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)

COPYRIGHT PROTECTED DOCUMENT

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

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/.

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.

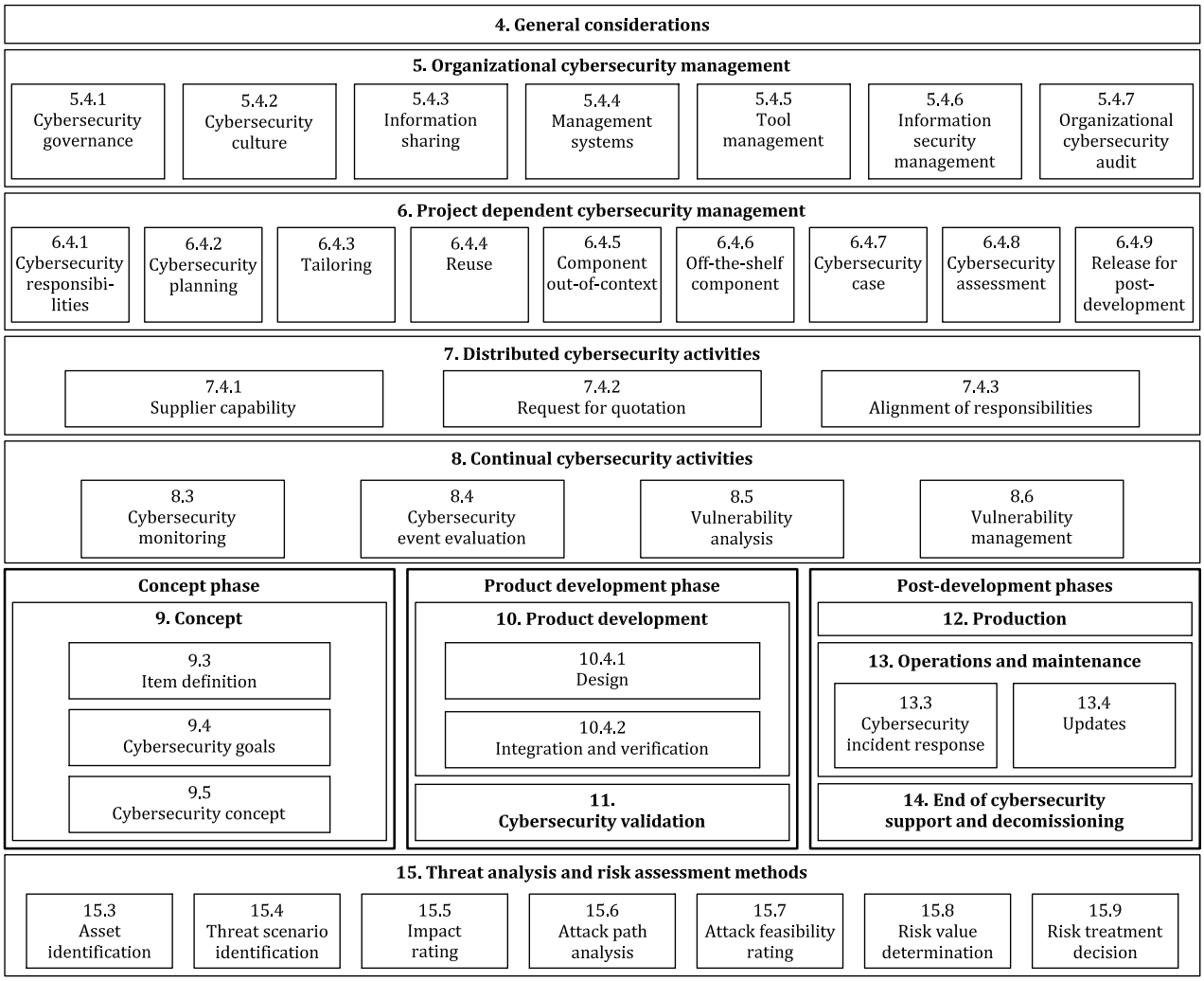


Figure 1 — Overview of this document

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.

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.

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

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.]

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.

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.]

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

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.

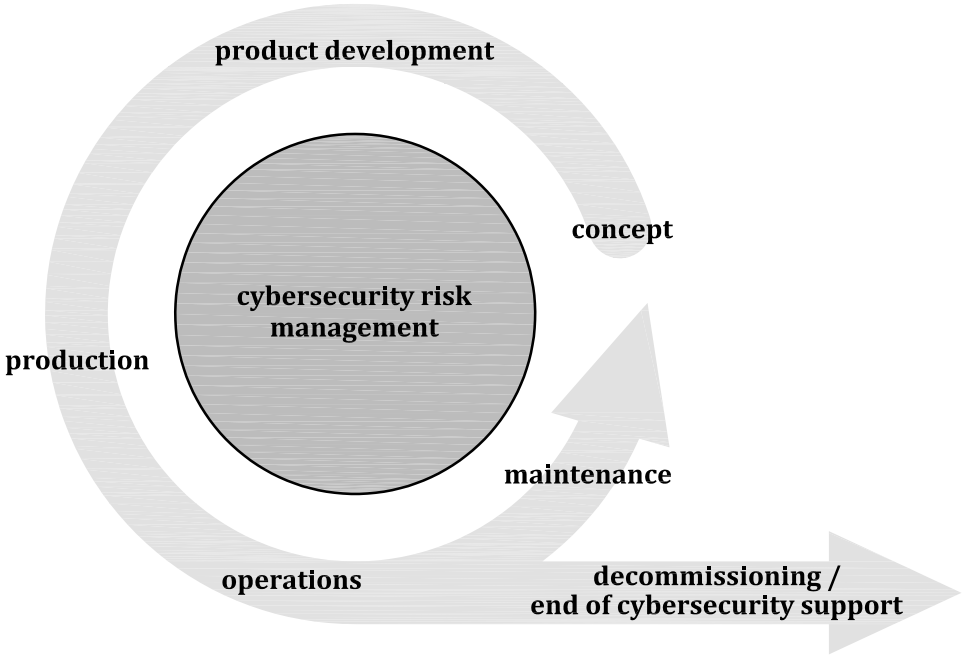


Figure 2 — Overall cybersecurity risk management

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.

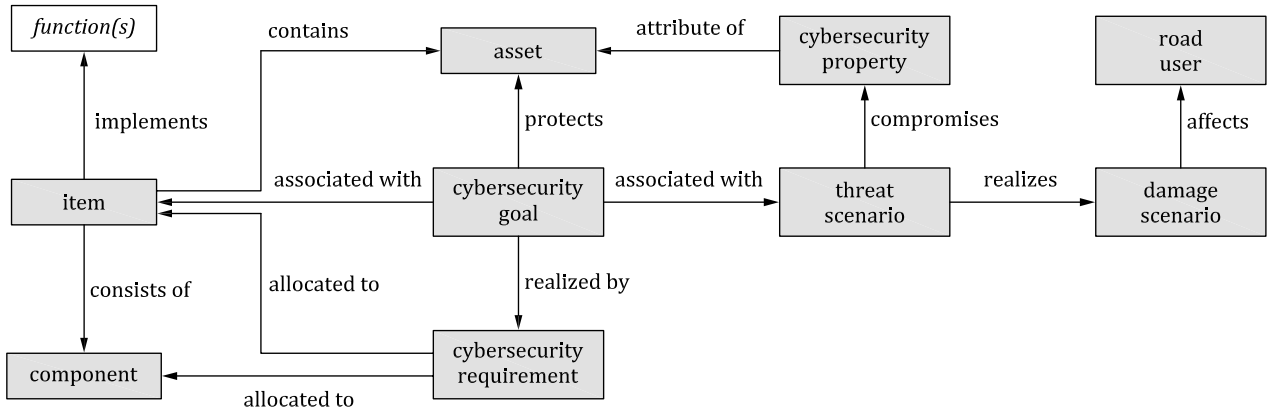


Figure 3 — Relationship between item, function, component and related terms

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;

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.

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]).

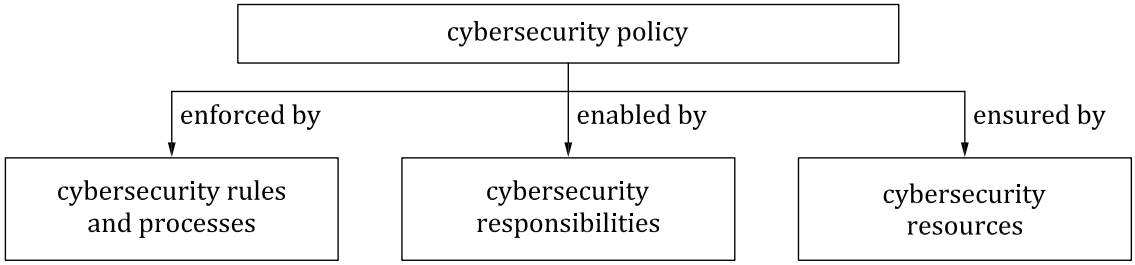


Figure 4 — Cybersecurity governance

[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;

— 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;

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].

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.

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.

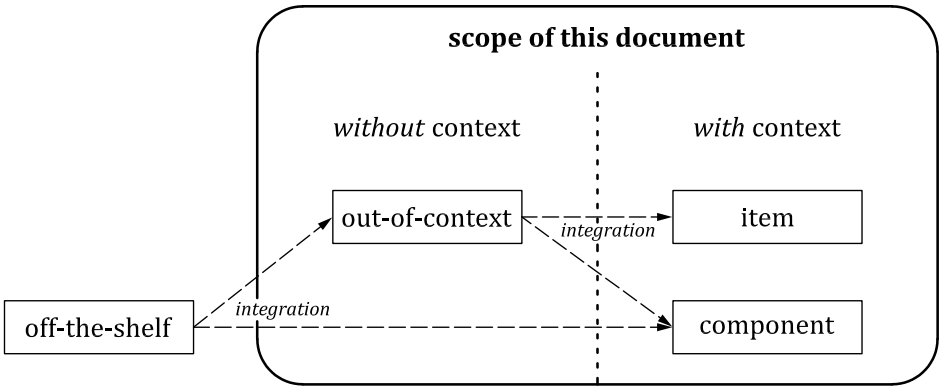


Figure 5 — Integration of off-the-shelf and out-of-context components

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.

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]).

[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).

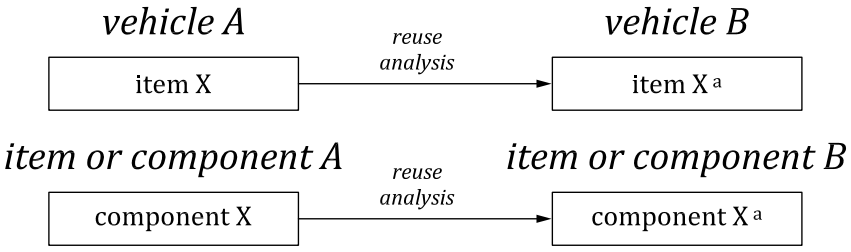
6.4.4 Reuse

[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).



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.

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.

[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.

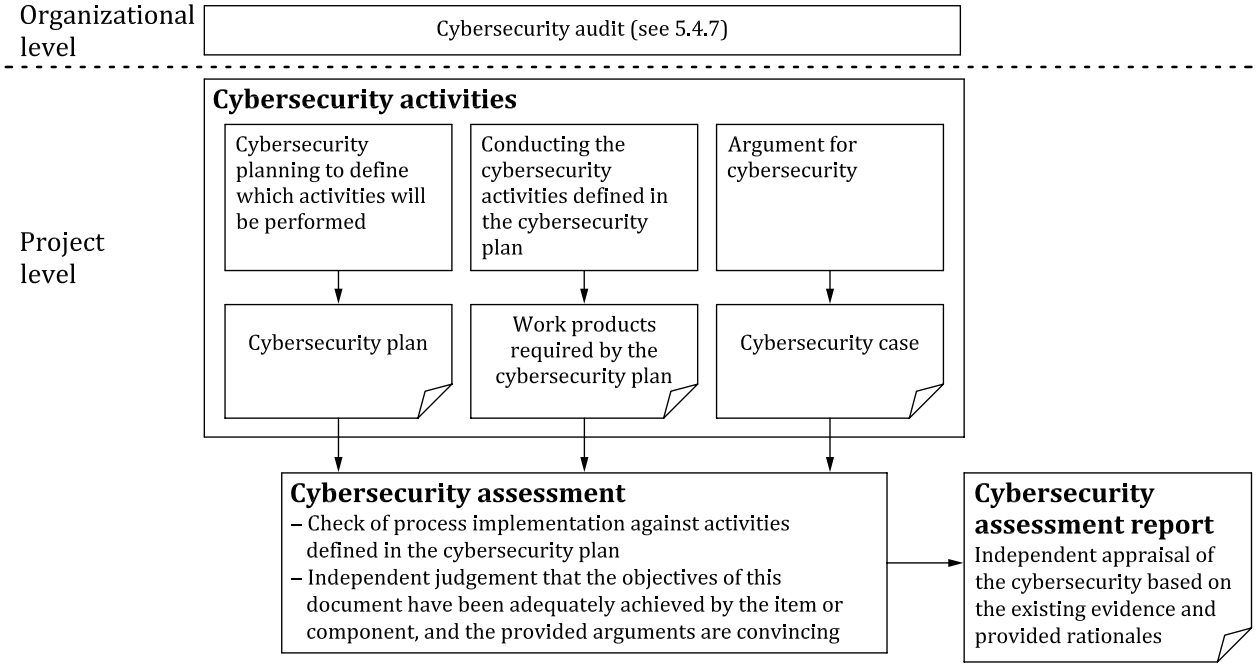


Figure 7 — Cybersecurity assessment in relation to other cybersecurity activities

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;

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

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.

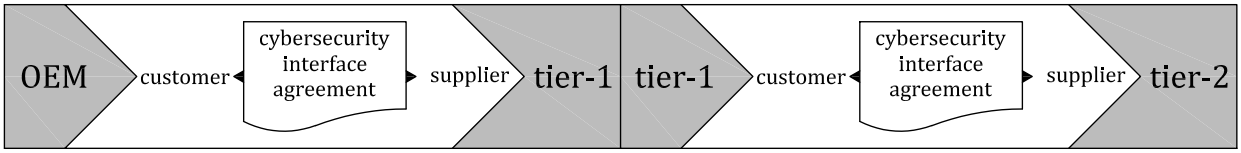


Figure 8 — Use cases for customer/supplier relationships in the supply chain

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

— 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.

[RQ-07-06] If there is an identified vulnerability to be managed in accordance with [RQ-08-07], the customer and supplier shall agree on actions and responsibility for those actions.

[RQ-07-07] If requirements are unclear, not feasible, or conflict with other cybersecurity requirements or requirements from other disciplines, then customer and supplier shall each notify the other so that appropriate decisions and actions can be taken.

[RC-07-08] Responsibilities should be specified in a responsibility assignment matrix.

NOTE 2 A RASIC table can be used, see Annex C.

7.5 Work products

[WP-07-01] Cybersecurity interface agreement, resulting from the requirements of 7.4.3

8 Continual cybersecurity activities

8.1 General

Continual cybersecurity activities are performed during all the phases of the lifecycle and can be done outside of a specific project.

Cybersecurity monitoring (see 8.3) collects cybersecurity information and analyses the cybersecurity information for triage based on defined triggers.

Cybersecurity event evaluation (see 8.4) determines if the cybersecurity event presents a weakness for an item or component.

Vulnerability analysis (see 8.5) examines weaknesses and assesses if a particular weakness can be exploited.

Vulnerability management (see 8.6) tracks and oversees the treatment of identified vulnerabilities in items and components until their end of cybersecurity support.

8.2 Objectives

The objectives of this clause are to:

a) monitor cybersecurity information to identify cybersecurity events;

b) evaluate cybersecurity events to identify weaknesses;

c) identify vulnerabilities from weaknesses; and

d) manage identified vulnerabilities.

8.3 Cybersecurity monitoring

8.3.1 Inputs

8.3.1.1 Prerequisites

The following information shall be available:

— rules and processes included in [WP-05-01] for the development of triggers.

8.3.1.2 Further supporting information

The following information can be considered:

— item definition [WP-09-01];

— cybersecurity claims [WP-09-04];

— cybersecurity specifications [WP-10-01];

— threat scenarios [WP-15-03];

— past vulnerability analyses [WP-08-05];

— information received from the field.

EXAMPLE Vulnerability scanning reports, repair information, consumer usage information.

8.3.2 Requirements and recommendations

[RQ-08-01] Sources shall be selected for collection of cybersecurity information.

NOTE 1 Internal and/or external sources can be selected.

NOTE 2 Internal sources can include those listed in 8.3.1.2.

NOTE 3 External sources can include:

— researchers;

— commercial or non-commercial sources;

— organization's supply chain;

— customers of the organization; and/or

— government sources.

EXAMPLE Sources for state-of-the-art attack methods.

[RQ-08-02] Triggers shall be defined and maintained for the triage of cybersecurity information.

NOTE 4 Triggers can include keywords, reference for configuration information, names of components or suppliers.

[RQ-08-03] Cybersecurity information shall be collected and triaged to determine if the cybersecurity information becomes one or more cybersecurity events.

8.3.3 Work products

[WP-08-01] Sources for cybersecurity information, resulting from [RQ-08-01]

[WP-08-02] Triggers, resulting from [RQ-08-02]

[WP-08-03] Cybersecurity events, resulting from [RQ-08-03]

8.4 Cybersecurity event evaluation

8.4.1 Inputs

8.4.1.1 Prerequisites

The following information shall be available:

— cybersecurity events [WP-08-03];

— cybersecurity requirements for post-development [WP-10-02], if applicable; and

— configuration information in accordance with [RQ-05-12].

8.4.1.2 Further supporting information

The following information can be considered:

— item definition [WP-09-01];

— cybersecurity specifications [WP-10-01];

— past vulnerability analyses [WP-08-05].

8.4.2 Requirements and recommendations

[RQ-08-04] A cybersecurity event shall be evaluated to identify weaknesses in an item and/or component.

NOTE 1 This activity can be combined with triage of [RQ-08-03].

NOTE 2 If a weakness exists and there is a remediation available (e.g. a patch provided by a supplier for a vulnerability in a component), the organization can handle the remediation (see 8.6) as an assumed vulnerability without any other activity.

NOTE 3 Threat scenarios [WP-15-03] can be updated based on the result of this evaluation.

8.4.3 Work products

[WP-08-04] Weaknesses from cybersecurity events, resulting from [RQ-08-04]

8.5 Vulnerability analysis

8.5.1 Inputs

8.5.1.1 Prerequisites

The following information shall be available:

— item definition [WP-09-01] or cybersecurity specifications [WP-10-01].

NOTE The item definition is used if the vulnerability analysis is performed on an item, and the cybersecurity specifications are used if the vulnerability analysis is performed on a component.

8.5.1.2 Further supporting information

The following information can be considered:

— weaknesses from cybersecurity events [WP-08-04];

— weaknesses found during product development [WP-10-05];

— past vulnerability analyses [WP-08-05];

— attack paths [WP-15-05];

— verification reports [WP-10-04] and [WP-10-07];

— information from past cybersecurity incidents.

8.5.2 Requirements and recommendations

[RQ-08-05] Weaknesses shall be analysed to identify vulnerabilities.

NOTE 1 The analysis can include:

— analysis of the architecture;

— attack path analysis in accordance with 15.6; and/or

— attack feasibility rating in accordance with 15.7.

NOTE 2 A root cause analysis can be performed to determine any underlying factors that contribute to the possibility of a weakness being a vulnerability.

EXAMPLE 1 Attack path analysis reveals no attack path exists and therefore, the weakness is not treated as a vulnerability.

EXAMPLE 2 The attack feasibility rating is very low for exploiting the weakness and therefore, the weakness is not treated as a vulnerability.

[RQ-08-06] A rationale shall be provided for a weakness that is not identified as a vulnerability.

8.5.3 Work products

[WP-08-05] Vulnerability analysis, resulting from [RQ-08-05] and [RQ-08-06]

8.6 Vulnerability management

8.6.1 Inputs

8.6.1.1 Prerequisites

The following information shall be available:

— vulnerability analysis [WP-08-05].

8.6.1.2 Further supporting information

None.

8.6.2 Requirements and recommendations

[RQ-08-07] Vulnerabilities shall be managed such that for each vulnerability:

a) the corresponding cybersecurity risks are assessed and treated in accordance with 15.9 such that no unreasonable risks remain; or

b) the vulnerability is eliminated by applying an available remediation independent of a TARA.

EXAMPLE Patches for open source software.

NOTE 1 If vulnerability management results in a change to an item or component, change management is applied in accordance with [RQ-05-11].

NOTE 2 Information about vulnerabilities can be shared within the context of distributed cybersecurity activities (see 7.4.3, e.g. sharing knowledge of attack paths) and to other interested parties (see 5.4.3).

[RQ-08-08] If a risk treatment decision in accordance with 15.9 necessitates cybersecurity incident response, then 13.3 shall be applied.

NOTE 3 The cybersecurity incident response process can be applied independent of a TARA.

8.6.3 Work products

[WP-08-06] Evidence of managed vulnerabilities, resulting from [RQ-08-07]

9 Concept

9.1 General

The concept phase involves consideration of vehicle level functionality, as implemented in items. In this clause, the item and its operational environment are identified as an "Item definition" (see 9.3). The item definition forms the basis for the subsequent activities.

This clause also specifies cybersecurity goals for the item (see 9.4), which are the highest level of requirements. For this purpose, cybersecurity risks are assessed, which is achieved by using the methods of Clause 15 (see also Annex H, Figure H.1). In addition, 9.4 specifies cybersecurity claims, which are used to explain why risk retention or sharing are considered adequate.

The cybersecurity concept (see 9.5) consists of cybersecurity requirements and requirements on the operational environment, both of which are derived from the cybersecurity goals and based on a comprehensive view of the item.

9.2 Objectives

The objectives of this clause are to:

a) define the item, its operational environment and their interactions in the context of cybersecurity;

b) specify cybersecurity goals and cybersecurity claims; and

c) specify the cybersecurity concept to achieve cybersecurity goals.

9.3 Item definition

9.3.1 Inputs

9.3.1.1 Prerequisites

None.

9.3.1.2 Further supporting information

The following information can be considered:

— existing information regarding the item and the operational environment.

EXAMPLE In-vehicle E/E system architecture including in-vehicle network, networks external to the vehicle; reference model(s) and the documentation of earlier developments.

9.3.2 Requirements and recommendations

[RQ-09-01] The following information on the item shall be identified:

a) item boundary;

NOTE 1 The item boundary distinguishes the item from its operational environment. The description of the item boundary can include interfaces with other items internal to the vehicle and/or with E/E systems external to the vehicle.

b) item functions; and

NOTE 2 This describes the intended behaviour of the item during the lifecycle phases [e.g. product development (testing), production, operations and maintenance, decommissioning] and includes the vehicle functionality that is realized by the item.

c) preliminary architecture.

NOTE 3 A description of preliminary architecture can include identification of components of the item and their connections, and external interfaces of the item.

NOTE 4 The item definition, especially the item boundary, as described in this document can differ from the item definition from another discipline, e.g. such as functional safety in accordance with the ISO 26262 series[16].

NOTE 5 Information on constraints and applicable cybersecurity standards can be considered.

NOTE 6 Development of a component out-of-context (see 6.4.5) can be based on a definition of an assumed (generic) item and description of the functions of the components within the item.

[RQ-09-02] Information about the operational environment of the item relevant to cybersecurity shall be described.

NOTE 7 The description of the operational environment and its interactions with the item can enable identifying and/or analysing relevant threat scenarios and attack paths.

NOTE 8 Relevant information can include assumptions, e.g. an assumption that every public key infrastructure certificate authority upon which the item relies is appropriately managed.

9.3.3 Work products

[WP-09-01] Item definition, resulting from the requirements of 9.3.2

9.4 Cybersecurity goals

9.4.1 Inputs

9.4.1.1 Prerequisites

The following information shall be available:

— item definition [WP-09-01].

9.4.1.2 Further supporting information

The following information can be considered:

— cybersecurity events [WP-08-03].

9.4.2 Requirements and recommendations

[RQ-09-03] An analysis based on the item definition shall be performed that involves:

a) asset identification in accordance with 15.3;

b) threat scenario identification in accordance with 15.4;

c) impact rating in accordance with 15.5;

d) attack path analysis in accordance with 15.6;

e) attack feasibility rating in accordance with 15.7; and

f) risk value determination in accordance with 15.8.

NOTE 1 If the item definition does not provide sufficient information for the analysis, such information can be assumed.

[RQ-09-04] Based on the results of [RQ-09-03], risk treatment options shall be determined for each threat scenario in accordance with 15.9.

NOTE 2 Avoiding a risk by removing the risk source can lead to change in the item in accordance with change management (see 5.4.4).

[RQ-09-05] If the risk treatment decision for a threat scenario includes reducing the risk, then one or more corresponding cybersecurity goals shall be specified.

NOTE 3 A cybersecurity goal is a requirement to protect assets against a threat scenario.

NOTE 4 If applicable, a CAL can be determined for cybersecurity goals (see Annex E).

NOTE 5 Cybersecurity goals can be specified for any lifecycle phase of the item.

[RQ-09-06] If the risk treatment decision for a threat scenario includes:

a) sharing the risk; or

b) retaining the risk due to one or more assumptions used during the analysis of [RQ-09-03],

then one or more corresponding cybersecurity claims shall be specified.

NOTE 6 Cybersecurity claims can be considered for cybersecurity monitoring.

[RQ-09-07] A verification shall be performed to confirm:

a) correctness and completeness of the result of [RQ-09-03] with respect to the item definition;

b) completeness, correctness and consistency of the risk treatment decisions of [RQ-09-04] with respect to the results of [RQ-09-03];

c) completeness, correctness and consistency of the cybersecurity goals of [RQ-09-05] and of the cybersecurity claims of [RQ-09-06] with respect to the risk treatment decisions of [RQ-09-04]; and

d) consistency of all cybersecurity goals of [RQ-09-05] and cybersecurity claims of [RQ-09-06] of the item.

9.4.3 Work products

[WP-09-02] TARA, resulting from [RQ-09-03] and [RQ-09-04]

[WP-09-03] Cybersecurity goals, resulting from [RQ-09-05]

[WP-09-04] Cybersecurity claims, resulting from [RQ-09-06]

[WP-09-05] Verification report for cybersecurity goals, resulting from [RQ-09-07]

9.5 Cybersecurity concept

9.5.1 Inputs

9.5.1.1 Prerequisites

The following information shall be available:

— item definition [WP-09-01];

— cybersecurity goals [WP-09-03]; and

— cybersecurity claims [WP-09-04].

9.5.1.2 Further supporting information

The following information can be considered:

— TARA [WP-09-02].

9.5.2 Requirements and recommendations

[RQ-09-08] Technical and/or operational cybersecurity controls and their interactions to achieve the cybersecurity goals shall be described, taking into account:

a) dependencies between the functions of the item; and/or

b) cybersecurity claims.

NOTE 1 The description can include:

— conditions for achieving cybersecurity goals, e.g. prevention of the compromise, detection and monitoring of the compromise,

— functions dedicated to address specific aspects of threat scenarios, e.g. use of a secure communication channel.

NOTE 2 The description can serve to evaluate designs and to determine targets for cybersecurity validation.

[RQ-09-09] Cybersecurity requirements of the item and requirements on the operational environment shall be defined for the cybersecurity goals in accordance with the description of [RQ-09-08].

NOTE 3 The cybersecurity requirements can depend on or include, specific features of the item, such as update capabilities or the capability to obtain user consent during operations.

NOTE 4 Requirements on the operational environment are realized outside of the item but they are included in the cybersecurity validation for the item to confirm whether the corresponding cybersecurity goals are achieved.

NOTE 5 Requirements on other items as part of the operational environment can be cybersecurity requirements on those items.

[RQ-09-10] The cybersecurity requirements shall be allocated to the item, and if applicable to one or more of its components.

NOTE 6 The description of cybersecurity controls complements the specification and allocation of cybersecurity requirements and of requirements on the operational environment, which all together constitute the cybersecurity concept.

[RQ-09-11] The results of [RQ-09-08], [RQ-09-09] and [RQ-09-10] shall be verified to confirm:

a) completeness, correctness, and consistency with respect to cybersecurity goals; and

b) consistency with respect to cybersecurity claims.

9.5.3 Work products

[WP-09-06] Cybersecurity concept, resulting from [RQ-09-08], [RQ-09-09] and [RQ-09-10]

[WP-09-07] Verification report for the cybersecurity concept, resulting from [RQ-09-11]

10 Product development

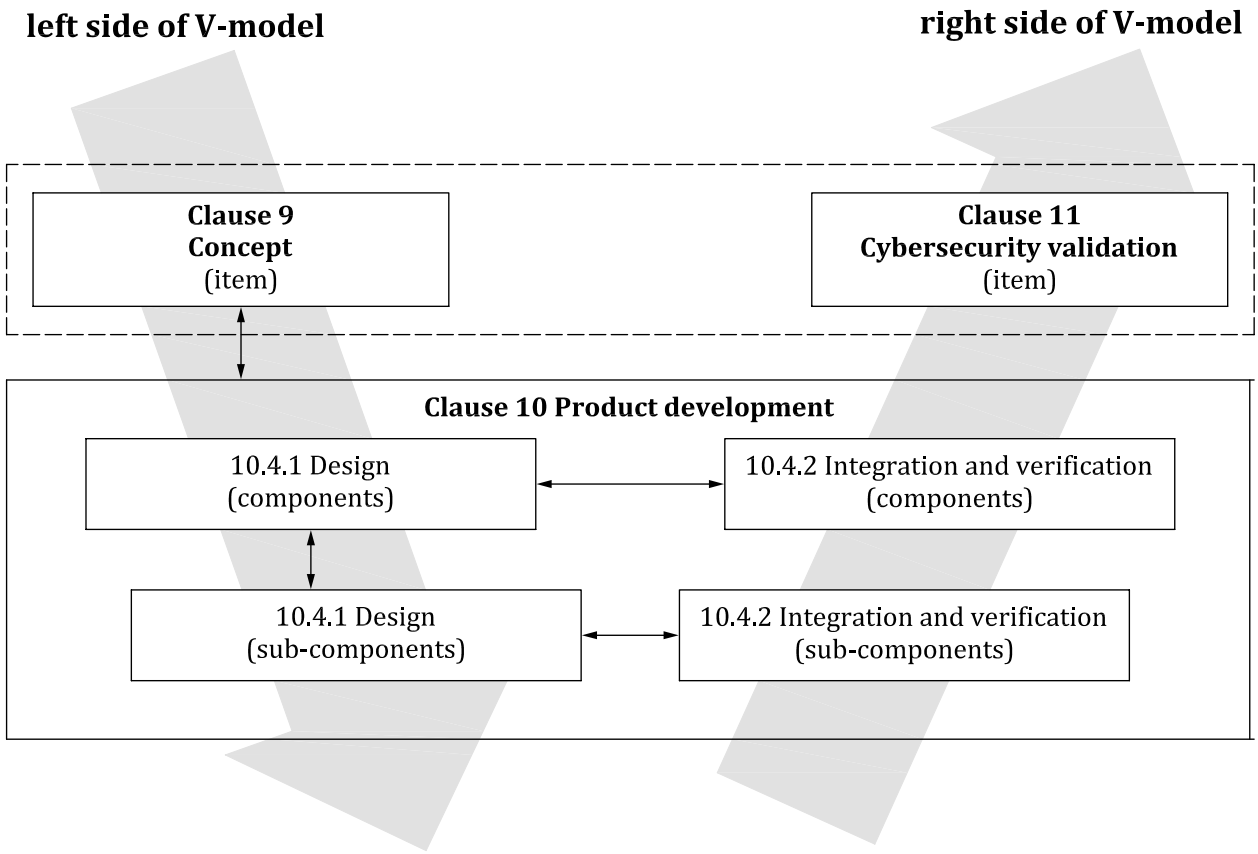
10.1 General

This clause describes the specification of the cybersecurity requirements and architectural design (see 10.4.1).

Additionally, this clause describes integration and verification activities (see 10.4.2).

These cybersecurity activities are performed iteratively until no further refinements of cybersecurity controls are needed. The cybersecurity specifications are defined and confirmed through verification activities for the fulfilment of the cybersecurity concept.

Figure 9 illustrates an example of how product development activities can be applied to a V-model-based workflow, where 10.4.1 corresponds to the left side of the V-model and 10.4.2 corresponds to the right side. In this example, two layers of abstraction are assumed under the item level, namely component level and sub-component level. This workflow can be extended to cover any level of abstraction.



Key

↕ Vertical bi-directional arrows depict verifications against the cybersecurity specification from a higher level of architectural abstraction during design as described in 10.4.1.

↔ Horizontal bi-directional arrows depict verifications of the implemented and integrated component against its cybersecurity specifications as described in 10.4.2.

Figure 9 — Example of product development activities in the V-model

Development approaches or methods that differ from the V-model (e.g. agile software development) can be applied.

CAL can be used to scale the depth and rigour of the activities in this clause and the methods used for them (see Annex E).

10.2 Objectives

The objectives of this clause are to:

a) define cybersecurity specifications;

NOTE 1 These can include the specification of cybersecurity-related components that are not present in the existing architectural design.

b) verify that the defined cybersecurity specifications conform to the cybersecurity specifications from higher levels of architectural abstraction;

c) identify weaknesses in the component; and

NOTE 2 Vulnerability analysis and management are described in Clause 8.

d) provide evidence that the results of the implementation and integration of components conform to the cybersecurity specifications.

10.3 Inputs

10.3.1 Prerequisites

The following information shall be available:

— cybersecurity specifications from higher levels of architectural abstraction [WP-10-01];

NOTE 1 This can be limited to the information relevant for the component under development, e.g.

— cybersecurity requirements allocated to the component under development;

— external interface specifications of the component under development;

— information assumed on the operational environment of the component under development.

NOTE 2 For development at the highest level of architectural abstraction, the cybersecurity concept [WP-09-06] for the item and the item definition [WP-09-01] are used instead of the cybersecurity specifications from higher levels of architectural abstraction.

10.3.2 Further supporting information

The following information can be considered:

— item definition [WP-09-01];

— cybersecurity concept [WP-09-06];

— existing architectural design;

— already established cybersecurity controls;

— known weaknesses and vulnerabilities from reused components.

10.4 Requirements and recommendations

10.4.1 Design

[RQ-10-01] Cybersecurity specifications shall be defined based on:

a) cybersecurity specifications from higher levels of architectural abstraction;

b) cybersecurity controls selected for implementation, if applicable; and

EXAMPLE 1 Use of a separate microcontroller with an embedded hardware trust anchor for secure key store functionality and isolation of the trust anchor regarding non-secure external connections.

NOTE 1 Cybersecurity controls can be selected from trusted catalogues.

c) existing architectural design, if applicable.

NOTE 2 Cybersecurity specifications include the specification of interfaces between sub-components of the defined architectural design related to the fulfilment of the defined cybersecurity requirements, including their usage, static and dynamic aspects.

NOTE 3 When defining cybersecurity specifications, cybersecurity implications of post-development phases can be considered, e.g. secure management of the key store; deactivation of debug interfaces; procedures to delete personally identifiable information.

NOTE 4 The cybersecurity specifications can include the identification of configuration and calibration parameters relevant for fulfilling the cybersecurity requirements, as well as their settings or permitted range of values, e.g. the correct configuration for the integration of the hardware security module.

NOTE 5 Capability of a component necessary to implement the cybersecurity controls can be considered, e.g. processor performance, memory resources.

[RQ-10-02] The defined cybersecurity requirements shall be allocated to components of the architectural design.

[RQ-10-03] Procedures to ensure cybersecurity after the development of the component shall be specified, if applicable.

EXAMPLE 2 Procedures for correct integration and initialization of cybersecurity controls, as well as maintaining cybersecurity throughout production.

[RQ-10-04] If design, modelling or programming notations or languages are used for the cybersecurity specifications or their implementation, the following shall be considered when selecting such a notation or language:

a) an unambiguous and comprehensible definition in both syntax and semantics;

b) support for achievement of modularity, abstraction and encapsulation;

c) support for the use of structured constructs;

d) support for the use of secure design and implementation techniques;

e) ability to integrate already existing components; and

EXAMPLE 3 Library, framework, software component written in another language.

f) resilience of the language against vulnerabilities due to its improper use.

EXAMPLE 4 Resilience against buffer overflows.

NOTE 6 For software development, implementation includes coding using programming languages.

[RQ-10-05] Criteria (see [RQ-10-04]) for suitable design, modelling or programming languages for cybersecurity that are not addressed by the language itself shall be covered by design, modelling and coding guidelines, or by the development environment.

EXAMPLE 5 Use of MISRA C:2012 [17] or CERT C [18] for secure coding in the “C” programming language.

EXAMPLE 6 Criteria for suitable design, modelling and programming languages:

— use of language subsets;

— enforcement of strong typing; and/or

— use of defensive implementation techniques.

[RC-10-06] Established and trusted design and implementation principles should be applied to avoid or minimize the introduction of weaknesses.

NOTE 7 Examples of design principles for architectural design for cybersecurity are given in NIST Special Publication 800-160 Vol. 1[19], appendix F.1.

[RQ-10-07] The architectural design defined in [RQ-10-01] shall be analysed to identify weaknesses.

NOTE 8 Known weaknesses and vulnerabilities from reused components can be considered.

NOTE 9 Identified weaknesses are analysed for vulnerabilities (see 8.5) and identified vulnerabilities are managed (see 8.6). However, identified weaknesses can be resolved with changes to the architectural design without performing a vulnerability analysis.

[RQ-10-08] The defined cybersecurity specifications shall be verified to ensure completeness, correctness, and consistency with the cybersecurity specifications from higher levels of architectural abstraction.

NOTE 10 Verification methods can include:

— review;

— analysis;

— simulation; and/or

— prototyping.

10.4.2 Integration and verification

[RQ-10-09] Integration and verification activities shall verify that the implementation and integration of components fulfil the defined cybersecurity specifications.

[RQ-10-10] The integration and verification activities of [RQ-10-09] shall be specified considering:

a) the defined cybersecurity specifications;

b) configurations intended for series production, if applicable;

c) sufficient capability to support the functionality specified in the defined cybersecurity specifications; and

d) conformity with the modelling, design and coding guidelines of [RQ-10-05], if applicable.

NOTE 1 This can include the vehicle integration and verification.

NOTE 2 Methods for verification can include:

— requirements-based test;

— interface test;

— resource usage evaluation;

— verification of the control flow and data flow;

— dynamic analysis; and/or

— static analysis.

NOTE 3 If verification by testing is adopted, test cases and test environments can be selected, considering:

— level of integration for testing to achieve the verification objectives;

— necessity for additional tests during subsequent integration activities based on an analysis of the selected test environment, e.g. due to different bit widths of data words and address words of the target processor for final integration compared to a processor emulation or development environment.

NOTE 4 Methods for deriving test cases can include:

— analysis of requirements;

— generation and analysis of equivalence classes;

— boundary value analysis; and/or

— error guessing based on knowledge or experience.

[RQ-10-11] If verification by testing is adopted, test coverage shall be evaluated using defined test coverage metrics to determine sufficiency of the test activities.

NOTE 5 Standard test coverage metrics can be inadequate for cybersecurity, e.g. statement coverage for software.

[RC-10-12] Testing should be performed in order to confirm that unidentified weaknesses and vulnerabilities remaining in the component are minimized.

NOTE 6 Unnecessary functionalities can contain a weakness.

NOTE 7 Testing methods can include:

— functional testing;

— vulnerability scanning;

— fuzz testing; and/or

— penetration testing.

NOTE 8 Identified weaknesses are analysed for vulnerabilities (see 8.5) and identified vulnerabilities are managed (see 8.6). However, identified weaknesses can be resolved with changes to the architectural design without performing a vulnerability analysis.

[RQ-10-13] If testing in accordance with [RC-10-12] is not performed, then a rationale shall be provided.

NOTE 9 The rationale can include the following considerations:

— feasibility to access the attack surface of the component;

— capabilities to (directly or indirectly) access the component in combination with compromise of other components; and/or

— simplicity of the component.

10.5 Work products

[WP-10-01] Cybersecurity specifications, resulting from [RQ-10-01] and [RQ-10-02]

[WP-10-02] Cybersecurity requirements for post-development, resulting from [RQ-10-03]

[WP-10-03] Documentation of the modelling, design or programming languages and coding guidelines, if applicable, resulting from [RQ-10-04] and [RQ-10-05]

[WP-10-04] Verification report for the cybersecurity specifications, resulting from [RQ-10-08]

[WP-10-05] Weaknesses found during product development, resulting from [RQ-10-07] and [RC-10-12], if applicable

[WP-10-06] Integration and verification specification, resulting from [RQ-10-10]

[WP-10-07] Integration and verification report, resulting from [RQ-10-09], [RQ-10-11] and [RC-10-12]

11 Cybersecurity validation

11.1 General

This clause describes activities for cybersecurity validation at the vehicle level for the item (see Figure 9). The item is considered in its operational environment at the vehicle level along with the configurations intended for series production.

11.2 Objectives

The objectives of this clause are to:

a) validate the cybersecurity goals and cybersecurity claims;

b) confirm the item achieves the cybersecurity goals; and

c) confirm that no unreasonable risks remain.

11.3 Inputs

11.3.1 Prerequisites

The following information shall be available:

— item definition [WP-09-01];

— cybersecurity goals [WP-09-03]; and

— cybersecurity claims [WP-09-04], if applicable.

11.3.2 Further supporting information

The following information can be considered:

— cybersecurity concept [WP-09-06];

— work products from product development (see 10.5).

11.4 Requirements and recommendations

[RQ-11-01] Validation activities at the vehicle level for the item considering the configurations for series production shall confirm:

a) adequacy of the cybersecurity goals with respect to the threat scenarios and corresponding risk;

NOTE 1 If any risks not addressed by cybersecurity goals are identified during validation, they can be addressed in accordance with 9.4.

b) achievement of the cybersecurity goals of the item;

c) validity of the cybersecurity claims; and

d) validity of the requirements on the operational environment, if applicable.

NOTE 2 Validation activities can include:

— confirmation of achievement of cybersecurity goals by reviewing the work products of 9.5 and Clause 10;

— penetration testing to demonstrate adequacy and achievement of cybersecurity goals; and/or

— review of all managed risks identified through Clauses 9 and 10.

NOTE 3 CAL can be used to scale the depth and rigour of the penetration testing (see Annex E).

NOTE 4 Weaknesses identified during the validation activities of [RQ-11-01] are analysed for vulnerabilities (see 8.5) and identified vulnerabilities are managed (see 8.6).

[RQ-11-02] A rationale for the selection of validation activities shall be provided.

11.5 Work products

[WP-11-01] Validation report, resulting from [RQ-11-01] and [RQ-11-02]

12 Production

12.1 General

Production covers the manufacturing and assembly of an item or component, including the vehicle level. A production control plan is created to ensure that cybersecurity requirements for post-development are applied to the item or component and to ensure that vulnerabilities cannot be introduced during production.

12.2 Objectives

The objectives of this clause are to:

a) apply the cybersecurity requirements for post-development; and

b) prevent the introduction of vulnerabilities during production.

12.3 Inputs

12.3.1 Prerequisites

The following information shall be available:

— release for post-development report [WP-06-04]; and

— cybersecurity requirements for post-development [WP-10-02].

12.3.2 Further supporting information

None.

12.4 Requirements and recommendations

[RQ-12-01] A production control plan shall be created that applies the cybersecurity requirements for post-development.

NOTE 1 The production control plan can be included as part of an overall production plan.

[RQ-12-02] The production control plan shall include:

a) sequence of steps that apply the cybersecurity requirements for post-development;

b) production tools and equipment;

c) cybersecurity controls to prevent unauthorized alteration during production; and

EXAMPLE 1 Physical controls that prevent physical access to production servers holding software.

EXAMPLE 2 Logical controls that apply cryptographic techniques and/or access controls.

d) methods to confirm that the cybersecurity requirements for post-development are met.

NOTE 2 Methods can include inspection and calibration checks.

NOTE 3 To manufacture an item or component and install the hardware and software, the production process can use privileged access. Such access can introduce vulnerabilities in the item or component if used in an unauthorized manner after production.

[RQ-12-03] The production control plan shall be implemented.

12.5 Work products

[WP-12-01] Production control plan, resulting from [RQ-12-01] and [RQ-12-02]

13 Operations and maintenance

13.1 General

This clause describes cybersecurity incident response (see 13.3) and updates (see 13.4) to items or components in the field.

Cybersecurity incident response occurs when an organization invokes it as part of vulnerability management (see 8.6).

Updates are changes made to an item or component during post-development and can include additional information, e.g. technical specifications, integration manuals, user manuals. Organizations can issue updates for various reasons, e.g. addressing vulnerabilities or safety issues, providing functional improvements. The work products concerning updates are documented as work products of other clauses.

Modifications of items or components that are in the concept, product development or production phases are covered by change management (see 5.4.4) instead of this clause.

13.2 Objectives

The objectives of this clause are to:

a) determine and implement remedial actions for cybersecurity incidents; and

b) maintain cybersecurity during and after updates to items or components after production until their end of cybersecurity support.

13.3 Cybersecurity incident response

13.3.1 Inputs

13.3.1.1 Prerequisites

None.

13.3.1.2 Further supporting information

The following information can be considered:

— cybersecurity information related to the vulnerability that caused the cybersecurity incident response;

— vulnerability analysis [WP-08-05].

13.3.2 Requirements and recommendations

[RQ-13-01] For each cybersecurity incident, a cybersecurity incident response plan shall be created that includes:

a) remedial actions;

NOTE 1 Remedial actions are determined by vulnerability management in 8.6.

b) a communication plan;

NOTE 2 The creation of a communication plan can involve internal interested parties, e.g. marketing or public relations, product development teams, legal, customer relations, quality management, purchasing.

NOTE 3 A communication plan can include identification of internal and external communication partners (e.g. development, researchers, the general public, authorities) and development of specific information for these audiences.

c) assigned responsibilities for the remedial actions;

NOTE 4 Those responsible can have:

— expertise in affected items or components, including legacy items and components;

— organizational knowledge (e.g. business processes, communications, purchasing, legal); and/or

— decision authority.

d) a procedure for recording new cybersecurity information relevant to the cybersecurity incident;

NOTE 5 New cybersecurity information can be collected in accordance with 8.3, e.g. information on:

— affected components;

— related incidents and vulnerabilities;

— forensic data such as data logs, crash sensor data; and/or

— end-user complaints.

e) a method for determining progress;

EXAMPLE Measures of progress are:

— percentage of affected items or components that are remediated; and/or

— percentage of items or components affected by remedial actions.

f) criteria for closure of the cybersecurity incident response; and

g) actions for the closure.

[RQ-13-02] The cybersecurity incident response plan shall be implemented.

13.3.3 Work products

[WP-13-01] Cybersecurity incident response plan, resulting from [RQ-13-01]

13.4 Updates

13.4.1 Inputs

13.4.1.1 Prerequisites

The following information shall be available:

— release for post-development report [WP-06-04].

13.4.1.2 Further supporting information

The following information can be considered:

— cybersecurity incident response plan [WP-13-01];

— cybersecurity requirements for post-development [WP-10-02] relevant to the update.

13.4.2 Requirements and recommendations

[RQ-13-03] Updates and update-related capabilities within the vehicle shall be developed in accordance with this document.

13.4.3 Work products

None.

14 End of cybersecurity support and decommissioning

14.1 General

Decommissioning is different from end of cybersecurity support. An organization can end cybersecurity support for an item or component, but that item or component can still function as designed in the field. Both decommissioning and end of cybersecurity support can present cybersecurity implications, but those implications are considered separately.

Decommissioning can occur without the organization's knowledge and in such a way that decommissioning procedures cannot be enforced, therefore the act of decommissioning is out of scope of this document.

End of cybersecurity support and decommissioning are considered in the concept and product development phases.

14.2 Objectives

The objectives of this clause are to:

a) communicate the end of cybersecurity support; and

b) enable decommissioning of items and components with regard to cybersecurity.

14.3 End of cybersecurity support

14.3.1 Inputs

None.

14.3.2 Requirements and recommendations

[RQ-14-01] A procedure shall be created to communicate to customers when an organization decides to end cybersecurity support for an item or component.

NOTE 1 These communications can be handled under contract requirements between suppliers and customers.

NOTE 2 Communication to vehicle owners can be delivered by an announcement.

14.3.3 Work products

[WP-14-01] Procedures to communicate the end of cybersecurity support, resulting from [RQ-14-01]

14.4 Decommissioning

14.4.1 Inputs

14.4.1.1 Prerequisites

The following information shall be available:

— cybersecurity requirements for post-development [WP-10-02].

14.4.1.2 Further supporting information

None.

14.4.2 Requirements and recommendations

[RQ-14-02] The cybersecurity requirements for post-development with regard to decommissioning shall be made available.

NOTE Appropriate documentation (e.g. instructions, user manuals) relating to such requirements can enable decommissioning with regard to cybersecurity.

14.4.3 Work products

None.

15 Threat analysis and risk assessment methods

15.1 General

This clause describes methods to determine the extent to which a road user can be impacted by a threat scenario. These methods and their work products are collectively known as a threat analysis and risk assessment (TARA) and are performed from the viewpoint of affected road users. The methods defined in this clause are generic modules that can be invoked systematically, and from any point in the lifecycle of an item or component:

— asset identification (see 15.3);

— threat scenario identification (see 15.4);

— impact rating (see 15.5);

— attack path analysis (see 15.6);

— attack feasibility rating (see 15.7);

— risk value determination (see 15.8); and

— risk treatment decision (see 15.9).

Because these are generic modules, the work products defined in this clause are documented as parts of work products produced by other clauses.

See Annex H for an illustration of these methods with a practical example.

Organization specific scales for impact rating, attack feasibility rating and risk value determination can be applied and mapped to the corresponding scales defined in this document.

15.2 Objectives

The objectives of this clause are to:

a) identify assets, their cybersecurity properties and their damage scenarios;

b) identify threat scenarios;

c) determine the impact rating of damage scenarios;

d) identify the attack paths that realize threat scenarios;

e) determine the ease with which attack paths can be exploited;

f) determine the risk values of threat scenarios; and

g) select appropriate risk treatment options for threat scenarios.

15.3 Asset identification

15.3.1 Inputs

15.3.1.1 Prerequisites

The following information shall be available:

— item definition [WP-09-01].

15.3.1.2 Further supporting information

The following information can be considered:

— cybersecurity specifications [WP-10-01].

15.3.2 Requirements and recommendations

[RQ-15-01] Damage scenarios shall be identified.

NOTE 1 A damage scenario can include:

— relation between the functionality of the item and the adverse consequence;

— description of harm to the road user; and/or

— relevant assets.

[RQ-15-02] Assets with cybersecurity properties whose compromise leads to a damage scenario shall be identified.

NOTE 2 The identification of assets can be based on:

— analysing the item definition;

— performing an impact rating;

— deriving assets from threat scenarios; and/or

— using predefined catalogues.

EXAMPLE 1 The asset is personal information (customer personal preferences) stored in an infotainment system and its cybersecurity property is confidentiality. The damage scenario is disclosure of the personal information without the customer's consent resulting from the loss of confidentiality.

EXAMPLE 2 The asset is data communication of the braking function and its cybersecurity property is integrity. The damage scenario is collision with following vehicle (rear-end collision) caused by unintended full braking when the vehicle is travelling at high speed.

15.3.3 Work products

[WP-15-01] Damage scenarios, resulting from [RQ-15-01]

[WP-15-02] Assets with cybersecurity properties, resulting from [RQ-15-02]

15.4 Threat scenario identification

15.4.1 Inputs

15.4.1.1 Prerequisites

The following shall be available:

— item definition [WP-09-01].

15.4.1.2 Further supporting information

The following information can be considered:

— cybersecurity specifications [WP-10-01];

— damage scenarios [WP-15-01];

— assets with cybersecurity properties [WP-15-02].

15.4.2 Requirements and recommendations

[RQ-15-03] Threat scenarios shall be identified and include:

— targeted asset;

— compromised cybersecurity property of the asset; and

— cause of compromise of the cybersecurity property.

NOTE 1 Further information can be included or associated with a threat scenario, e.g. damage scenarios, technical interdependencies between assets, attackers, methods, tools, and attack surfaces.

NOTE 2 The method for threat scenario identification can use group discussion and/or systematic approaches, for example:

— elicitation of malicious use cases resulting from reasonably foreseeable misuse and/or abuse;

— threat modelling approaches based on frameworks such as EVITA [20], TVRA [21], PASTA [22], STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege).

NOTE 3 A damage scenario can correspond to multiple threat scenarios and a threat scenario can lead to multiple damage scenarios.

EXAMPLE Spoofing of CAN messages for the braking ECU leads to loss of integrity of the CAN messages and thereby to loss of integrity of the braking function.

15.4.3 Work products

[WP-15-03] Threat scenarios, resulting from [RQ-15-03]

15.5 Impact rating

15.5.1 Inputs

15.5.1.1 Prerequisites

The following shall be available:

— damage scenarios [WP-15-01].

15.5.1.2 Further supporting information

The following information can be considered:

— item definition [WP-09-01];

— assets with cybersecurity properties [WP-15-02].

15.5.2 Requirements and recommendations

[RQ-15-04] The damage scenarios shall be assessed against potential adverse consequences for road users in the impact categories of safety, financial, operational, and privacy (S, F, O, P) respectively.

NOTE 1 This document does not provide relationships (e.g. weighting) between different impact categories.

NOTE 2 Additional impact categories can be considered.

NOTE 3 If additional impact categories are considered, then the rationale and explanation of these categories can be shared in the supply chain in accordance with Clause 7.

[RQ-15-05] The impact rating of a damage scenario shall be determined for each impact category to be one of the following:

— severe;

— major;

— moderate; or

— negligible.

NOTE 4 Financial, operational and privacy related impacts can be rated in accordance with tables given in Annex F.

[RQ-15-06] Safety related impact ratings shall be derived from ISO 26262-3:2018, 6.4.3.

NOTE 5 Table F.1 in Annex F can be used for mapping safety impact criteria to impact ratings.

NOTE 6 Evaluation for functional safety can be reused for this purpose.

[PM-15-07] If a damage scenario results in an impact rating and an argument can be made that every impact of another impact category is considered less critical, then further analysis for that other impact category may be omitted.

EXAMPLE The safety impact of a damage scenario is rated “severe”, consequently financial impact of that damage scenario is not further analysed.

15.5.3 Work products

[WP-15-04] Impact ratings with associated impact categories, resulting from [RQ-15-04] to [RQ-15-06]

15.6 Attack path analysis

15.6.1 Inputs

15.6.1.1 Prerequisites

The following information shall be available:

— item definition [WP-09-01] or cybersecurity specifications [WP-10-01]; and

NOTE The item definition is used if the attack path analysis is performed on an item, and the cybersecurity specifications are used if the attack path analysis is performed on a component.

— threat scenarios [WP-15-03].

15.6.1.2 Further supporting information

The following information can be considered:

— weaknesses from cybersecurity events [WP-08-04];

— weaknesses found during product development [WP-10-05];

— architectural design;

— previously identified attack paths [WP-15-05], if available;

— vulnerability analysis [WP-08-05].

15.6.2 Requirements and recommendations

[RQ-15-08] The threat scenarios shall be analysed to identify attack paths.

NOTE 1 An attack path analysis can be based on:

— top-down approaches that deduce attack paths by analysing the different ways in which a threat scenario could be realised, e.g. attack trees, attack graphs; and/or

— bottom-up approaches that build attack paths from the vulnerabilities identified.

NOTE 2 If a partial attack path does not lead to the realization of a threat scenario, the analysis of this partial attack path can be stopped.

[RQ-15-09] An attack path shall be associated with the threat scenarios that can be realized by the attack path.

NOTE 3 In early stages of product development, attack paths are often incomplete or imprecise as specific implementation details are not yet known to be able to identify specific vulnerabilities. During product development, the attack paths can be updated as more information becomes available, e.g. after a vulnerability analysis.

EXAMPLE

— Threat scenario: spoofing of CAN messages for the braking ECU leads to loss of integrity of the CAN messages and thereby to loss of integrity of the braking function.

— Attack path realizing the above threat scenario:

  i. the telematics ECU is compromised via the cellular interface;

  ii. the gateway ECU is compromised via CAN communication from the telematics ECU;

  iii. the gateway ECU forwards malicious braking request signals (unwanted rapid deceleration).

15.6.3 Work products

[WP-15-05] Attack paths, resulting from [RQ-15-08] and [RQ-15-09]

15.7 Attack feasibility rating

15.7.1 Inputs

15.7.1.1 Prerequisites

The following information shall be available:

— attack paths [WP-15-05].

15.7.1.2 Further supporting information

The following information can be considered:

— architectural design;

— vulnerability analysis [WP-08-05].

15.7.2 Requirements and recommendations

[RQ-15-10] For each attack path, the attack feasibility rating shall be determined as described in Table 1.

Table 1 — Attack feasibility ratings and respective descriptions

Attack feasibility rating	Description
High	The attack path can be accomplished utilizing low effort.
Medium	The attack path can be accomplished utilizing medium effort.
Low	The attack path can be accomplished utilizing high effort.
Very low	The attack path can be accomplished utilizing very high effort.

[RC-15-11] The attack feasibility rating method should be defined based on one of the following approaches:

a) attack potential-based approach;

b) CVSS-based approach; or

c) attack vector-based approach.

NOTE 1 Selection of the approach can depend upon the phase in the lifecycle and available information.

[RC-15-12] If an attack potential-based approach is used, the attack feasibility rating should be determined based on core factors including:

a) elapsed time;

b) specialist expertise;

c) knowledge of the item or component;

d) window of opportunity; and

e) equipment.

NOTE 2 The core attack potential factors can be derived from ISO/IEC 18045 [23].

NOTE 3 G.2 provides guidelines on determining attack feasibility based on attack potential.

[RC-15-13] If a CVSS-based approach is used, the attack feasibility rating should be determined based on the exploitability metrics of the base metric group, including:

a) attack vector;

b) attack complexity;

c) privileges required; and

d) user interaction.

NOTE 4 G.3 provides guidelines on determining attack feasibility based on a CVSS-based approach.

[RC-15-14] If an attack vector-based approach is used, the attack feasibility rating should be determined based on evaluating the predominant attack vector (cf. CVSS [24] 2.1.1) of the attack path.

NOTE 5 G.4 provides guidelines on determining attack feasibility based on an attack vector-based approach.

NOTE 6 During the early stages of development (e.g. concept phase), when there is insufficient information to identify specific attack paths, an attack vector-based approach can be suitable to estimate attack feasibility.

15.7.3 Work products

[WP-15-06] Attack feasibility ratings, resulting from [RQ-15-10]

15.8 Risk value determination

15.8.1 Inputs

15.8.1.1 Prerequisites

The following information shall be available:

— threat scenarios [WP-15-03];

— impact ratings with associated impact categories [WP-15-04]; and

— attack feasibility ratings [WP-15-06].

15.8.1.2 Further supporting information

None.

15.8.2 Requirements and recommendations

[RQ-15-15] For each threat scenario the risk value shall be determined from the impact of the associated damage scenarios and the attack feasibility of the associated attack paths.

NOTE 1 If a threat scenario corresponds to more than one damage scenario and/or an associated damage scenario has impacts in more than one impact category, a separate risk value can be determined separately for each of those impact ratings.

NOTE 2 If the threat scenario corresponds to more than one attack path, the associated attack feasibility ratings can be appropriately aggregated, e.g. the threat scenario is assigned the maximum of the attack feasibility ratings of the corresponding attack paths.

[RQ-15-16] The risk value of a threat scenario shall be a value between (and including) 1 and 5, where a value of 1 represents minimal risk.

EXAMPLE Methods for risk value determination:

— risk matrices;

— risk formulas.

15.8.3 Work products

[WP-15-07] Risk values, resulting from [RQ-15-15] and [RQ-15-16]

15.9 Risk treatment decision

15.9.1 Inputs

15.9.1.1 Prerequisites

The following information shall be available:

— item definition [WP-09-01];

— threat scenarios [WP-15-03]; and

— risk values [WP-15-07].

15.9.1.2 Further supporting information

The following information can be considered:

— cybersecurity specifications [WP-10-01];

— previous risk treatment decisions of the item or component, or of similar items or components;

— impact ratings with associated impact categories [WP-15-04];

— attack paths [WP-15-05];

— attack feasibility ratings [WP-15-06].

15.9.2 Requirements and recommendations

[RQ-15-17] For each threat scenario, considering its risk values, one or more of the following risk treatment option(s) shall be determined:

a) avoiding the risk;

EXAMPLE 1 Avoiding the risk by removing the risk sources, deciding not to start or continue with the activity that gives rise to the risk.

b) reducing the risk;

c) sharing the risk;

EXAMPLE 2 Sharing risk through contracts or transferring risk by buying insurance.

d) retaining the risk.

NOTE The rationales for retaining the risk and sharing the risk are recorded as cybersecurity claims and are subject to cybersecurity monitoring and vulnerability management in accordance with Clause 8.

15.9.3 Work products

[WP-15-08] Risk treatment decisions, resulting from [RQ-15-17]

Annex A
(informative)

Summary of cybersecurity activities and work products

A.1 General

Table A.1 provides a summary of the cybersecurity activities and their corresponding work products. This can help the organization to manage these activities, to ensure coverage of the cybersecurity activities, and to understand the potential workload of the project. The activities during the concept and product development phases are defined in the cybersecurity plan. The work products of these activities are thus in the scope of a cybersecurity assessment. All work products listed from Clause 15 are documented as work products in other clauses.

A.2 Overview of cybersecurity activities and work products

Table A.1 — Cybersecurity activities and work products of this document

Sub-clauses	Work products
Organizational cybersecurity management	
5.4.1 Cybersecurity governance	[WP-05-01] Cybersecurity policy, rules and processes
5.4.2 Cybersecurity culture	[WP-05-01] Cybersecurity policy, rules and processes [WP-05-02] Evidence of competence management, awareness management and continuous improvement
5.4.3 Information sharing	[WP-05-01] Cybersecurity policy, rules and processes
5.4.4 Management systems	[WP-05-03] Evidence of the organization's management systems
5.4.5 Tool management	[WP-05-04] Evidence of tool management
5.4.6 Information security management	[WP-05-03] Evidence of the organization's management systems
5.4.7 Organizational cybersecurity audit	[WP-05-05] Organizational cybersecurity audit report
Project dependent cybersecurity management	
6.4.1 Cybersecurity responsibilities	[WP-06-01] Cybersecurity plan
6.4.2 Cybersecurity planning	[WP-06-01] Cybersecurity plan
6.4.3 Tailoring	[WP-06-01] Cybersecurity plan
6.4.4 Reuse	[WP-06-01] Cybersecurity plan
6.4.5 Component out-of-context	[WP-06-01] Cybersecurity plan
6.4.6 Off-the-shelf component	[WP-06-01] Cybersecurity plan
6.4.7 Cybersecurity case	[WP-06-02] Cybersecurity case
6.4.8 Cybersecurity assessment	[WP-06-03] Cybersecurity assessment report
6.4.9 Release for post-development	[WP-06-04] Release for post-development report
Distributed cybersecurity activities	
7.4.1 Supplier capability	None
7.4.2 Request for quotation	None
7.4.3 Alignment of responsibilities	[WP-07-01] Cybersecurity interface agreement
Continual cybersecurity activities	

Table A.1 *(continued)*

Sub-clauses	Work products
8.3 Cybersecurity monitoring	[WP-08-01] Sources for cybersecurity information
	[WP-08-02] Triggers
	[WP-08-03] Cybersecurity events
8.4 Cybersecurity event evaluation	[WP-08-04] Weaknesses from cybersecurity events
8.5 Vulnerability analysis	[WP-08-05] Vulnerability analysis
8.6 Vulnerability management	[WP-08-06] Evidence of managed vulnerabilities
Concept phase	
9.3 Item definition	[WP-09-01] Item definition
9.4 Cybersecurity goals	[WP-09-02] TARA
	[WP-09-03] Cybersecurity goals
	[WP-09-04] Cybersecurity claims
	[WP-09-05] Verification report for cybersecurity goals
9.5 Cybersecurity concept	[WP-09-06] Cybersecurity concept
	[WP-09-07] Verification report of cybersecurity concept
Product development phase	
10.4.1 Design	[WP-10-01] Cybersecurity specifications
	[WP-10-02] Cybersecurity requirements for post-development
	[WP-10-03] Documentation of the modelling, design, or programming languages and coding guidelines
	[WP-10-04] Verification report for the cybersecurity specifications
	[WP-10-05] Weaknesses found during product development
10.4.2 Integration and verification	[WP-10-05] Weaknesses found during product development
	[WP-10-06] Integration and verification specification
	[WP-10-07] Integration and verification report
Clause 11 Cybersecurity validation	[WP-11-01] Validation report
Post-development phases	
Clause 12 Production	[WP-12-01] Production control plan
13.3 Cybersecurity incident response	[WP-13-01] Cybersecurity incident response plan
13.4 Updates	None
14.3 End of cybersecurity support	[WP-14-01] Procedures to communicate the end of cybersecurity support
14.4 Decommissioning	None
Threat analysis and risk assessment methods	
15.3 Asset identification	[WP-15-01] Damage scenarios
	[WP-15-02] Assets with cybersecurity properties
15.4 Threat scenario identification	[WP-15-03] Threat scenarios
15.5 Impact rating	[WP-15-04] Impact ratings with associated impact categories
15.6 Attack path analysis	[WP-15-05] Attack paths
15.7 Attack feasibility rating	[WP-15-06] Attack feasibility ratings
15.8 Risk value determination	[WP-15-07] Risk values
15.9 Risk treatment decision	[WP-15-08] Risk treatment decisions

Annex B
(informative)

Examples of cybersecurity culture

Table B.1 provides examples of weak and strong cybersecurity culture.

Table B.1 — Examples of weak and strong cybersecurity culture

Examples indicative of a weak cybersecurity culture	Examples indicative of a strong cybersecurity culture
Accountability for decisions related to cybersecurity is not traceable.	The process ensures that accountability for decisions related to cybersecurity is traceable.
Performance (of the implemented functionality or feature), cost or schedule take precedence over cybersecurity.	Cybersecurity and safety have the highest priority.
The reward system favours cost and schedule over cybersecurity.	The reward system supports and motivates the effective achievement of cybersecurity and penalizes those who take shortcuts that jeopardize cybersecurity.
Cybersecurity personnel force inappropriate and very strict adherence to cybersecurity without considering specific needs of projects/activities.	Cybersecurity personnel act as role models with a good sense for appropriateness and practical implementation that leads to trust in their actions by the entire organization.
Personnel assessing cybersecurity and its governing processes are influenced unduly by those responsible for executing the processes.	The process provides adequate checks and balances, e.g. the appropriate degree of independence in cybersecurity assessment.
Passive attitude towards cybersecurity, e.g.: — heavy dependence on testing at the end of the development; — not being prepared for potential weaknesses or incidents in the field; — management reacting only when there is a cybersecurity incident in production, in the field or if there is a lot of attention in the media about competitor products.	Proactive attitude towards cybersecurity, e.g.: — cybersecurity issues are discovered and resolved from the earliest stage in the product lifecycle (cybersecurity by design); — the organization is prepared to react fast to vulnerabilities or incidents in the field.
The required resources for cybersecurity are not allocated.	The required resources for cybersecurity are allocated. Skilled resources have the competence commensurate with the activity assigned.

Table B.1 *(continued)*

Examples indicative of a weak cybersecurity culture	Examples indicative of a strong cybersecurity culture
— "Groupthink" confirmation bias (i.e. uncritical acceptance or conformity to prevailing points of view). — "Stacking the deck" (i.e. choose members to ensure desired outcome) when forming review groups to prevent potential dissention. — Dissenter is ostracized or labelled as "not a team player" (e.g. uncooperative, intransigent, toxic person). — Dissent reflects negatively on performance reviews. — Minority dissenter is labelled or treated as a "troublemaker", "not a team player" or a "whistle-blower" (i.e. agitator, undesirable or a snitch). — Employees who express concerns fear repercussion.	The process uses diversity to its advantage: — intellectual diversity is sought, valued and integrated in all processes; — behaviour which counters the use of diversity is discouraged and penalized. The supporting communication and decision-making channels exist and the management encourages their usage: — self-disclosure is encouraged; — responsible disclosure by anyone (internal or external) of potential vulnerability is encouraged; — the discovery and resolution process continues in the field, in manufacturing and in development of other products.
No systematic continuous improvement processes, learning cycles or other forms of lessons learned.	Continuous improvement is integral to all processes.
Processes are ad hoc or implicit.	Defined, traceable, and controlled processes are followed.

Annex C
(informative)

Example of cybersecurity interface agreement template

C.1 General

In case different organizations are participating in distributed cybersecurity activities, it is important to agree on responsibilities, level of disclosure of information, and level of achievement for each milestone, between different organizations.

This annex provides an example template of a cybersecurity interface agreement in accordance with [RQ-07-04]. This template gives guidance on how to define roles and responsibilities for distributed cybersecurity activities between customer and supplier (Figure C.1).

Other information can also be added to the template, such as point of contact, target milestones, methods or tools for collaborations.

C.2 Example template

The column entries in this example template are:

a) **Phase**: phase of this document;

b) **Work product**: work products of this document that are related to the interface of the distributed activities;

c) **Doc ref**: relevant clauses of this document;

d) **Supplier**: supplier responsibilities by RASIC;

e) **Customer**: customer responsibilities by RASIC;

NOTE 1 The template uses RASIC to demonstrate the assignment of responsibilities for specific work products between organizations. RASIC can be used as follows:

— R (responsible): the organization that is responsible to conduct the activity;

— A (accountable): the organization that has the authority to approve the activity once it is complete;

— S (supporting): the organization that will help the organization responsible for the activity;

— I (informed): the organization that is informed of the progress of the activity and any decisions being made; and

— C (consulted): the organization that offers advice or guidance but does not actively work on the activity.

f) **Level of confidentiality**: supplier and customer agree on the confidentiality of each work product; and

NOTE 2 Possible levels of confidentiality can be:

— highly confidential: only the organization who created the work product is allowed to access it;

— confidential: both customer and supplier are allowed to access the work product;

— confidential with third parties: this work product is allowed to be shared with authorized external parties per 5.4.3; and

— public: the work product can be shared without any restrictions.

g) **Comment**: additional information concerning results of negotiation and discussion between organizations.

Phase	**Work product**	**Doc ref.**	**Supplier**					**Customer**					**Level of confidentiality**	**Comment**
			R	A	S	I	C	R	A	S	I	C		
Concept	Item definition													
	Treat analysis and risk assessment													
	Cybersecurity concept													
	Verification report of cybersecurity concept													
Product develop-ment	Cybersecurity specification													

Figure C.1 — Example of a cybersecurity interface agreement template

Annex D
(informative)

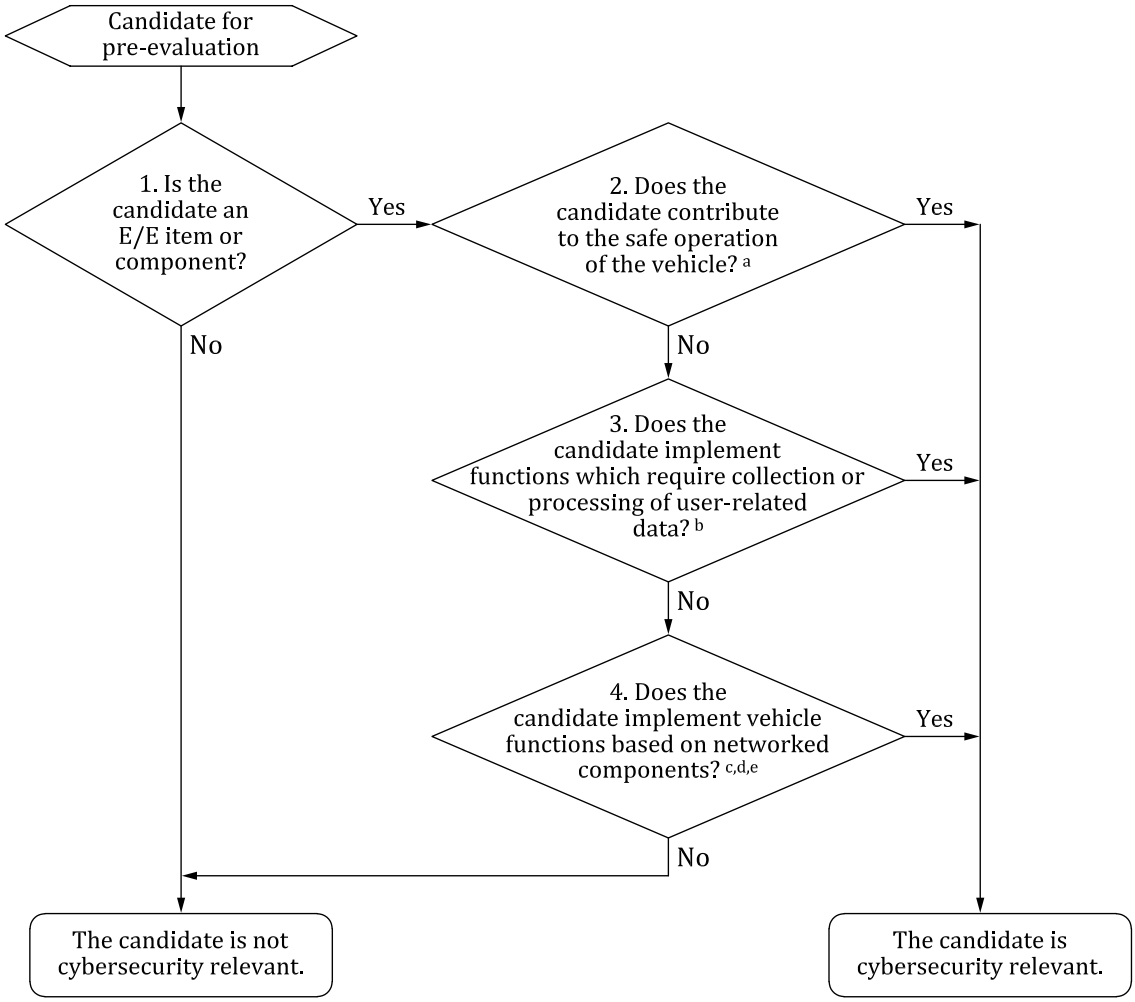
Cybersecurity relevance – example methods and criteria

D.1 General

This annex provides example methods to determine if an item or component is cybersecurity relevant (see [RQ-06-02]).

D.2 Methods

The cybersecurity relevance of a candidate item or component can be determined using the decision diagram in Figure D.1 that gives example criteria.



[a] EXAMPLE Motion control modules and modules with automotive safety integrity level (ASIL) designations.

[b] EXAMPLE Data related to drivers or passengers, or to potentially sensitive information such as location data.

[c] EXAMPLE Internal connections -- CAN, Ethernet, media-oriented systems transport (MOST), transmission control protocol/internet protocol (TCP/IP).

[d] EXAMPLE External connections -- function interface to backend server; cellular telecommunications network, on- board diagnostic (OBD-II) interface.

[e] EXAMPLE Wireless connected sensors or actuators – remote key-less entry (RKE), near field communication (NFC), tyre pressure monitoring system (TPMS).

Figure D.1 — Cybersecurity relevance example method and criteria

Cybersecurity relevance can also be determined based on experience and multiple expert judgements, e.g. involving safety experts and cybersecurity experts.

Annex E
(informative)

Cybersecurity assurance levels

E.1 General

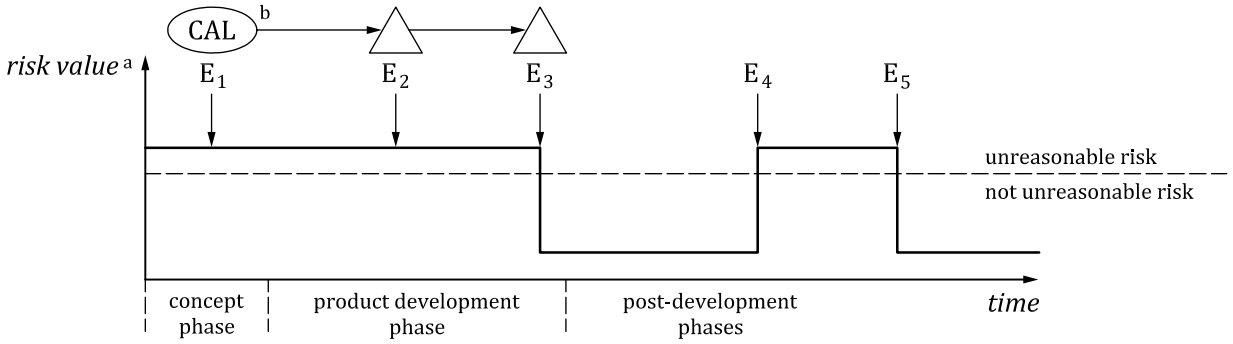
This annex describes a cybersecurity assurance level (CAL) classification scheme that can be used to specify and communicate a set of assurance requirements, in terms of levels of rigour to provide confidence that protection of the assets of an item or component is adequately developed. This CAL classification scheme does not specify technical requirements for cybersecurity controls, however it can be used to drive the cybersecurity engineering, providing a common language for communicating cybersecurity assurance requirements among the organizations involved.

A CAL can be determined by the organization developing an item or assumed by an organization developing a component out of context.

Once determined, a CAL specifies the amount of rigour required in the subsequent product development activities to address threat scenarios requiring reducing the risk. This can be achieved by assigning the CAL as an attribute of a cybersecurity goal, which is inherited by refined cybersecurity requirements.

E.2 Determining a CAL

A CAL is indirectly related to risk; however, it cannot be directly determined from a risk value. This is because the risk value is dynamic, varying over time depending on the evolving specification, design, implementation and operational environment of the item or component, whereas the CAL expresses a level of assurance that is to remain fixed over time. Therefore, a CAL can be determined at the start of development during the concept phase using parameters that are expected to remain stable until end of cybersecurity support, for example parameters based on the assets of an item and aspects of their associated risks, before consideration of the implementation of cybersecurity controls. The relationship between a CAL and associated risk is illustrated in Figure E.1.



Key

E_1 Event 1: cybersecurity requirement is specified.

E_2 Event 2: cybersecurity control is implemented.

E_3 Event 3: test shows cybersecurity control is effective.

E_4 Event 4: vulnerability is discovered in the field.

E_5 Event 5: vulnerability is fixed.

CAL is determined and assigned.

CAL is applied in cybersecurity activities.

a Risk value is dynamic and can vary depending on current specification, design or implementation.

b The expected level of assurance determined at E_1 given the criticality of the assets to be protected prescribes the rigour of subsequent cybersecurity activities at E_2, E_3.

Figure E.1 — Relationship between a CAL and risk

A CAL can be determined based on consideration of the identified threat scenarios (see 15.4). Table E.1 gives an example based on four CALs, each corresponding to an increasing level of assurance based on the cybersecurity engineering methods used. The example shows CALs assigned based on the maximum impact and the attack vector of the relevant threat scenarios.

Table E.1 — Example CAL determination based on impact and attack vector parameters

		Attack vector[b]			
		Physical	**Local**	**Adjacent**	**Network**
Impact	Severe	CAL2	CAL3	CAL4	CAL4
	Major	CAL1	CAL2	CAL3	CAL4
	Moderate	CAL1	CAL1	CAL2	CAL3
	Negligible	---[a]	---[a]	---[a]	---[a]

a See [PM-06-08].

b Attack vector is a static parameter of attack feasibility.

Sharing a documented rationale for the determination of a CAL between customer and supplier can improve mutual understanding. A CAL classification scheme and determined CALs can also be part of the cybersecurity interface agreement between customer and supplier.

A single CAL can be assigned to all cybersecurity goals of an item or different CALs can be assigned to each cybersecurity goal. If cybersecurity goals are combined, the highest of the individual CALs is assigned to the combined cybersecurity goal.

E.3 Using a CAL

E.3.1 General considerations

A CAL classification scheme can be used to determine the level of rigour with which cybersecurity activities are performed, in terms of the effort necessary to provide the required assurance.

A CAL can be used to select:

a) methods used for development and verification;

b) methods to identify weaknesses and analyse vulnerabilities; and

c) approaches for cybersecurity assessment.

Table E.2 provides an example of a number of CALs and guidance for their usage during the concept and the product development phases. For each increase in CAL, the corresponding methods represent a meaningful increase in the assurance of the item or component by the design, verification, and cybersecurity assessment. Examples in Tables E.2, E.3 and E.4 are provided to enable industry experience to be gained in using CALs to scale the activities described in this document.

Table E.2 — Example number of CALs and expected rigour in cybersecurity assurance measures

CAL	Description	a) Methods to provide confidence that cybersecurity activities are performed with appropriate rigour	b) Methods to provide confidence that unmanaged vulnerabilities do not remain	c) Independence scheme to provide confidence that the cybersecurity activities performed are appropriate
CAL1	Low to moderate cybersecurity assurance is required	Requirement based testing	Activities such as analysis and/or testing to search for vulnerabilities based on known information	Not needed
CAL2	Moderate cybersecurity assurance is required			Cybersecurity assessments are carried out by a different person than the originator
CAL3	Moderate to high cybersecurity assurance is required	All interactions between components are tested	Activities such as analysis and/or testing to search for vulnerabilities by exploratory methods	Cybersecurity assessments are carried out by a person in a different team than the originator
CAL4	High cybersecurity assurance is required	All combinations of interactions between components are tested		Cybersecurity assessments are carried out by a person who is independent regarding management, resources and release authority from the originating department

E.3.2 Concept

This subclause provides an example on the usage of a CAL classification scheme to adapt the rigour and extent of development measures.

In the concept phase, with the definition of the cybersecurity concept and the allocation of cybersecurity requirements to components of the preliminary architecture, CALs can be used as follows as an extension to [RQ-09-10]:

a) cybersecurity requirements derived from a cybersecurity goal inherit the CAL from that cybersecurity goal;

b) if multiple cybersecurity requirements with different CALs inherited from multiple cybersecurity goals are allocated to an architectural component, the highest CAL is assigned to the component;

c) if the component is confirmed as protected from the other components in the architecture, the CAL assigned to the component can be reduced or rendered unnecessary, based on a rationale.

E.3.3 Product development

An application of a CAL classification scheme in product development can be to use CAL-dependent methods and measures.

In product development, if cybersecurity requirements are allocated to components, and isolation from other components cannot be confirmed, then the components can be developed in accordance with the highest CAL for those cybersecurity requirements.

Tables E.3 and E.4 provide examples of how CAL can be applied to a sample of cybersecurity activities; further cybersecurity activities can be addressed in a similar way.

Table E.3 provides an example of how CAL can be used to determine the level of independence with which the respective activities are performed.

Table E.3 — Example of level of independence of cybersecurity activities

Activity	Require-ments	Level of independence applies to[a]				Scope
		CAL1	CAL2	CAL3	CAL4	
Verification of cybersecurity concept and design activities	[RQ-09-11] [RQ-10-08]	I1	I1	I2	I2	Applies to the highest CAL among the cybersecurity requirements
Verification of the implementation and integration of components	[RQ-10-09]	I1	I1	I2	I2	
Cybersecurity validation	[RQ-11-01]	I1	I1	I2	I2	
Cybersecurity assessment	[RQ-06-27]	—	I1	I2	I3	

[a] The notations are defined as follows:

—: no suggestion regarding the independence of this activity;

I1: the activity is performed by a different person in relation to the person(s) responsible for the creation of the considered work product(s);

I2: the activity is performed by a person who is independent from the team that is responsible for the creation of the considered work product(s), i.e. by a person reporting to a different direct superior; and

I3: the activity is performed by a person who is independent, regarding management, resources and release authority, from the department responsible for the creation of the considered work product(s).

Table E.4 provides an example of how CALs can be used to determine parameters that influence the rigour of testing methods used for verification and validation.

Table E.4 — Example of parameters of testing methods

Activity	Require-ments	Testing parameters apply to[a]				Scope
		CAL1	CAL2	CAL3	CAL4	
Functional testing	[RC-10-12] [RQ-11-01]	T1	T1	T2	T2	Applies to the highest CAL among the cybersecurity requirements
Vulnerability scanning	[RC-10-12] [RQ-11-01]	T1	T1	T1	T1	
Fuzz testing	[RC-10-12] [RQ-11-01]	—	T1	T2	T2	
Penetration testing	[RC-10-12] [RQ-11-01]	—	—	T1	T2	

[a] The notations are defined as follows:

—: no suggestion regarding testing parameters for this activity;

T1: testing parameter set 1:

— functional testing based on requirements;

— vulnerability scanning for known vulnerabilities;

— fuzz testing with random of selection of inputs;

— penetration testing assuming moderate attacker expertise, knowledge of the item or component and/or resources;

T2: testing parameters set 2:

— functional testing based on requirements and interactions between components;

— vulnerability scanning for known vulnerabilities;

— fuzz testing with an increased number of test case iterations and/or adaptive selection of inputs;

— penetration testing assuming higher attacker expertise, knowledge of the item or component and/or resources.

Annex F
(informative)

Guidelines for impact rating

F.1 General

This annex gives examples of criteria for impact rating (see 15.5) for damage scenarios involving safety, financial, operational and privacy damage. The tables (see Table F.1 through Table F.4) in this annex can be used for impact rating.

Considerations on how the scalability of damage (i.e. impact to multiple road users in a single damage scenario) modify the impact rating have not been included in the examples given, but can be added to the organization-specific rating criteria as appropriate (e.g. Reference [20], C.1.2, Table 4).

F.2 Impact rating for safety damage

Table F.1 — Example safety impact rating criteria

Impact rating	Criteria for safety impact rating
Severe	S3: Life-threatening injuries (survival uncertain), fatal injuries
Major	S2: Severe and life-threatening injuries (survival probable)
Moderate	S1: Light and moderate injuries
Negligible	S0: No injuries [a]
[a] Rating for S0 can be based on ISO 26262-3:2018, Table B.1.	

Safety impact rating criteria are taken from ISO 26262-3:2018.

Controllability and exposure in accordance with ISO 26262-3:2018 can also be considered for rating impact on safety, if a rationale is provided.

F.3 Impact rating for financial damage

Table F.2 — Example financial impact rating criteria

Impact rating	Criteria for financial impact rating
Severe	The financial damage leads to catastrophic consequences which the affected road user might not overcome.
Major	The financial damage leads to substantial consequences which the affected road user will be able to overcome.
Moderate	The financial damage leads to inconvenient consequences which the affected road user will be able to overcome with limited resources.
Negligible	The financial damage leads to no effect, negligible consequences or is irrelevant to the road user.

F.4 Impact rating for operational damage

Table F.3 — Example operational impact rating criteria

Impact rating	Criteria for operational impact rating
Severe	The operational damage leads to the loss or impairment of a core vehicle function. EXAMPLE 1 Vehicle not working or showing unexpected behaviour of core functions such as enabling of limp home mode or autonomous driving to an unintended location.
Major	The operational damage leads to the loss or impairment of an important vehicle function. EXAMPLE 2 Significant annoyance of the driver.
Moderate	The operational damage leads to partial degradation of a vehicle function. EXAMPLE 3 User satisfaction negatively affected.
Negligible	The operational damage leads to no impairment or non-perceivable impairment of a vehicle function.

These criteria might or might not have safety consequences as well.

F.5 Impact rating for privacy damage

Table F.4 — Example privacy impact rating criteria

Impact rating	Criteria for privacy impact rating
Severe	The privacy damage leads to significant or even irreversible impact to the road user. The information regarding the road user is highly sensitive and easy to link to a PII principal.
Major	The privacy damage leads to serious impact to the road user. The information regarding the road user is: a) highly sensitive and difficult to link to a PII principal; or b) sensitive and easy to link to a PII principal.
Moderate	The privacy damage leads to inconvenient consequences to the road user. The information regarding the road user is: a) sensitive but difficult to link to a PII principal; or b) not sensitive but easy to link to a PII principal.
Negligible	The privacy damage leads to no effect or, negligible consequences or is irrelevant to the road user. The information regarding the road user is not sensitive and difficult to link to a PII principal.

Personally identifiable information (PII) and PII principal can be defined in accordance with ISO/IEC 29100 [25].

Annex G
(informative)

Guidelines for attack feasibility rating

G.1 General

This annex provides guidelines on how the following approaches can be applied for attack feasibility rating (see 15.7):

— attack potential-based;

— CVSS-based; and

— attack vector-based.

Considerations whether an attack has the potential to scale (i.e. be easily extended to multiple instances and targets) can be included in the rating of attack feasibility.

G.2 Guidelines for the attack potential-based approach

G.2.1 Background on attack potential

Attack potential is defined in ISO/IEC 18045 [23] as a measure of the effort to be expended in attacking an item or component, expressed in terms of an attacker's expertise and resources. Attack potential relies on five core parameters:

— elapsed time;

— specialist expertise;

— knowledge of the item or component;

— window of opportunity; and

— equipment.

This subclause gives examples of customization and example mappings to attack feasibility.

G.2.2 Example of adaptation of the parameters

G.2.2.1 Example customization of elapsed time

The elapsed time parameter includes the time to identify a vulnerability and develop and (successfully) apply an exploit. Therefore, this rating is based on the state of expert knowledge at the time of rating, see Table G.1.

Table G.1 — Elapsed time

≤1 day
≤1 week
≤1 month
≤6 months
>6 months

G.2.2.2 Example customization of specialist expertise

The expertise parameter is related to the capabilities of the attacker, relative to their skill and experience, see Table G.2.

Table G.2 — Specialist expertise

Layman: Unknowledgeable compared to experts or proficient persons, with no particular expertise. EXAMPLE 1 Ordinary person using step-by-step descriptions of an attack that is publicly available.
Proficient: Knowledgeable in that they are familiar with the security behaviour of the product or system type. EXAMPLE 2 Experienced owner, ordinary technician knowing simple and popular attacks like odometer tuning, installation of counterfeit parts.
Expert: Familiar with the underlying algorithms, protocols, hardware, structures, security behaviour, principles and concepts of security employed, techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc. implemented in the product or system type. EXAMPLE 3 Experienced technician or engineer.
Multiple experts: Different fields of expertise are required at an expert level for distinct steps of an attack. EXAMPLE 4 Multiple highly experienced engineers who have expertise in different fields, and which are required at an expert level for distinct steps of an attack.

G.2.2.3 Example customization of knowledge of the item or component

The knowledge of the item or component parameter is related to the amount of information the attacker has acquired about the item or component, see Table G.3.

Table G.3 — Knowledge of the item or component

Public information: Public information concerning the item or component (e.g. as gained from the Internet). EXAMPLE 1 Information and documents published on the product homepage or on an internet forum.

Table G.3 *(continued)*

Restricted information: Restricted information concerning the item or component (e.g. knowledge that is controlled within the developer organization and shared with other organizations under a non-disclosure agreement). EXAMPLE 2 Internal documentation shared between manufacturer and supplier, requirements and design specifications.
Confidential information: Confidential information about the item or component (e.g. knowledge that is shared between discrete teams within the developer organization, access to which is constrained only to members of the specified teams). EXAMPLE 3 Immobilizer-related information, software source code.
Strictly confidential information: Strictly confidential information about the item or component (e.g. knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking). EXAMPLE 4 Customer specific calibrations or memory maps documented internally by the manufacturer and/or supplier.

G.2.2.4 Example customization of window of opportunity

The window of opportunity parameter is related to the access conditions (time, type) to successfully perform an attack. It combines access type (e.g. logical and physical) and access duration (e.g. unlimited and limited). Depending on the type of attack this might include discovery of possible targets, access to a target, exploit works on the target, time to perform attack on a target, remaining undiscovered, circumventing detections and cybersecurity controls, etc. (see Table G.4).

Table G.4 — Window of opportunity

Unlimited: High availability via public/untrusted network without any time limitation (i.e. asset is always accessible). Remote access without physical presence or time limitation as well as unlimited physical access to the item or component. EXAMPLE 1 Remote attack (e.g. vehicle-to-anything or cellular interfaces) without any preconditions, unlimited physical access by the owner for chip tuning.
Easy: High availability and limited access time. Remote access without physical presence to the item or component. EXAMPLE 2 Pairing time of Bluetooth, remote software update, remote attack that requires the vehicle standing still.
Moderate: Low availability of the item or component. Limited physical and/or logical access. Physical access to the vehicle interior or exterior without using any special tools. EXAMPLE 3 Attacker enters an unlocked car and got access to exposed physical interface, e.g. physical access via on-board diagnostic port.
Difficult: Very low availability of the item or component. Impractical level of access to the item or component to perform the attack. EXAMPLE 4 Decapping an IC to extract information, cracking a cryptographic key by brute force faster than the key is rotated.

G.2.2.5 Example customization of equipment

The equipment parameter is related to the tools the attacker has available to discover the vulnerability and/or to execute the attack, see Table G.5.

Table G.5 — Equipment

Standard: Equipment is readily available to the attacker. This equipment can be a part of the product itself (e.g. a debugger in an operating system), or can be readily obtained (e.g. internet sources, protocol analyser or simple attack scripts). EXAMPLE 1 Laptop, CAN adapter, on-board diagnostic dongle, ordinary tools (screwdriver, soldering iron, pliers).
Specialized: Equipment is not readily available to the attacker but can be acquired without undue effort. This can include purchase of moderate amounts of equipment (e.g. power analysis tools, use of hundreds of PCs linked across the internet would fall into this category), or development of more extensive attack scripts or programs. If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack this would be rated as bespoke. EXAMPLE 2 Specialized hardware debugging device, in-vehicle communication devices (hardware in the loop test rig, high-grade oscilloscope, signal generator), special chemicals.
Bespoke: Equipment is specially produced (e.g. very sophisticated software) and not readily available to the public (e.g. black market), or the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment is very expensive. EXAMPLE 3 Manufacturer-restricted tools, electron microscope.
Multiple bespoke: Is introduced to allow for a situation, where different types of bespoke equipment are required for distinct steps of an attack.

G.2.2.6 Example mapping between attack potential and attack feasibility

For each parameter, numerical values can be defined. Based on the ISO/IEC 18045 [23], the following scales are proposed based on the adaptation presented above, see Table G.6.

Table G.6 — Example aggregation of attack potential

Elapsed time		Specialist expertise		Knowledge of the item or component		Window of opportunity		Equipment	
Enumerate	**Value**	**Enumerate**	**Value**	**Enumerate**	**Value**	**Enumerate**	**Value**	**Enumerate**	**Value**
≤1 day	0	Layman	0	Public	0	Unlimited	0	Standard	0
≤1 week	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
≤1 month	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
≤6 months	17	Multiple experts	8	Strictly confidential	11	Difficult/ none	10	Multiple bespoke	9
>6 months	19								

According to ISO/IEC 18045 [23], attack potential corresponds to the addition of all parameters. Attack feasibility is mapped using Table G.7, based on a customization of ISO/IEC 18045 [23].

Table G.7 — Example attack potential mapping

Attack feasibility rating	Values
High	0 - 9
	10 - 13
Medium	14 - 19
Low	20 - 24
Very low	≥ 25

G.3 Guidelines for the CVSS-based approach

To rate information technology security vulnerabilities, the CVSS maintained by the forum of incident response and security teams (FIRST) [24] can be used. Within the base metrics group, the exploitability metrics (cf. Reference [24], 7.1) can be used to rate attack feasibility. Other CVSS metrics (e.g. impact metrics) are covered by aspects of this document, e.g. damage scenarios and impact assessment.

The exploitability metrics are:

— attack vector;

— attack complexity;

— privileges required; and

— user interaction.

They are described by FIRST [24]. Evaluation of the CVSS metrics yields numerical values for each metric according within a pre-defined range. The overall exploitability value can be calculated on the basis of a simple formula:

$$E = 8{,}22 \times V \times C \times P \times U$$

where

E is the exploitability value;

V is the numerical value associated to the attack vector, ranging from 0,2 to 0,85;

C is the numerical value associated with the attack complexity, ranging from 0,44 to 0,77;

P is the numerical value associated with the privileges required, ranging from 0,27 to 0,85; and

U is the numerical value associated with user interaction, ranging from 0,62 to 0,85.

Consequently, the exploitability values range between 0,12 and 3,89.

An example mapping of CVSS exploitability values to attack feasibility, is given in Table G.8. This is an example of equidistant exploitability steps.

Table G.8 — Example CVSS exploitability mapping

Attack feasibility rating	CVSS exploitability value
High	2,96 - 3,89
Medium	2,00 - 2,95
Low	1,06 - 1,99

Table G.8 *(continued)*

Attack feasibility rating	CVSS exploitability value
Very low	0,12 - 1,05

NOTE The procedure of using only the exploitability metrics as part of the bigger CVSS base metric group does not strictly conform to the CVSS requirements for metrics. To calculate the risk in accordance with this document, the missing impact metric can be compensated by the impact metrics of this document, see Annex F and Reference [24].

Without changing the exploitability metric values, their descriptions can be supplemented to give a better guidance with regard to the organization's business and items or components under development, and to reduce the potential for misinterpretations when applying the description to actual vulnerabilities. Such supplements can be organization-specific examples which are added to the metric value descriptions.

Apart from vulnerabilities, the CVSS exploitability metric can also be used to rate conceptual weaknesses, flaws, and gaps.

G.4 Guidelines for the attack vector-based approach

The attack vector-based approach reflects the context by which attack path exploitation is possible. Attack feasibility rating will be higher the more remote (logically and physically) an attacker can be in order to exploit the attack path. The assumption is that the number of potential attackers that can exploit a vulnerability using the internet is larger than the number of potential attackers that can exploit an attack path requiring physical access to the item or component, see Table G.9.

Table G.9 — Attack vector-based approach

Attack feasibility rating	Criteria
High	**Network:** Potential attack path is bound to network stack without any limitation. EXAMPLE 1 Cellular network connection making the ECU directly connected and accessible on the internet.
Medium	**Adjacent:** Potential attack path is bound to network stack; however, the connection is limited physically or logically. EXAMPLE 2 Bluetooth interface, virtual private network connection.
Low	**Local:** Potential attack path is not bound to network stack and threat agents require direct access to the item for realizing the attack path. EXAMPLE 3 Universal serial bus mass storage device, memory card.
Very low	**Physical:** Threat agents require physical access to realize the attack path.

Annex H
(informative)

Examples of application of TARA methods – headlamp system

H.1 General

The example of a headlamp system development and the respective work products in this annex are provided for illustrative purposes only and are not intended to imply any particular approach for practical use.

This annex can aid understanding of the requirements of this document by presenting examples of applications of Threat Analysis and Risk Assessment (TARA) methods. This example only presents the concept phase for illustrating TARA application and is presented in an abstracted, simplified manner. In particular it addresses:

— item definition; and

— TARA.

TARA is defined as modular methods for analysis and each module can be proceeded in any order, for example:

— identification of assets → identification of corresponding damage scenarios → impact rating → threat scenarios identification → attack path analysis → …

— selection of damage scenarios from catalogues → impact rating → threat scenario identification → identification of assets → …

The examples in this annex follow the order below:

i. asset identification;

ii. impact rating;

iii. threat scenario identification;

iv. attack path analysis;

v. attack feasibility rating;

vi. risk value determination;

vii. risk treatment decision.

In step v, two different approaches are applied for rating the attack feasibility. One approach uses attack vector-based approach (see [RC-15-14]) and the other approach uses attack potential-based approach (see [RC-15-12]).

Figure H.1 provides an overview of various interactions between Clause 9 and 15.

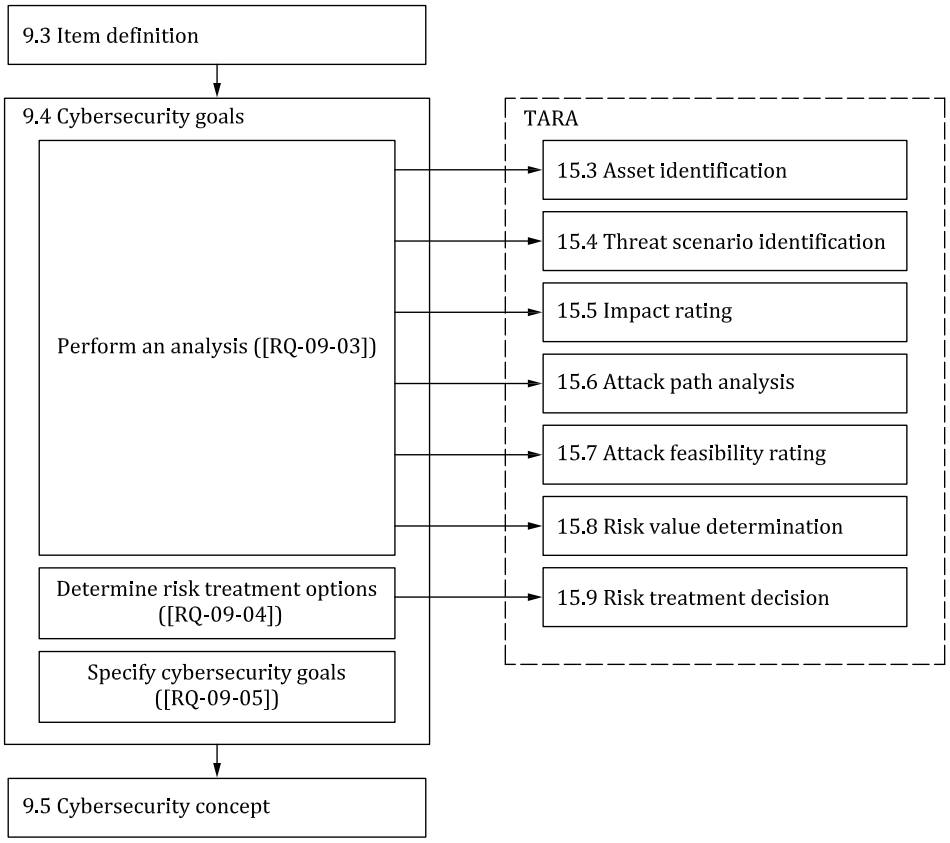


Figure H.1 — Interactions in concept phase

H.2 Example activities for concept phase of a headlamp system

H.2.1 Item definition

This subclause shows examples of selected work products of 9.3. An example item definition of the headlamp system is given in the following:

a) item boundary (see Figure H.2);

b) item functions;

— Functional overview of the item: the headlamp system turns on/off the headlamp in accordance with the switch by demand of the driver. If the headlamp is in high-beam mode, the headlamp system switches the headlamp automatically to the low-beam mode when an oncoming vehicle is detected. It also returns the headlamp automatically to the high-beam mode if the oncoming vehicle is no longer detected.

NOTE Regarding functionality of headlamp, the headlamp system does not depend on the navigation ECU and the gateway ECU.

c) preliminary architecture (see Figure H.2).

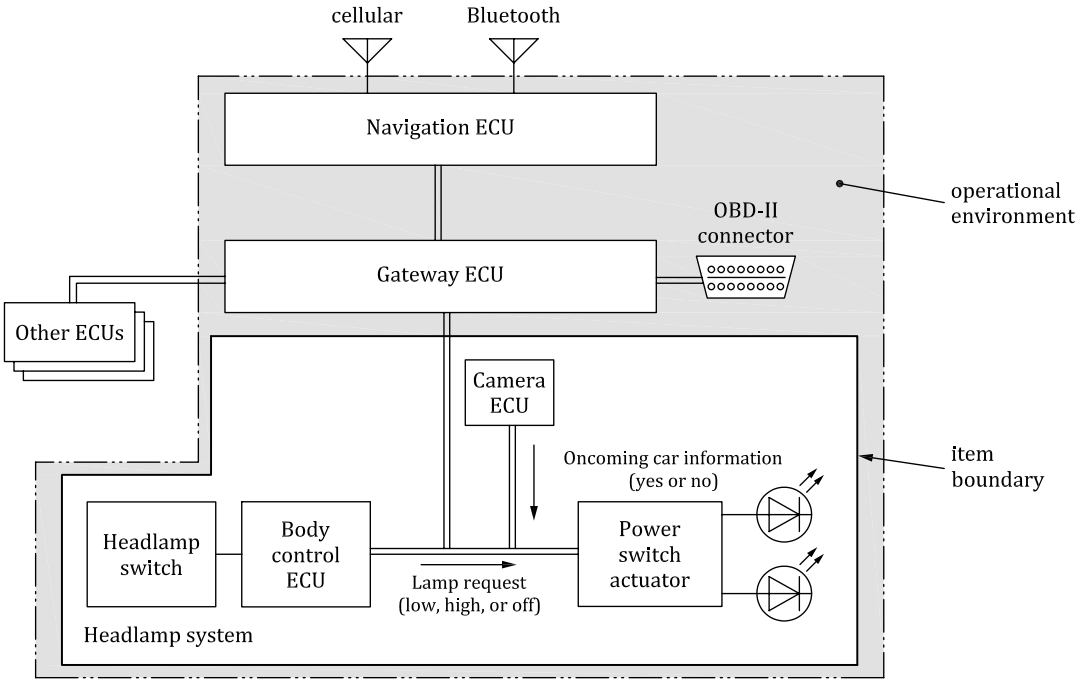


Figure H.2 — Example of item boundary and preliminary architecture of the headlamp system

During item definition, the operational environment of the item is described (see [RQ-09-02]). The operational environment provides supplemental information for analysis activities of the TARA. Table H.1 shows an example description of the operational environment that is used in this annex.

Table H.1 — Example description of the operational environment

The item (headlamp system) is connected with the gateway ECU, and the gateway ECU is connected with the navigation ECU by data communication.
Navigation ECU has external communication interfaces: — Bluetooth; — cellular. Assumption: — navigation ECU has a firewall to prevent invalid data communication from external interfaces.
Gateway ECU has external communication interfaces: — OBD-II. Assumption: — gateway ECU has strong security controls including a firewall function (developed as CAL4).

H.2.2 Asset identification

[RQ-09-03] calls asset identification in accordance with 15.3 to identify assets of the item and their damage scenarios. Table H.2 shows example results of asset identification.

Table H.2 — Example list of assets and damage scenarios

Asset	Cybersecurity property			Damage scenario
	C	I	A	
Data communication (lamp request)	—	X	X	Vehicle cannot be driven at night, because (the driver perceives) the headlamp function was inhibited while parked.
	—	X	—	Front collision with a narrow stationary object (e.g. a tree) caused by unintended turning-off of headlamp during night driving at medium speed.
Data communication (oncoming car information)	—	X	—	Drivers of oncoming vehicles are blinded, it is caused by not being able to change to low beam during night driving.
	—	—	X	Malfunctioning automatic high beam caused by headlamp always remaining at low beam during night driving.
Firmware of body control ECU	X	X	—	...

H.2.3 Impact rating

[RQ-09-03] also calls impact rating in accordance with 15.5 to rate the impact of damage scenarios. Table H.3 shows example results of impact rating.

Table H.3 — Example of impact ratings for damage scenarios

Damage scenario	Impact category	Impact rating
Vehicle cannot be driven at night, because (the driver perceives) the headlamp function was inhibited while parked.	O	Major
Front collision with a narrow stationary object (e.g. a tree) caused by unintended turning-off of headlamp during night driving at medium speed.	S	Severe (S3)
Malfunctioning automatic high beam caused by headlamp always remaining at low beam during night driving.	O	Moderate

H.2.4 Threat scenario identification

[RQ-09-03] also calls threat scenario identification in accordance with 15.4. Table H.4 shows example results of threat scenario identification.

Table H.4 — Example threat scenarios

Damage scenario	Threat scenario
Front collision with a narrow stationary object (e.g. a tree) caused by unintended turning-off of headlamp during night driving at medium speed	Spoofing of a signal leads to loss of integrity of the data communication of the “Lamp Request” signal to the power switch actuator ECU, potentially causing the headlamp to turn off unintentionally.
	Tampering with a signal sent by body control ECU leads to loss of integrity of the data communication of the “Lamp Request” signal to the power switch actuator ECU, potentially causing the headlamp to turn off unintentionally.
Malfunctioning automatic high beam caused by headlamp always remaining at low beam during night driving	Asset: oncoming car information Cybersecurity property: availability Associated cause: denial of service of oncoming car information

H.2.5 Attack path analysis

[RQ-09-03] also calls attack path analysis in accordance with 15.6. Table H.5 shows example results of attack path analysis and Figure H.3 shows an example of attack path analysis by attack tree analysis.

Analysis of attack paths can take into account assumptions. In this example, attack paths requiring physical access inside the item such as a microcontroller of the body control ECU can be excluded according to the assumption.

Table H.5 — Example attack paths for threat scenarios

Threat scenario	Attack path
Spoofing of a signal leads to loss of integrity of the data communication of the "Lamp Request" signal to the power switch actuator ECU, potentially causing the headlamp to turn off unintentionally	i. Attacker compromises navigation ECU from cellular interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (OFF).
	i. Attacker compromises navigation ECU from Bluetooth interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (OFF).
	i. Attacker gets local (see Table G.9) access to OBD connector. ii. Attacker sends malicious control signals from OBD connector. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (OFF).
Denial of service of oncoming car information	i. Attacker compromises navigation ECU from cellular interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Attacker floods the communication bus with a large number of messages.
	i. Attacker attaches a Bluetooth-enabled OBD dongle to OBD connector when vehicle is parking unlocked. ii. Attacker compromises driver's smartphone with Bluetooth interface. iii. Attacker sends message via smartphone and Bluetooth dongle to Gateway ECU. iv. Gateway ECU forwards malicious signals to power switch actuator. v. Attacker floods the communication bus with a large number of messages.

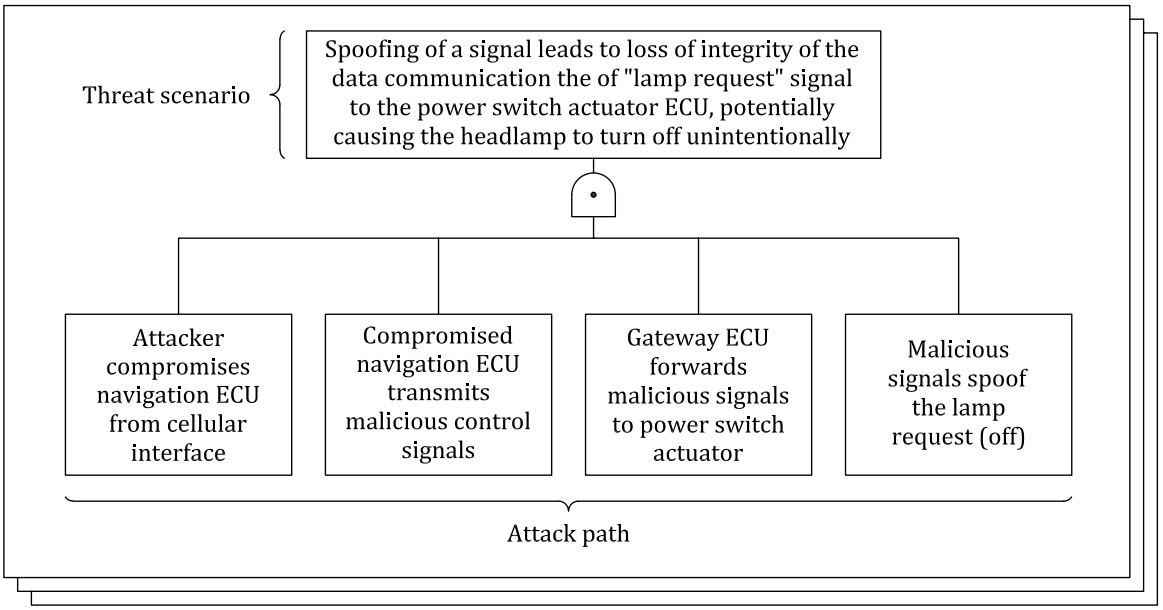


Figure H.3 — Example of an attack path derived by attack tree analysis

H.2.6 Attack feasibility rating

[RQ-09-03] also calls attack feasibility rating for each attack path in accordance with 15.7. Table H.6 shows an example result of attack feasibility rating in accordance with attack vector-based approach as described in G.4. Table H.7 shows an example results of attack feasibility rating in accordance with attack potential-based approach as described in G.2.

Table H.6 — Examples of attack feasibility rating with the attack vector-based approach

Attack path	Attack feasibility rating
i. Attacker compromises navigation ECU **from cellular interface**. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (ON).	High
i. Attacker compromises navigation ECU **from Bluetooth interface**. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (ON).	Medium
i. Attacker sends malicious control signals **from OBD2 connector**. ii. Gateway ECU forwards the malicious signals to power switch actuator. iii. Malicious signals spoof the lamp request (ON).	Low

NOTE 1 The attack vector-based approach is suitable for concept phase. Because during concept phase, it is not possible to gather all vulnerability information related item.

Based on recommendation (see [RC-15-11]), attack feasibility can also be determined based on attack potential-based approach, which is illustrated by examples in Table H.7.

Table H.7 — Examples of attack feasibility rating with the attack potential-based approach

Threat scenario	Attack path	Attack feasibility assessment						
		ET	SE	KoIC	WoO	Eq	Value	Attack feasibility rating
Denial of service of oncoming car information	i. Attacker compromises navigation ECU from cellular interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Attacker floods the communication bus with a large number of messages.	1	8	7	0	4	20	Low
	i. Attacker attaches a Bluetooth-enabled OBD dongle to OBD connector when vehicle is parking unlocked. ii. Attacker compromises driver's smartphone with Bluetooth interface. iii. Attacker sends message via smartphone and Bluetooth dongle to Gateway ECU. iv. Gateway ECU forwards malicious signals to power switch actuator. v. Attacker floods the communication bus with a large number of messages.	1	8	7	4	4	24	Low

Key

ET elapsed time

SE specialist expertise

KoIC knowledge of the item or component

WoO window of opportunity

Eq equipment

NOTE 2 Each organization can apply rationales to each of the ratings based on their own policy. For example, the window of opportunity is assigned 4 (moderate, refer to Table G.4) for the second attack path, because physical access is required. The attack feasibility rating is determined considering all feasibility values based on Table G.7.

H.2.7 Risk value determination

[RQ-09-03] also calls risk determination for each threat scenario in accordance with 15.8. Risk values can be determined utilizing risk matrices defined by the organization for mapping combinations of ratings of impact (see 15.5) and attack feasibility (see 15.7) to risk values. Table H.8 shows an example risk matrix and Table H.9 shows example results of risk determination using Table H.8.

Table H.8 — Risk matrix example

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	**2**	**3**	**4**	**5**
	Major	**1**	**2**	**3**	**4**
	Moderate	**1**	**2**	**2**	**3**
	Negligible	**1**	**1**	**1**	**1**

Table H.9 — Examples of determined risk values

Threat scenario	Aggregated attack feasibility rating	Impact rating	Risk value
Spoofing of a signal leads to loss of integrity of the data communication of "Lamp Request" signal for power switch actuator ECU	**High**	**Severe**	**S: 5**
Denial of service of oncoming car information	Low	Moderate	O: 2

Risk values may also be determined by a risk formula defined by the organization. An example is shown in the below formula and Table H.10.

$$R = 1 + I \times F$$

Table H.10 — Example translation of impact and attack feasibility to numerical values

Impact rating	Numerical value *I* for impact
Negligible	0
Moderate	1
Major	1,5
Severe	2

Attack feasibility rating	Numerical value *F* for attack feasibility
Very low	0
Low	1
Medium	1,5
High	2

For the specific threat scenarios displayed in Table H.9 the calculation using the example given in Table H.8 and the above formula would lead to the same risk values.

H.2.8 Risk treatment decision

[RQ-09-04] requires selecting treatment options in accordance with 15.9. Table H.11 shows example results of risk treatment decision.

Table H.11 — Example results of risk treatment decision

Threat scenario	Risk value	Risk treatment option
Spoofing of a signal leads to loss of integrity of the data communication of "Lamp Request" signal for power switch actuator ECU	S: 5	Reducing the risk
Denial of service of oncoming car information	O: 2	Reducing the risk

BIBLIOGRAPHY

[1] ISO 26262-1:2018, *Road vehicles — Functional safety — Part 1: Vocabulary*

[2] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[3] ISO 31000:2018, *Risk management — Guidelines*

[4] ISO/IEC/IEEE 15288:2015, *Systems and software engineering — System life cycle processes*

[5] ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[6] ISO/TR 4804, *Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation*

[7] IATF 16949, *Quality management system requirements for automotive production and relevant service parts organizations*

[8] ISO 9001, *Quality management systems — Requirements*

[9] ISO 10007, *Quality management — Guidelines for configuration management*

[10] ISO/IEC 33001, *Information technology — Process assessment — Concepts and terminology*

[11] ISO/IEC/IEEE 15288, *Systems and software engineering — System life cycle processes*

[12] ISO/IEC/IEEE 12207, *Systems and software engineering — Software life cycle processes*

[13] VDA QMC WORKING GROUP 13 / AUTOMOTIVE SIG. *Automotive SPICE Process Assessment / Reference Model, Version 3.1* [online]. Berlin: VDA QMC, November 2017. Available at: http://www.automotivespice.com/fileadmin/software-download/AutomotiveSPICE_PAM_31.pdf

[14] ISO 29147, *Information technology — Security techniques — Vulnerability disclosure*

[15] IEC 62443-2-1, *Industrial communication networks — Network and system security — Part 2-1: Establishing an industrial automation and control system security program*

[16] ISO 26262 (all parts), *Road vehicles — Functional safety*

[17] MISRA C 2012, *Guidelines for the use of the C language in critical systems, 3rd Edition, 1st Revision.* Nuneaton, England: HORIBA MIRA, February 2019. ISBN (print/electronic): 978-1-906400-21-7 / 978-1-906400-22-4.

[18] SEI CERT *C Coding Standard – Rules for developing safe, reliable and secure systems* [online]. Pittsburgh, Pennsylvania: Software Engineering Institue, Carnegie Mellon University, 2016 [viewed 2021-02-12]. Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=454220

[19] ROSS Ron, et al. (2018), *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [online]. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1. Updated March 2018 [viewed 2021-02-16]. Available at: https://doi.org/10.6028/NIST.SP.800-160v1

[20] E-SAFETY VEHICLE INTRUSION PROTECTED APPLICATIONS (EVITA) Deliverable D2.3: *Security requirements for automotive on-board networks based on dark-side scenarios* [online]. Edited by A. Ruddle et al. December 2009 [viewed 2021-01-17]. Available at: https://doi.org/10.5281/zenodo.1188418

[21] ETSI TS 102 165-1, *CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA), Version 5.2.3* [online]. October 2017 [viewed 2021-01-19]. Available at: https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf

[22] UcedaVélez, Tony and Morana, Marco M. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. Hoboken, New Jersey: Wiley, May 2015. ISBN: 978-1-118-98835-0.

[23] ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

[24] FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST). Common Vulnerability Scoring System (CVSS), *Common Vulnerability Scoring System v3.1: Specification Document,* [online]. Available at: https://www.first.org/cvss/v3.1/specification-document

[25] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[26] Automotive ISAC, *Automotive Cybersecurity Best Practices* [online]. Available at: https://www.automotiveisac.com/best-practices/

[27] FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST). Traffic Light Protocol (TLP), *FIRST Standards Definitions and Usage Guidance - Version 1.0*, [online]. Available at: https://www.first.org/tlp/

[28] ISO/IEC 2382[2)], *Information technology — Vocabulary*

[29] ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

[30] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[31] ISO/IEC 27010, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*

[32] ISO/IEC/IEEE 26511, *Systems and software engineering — Requirements for managers of information for users of systems, software, and services*

[33] IEC 31010, *Risk management — Risk assessment techniques*

[34] IEC 61508-7, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*

[35] JOHNSON Christopher, et al. (2016) *Guide to Cyber Threat Information Sharing* [online]. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-150, October 2016 [viewed 2021-02-16]. Available at: https://doi.org/10.6028/NIST.SP.800-150

[36] JOINT TASK FORCE TRANSFORMATION INITIATIVE 2012), *Guide for Conducting Risk Assessments* [online]. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. September 2012 [viewed 2021-02-16]. Available at: http://dx.doi.org/10.6028/NIST.SP.800-30r1

[37] SAE J3061, *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*

[38] SCARFONE Karen, et al. (2008), *Technical Guide to Information Security Testing and Assessment* [online]. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. September 2008 [viewed 2021-02-16]. Available at: https://doi.org/10.6028/NIST.SP.800-115

2) Available at: https://www.iso.org/obp/ui#iso:std:iso-iec:2382.

[39] TAKANEN Ari et al. *Fuzzing for Software Security and Quality Assurance, Second Edition.* Boston, Massachusetts/London: Artech House, January 2018. ISBN: 978-1-60807-850-9.

ICS 43.040.15

Price based on 81 pages