cybersecurity engineering. Clause 1 specifies engineering requirements for cybersecurity risk management of E/E systems in road vehicles, from concept to decommissioning. ISO published the first edition on August 31, 2021, and it cancels and supersedes SAE J3061:2016.

Does UN Regulation No. 155 require ISO/SAE 21434?

No. UN Regulation No. 155, in force since January 22, 2021, requires a vehicle manufacturer to hold a valid Certificate of Compliance for a cybersecurity management system (paragraph 7.3.1). It lists ISO/SAE 21434 only as an example in a footnote to paragraph 5.3.1(a), on the competence of approval authorities. The standard supports a cybersecurity management system but is not named as the way to comply.

What do clauses 5 to 15 cover?

Clause 5 is organizational cybersecurity management, 6 project dependent management, 7 distributed cybersecurity activities between customer and supplier, and 8 continual activities including vulnerability management. Clauses 9 to 14 follow the item: concept, product development, cybersecurity validation, production, operations and maintenance, and end of support and decommissioning. Clause 15 holds the threat analysis and risk assessment (TARA) methods.

Can a company be certified to ISO/SAE 21434?

The standard sets engineering requirements and its scope (clause 1) does not define a certification scheme. The certificate named in UN Regulation No. 155 is the Certificate of Compliance for a cybersecurity management system, issued by an approval authority under paragraph 6. ISO/PAS 5112:2022 gives guidelines for auditing a cybersecurity management system whose elements are based on the processes of ISO/SAE 21434.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Is a new edition of ISO/SAE 21434 coming?

ISO lists a systematic review of the standard that closed on October 2, 2026 with the outcome "to be revised" (stage 90.92), and shows a replacement project, ISO/SAE AWI 21434, as under development. No publication date is given, so the 2021 first edition remains the current edition.

License included / downloadable: No ISO/SAE 21434:2021 is a copyrighted ISO and SAE International publication that is sold by ISO, SAE and national standards bodies; the platform links to the official catalog record and does not reproduce the standard.

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