INTERNATIONAL STANDARD

ISO/SAE 21434

First edition
2021-08

Road vehicles — Cybersecurity engineering

Véhicules routiers — Ingénierie de la cybersécurité

Reference number
ISO/SAE 21434:2021(E)

Documents
Document Sharing Hub

© ISO/SAE International 2021

Full document details: ISO SAE 21434-2021

COPYRIGHT PROTECTED DOCUMENT

© ISO/SAE International 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced, or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO or SAE International at the respective address below or ISO's member body in the country of the requester.

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

SAE International
400 Commonwealth Dr.
Warrendale, PA, USA 15096
Phone: 877-606-7323 (inside USA and Canada)
Phone: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
Website: www.sae.org

Published in Switzerland by ISO, published in the USA by SAE International

Documents
Document Sharing Hub

© ISO/SAE International 2021 – All rights reserved

Full document details: ISO SAE 21434-2021

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.

SAE International is a global association of more than 128,000 engineers and related technical experts in the aerospace, automotive and commercial-vehicle industries. Standards from SAE International are used to advance mobility engineering throughout the world. The SAE Technical Standards Development Program is among the organization's primary provisions to those mobility industries it serves aerospace, automotive, and commercial vehicle. These works are authorized, revised, and maintained by the volunteer efforts of more than 9,000 engineers, and other qualified professionals from around the world. SAE subject matter experts act as individuals in the standards process, not as representatives of their organizations. Thus, SAE standards represent optimal technical content developed in a transparent, open, and collaborative process.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1 and the SAE Technical Standards Board Policy. 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 and SAE International 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).

SAE Technical Standards Board Rules provide that: “This document is published to advance the state of technical and engineering sciences. The use of this document is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user.”

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 jointly prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 32, *Electrical and electronic components and general system aspects*, and SAE TEVEES18A *Vehicle Cybersecurity Systems Engineering Committee*.

This first edition of ISO/SAE 21434 cancels and supersedes SAE J3061:2016[37].

The main changes are as follows:

— complete rework of contents and structure.

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. Alternatively, to provide feedback on this document, please visit https://www. sae. org/standards/content/ISO/SAE 21434/.

© ISO/SAE International 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

Introduction

Purpose of this document

This document addresses the cybersecurity perspective in engineering of electrical and electronic (E/E) systems within road vehicles. By ensuring appropriate consideration of cybersecurity, this document aims to enable the engineering of E/E systems to keep up with state-of-the-art technology and evolving attack methods.

This document provides vocabulary, objectives, requirements and guidelines related to cybersecurity engineering as a foundation for common understanding throughout the supply chain. This enables organizations to:

— define cybersecurity policies and processes;

— manage cybersecurity risk; and

— foster a cybersecurity culture.

This document can be used to implement a cybersecurity management system including cybersecurity risk management.

Organization of this document

An overview of the document structure is given in Figure 1. The elements of Figure 1 do not prescribe an execution sequence of the individual topics.

© ISO/SAE International 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

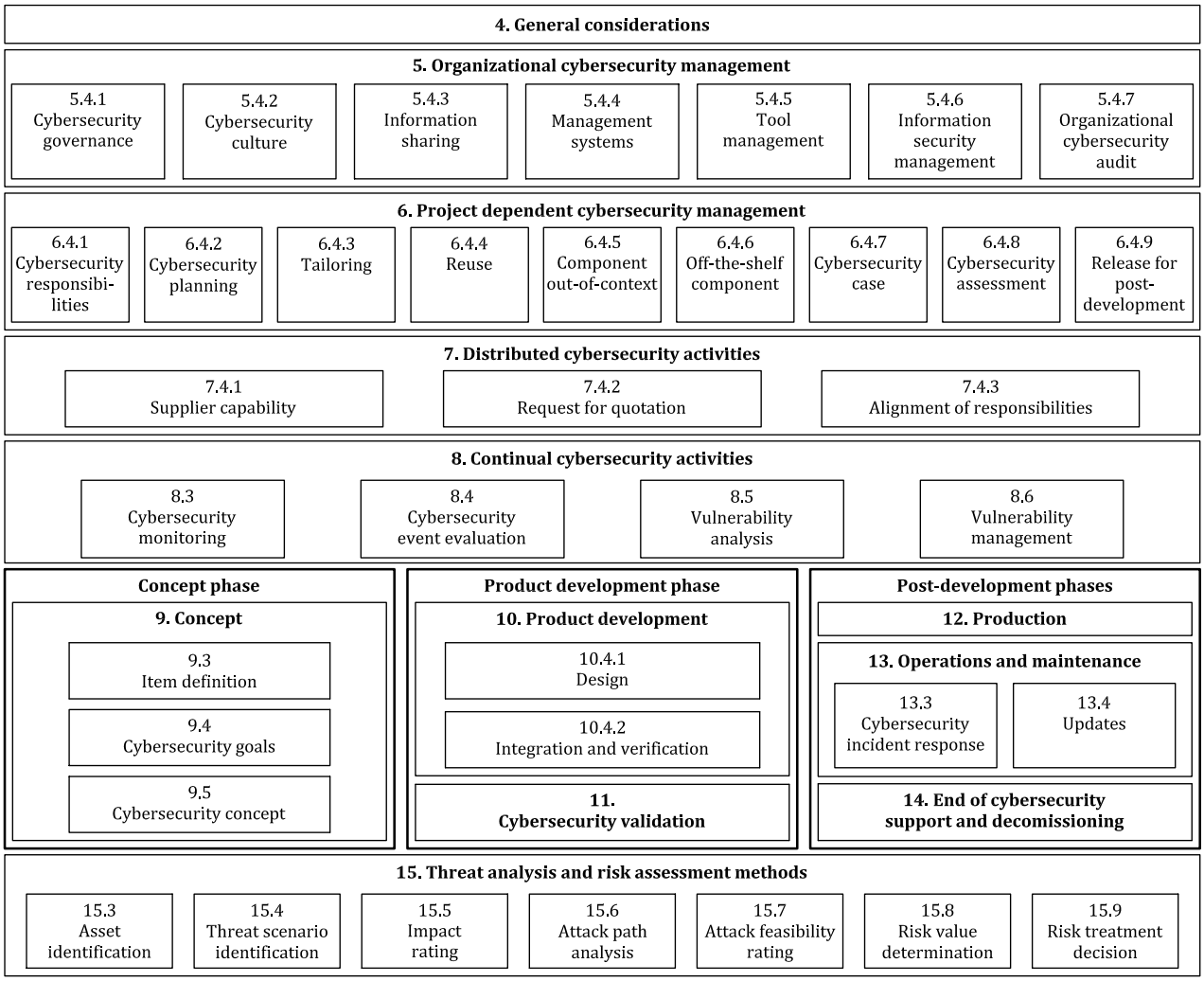


Figure 1 — Overview of this document

Clause 4 (General considerations) is informational and includes the context and perspective of the approach to road vehicle cybersecurity engineering taken in this document.

Clause 5 (Organizational cybersecurity management) includes the cybersecurity management and specification of the organizational cybersecurity policies, rules and processes.

Clause 6 (Project dependent cybersecurity management) includes the cybersecurity management and cybersecurity activities at the project level.

Clause 7 (Distributed cybersecurity activities) includes requirements for assigning responsibilities for cybersecurity activities between customer and supplier.

Clause 8 (Continual cybersecurity activities) includes activities that provide information for ongoing risk assessments and defines vulnerability management of E/E systems until end of cybersecurity support.

Clause 9 (Concept) includes activities that determine cybersecurity risks, cybersecurity goals and cybersecurity requirements for an item.

Clause 10 (Product development) includes activities that define the cybersecurity specifications, and implement and verify cybersecurity requirements.

Clause 11 (Cybersecurity validation) includes the cybersecurity validation of an item at the vehicle level.

© ISO/SAE International 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

Clause 12 (Production) includes the cybersecurity-related aspects of manufacturing and assembly of an item or component.

Clause 13 (Operations and maintenance) includes activities related to cybersecurity incident response and updates to an item or component.

Clause 14 (End of cybersecurity support and decommissioning) includes cybersecurity considerations for end of support and decommissioning of an item or component.

Clause 15 (Threat analysis and risk assessment methods) includes modular methods for analysis and assessment to determine the extent of cybersecurity risk so that treatment can be pursued.

Clauses 5 through 15 have their own objectives, provisions (i.e. requirements, recommendations, permissions) and work products. Work products are the results of cybersecurity activities that fulfil one or more associated requirements.

“Prerequisites” are mandatory inputs consisting of work products from a previous phase. “Further supporting information” is information that can be considered, which can be made available by sources that are different from the persons responsible for the cybersecurity activities.

A summary of cybersecurity activities and work products can be found in Annex A.

Provisions and work products are assigned unique identifiers consisting of a two-letter abbreviation (“RQ” for a requirement, “RC” for a recommendation, “PM” for a permission and “WP” for a work product), followed by two numbers, separated by hyphens. The first number refers to the clause, and the second gives the order in the consecutive sequence of provisions or work products, respectively, of that clause. For example, [RQ-05-14] refers to the 14th provision in Clause 5, which is a requirement.

© ISO/SAE International 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

Road vehicles — Cybersecurity engineering

1 Scope

This document specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces.

A framework is defined that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risk.

This document is applicable to series production road vehicle E/E systems, including their components and interfaces, whose development or modification began after the publication of this document.

This document does not prescribe specific technology or solutions related to cybersecurity.

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 26262-3:2018, *Road vehicles — Functional safety — Part 3: Concept phase*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological 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/

3.1.1
architectural design
representation that allows for identification of *components* (3.1.7), their boundaries, interfaces and interactions

3.1.2
asset
object that has value, or contributes to value

Note 1 to entry: An asset has one or more *cybersecurity properties* (3.1.20) whose compromise can lead to one or more *damage scenarios* (3.1.22).

3.1.3
attack feasibility
attribute of an *attack path* (3.1.4) describing the ease of successfully carrying out the corresponding set of actions

© ISO/SAE International 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

3.1.4
attack path
attack
set of deliberate actions to realize a *threat scenario* (3.1.33)

3.1.5
attacker
person, group, or organization that carries out an *attack path* (3.1.4)

3.1.6
audit
examination of a process to determine the extent to which the process objectives are achieved

[SOURCE: ISO 26262-1:2018 [1], 3.5, modified — The phrase “with regard to” was substituted by "to determine the extent to which" and "are achieved" was added.]

3.1.7
component
part that is logically and technically separable

3.1.8
customer
person or organization that receives a service or product

[SOURCE: ISO 9000:2015 [2], 3.2.4, modified — The phrase “could or does receive” was replaced by “receives”, the phrase “that is intended for or required by this person or organization” was omitted, and the example and note 1 to entry were omitted.]

3.1.9
cybersecurity
road vehicle cybersecurity
condition in which *assets* (3.1.2) are sufficiently protected against *threat scenarios* (3.1.33) to *items* (3.1.25) of road vehicles, their functions and their electrical or electronic *components* (3.1.7)

Note 1 to entry: In this document, for the sake of brevity, the term cybersecurity is used instead of road vehicle cybersecurity.

3.1.10
cybersecurity assessment
judgement of *cybersecurity* (3.1.9)

3.1.11
cybersecurity case
structured argument supported by evidence to state that *risks* (3.1.29) are not unreasonable

3.1.12
cybersecurity claim
statement about a *risk* (3.1.29)

Note 1 to entry: The cybersecurity claim can include a justification for retaining or sharing the risk.

3.1.13
cybersecurity concept
cybersecurity requirements of the *item* (3.1.25) and requirements on the *operational environment* (3.1.26), with associated information on *cybersecurity controls* (3.1.14)

3.1.14
cybersecurity control
measure that is modifying *risk* (3.1.29)

[SOURCE: ISO 31000:2018 [3], 3.8, modified — The word "cybersecurity" was added to the term, the phrase “maintains and/or” was deleted, the notes to entry were deleted.]

© ISO/SAE International 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

3.1.15
cybersecurity event
cybersecurity information (3.1.18) that is relevant for an *item* (3.1.25) or *component* (3.1.7)

3.1.16
cybersecurity goal
concept-level cybersecurity requirement associated with one or more *threat scenarios* (3.1.33)

3.1.17
cybersecurity incident
situation in the field that can involve *vulnerability* (3.1.38) exploitation

3.1.18
cybersecurity information
information with regard to *cybersecurity* (3.1.9) for which relevance is not yet determined

3.1.19
cybersecurity interface agreement
agreement between *customer* (3.1.8) and supplier concerning *distributed cybersecurity activities* (3.1.23)

3.1.20
cybersecurity property
attribute that can be worth protecting

Note 1 to entry: Attributes include confidentiality, integrity and/or availability.

3.1.21
cybersecurity specification
cybersecurity requirements and corresponding *architectural design* (3.1.1)

3.1.22
damage scenario
adverse consequence involving a vehicle or vehicle function and affecting a *road user* (3.1.31)

3.1.23
distributed cybersecurity activities
cybersecurity activities for the *item* (3.1.25) or *component* (3.1.7) whose responsibilities are distributed between *customer* (3.1.8) and supplier

3.1.24
impact
estimate of magnitude of damage or physical harm from a *damage scenario* (3.1.22)

3.1.25
item
component or set of *components* (3.1.7) that implements a function at the vehicle level

Note 1 to entry: A system can be an item if it implements a function at the vehicle level, otherwise it is a component.

[SOURCE: ISO 26262-1:2018 [1], 3.8, modified — The term “system” has been replaced by “component”, the phrases “to which ISO 26262 is applied” and “or part of a function” have been omitted and the Note 1 to entry has been replaced.]

3.1.26
operational environment
context considering interactions in operational use

Note 1 to entry: Operational use of an *item* (3.1.25) or a *component* (3.1.7) can include use in a vehicle function, in production, and/or in service and repair.

© ISO/SAE International 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

3.1.27
out-of-context
not developed in the context of a specific *item* (3.1.25)

EXAMPLE Processing unit with assumed cybersecurity requirements to be integrated in different items.

3.1.28
penetration testing
cybersecurity testing in which real-world attacks are mimicked to identify ways to compromise *cybersecurity goals* (3.1.16)

3.1.29
risk
cybersecurity risk
effect of uncertainty on *road vehicle cybersecurity* (3.1.9) expressed in terms of *attack feasibility* (3.1.3) and *impact* (3.1.24)

3.1.30
risk management
coordinated activities to direct and control an organization with regard to *risk* (3.1.29)

[SOURCE: ISO 31000:2018 [3], 3.2]

3.1.31
road user
person who uses a road

EXAMPLE Passenger, pedestrian, cyclist, motorist, or vehicle owner.

3.1.32
tailor, verb
to omit or perform an activity in a different manner compared to its description in this document

3.1.33
threat scenario
potential cause of compromise of *cybersecurity properties* (3.1.20) of one or more *assets* (3.1.2) in order to realize a *damage scenario* (3.1.22)

3.1.34
triage
analysis to determine the relevance of *cybersecurity information* (3.1.18) to an *item* (3.1.25) or *component* (3.1.7)

3.1.35
trigger
criterion for *triage* (3.1.34)

3.1.36
validation
confirmation, through the provision of objective evidence, that the *cybersecurity goals* (3.1.16) of the *item* (3.1.25) are adequate and are achieved

[SOURCE: ISO/IEC/IEEE 15288:2015 [4], 4.1.53, modified — The phrase “requirements for a specific intended use or application have been fulfilled” has been replaced by “cybersecurity goals of the item are adequate and are achieved”, note 1 to entry has been omitted.]

3.1.37
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

[SOURCE: ISO/IEC/IEEE 15288:2015 [4], 4.1.54, modified — The note 1 to entry has been omitted.]

© ISO/SAE International 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

3.1.38
vulnerability
weakness (3.1.40) that can be exploited as part of an *attack path* (3.1.4)

[SOURCE: ISO/IEC 27000:2018 [5], 3.77, modified — The phrase "of an asset or control" has been omitted; the phrase "by one or more threats" has been replaced by "as part of an attack path".]

3.1.39
vulnerability analysis
systematic identification and evaluation of *vulnerabilities* (3.1.38)

3.1.40
weakness
defect or characteristic that can lead to undesirable behaviour

EXAMPLE 1 Missing requirement or specification.

EXAMPLE 2 Architectural or design flaw, including incorrect design of a security protocol.

EXAMPLE 3 Implementation weakness, including hardware and software defect, incorrect implementation of a security protocol.

EXAMPLE 4 Flaw in the operational process or procedure, including misuse and inadequate user training.

EXAMPLE 5 Use of an outdated or deprecated function, including cryptographic algorithms.

3.2 Abbreviated terms

CAL	cybersecurity assurance level
CVSS	common vulnerability scoring system
E/E	electrical and electronic
ECU	electronic control unit
OBD	on-board diagnostic
OEM	original equipment manufacturer
PM	permission
RC	recommendation
RQ	requirement
RASIC	responsible, accountable, supporting, informed, consulted
TARA	threat analysis and risk assessment
WP	work product

4 General considerations

An item comprises all electronic equipment and software (i.e. its components) in a vehicle involved in the realization of a specific functionality at vehicle level, e.g. braking. An item or a component interacts with its operational environment.

The application of this document is limited to cybersecurity-relevant items and components of a series production road vehicle (i.e. not a prototype) including aftermarket and service parts. Systems external

© ISO/SAE International 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

to the vehicle (e.g. back-end servers) can be considered for cybersecurity purposes but are not in the scope of this document.

This document describes cybersecurity engineering from the perspective of a single item. The suitable allocation of functionality to items within the E/E architecture of a road vehicle is not specified in this document. For the vehicle as a whole, the vehicle E/E architecture or the set of the cybersecurity cases of its cybersecurity-relevant items and components can be considered. If cybersecurity activities described in this document are performed on items and components, then unreasonable vehicle cybersecurity risk is addressed.

The overall cybersecurity risk management of an organization described in this document applies throughout all lifecycle phases as illustrated in Figure 2.

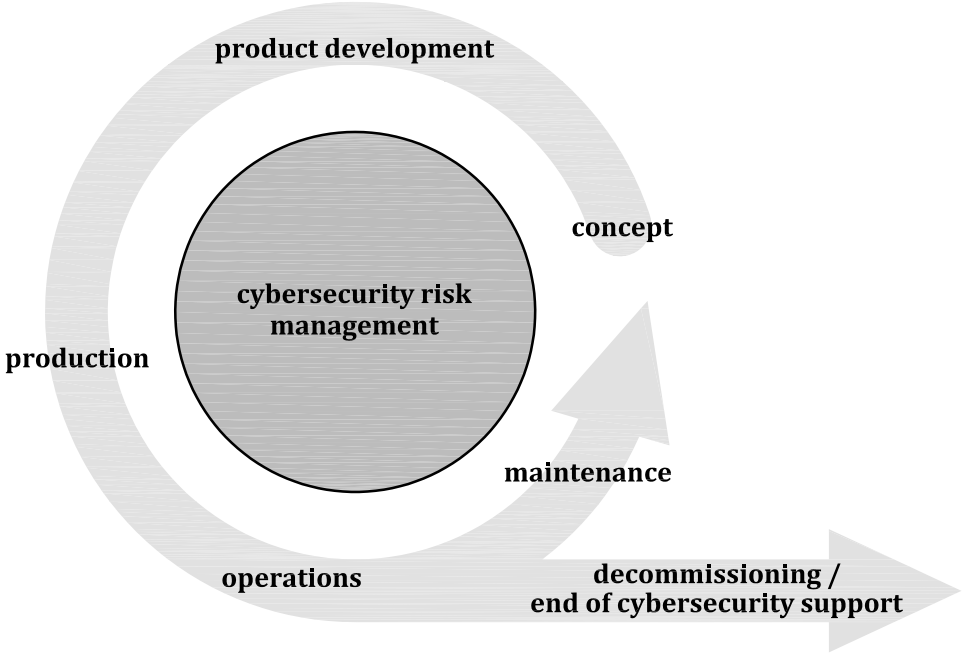


Figure 2 — Overall cybersecurity risk management

Cybersecurity risk management is applied throughout the supply chain to support cybersecurity engineering. Automotive supply chains exhibit diverse models of collaboration. Not all cybersecurity activities apply to all organizations involved in a specific project. Cybersecurity activities can be tailored to accommodate the needs of a specific situation (see Clause 6). Development partners for a specific item or component agree on the work-split so that the applicable cybersecurity activities are performed (see Clause 7).

Figure 3 shows the relationship between an item, function, component and related terms.

© ISO/SAE International 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

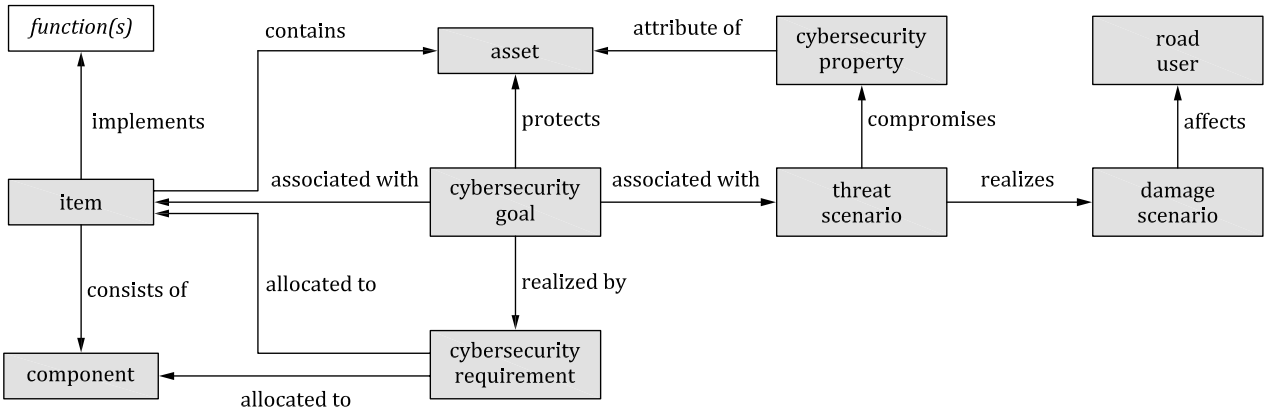


Figure 3 — Relationship between item, function, component and related terms

Clause 15 describes modular methods for assessment of cybersecurity risk that are invoked in cybersecurity activities described in other clauses.

Analysis activities in the context of cybersecurity engineering identify and explore potential actions performed by abstract adversarial actors with malicious intent and the damage that can arise from the compromise of cybersecurity of the vehicle E/E systems. Coordination between cybersecurity engineering and expertise from other disciplines can support the in-depth analysis and mitigation of specific cybersecurity risks (cf. ISO/TR 4804 [6]). Cybersecurity monitoring, remediation and incident response activities complement concept and product development activities as a reactive approach acknowledging the changing conditions in the environment (e.g. new attack technologies) and the ongoing need to identify and manage weaknesses and vulnerabilities in road vehicle E/E systems.

A defence-in-depth approach can be used to mitigate cybersecurity risk. The defence-in-depth approach utilizes layers of cybersecurity controls to improve the cybersecurity of the vehicle. If an attack is able to penetrate or bypass one layer, another layer can help contain the attack and maintain protection of the assets.

5 Organizational cybersecurity management

5.1 General

To enable cybersecurity engineering, the organization institutes and maintains cybersecurity governance and a cybersecurity culture, including cybersecurity awareness management, competence management and continuous improvement. This involves specifying organizational rules and processes that are independently audited against the objectives of this document.

To support cybersecurity engineering, the organization implements management systems for cybersecurity including managing tools and applying a quality management system.

5.2 Objectives

The objectives of this clause are to:

a) define a cybersecurity policy and the organizational rules and processes for cybersecurity;

b) assign the responsibilities and corresponding authorities that are required to perform cybersecurity activities;

c) support the implementation of cybersecurity, including the provision of resources and the management of the interactions between cybersecurity processes and related processes;

d) manage the cybersecurity risk;

© ISO/SAE International 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

e) institute and maintain a cybersecurity culture, including competence management, awareness management and continuous improvement;

f) support and manage the sharing of cybersecurity information;

g) institute and maintain management systems that support the maintenance of cybersecurity;

h) provide evidence that the use of tools does not adversely affect cybersecurity; and

i) perform an organizational cybersecurity audit.

5.3 Inputs

5.3.1 Prerequisites

None.

5.3.2 Further supporting information

The following information can be considered:

— existing evidence of conformity with standards that support quality management.

EXAMPLE IATF 16949 [7] in conjunction with ISO 9001 [8], ISO 10007 [9], Automotive SPICE®[1)], the ISO/IEC 330xx family of standards [10], ISO/IEC/IEEE 15288 [11] and ISO/IEC/IEEE 12207 [12].

5.4 Requirements and recommendations

5.4.1 Cybersecurity governance

[RQ-05-01] The organization shall define a cybersecurity policy that includes:

a) acknowledgement of road vehicle cybersecurity risks; and

b) the executive management's commitment to manage the corresponding cybersecurity risks.

NOTE 1 The cybersecurity policy can include links to the organization's objectives and other policies.

NOTE 2 The cybersecurity policy can include a statement regarding the risk treatment of generic threat scenarios with respect to the organization's products or services portfolio, considering the context, either external or internal.

[RQ-05-02] The organization shall establish and maintain rules and processes to:

a) enable the implementation of the requirements of this document; and

b) support the execution of the corresponding activities.

EXAMPLE 1 Process definitions, technical rules, guidelines, methods and templates.

NOTE 3 Cybersecurity risk management can include effort-benefit considerations of activities.

NOTE 4 Rules and processes cover concept, product development, production, operation, maintenance, and decommissioning, including TARA methods, information sharing, cybersecurity monitoring, cybersecurity incident response, and triggers.

NOTE 5 Rules and processes regarding vulnerability disclosure, for example as part of information sharing, can be specified in accordance with ISO 29147 [14].

---

1) Automotive SPICE® [13] is an example of suitable products available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of these products.

© ISO/SAE International 2021 – All rights reserved
Document Sharing Hub
Full document details: ISO SAE 21434-2021

NOTE 6 Figure 4 outlines the relationship between an overarching cybersecurity policy (see [RQ-05-01]), and organization-specific cybersecurity rules and processes (see [RQ-05-02]), responsibilities (see [RQ-05-03]) and resources (see [RQ-05-04]).

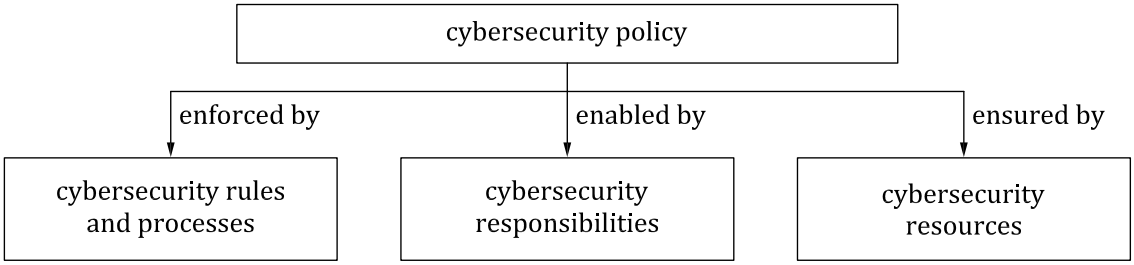


Figure 4 — Cybersecurity governance

[RQ-05-03] The organization shall assign and communicate the responsibilities and corresponding organizational authority to achieve and maintain cybersecurity.

NOTE 7 This relates to organizational as well as to project-dependent activities.

[RQ-05-04] The organization shall provide the resources to address cybersecurity.

NOTE 8 Resources include the persons responsible for cybersecurity risk management, development, and incident management.

EXAMPLE 2 Skilled personnel and suitable tools to perform cybersecurity activities.

[RQ-05-05] The organization shall identify disciplines related to, or interacting with, cybersecurity and establish and maintain communication channels between those disciplines in order to:

a) determine if and how cybersecurity will be integrated into existing processes; and

b) coordinate the exchange of relevant information.

NOTE 9 Coordination can include sharing of processes and using strategies and tools between disciplines.

NOTE 10 Disciplines include information technology security, functional safety, and privacy.

EXAMPLE 3 Interdisciplinary exchange of:

— threat scenarios and hazard (cf. ISO 26262-1:2018 [1], 3.75) information;

— cybersecurity goals and safety goals (cf. ISO 26262-1:2018 [1], 3.139); and/or

— cybersecurity requirements conflicting or competing with functional safety requirements (cf. ISO 26262-1:2018 [1], 3.69).

5.4.2 Cybersecurity culture

[RQ-05-06] The organization shall foster and maintain a strong cybersecurity culture.

NOTE 1 See Annex B for examples.

[RQ-05-07] The organization shall ensure that persons to which cybersecurity roles and responsibilities are assigned have the competences and awareness to fulfil these.

NOTE 2 A competence, awareness and training program can include:

— organizational rules and processes regarding cybersecurity, including cybersecurity risk management;

— organizational rules and processes regarding disciplines related to cybersecurity, such as functional safety and privacy;

© ISO/SAE International 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

— domain knowledge;

— systems engineering;

— cybersecurity-related methods, tools and guidelines; and/or

— known attack methods and cybersecurity controls.

[RQ-05-08] The organization shall institute and maintain a continuous improvement process.

EXAMPLE Continuous improvement process, including:

— learning from previous experiences, including cybersecurity information gathered by cybersecurity monitoring and observation of internal and external cybersecurity-related information;

— learning from information related to cybersecurity regarding products of similar application in the field;

— deriving improvements to be applied during subsequent cybersecurity activities;

— communicating lessons learned about cybersecurity to the appropriate persons; and

— checking the adequacy of the organizational rules and processes in accordance with [RQ-05-02].

NOTE 3 Continuous improvement applies to all cybersecurity activities in this document.

5.4.3 Information sharing

[RQ-05-09] The organization shall define the circumstances under which information sharing related to cybersecurity is required, permitted, or prohibited, internal or external to the organization.

NOTE Circumstances to share information can be based on:

— types of information that can be shared;

— approval processes for sharing;

— requirements for redacting information;

— rules for source attribution;

— types of communications for specific parties;

— vulnerability disclosure procedures (see NOTE 5 in 5.4.1); and/or

— requirements for receiving party on handling of highly sensitive information.

[RC-05-10] The organization should align its information security management of the shared data with other parties in accordance with [RQ-05-09].

EXAMPLE Alignment of security classification levels of public, internal, confidential, third-party confidential.

5.4.4 Management systems

[RQ-05-11] The organization shall institute and maintain a quality management system in accordance with International Standards, or equivalent, to support cybersecurity engineering, addressing:

EXAMPLE 1 IATF 16949 [7] in conjunction with ISO 9001 [8].

a) change management;

NOTE 1 The scope of change management in cybersecurity is to manage changes in items and their components so that the applicable cybersecurity goals and requirements continue to be fulfilled, e.g. a review of the changes in production processes against the production control plan to prevent such changes from introducing new vulnerabilities.

b) documentation management;

© ISO/SAE International 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

NOTE 2 A work product can be combined or mapped to different documentation repositories.

c) configuration management; and

d) requirements management.

[RQ-05-12] The configuration information required for maintaining cybersecurity of a product in the field shall remain available until the end of cybersecurity support for the product, in order to enable remedial actions.

NOTE 3 Archiving the build environment can be useful to ensure later usage of configuration information.

EXAMPLE 2 Bill of materials, software configuration.

[RC-05-13] A cybersecurity management system for the production processes should be established in order to support the activities of Clause 12.

EXAMPLE 3 IEC 62443 2-1 [15].

5.4.5 Tool management

[RQ-05-14] Tools that can influence the cybersecurity of an item or component shall be managed.

EXAMPLE 1 Tools used for concept or product development, such as model based development, static checkers, verification tools.

EXAMPLE 2 Tools used during production such as a flash writer, end of line tester.

EXAMPLE 3 Tools used for maintenance, such as an on-board diagnostic tool or reprogramming tool.

NOTE Such management can be established by:

— application of the user manual with errata;

— protection against unintended usage or action;

— access control for the tool users; and/or

— authentication of the tool.

[RC-05-15] An appropriate environment to support remedial actions for cybersecurity incidents (see 13.3) should be reproducible until the end of cybersecurity support for the product.

EXAMPLE 4 Testing, software build and development environments for reproducing and managing vulnerabilities.

EXAMPLE 5 Toolchain and compilers used for building the software of the product.

5.4.6 Information security management

[RC-05-16] Work products should be managed in accordance with an information security management system.

EXAMPLE Work products can be stored on a file server that protects them from unauthorized alteration or deletion.

5.4.7 Organizational cybersecurity audit

[RQ-05-17] A cybersecurity audit shall be performed independently to judge whether the organizational processes achieve the objectives of this document.

NOTE 1 A cybersecurity audit can be included in, or combined with, an audit in accordance with a quality management system standard, e.g. IATF 16949 [7] in conjunction with ISO 9001 [8].

© ISO/SAE International 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

NOTE 2 Independence can be based on, for example, the ISO 26262 series [16].

NOTE 3 Persons that perform the audit can be internal or external to the organization.

NOTE 4 To ensure that organizational processes remain appropriate for cybersecurity, an audit can be performed periodically.

NOTE 5 Figure 7 illustrates the organizational cybersecurity audit in relation to other cybersecurity activities.

5.5 Work products

[WP-05-01] Cybersecurity policy, rules and processes, resulting from the requirements of 5.4.1 to 5.4.3

[WP-05-02] Evidence of competence management, awareness management resulting from [RQ-05-07] and continuous improvement resulting from [RQ-05-08] of 5.4.2

[WP-05-03] Evidence of the organization's management systems, resulting from the requirements of 5.4.4 and 5.4.6

[WP-05-04] Evidence of tool management, resulting from the requirements of 5.4.5

[WP-05-05] Organizational cybersecurity audit report, resulting from the requirements of 5.4.7

6 Project dependent cybersecurity management

6.1 General

This clause describes the requirements regarding the management of cybersecurity development activities for a specific project.

Project dependent cybersecurity management includes the allocation of responsibilities (see 6.4.1) and planning of the cybersecurity activities (see 6.4.2). This document defines requirements in a generic manner such that it can be applied to a variety of items and components. In addition, tailoring can be applied (see 6.4.3) that is based on a rationale and is defined in the cybersecurity plan. Examples of when tailoring can be used include:

— reuse (see 6.4.4),

— component out-of-context (see 6.4.5),

— use of an off-the-shelf component (see 6.4.6),

— update (see 13.4).

Reuse of items and components is a possible development strategy that can be applied, with or without modifications to an item, component, or their operational environment. However, modifications can introduce vulnerabilities that might not have been considered for the original item or component. Furthermore, there might have been a change in known attacks, for example:

— an evolution of attack techniques,

— newly emerged vulnerabilities, e.g. learned from cybersecurity monitoring (see 8.3) and/or cybersecurity event evaluation (see 8.4), or

— a change of the assets since the original development.

If the original item or component was developed in accordance with this document, the reuse of that item or component is based on the existing work products. If the item or component was not originally developed in accordance with this document, the reuse can be based on the existing documentation with a rationale.

© ISO/SAE International 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

A component can be developed out-of-context, i.e. based on an assumed context. An organization can develop generic components for different applications and for different customers, prior to engagement or commercial agreement with a customer. The supplier can make assumptions about the context and intended use. Based on this, the supplier can derive requirements for the out-of-context development. For example, a microcontroller can be developed out-of-context.

An off-the-shelf component is a component that is not developed on behalf of a specific customer and that can be used without modification of its design or implementation, e.g. a third-party software library, an open source software component. An off-the-shelf component is not assumed to have been developed in accordance with this document.

Figure 5 shows that both an off-the-shelf component and an out-of-context component can be integrated into an item or component in accordance with this document. The integration can involve activities similar to reuse analysis in 6.4.4, and if changes are made to address invalid assumptions then change management (see 5.4.4) applies. The changes can be made to a component that is intended to be integrated and/or to the component or item that is the target of the integration.

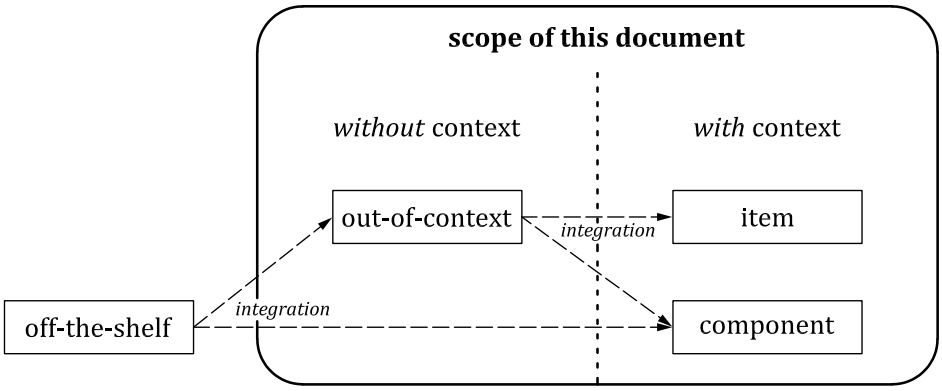


Figure 5 — Integration of off-the-shelf and out-of-context components

The cybersecurity case (see 6.4.7) is an input to a cybersecurity assessment and to the release for post-development.

The cybersecurity assessment (see 6.4.8) judges independently the cybersecurity of an item or component and is an input for the decision to the release for post-development (see 6.4.9).

6.2 Objectives

The objectives of this clause are to:

a) assign the responsibilities regarding the project's cybersecurity activities;

b) plan the cybersecurity activities, including the definition of the tailored cybersecurity activities;

c) create a cybersecurity case;

d) perform a cybersecurity assessment, if applicable; and

e) decide whether the item or component can be released for post-development from a cybersecurity perspective.

6.3 Inputs

6.3.1 Prerequisites

None.

© ISO/SAE International 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

6.3.2 Further supporting information

The following information can be considered:

— organizational cybersecurity audit report [WP-05-03];

— project plan.

6.4 Requirements and recommendations

6.4.1 Cybersecurity responsibilities

[RQ-06-01] The responsibilities regarding the project's cybersecurity activities shall be assigned and communicated in accordance with [RQ-05-03].

NOTE Responsibilities for cybersecurity activities can be transferred provided that this is communicated and that the relevant information is made available.

6.4.2 Cybersecurity planning

[RQ-06-02] In order to decide cybersecurity activities needed for the item or component, the item or component shall be analysed to determine:

a) whether the item or component is cybersecurity relevant;

NOTE 1 Annex D provides a method and criteria that can be used to assess the cybersecurity relevance.

NOTE 2 If the item or component is determined as not cybersecurity relevant, then there are no cybersecurity activities, thus cybersecurity planning is not continued.

b) if the item or component is cybersecurity relevant, whether the item or component is a new development or a reuse; and

c) whether tailoring in accordance with 6.4.3 is applied.

[RQ-06-03] The cybersecurity plan shall include the:

a) objective of an activity;

b) dependencies on other activities or information;

c) personnel responsible for performing an activity;

d) required resources for performing an activity;

e) starting point or end point, and the expected duration of an activity; and

f) identification of the work products to be produced.

[RQ-06-04] The responsibilities for developing and maintaining the cybersecurity plan, and for tracking the progress of the cybersecurity activities against the cybersecurity plan shall be assigned in accordance with [RQ-05-03] and [RQ-05-04].

[RQ-06-05] The cybersecurity plan shall either be:

a) referenced in the project plan for the development; or

b) included in the project plan, such that the cybersecurity activities are distinguishable.

NOTE 3 The cybersecurity plan can incorporate cross-references to other plans (e.g. the project plan) which are also under configuration management (see also [RQ-06-09]).

© ISO/SAE International 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

[RQ-06-06] The cybersecurity plan shall specify the activities that are required for cybersecurity during the concept and product development phases in accordance with the relevant requirements of Clauses 9, 10, 11 and 15.

[RQ-06-07] The cybersecurity plan shall be updated when a change or a refinement of the activities to be performed is identified.

NOTE 4 The cybersecurity plan can be refined in incremental steps during development. For example, the cybersecurity plan can be updated based on the result of cybersecurity activities, such as the TARA (see Clause 15).

[PM-06-08] For threat scenarios of risk value 1 that are determined from an analysis in accordance with 15.8, conformity with 9.5, Clause 10 and Clause 11 may be omitted.

NOTE 5 These threat scenarios can have consequences with regard to cybersecurity and if so, the corresponding risks are treated, albeit potentially with less rigour than defined in this document.

NOTE 6 The sufficiency of the treatment of such risks can be argued based on a rationale defined in the cybersecurity case. The rationale can be based on conformity with a quality management standard, such as IATF 16949 [7] in conjunction with ISO 9001 [8], in combination with additional measures, for example:

— cybersecurity awareness assurance;

— cybersecurity training of quality personnel; and/or

— cybersecurity specific measures defined in the organization's quality management system.

[RQ-06-09] The work products identified in the cybersecurity plan shall be updated and maintained for accuracy until and at the release for post-development.

[RQ-06-10] If cybersecurity activities are distributed, customer and supplier shall each define a cybersecurity plan regarding their respective cybersecurity activities and interfaces in accordance with Clause 7.

[RQ-06-11] The cybersecurity plan shall be subject to configuration management and documentation management, in accordance with 5.4.4.

[RQ-06-12] The work products identified in the cybersecurity plan shall be subject to configuration management, change management, requirements management, and documentation management, in accordance with 5.4.4.

6.4.3 Tailoring

[PM-06-13] A cybersecurity activity may be tailored.

[RQ-06-14] If a cybersecurity activity is tailored, then a rationale why the tailoring is adequate and sufficient to achieve the relevant objectives of this document shall be provided and reviewed.

NOTE Activities that are not performed because they are performed by another entity in the supply chain are not considered as tailored, but as distributed cybersecurity activities (see Clause 7). However, distribution of cybersecurity activities can lead to joint tailoring (see 7.4.3).

6.4.4 Reuse

[RQ-06-15] A reuse analysis shall be carried out if an item or component has been developed and:

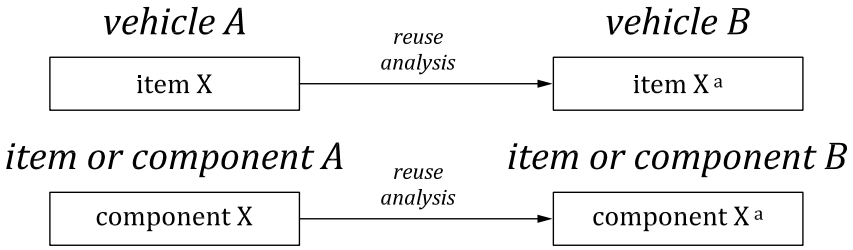
a) modifications are planned;

b) is planned to be reused in another operational environment; or

EXAMPLE 1 Modifications to the environment resulting from the installation of the existing item or component in a new operational environment, or from the upgrading of other items or components interacting with it (see Figure 6).

© ISO/SAE International 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021



a Can be changed as a result of the reuse analysis.

Figure 6 — Reuse analysis examples

c) is planned to be reused without modification and there are relevant changes to the information concerning the item or component.

EXAMPLE 2 Change in the known attacks and vulnerabilities, or change of the threat scenarios.

NOTE 1 Existing work products are considered in determining whether a reuse is possible.

NOTE 2 Modifications can include design modifications and/or implementation modifications where:

— design modifications can result from requirement modifications, e.g. functional or performance enhancement;

— implementation modifications can result from corrections to software, or the use of new production or maintenance tools, e.g. model-based development.

NOTE 3 A change to configuration data or calibration data is considered a modification if it impacts the functional behaviour, the assets, or cybersecurity properties of the item or component.

[RQ-06-16] A reuse analysis of an item or component shall:

a) identify the modifications to the item or component and the modifications of its operational environment;

b) analyse the cybersecurity implications of the modifications, including the effects on the validity of cybersecurity claims and previously made assumptions;

EXAMPLE 3 Implications on cybersecurity requirements, design and implementation, operational environment, validity of assumptions and operating modes, maintenance, susceptibility to known attacks and exposure of known vulnerabilities or assets.

c) identify the affected or missing work products; and

EXAMPLE 4 TARA considering new or modified assets, threat scenarios or risk values.

d) specify the cybersecurity activities necessary to conform with this document in the cybersecurity plan (see 6.4.2).

NOTE 4 This can imply tailoring (see 6.4.3).

[RQ-06-17] A reuse analysis of a component shall evaluate whether:

a) the component is able to fulfil the allocated cybersecurity requirements from the item or component, in which it is to be integrated; and

b) the existing documentation is sufficient to support the integration into an item, or into another component.

© ISO/SAE International 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

6.4.5 Component out-of-context

[RQ-06-18] Assumptions on the intended use and context, including the external interfaces, for a component developed out-of-context shall be documented in the corresponding work products.

[RQ-06-19] For the development of a component out-of-context, the cybersecurity requirements shall be based on the assumptions of [RQ-06-18].

[RQ-06-20] For the integration of a component developed out-of-context, the cybersecurity claims and assumptions of [RQ-06-18] shall be validated.

6.4.6 Off-the-shelf component

[RQ-06-21] When integrating an off-the-shelf component, the cybersecurity-relevant documentation shall be gathered and analysed to determine whether:

a) allocated cybersecurity requirements can be fulfilled;

b) the component is suitable for the specific application context of the intended use; and

c) existing documentation is sufficient to support the cybersecurity activities.

[RQ-06-22] If the existing documentation is insufficient to support the integration of the off-the-shelf component, then the cybersecurity activities to conform with this document shall be identified and performed.

EXAMPLE Insufficient documentation concerning vulnerabilities.

NOTE This can imply tailoring (see 6.4.3).

6.4.7 Cybersecurity case

[RQ-06-23] A cybersecurity case shall be created to provide the argument for the cybersecurity of the item or component, supported by work products.

NOTE 1 Parts of the argument can be implicit (e.g. if part of the argument is evident from the compiled set of work products then that part of the argument can be omitted).

NOTE 2 In distributed development, the cybersecurity case of the item can be a combination of the cybersecurity cases of the customer and of the suppliers, which references evidence from the work products generated by the respective parties. Then the overall argument of the item is supported by arguments from all parties.

NOTE 3 The cybersecurity case considers the cybersecurity requirements for post-development [WP-10-02].

6.4.8 Cybersecurity assessment

[RQ-06-24] A decision whether to perform a cybersecurity assessment for an item or component shall be made supported by a rationale applying a risk-based approach.

NOTE 1 The rationale can be based on:

— TARA results (see Clause 15);

— complexity of the item or component to be developed; and/or

— criteria defined by organizational rules and processes (see 5.4.1).

NOTE 2 If the cybersecurity assessment is not performed, the rationale can be documented in the cybersecurity case.

© ISO/SAE International 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

[RQ-06-25] The rationale of [RQ-06-24] shall be reviewed independently.

NOTE 3 The independence scheme can be based on the ISO 26262 series [16].

[RQ-06-26] The cybersecurity assessment shall judge the cybersecurity of the item or component.

NOTE 4 The available evidence is provided by the documented results of the cybersecurity activities, i.e. the work products (see Annex A).

NOTE 5 Figure 7 illustrates the relationship between the organizational cybersecurity audit, the project level cybersecurity assessment and other cybersecurity activities.

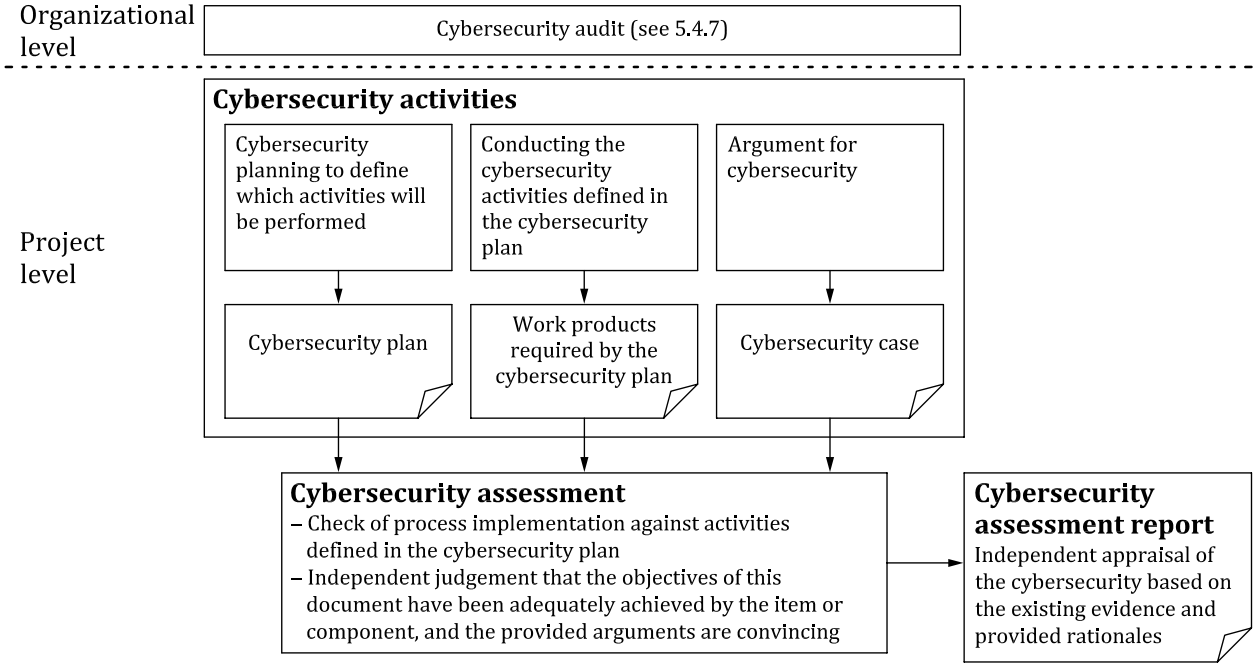


Figure 7 — Cybersecurity assessment in relation to other cybersecurity activities

NOTE 6 A cybersecurity assessment can be performed in incremental steps to facilitate an early resolution of identified issues.

NOTE 7 A cybersecurity assessment can be repeated or supplemented, e.g. due to a change, when a previous cybersecurity assessment provided a negative recommendation, or when a vulnerability is discovered.

[RQ-06-27] A person responsible to plan and perform independently a cybersecurity assessment shall be appointed in accordance with [RQ-06-01].

NOTE 8 The independence scheme can be based on the ISO 26262 series [16].

EXAMPLE A person from a different team or department within the organization such as quality assurance, a person from an independent organization.

[RQ-06-28] A person who carries out a cybersecurity assessment shall have:

a) access to the relevant information and tools; and

b) the cooperation of the personnel performing the cybersecurity activities.

[PM-06-29] A cybersecurity assessment may be based on a judgement of whether the objectives of this document are achieved.

[RQ-06-30] The scope of a cybersecurity assessment shall include:

a) the cybersecurity plan and all work products identified in the cybersecurity plan;

© ISO/SAE International 2021 – All rights reserved
Documents Document Sharing Hub
Full document details: ISO SAE 21434-2021

b) the treatment of the cybersecurity risks;

c) the appropriateness and effectiveness of implemented cybersecurity controls and cybersecurity activities performed for the project; and

NOTE 9 The appropriateness and effectiveness can be judged by using prior reviews that were performed for verification purposes.

d) the rationales, if provided, that demonstrate the achievement of the objectives of this document.

NOTE 10 A person responsible for the creation of a work product can provide a rationale why the corresponding objectives of this document are achieved in order to facilitate a cybersecurity assessment, considering [PM-06-13].

NOTE 11 Fulfilment of all corresponding requirements is sufficient rationale for having achieved an objective of this document.

[RQ-06-31] A cybersecurity assessment report shall include a recommendation for acceptance, conditional acceptance, or rejection of the cybersecurity of the item or component.

NOTE 12 The assessment report can also include recommendations for continuous improvement.

[RQ-06-32] If a recommendation for conditional acceptance in accordance with [RQ-06-31] is made, then the cybersecurity assessment report shall include the conditions for acceptance.

6.4.9 Release for post-development

[RQ-06-33] The following work products shall be available prior to the release for post-development:

a) the cybersecurity case [WP-06-02];

b) if applicable, the cybersecurity assessment report [WP-06-03]; and

c) the cybersecurity requirements for post-development [WP-10-02].

[RQ-06-34] The following conditions shall be fulfilled for the release for post-development of the item or component:

a) the argument for cybersecurity provided by the cybersecurity case is convincing;

b) the cybersecurity case is confirmed by the cybersecurity assessment, if applicable; and

c) the cybersecurity requirements for the post-development phases are accepted.

NOTE Changes can result in re-evaluating the release for post-development, e.g. changes to the cybersecurity claims.

6.5 Work products

[WP-06-01] Cybersecurity plan, resulting from the requirements of 6.4.1 to 6.4.6

[WP-06-02] Cybersecurity case, resulting from the requirements of 6.4.7

[WP-06-03] Cybersecurity assessment report, if applicable, resulting from the requirements of 6.4.8

[WP-06-04] Release for post-development report, resulting from the requirements of 6.4.9

© ISO/SAE International 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

7 Distributed cybersecurity activities

7.1 General

This clause applies if responsibilities for cybersecurity activities for an item or component are distributed.

This clause describes management of distributed cybersecurity activities and applies to:

a) items and components developed in a distributed activity;

b) interactions between a customer and a supplier; and

c) all phases where an agreement is applicable to the customer/supplier interface.

Internal suppliers can be managed in the same way as external suppliers.

For example, a tier-1 organization can be a supplier to an OEM during development and in another contractual relationship the tier-1 organization can be a customer of a tier-2 organization for a component. This is illustrated in Figure 8.

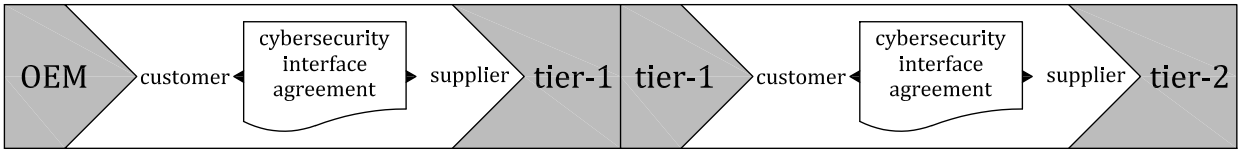


Figure 8 — Use cases for customer/supplier relationships in the supply chain

7.2 Objectives

The objective of this clause is to define the interactions, dependencies, and responsibilities for distributed cybersecurity activities between customers and suppliers.

7.3 Inputs

None.

7.4 Requirements and recommendations

7.4.1 Supplier capability

[RQ-07-01] The capability of a candidate supplier to develop and, if applicable, perform post-development activities in accordance with this document shall be evaluated.

NOTE 1 This evaluation supports supplier selection and can be based on the supplier's capability to conform to this document, or on an evaluation of the previous implementation of another national or international standard with regard to cybersecurity engineering.

[RC-07-02] To support a customer's evaluation of supplier capability, a supplier should provide a record of cybersecurity capability.

NOTE 2 A record of cybersecurity capability can include:

— evidence of the organization's capability concerning cybersecurity (e.g. cybersecurity best practices from development, post-development, governance, quality, and information security);

— evidence of continual cybersecurity activities (see Clause 8) and cybersecurity incident response (see Clause 13); and

© ISO/SAE International 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021

— summary of previous cybersecurity assessment reports.

7.4.2 Request for quotation

[RQ-07-03] A request for quotation from a customer to a candidate supplier shall include:

a) a formal request to conform to this document;

b) the expectation that cybersecurity responsibilities will be taken on by the supplier in accordance with 7.4.3; and

c) the cybersecurity goals and/or set of cybersecurity requirements relevant to the item or component for which the supplier is quoting.

EXAMPLE Cybersecurity requirements related to message authentication.

7.4.3 Alignment of responsibilities

[RQ-07-04] A customer and a supplier shall specify the distributed cybersecurity activities in a cybersecurity interface agreement including:

a) appointment of customer's and supplier's points of contact regarding cybersecurity;

b) identification of cybersecurity activities that are to be performed by customer and supplier, respectively;

EXAMPLE 1 Cybersecurity validation at the vehicle level performed by the customer.

EXAMPLE 2 The distribution of cybersecurity activities regarding post-development.

EXAMPLE 3 The cybersecurity assessment concerning the components or work products developed by the supplier can be performed by a third party, the customer or the supplier.

c) if applicable, a joint tailoring of cybersecurity activities in accordance with 6.4.3;

d) the information and the work products to be shared;

NOTE 1 The shared information can include:

— distribution, reviews and cybersecurity issue feedback mechanism;

— information exchange procedures for vulnerabilities and other cybersecurity-related findings, e.g. concerning risk;

— interface-related processes, methods and tools to ensure compatibility between the customer and the supplier, such as proper handling of data and securing the communication networks used to pass that data;

— definition of roles,

— methods for communicating and documenting changes in the item or component, including potential reiteration of the TARA;

— alignment on requirements management tools; and/or

— results of cybersecurity assessments.

e) milestones regarding the distributed cybersecurity activities; and

f) definition of the end of cybersecurity support for the item or component.

[RC-07-05] The cybersecurity interface agreement should be mutually agreed upon between customer and supplier prior to the start of the distributed cybersecurity activities.

© ISO/SAE International 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO SAE 21434-2021