PUBLICLY AVAILABLE SPECIFICATION

ISO/PAS 5112

First edition
2022-03

Road vehicles — Guidelines for auditing cybersecurity engineering

Véhicules routiers — Lignes directrices pour l'audit de l'ingénierie de la cybersécurité

Reference number
ISO/PAS 5112:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 32, *Electrical and electronic components and general system aspects*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document is related to ISO/SAE 21434 *Road vehicles — Cybersecurity engineering* and extends ISO 19011 *Guidelines for auditing management systems* to the automotive domain.

This document is intended for organizations involved in automotive cybersecurity engineering in any part of the automotive supply chain and for organizations needing to conduct audits. This document can be used for audits of varying scope.

This document is adapted to fit the scope of an automotive cybersecurity engineering audit programme. Cybersecurity audits in this document are aimed at cybersecurity activities at the organizational level. While results from past projects can be used as evidence for implemented and applied processes, the project and product levels are not in the focus of this document.

This document provides guidelines on the management of an audit programme, on the planning and conducting of management system audits, as well as on the competence and evaluation of an audit team. An audit can be conducted against a range of audit criteria. This document gives a set of audit criteria based on ISO/SAE 21434 objectives. In addition, Annex A contains an example questionnaire that can be adapted.

This document can be used for internal audits (first party), for audits conducted by organizations on their external parties (second party) and for external audits conducted by third parties (e.g. for the purpose of certification). This document can also be useful to organizations involved in auditor training or personnel certification.

Road vehicles — Guidelines for auditing cybersecurity engineering

1 Scope

In addition to the guidelines in ISO 19011, this document provides guidelines to organizations that contribute to the achievement of road vehicle cybersecurity throughout the supply chain on:

- managing an audit programme for a cybersecurity management system (CSMS);
- conducting organizational CSMS audits;
- competencies of CSMS auditors; and
- providing evidence during CSMS audits.

Elements of the CSMS are based on the processes described in ISO/SAE 21434. This document is applicable to those needing to understand or conduct internal or external audits of a CSMS or to manage a CSMS audit programme.

This document does not provide guidelines on cybersecurity assessments.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/SAE 21434:2021, *Road vehicles — Cybersecurity engineering*

ISO 19011:2018, *Guidelines for auditing management systems*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/SAE 21434, ISO 19011 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1
audit
examination of a process to determine the extent to which the process objectives are achieved

Note 1 to entry: “Audit” is defined in ISO 19011 and ISO/SAE 21434. The definition of ISO/SAE 21434 is used in this document to support compatibility between this document and ISO/SAE 21434.

[SOURCE: ISO/SAE 21434:2021, 3.1.6, modified — Note 1 to entry has been added.]

3.2
cybersecurity management system
CSMS
systematic risk-based approach defining organisational processes, responsibilities and governance to manage *risk* (3.3) associated with threats to road vehicles and protect them from threats

[SOURCE: Reference [9], 2.3, modified — added “road” to clarify application domain, replaced “treat” with “manage”, removed “cyber”, replaced “cyber attacks” with “threats”.]

3.3
risk
cybersecurity risk
effect of uncertainty on road vehicle cybersecurity expressed in terms of attack feasibility and impact

Note 1 to entry: ISO 19011 uses a broader definition of the term risk.

[SOURCE: ISO/SAE 21434:2021, 3.1.29, modified — Note 1 to entry has been added.]

3.4
supply chain
set of organizations with a linked set of resources and processes, each of which acts as a customer, supplier, or both to form successive supplier relationships established upon placement of a purchase order, agreement, or other formal sourcing agreement.

Note 1 to entry: A supply chain includes organizations involved in the manufacturing, design and development of vehicles, or service providers involved in the operation, management, and delivery of services.

Note 2 to entry: The supply chain view is relative to the position of the customer.

[SOURCE: ISO/IEC 27036-1:2021, 3.10, modified — “acquirer” replaced by “customer" and Note 1 to entry has been modified.]

4 Principles of auditing

The principles of auditing of ISO 19011:2018, Clause 4 apply. In addition, the following guidance applies.

The guidelines given in this document are aimed at what ISO/SAE 21434 defines as an organizational cybersecurity audit. Product level topics are not in the scope of this document. Regarding products, a cybersecurity assessment based on ISO/SAE 21434 is used to judge the cybersecurity of the item or component.

5 Managing an audit programme

5.1 General

The guidelines of ISO 19011:2018, 5.1 apply.

5.2 Establishing audit programme objectives

The guidelines of ISO 19011:2018, 5.2 apply. In addition, the following guidance applies.

The audit programme objectives can be based on consideration of the following:

a) demonstration of the achievement of the objectives of ISO/SAE 21434;

b) specific cybersecurity risks associated with the auditee's products;

c) specifics related to the organization’s role in the automotive supply chain; and

EXAMPLE 1 An organization’s role can be original equipment manufacturer (OEM), tier 1 supplier, tier 2 supplier, component manufacturer.

NOTE Organizations in the supply chain include organizations which develop components out of context, e.g. before the placement of a purchase order, agreement, or other formal sourcing agreement.

d) clarification of whether the audit includes an evaluation of methods applied in the CSMS processes.

EXAMPLE 2 Specific audit programme objectives can include:

- verification of conformity of the CSMS with relevant legal and contractual requirements;
- obtaining and maintaining confidence in the auditee’s CSMS to identify, analyse and evaluate the cybersecurity risk and to take corresponding necessary action; and
- evaluating the effectiveness of the CSMS to address cybersecurity risks.

5.3 Determining and evaluating audit programme risks and opportunities

The guidelines of ISO 19011:2018, 5.3 apply.

5.4 Establishing the audit programme

5.4.1 Roles and responsibilities of the individual(s) managing the audit programme

The guidelines of ISO 19011:2018, 5.4.1 apply.

5.4.2 Competence of individual(s) managing audit programme

The guidelines of ISO 19011:2018, 5.4.2 apply. In addition, the following guidance applies.

The individual(s) managing the CSMS audit programme should have the following competences:

a) knowledge of the standards regarding cybersecurity that are used by the auditee to establish and maintain the CSMS;

b) knowledge of the general processes used by the automotive industry that are relevant for the phase of the cybersecurity lifecycle which is evaluated within the specific scope of the audit (e.g. processes for software development in the automotive domain);

c) ability to map the organization-specific processes, guidelines and rules with the audit criteria; and

d) if a combined audit is conducted, the ability to coordinate with other management system audit programmes.

EXAMPLE A combined audit with IATF 16949[8].

NOTE Considered competence can also include experience in audit or assessment of automotive processes based on automotive standards or guidelines, e.g. IATF 16949 [8], ISO 9001[2], the ISO 26262 series[5], ASPICE[10].

5.4.3 Establishing extent of audit programme

The guidelines of ISO 19011:2018, 5.4.3 apply. In addition, the following guidance applies.

The extent of an audit programme can vary and can be impacted by the following factors:

a) size of the auditee and extent to which the auditee is involved in cybersecurity processes;

b) the cybersecurity-related supply chain and determination of which entities in the supply chain are in scope; and

c) importance of preserving cybersecurity property of information within the scope of the cybersecurity processes.

5.4.4 Determining audit programme resources

The guidelines of ISO 19011:2018, 5.4.4 apply.

5.5 Implementing audit programme

5.5.1 General

The guidelines of ISO 19011:2018, 5.5.1 apply.

5.5.2 Defining the objectives, scope and criteria for an individual audit

The guidelines of ISO 19011:2018, 5.5.2 apply. In addition, the following guidance applies.

The audit scope should include the CSMS processes used by the auditee during the phases of the cybersecurity lifecycle that are within the specific scope of the audit.

EXAMPLE 1 A tier 2 supplier might not be audited for all phases of the cybersecurity lifecycle.

The audit criteria should be defined following 6.4.8 and 6.4.9.

The audit scope may include the whole organization or one or more clearly delineated organizational units.

NOTE 1 Clearly delineated organizational units are those that have separate organizational structures and processes.

If the CSMS process depends on interactions with other organizational processes, the interfaces and dependencies should be identified.

NOTE 2 Interfaces can include how work products are exchanged.

Shared functions outside the organization may be included in the scope of the audit with clearly defined interfaces. If an organization depends on another organization to achieve the objectives of CSMS processes, the contributing organization should be identified. The extent to which the organization manages the dependencies on external organizations to realize its CSMS should be determined.

Distributed cybersecurity activities, defined in a cybersecurity interface agreement, may be included in the scope of the audit.

EXAMPLE 2 Cybersecurity monitoring and cybersecurity incident response.

The audit objectives can include the confirmation of the suitability of the implemented processes and applied methods and criteria to achieve the objectives of ISO/SAE 21434.

The auditee may perform an internal audit to identify and resolve shortcomings in the CSMS before an external audit is conducted. If an external audit is planned as part of the audit programme, the scope and objectives of both internal and external audits should be aligned.

A subsequent follow-up audit to address identified minor non-conformities of a conditionally-passed audit may focus solely on the identified deficiencies noted.

5.5.3 Selecting and determining audit methods

The guidelines of ISO 19011:2018, 5.5.3 apply.

5.5.4 Selecting audit team members

The guidelines of ISO 19011:2018, 5.5.4 apply.

5.5.5 Assigning responsibility for an individual audit to the audit team leader

The guidelines of ISO 19011:2018, 5.5.5 apply.

5.5.6 Managing audit programme results

The guidelines of ISO 19011:2018, 5.5.6 apply.

5.5.7 Managing and maintaining audit programme records

The guidelines of ISO 19011:2018, 5.5.7 apply.

5.6 Monitoring audit programme

The guidelines of ISO 19011:2018, 5.6 apply.

5.7 Reviewing and improving audit programme

The guidelines of ISO 19011:2018, 5.7 apply.

6 Conducting an audit

6.1 General

The guidelines of ISO 19011:2018, 6.1 apply.

6.2 Initiating audit

6.2.1 General

The guidelines of ISO 19011:2018, 6.2.1 apply.

6.2.2 Establishing contact with auditee

The guidelines of ISO 19011:2018, 6.2.2 apply. In addition, the following guidance applies.

Auditor and auditee should mutually agree on information that is not to be disclosed.

Information can be classified as confidential and sensitive. Access to such information can be limited to selected audit team members.

EXAMPLE Documents can only be viewed in an area controlled by the auditee. Transfer and processing of the documents outside this environment is prohibited.

6.2.3 Determining feasibility of audit

The guidelines of ISO 19011:2018, 6.2.3 apply.

6.3 Preparing audit activities

6.3.1 Performing review of documented information

The guidelines of ISO 19011:2018, 6.3.1 apply.