cannot be utilized for any conformance or compliance purposes.

SURFACE VEHICLE STANDARD	ISO/SAE DIS 21434
	Issued 2020-02-12
Road Vehicles - Cybersecurity Engineering	

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.

© ISO/SAE International 2020

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

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

SAE International
Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org

Published in Switzerland and USA.

This document was jointly prepared in the ISO/SAE Cybersecurity Engineering Joint Working Group, with experts from ISO Technical Committee 22 Road Vehicles, Subcommittee 32 Electrical and electronic components and general system aspects and SAE Vehicle Cybersecurity Systems Engineering Committee.

This first edition cancels and supersedes the SAE J3061_201601.

A list of all parts in the ISO/SAE 21434 series can be found on the ISO and SAE websites.

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/SAE21434.D1.

DRAFT

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 changing technology and attack methods.

This document provides vocabulary, objectives, requirements and guidelines 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 in accordance with ISO 31000. This document is intended to supersede SAE J3061 recommended practice.

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.

DRAFT

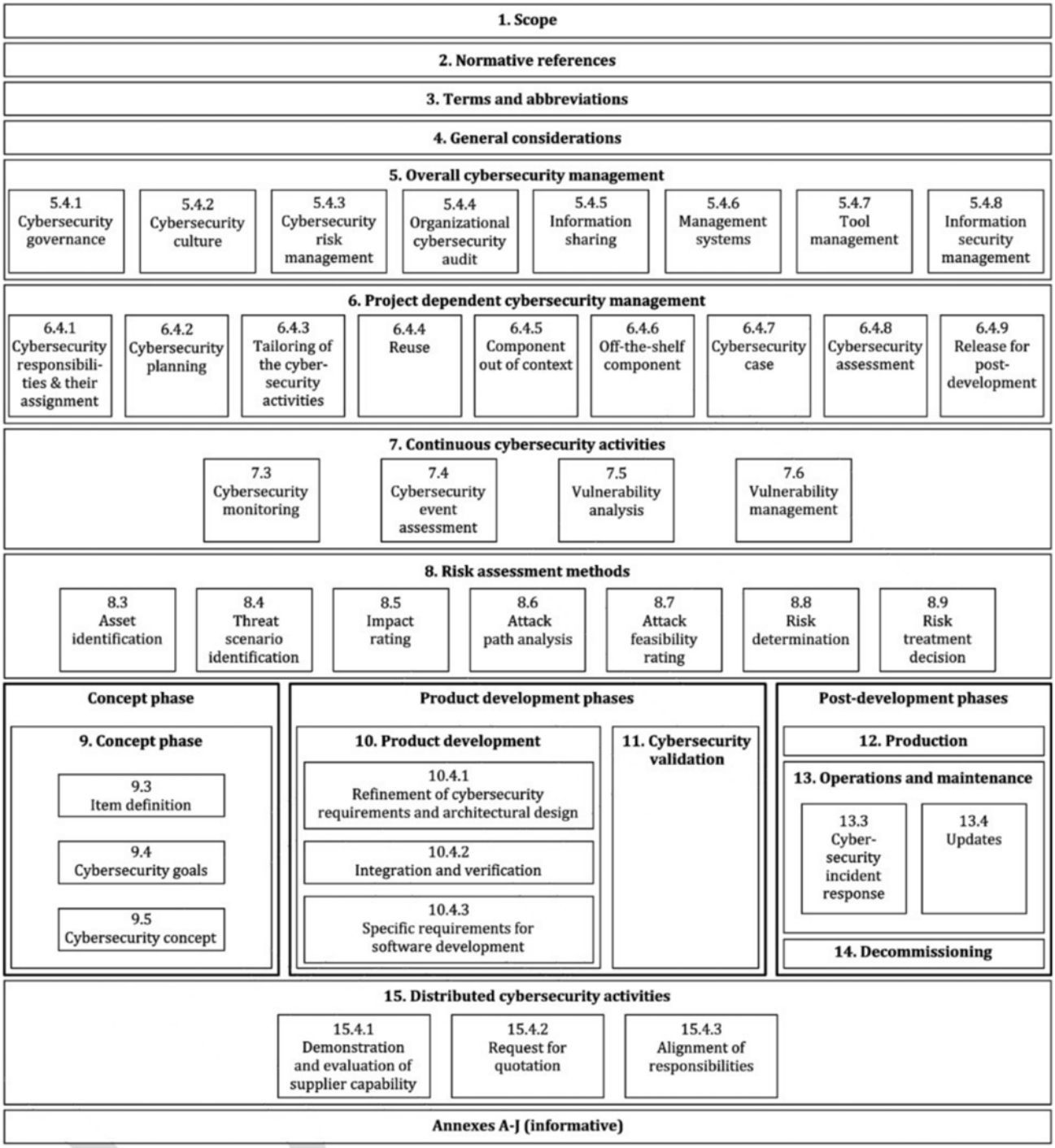


Figure 1 - Overview of this document

Clauses 5 and 6 (Management of Cybersecurity) include the implementation of the organizational cybersecurity policy, rules, and processes for overall cybersecurity management and for project dependent cybersecurity management.

Clause 7 (Continuous Cybersecurity Activities) defines activities that provide information for ongoing risk assessments and vulnerability management of E/E systems until end of support.

Clause 8 (Risk Assessment Methods) defines methods to determine the extent of cybersecurity risk.

Clause 9 (Concept Phase) defines an item and the relevant assets, provides cybersecurity risk determination, and defines the cybersecurity goals.

Clause 10 (Product Development) defines the cybersecurity specification, implements and verifies cybersecurity requirements specific to an item or component.

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

Clause 12 (Production) specifies the cybersecurity related aspects of fabrication, assembly and/or calibration of an item or component.

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

Clause 14 (Decommissioning) includes cybersecurity considerations that relate to the decommissioning of an item or component.

Clause 15 (Distributed Activities) includes requirements for supplier management.

DRAFT

TABLE OF CONTENTS

1. SCOPE 10

2. NORMATIVE REFERENCES 10

3. TERMS AND ABBREVIATIONS 10
3.1 Terms and Definitions 10
3.2 Abbreviated Terms 14

4. GENERAL CONSIDERATIONS 14

5. OVERALL CYBERSECURITY MANAGEMENT 16
5.1 General 16
5.2 Objectives 16
5.3 Inputs 17
5.3.1 Prerequisites 17
5.3.2 Further Supporting Information 17
5.4 Requirements and Recommendations 17
5.4.1 Cybersecurity Governance 17
5.4.2 Cybersecurity Culture 18
5.4.3 Cybersecurity Risk Management 19
5.4.4 Organizational Cybersecurity Audit 19
5.4.5 Information Sharing 20
5.4.6 Management Systems 20
5.4.7 Tool Management 21
5.4.8 Information Security Management 21
5.5 Work Products 21

6. PROJECT DEPENDENT CYBERSECURITY MANAGEMENT 22
6.1 General 22
6.2 Objectives 22
6.3 Inputs 23
6.3.1 Prerequisites 23
6.3.2 Further Supporting Information 23
6.4 Requirements and Recommendations 23
6.4.1 Cybersecurity Responsibilities and Their Assignment 23
6.4.2 Cybersecurity Planning 23
6.4.3 Tailoring of the Cybersecurity Activities 24
6.4.4 Reuse 25
6.4.5 Component Out of Context 26
6.4.6 Off-the-Shelf Component 26
6.4.7 Cybersecurity Case 26
6.4.8 Cybersecurity Assessment 26
6.4.9 Release for Post-Development 28
6.5 Work Products 29

7. CONTINUOUS CYBERSECURITY ACTIVITIES 29
7.1 General 29
7.2 Objectives 29
7.3 Cybersecurity Monitoring 29
7.3.1 Inputs 29
7.3.2 Requirements and Recommendations 30
7.3.3 Work Products 30
7.4 Cybersecurity Event Assessment 30
7.4.1 Inputs 30
7.4.2 Requirements and Recommendations 31
7.4.3 Work Products 31

DRAFT

7.5 Vulnerability Analysis ... 31
7.5.1 Inputs ... 31
7.5.2 Requirements and Recommendations ... 31
7.5.3 Work Products ... 32
7.6 Vulnerability Management ... 32
7.6.1 Inputs ... 32
7.6.2 Requirements and Recommendations ... 32
7.6.3 Work Products ... 33

8. RISK ASSESSMENT METHODS ... 33
8.1 General ... 33
8.2 Objectives ... 34
8.3 Asset Identification ... 34
8.3.1 Inputs ... 34
8.3.2 Requirements and Recommendations ... 34
8.3.3 Work Products ... 35
8.4 Threat Scenario Identification ... 35
8.4.1 Inputs ... 35
8.4.2 Requirements and Recommendations ... 35
8.4.3 Work Products ... 36
8.5 Impact Rating ... 36
8.5.1 Inputs ... 36
8.5.2 Requirements and Recommendations ... 36
8.5.3 Work Products ... 37
8.6 Attack Path Analysis ... 37
8.6.1 Inputs ... 37
8.6.2 Requirements and Recommendations ... 37
8.6.3 Work Products ... 38
8.7 Attack Feasibility Rating ... 39
8.7.1 Inputs ... 39
8.7.2 Requirements and Recommendations ... 39
8.7.3 Work Products ... 40
8.8 Risk Determination ... 40
8.8.1 Inputs ... 40
8.8.2 Requirements and Recommendations ... 40
8.8.3 Work Products ... 40
8.9 Risk Treatment Decision ... 40
8.9.1 Inputs ... 40
8.9.2 Requirements and Recommendations ... 41
8.9.3 Work Products ... 41

9. CONCEPT PHASE ... 41
9.1 General ... 41
9.2 Objectives ... 42
9.3 Item Definition ... 42
9.3.1 Inputs ... 42
9.3.2 Requirements and Recommendations ... 42
9.3.3 Work Products ... 43
9.4 Cybersecurity Goals ... 43
9.4.1 Inputs ... 43
9.4.2 Requirements and Recommendations ... 44
9.4.3 Work Products ... 45
9.5 Cybersecurity Concept ... 45
9.5.1 Inputs ... 45
9.5.2 Requirements and Recommendations ... 46
9.5.3 Work Products ... 46

10. PRODUCT DEVELOPMENT ... 46
10.1 General ... 46
10.2 Objectives ... 49
10.3 Inputs ... 49
10.3.1 Prerequisites ... 49
10.3.2 Further Supporting Information ... 50

DRAFT

10.4 Requirements and Recommendations ... 50
10.4.1 Refinement of Cybersecurity Requirements and Architectural Design ... 50
10.4.2 Integration and Verification ... 53
10.4.3 Specific Requirements for Software Development ... 56
10.5 Work Products ... 57

11. CYBERSECURITY VALIDATION ... 57
11.1 General ... 57
11.2 Objectives ... 57
11.3 Inputs ... 57
11.3.1 Prerequisites ... 57
11.3.2 Further Supporting Information ... 58
11.4 Requirements and Recommendations ... 58
11.5 Work Products ... 58

12. PRODUCTION ... 58
12.1 General ... 58
12.2 Objectives ... 58
12.3 Inputs ... 59
12.3.1 Prerequisites ... 59
12.3.2 Further Supporting Information ... 59
12.4 Requirements and Recommendations ... 59
12.5 Work Products ... 60

13. OPERATIONS AND MAINTENANCE ... 60
13.1 General ... 60
13.2 Objectives ... 60
13.3 Cybersecurity Incident Response ... 60
13.3.1 Inputs ... 60
13.3.2 Requirements and Recommendations ... 60
13.3.3 Work Products ... 61
13.4 Updates ... 61
13.4.1 Inputs ... 61
13.4.2 Requirements and Recommendations ... 62
13.4.3 Work Products ... 62

14. DECOMMISSIONING ... 62
14.1 General ... 62
14.2 Objectives ... 62
14.3 Inputs ... 62
14.3.1 Prerequisites ... 62
14.3.2 Further Supporting Information ... 62
14.4 Requirements and Recommendations ... 63
14.5 Work Products ... 63

15. DISTRIBUTED CYBERSECURITY ACTIVITIES ... 63
15.1 General ... 63
15.2 Objectives ... 63
15.3 Inputs ... 63
15.3.1 Prerequisites ... 63
15.3.2 Further Supporting Information ... 63
15.4 Requirements and Recommendations ... 63
15.4.1 Demonstration and Evaluation of Supplier Capability ... 63
15.4.2 Request for Quotation ... 64
15.4.3 Alignment of Responsibilities ... 64
15.5 Work Products ... 65

DRAFT

ANNEX A (INFORMATIVE) SUMMARY OF CYBERSECURITY ACTIVITIES AND WORK PRODUCTS 66
ANNEX B (INFORMATIVE) EXAMPLES OF CYBERSECURITY CULTURE 68
ANNEX C (INFORMATIVE) CYBERSECURITY INTERFACE AGREEMENT TEMPLATE EXAMPLE 69
ANNEX D (INFORMATIVE) CYBERSECURITY RELEVANCE: EXAMPLE METHOD AND CRITERIA 71
ANNEX E (INFORMATIVE) CYBERSECURITY ASSURANCE LEVELS 72
ANNEX F (INFORMATIVE) VERIFICATION AND VALIDATION 77
ANNEX G (INFORMATIVE) EXAMPLE USE CASE AND WORK PRODUCTS: HEADLAMP SYSTEM 80
ANNEX H (INFORMATIVE) IMPACT RATING FOR SAFETY, FINANCIAL, OPERATIONAL AND PRIVACY DAMAGE 97
ANNEX I (INFORMATIVE) GUIDELINES FOR DETERMINING ATTACK FEASIBILITY RATING 99
ANNEX J (INFORMATIVE) MATRICES FOR RISK DETERMINATION 105

DRAFT

1. SCOPE

This document specifies requirements for cybersecurity risk management regarding engineering for concept, development, production, operation, maintenance, and decommissioning for road vehicle electrical and electronic (E/E) systems, 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 the 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 31000, Risk management - Guidelines

ISO 26262-3:2018, Road vehicles - Functional Safety - Part 3: Concept phase

3. TERMS AND ABBREVIATIONS

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 http://www.iso.org/obp

IEC Electropedia: available at http://www.electropedia.org/

3.1.1 ASSET

Something for which the compromise of its *cybersecurity properties* (3.1.17) can lead to damage to an *item's* (3.1.21) *stakeholder* (3.1.29).

3.1.2 ATTACK

Attempted deliberate action or interaction with the item or component or its environment that has the potential to result in an adverse consequence.

3.1.3 ATTACK FEASIBILITY

Qualified attribute of an *attack path* (3.1.4) describing the ease of successfully carrying out the corresponding *attack* (3.1.2).

3.1.4 ATTACK PATH

Set of actions that could lead to the realization of a *threat scenario* (3.1.31).

3.1.5 ATTACKER

Person, group, or organization that conducts an *attack* (3.1.2).

3.1.6 AUDIT

Examination of an implemented process to determine the extent to which the process objectives are fulfilled.

[Modified from SOURCE: ISO 26262-1:2018[1]]

3.1.7 CUSTOMER

Person or organization that receives a service or product.

[Modified from SOURCE: ISO 9000]

3.1.8 CYBERSECURITY

Road Vehicle Cybersecurity

Condition in which *assets* (3.1.1) are sufficiently protected against threat scenarios to electrical or electronic components of road vehicles and their functions.

Note 1 to Entry: In this document, for the sake of brevity, only the term cybersecurity is used.

3.1.9 CYBERSECURITY ASSESSMENT

Judgement of the achieved degree of *cybersecurity* (3.1.8).

3.1.10 CYBERSECURITY CLAIM

Statement on a *risk* (3.1.25) that is accepted.

Note to Entry: Includes a description of why the risk is acceptable and a specification under which conditions the risk needs to be re-evaluated.

3.1.11 CYBERSECURITY CONCEPT

Collection of allocated cybersecurity requirements which achieve identified *cybersecurity goals* (3.1.14).

3.1.12 CYBERSECURITY CONTROL

Measure that is modifying *risk* (3.1.25).

[Modified from SOURCE: ISO 31000:2018]

3.1.13 CYBERSECURITY EVENT

Cybersecurity information (3.1.15) that has been confirmed as potentially relevant to an *item* (3.1.21) or component.

3.1.14 CYBERSECURITY GOAL

Concept level cybersecurity requirement associated with one or more *threat scenarios* (3.1.31).

Note to Entry: The statement of the cybersecurity goal can refer to an asset, attack path or to the damage scenario associated with the threat scenario.

3.1.15 CYBERSECURITY INFORMATION

Information derived from data collected by the monitoring process for which relevance to an item or component has not been determined.

DRAFT

3.1.16 CYBERSECURITY INTERFACE AGREEMENT

Agreement between *customer* (3.1.7) and supplier concerning distributed cybersecurity activities.

3.1.17 CYBERSECURITY PROPERTY

Attribute of an *asset* (3.1.1) including confidentiality, integrity, and availability.

3.1.18 DAMAGE SCENARIO

Adverse consequence or undesirable result due to the compromise of a *cybersecurity property* (3.1.16) (or properties) of an *asset* (3.1.1), or of a group of *assets.*

3.1.19 EMBEDDED SOFTWARE

Fully-integrated software to be executed on a processing element.

[SOURCE: ISO 26262-1:2018[1]]

3.1.20 IMPACT

Estimate of magnitude of damage or physical harm from a *damage scenario* (3.1.18).

3.1.21 ITEM

System or combination of systems to implement a function at the vehicle level.

[Modified from SOURCE: ISO 26262-1:2018[1]]

3.1.22 OUT OF CONTEXT

Not developed in the context of a specific *item* (3.1.21).

3.1.23 PENETRATION TESTING

Cybersecurity testing in which real-world attacks are mimicked to identify ways to compromise *cybersecurity goals* (3.1.14).

[SOURCE: NIST SP 800-115[21]]

3.1.24 RESIDUAL RISK

Risk (3.1.25) remaining after risk treatment.

[SOURCE: ISO/IEC 27000[9]]

3.1.25 RISK

Effect of uncertainty on *road vehicle cybersecurity* (3.1.8) expressed in terms of *attack feasibility* (3.1.3) and *impact* (3.1.20).

[Modified from SOURCE: ISO 31000:2018]

3.1.26 RISK MANAGEMENT

Coordinated activities to direct and control an organization with regard to *risk* (3.1.25).

[Modified from SOURCE: ISO 31000:2018]

DRAFT

3.1.27 ROAD USER

Person who uses a road, such as a pedestrian, cyclist, motorist, or an actor providing transportation.

3.1.28 SERIES PRODUCTION ROAD VEHICLE

Road vehicle that is intended primarily to be used for public roads and is not a prototype.

Note 1 to Entry: Vehicle type classification can vary between regions.

EXAMPLE 1: A vehicle that is sold for use by the general public.

EXAMPLE 2: A vehicle that is sold to be used amongst the general public.

[Modified from SOURCE: ISO 26262-1:2018[1]]

3.1.29 STAKEHOLDER

Person or organization that can be affected by a *damage scenario* (3.1.18).

[Modified from SOURCE: ISO 31000:2018]

3.1.30 TARGET ENVIRONMENT

Environment on which specific software is intended to be executed.

EXAMPLE 1: For application software the target environment is the microcontroller and its software.

EXAMPLE 2: For embedded software the target environment is the ECU in the system context.

3.1.31 THREAT SCENARIO

Statement of potential negative actions that lead to a *damage scenario* (3.1.18).

3.1.32 TRIAGE

Analysis to determine the relevance of *cybersecurity information* (3.1.15) to an item or component.

3.1.33 TRIGGER

Criterion used by cybersecurity monitoring for *triage* (3.1.32).

3.1.34 VALIDATION

Confirmation, through the provision of objective evidence, that the cybersecurity goals of the item are adequate and are achieved.

[Modified from SOURCE: ISO/IEC/IEEE 15288:2015[14]]

3.1.35 VERIFICATION

Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

[SOURCE: ISO/IEC/IEEE 15288:2015[14]]

DRAFT

3.1.36 VULNERABILITY

Weakness that can be exploited by a threat scenario (3.1.31).

[Modified from SOURCE: ISO/IEC 27000:2016[9]]

3.1.37 VULNERABILITY ANALYSIS

Systematic identification and evaluation of *vulnerabilities* (3.1.36).

3.2 Abbreviated Terms

CAL	Cybersecurity Assurance Level
CVSS	Common Vulnerability Scoring System
ECU	Electronic Control Unit
OEM	Original Equipment Manufacturer
PM	Permission
RC	Recommendation
RQ	Requirement
RASIC	Responsible, Accountable, Supporting, Informed, Consulted
WP	Work Product

4. GENERAL CONSIDERATIONS

The application of this document is limited to cybersecurity relevant items and components inside or on the vehicle perimeter including aftermarket and service parts. Systems outside the vehicle perimeter can be considered for cybersecurity purposes but are not in the scope of this document. The following are examples of what can be considered for the vehicle level as a whole:

a) the vehicle E/E architecture; and

b) the cybersecurity cases of the cybersecurity relevant items and components (see [WP-06-02]).

The relationship between the item and component and its applicable cybersecurity requirements is shown in Figure 2.

DRAFT

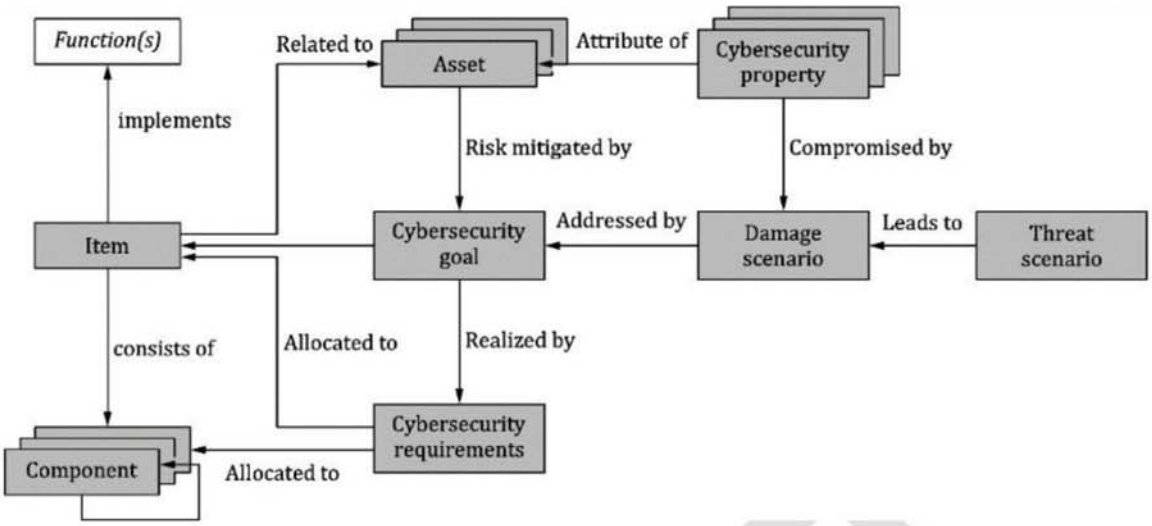


Figure 2 - Requirement generation for cybersecurity relevant items or components

Cybersecurity risk is not aggregated at the vehicle level. If the item and component level activities described in this document are performed, then unreasonable vehicle cybersecurity risk is addressed.

Clause 8 describes modularized methods for analysis and assessment of cybersecurity risk that are invoked in the cybersecurity activities described in the other clauses.

A defense-in-depth approach can be used to mitigate threat scenarios and risk. The defense-in-depth approach utilizes layers of cybersecurity measures to improve the cybersecurity of the item or vehicle. If an attack is able to penetrate or bypass one layer, another cybersecurity layer can help contain the attack and continue to maintain a sufficient degree of cybersecurity.

Cybersecurity management is applied throughout the supply chain to support cybersecurity engineering.

Every clause within this document has its own objectives, requirements and work products. Work products are documented results from one or more associated requirements. A summary of all cybersecurity activities and work products can be found in Annex A.

The annexes in this document are all informative and are used to provide additional information to the main body of the document for several reasons, for example:

- when the information or table is very long;
- to set apart special types of information;
- to present information regarding a particular application of the document.

Notes are used for giving additional information intended to assist the understanding or use of the text of the document.

Examples illustrate concepts presented in the document.

5. OVERALL 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 organization-specific rules (see [RQ-05-02]) and processes that are independently audited against the objectives of this document (see 5.4.4). These rules and processes cover concept, development, production, operation, maintenance, and decommissioning, including cybersecurity risk management, information sharing, vulnerability disclosure, cybersecurity monitoring, and incident response.

To support cybersecurity engineering, the organization implements management systems for cybersecurity, in particular a quality management system (see 5.4.6), and manages the tools used for cybersecurity engineering (see 0).

The organizations addressed include vehicle manufacturers and their supply chain.

The overall cybersecurity risk management of an organization is implemented in accordance with both this clause and ISO 31000 and applies throughout all phases. Figure 3 illustrates the mapping of the general clauses of ISO 31000 and its adaptation for the purpose of this document.

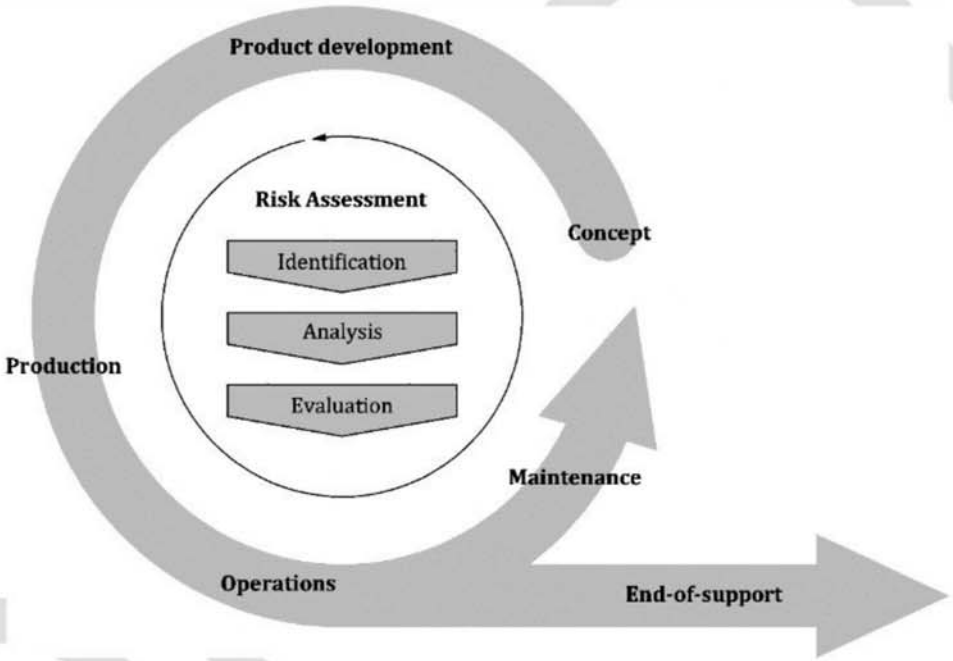


Figure 3 - Mapping of ISO 31000 against this document

5.2 Objectives

The objectives of this clause are to:

a) define a cybersecurity policy and the organization-specific 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) institute and maintain a cybersecurity culture, including competence management, awareness management and continuous improvement;

e) perform an organizational cybersecurity audit;

f) manage the sharing of cybersecurity information;

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

h) provide evidence that the tools used do not adversely affect cybersecurity.

5.3 Inputs

5.3.1 Prerequisites

None.

5.3.2 Further Supporting Information

The following information can be considered:

- existing evidence of compliance with standards that support quality management.

EXAMPLE: IATF 16949[16] in conjunction with ISO 9001[3] regarding quality management

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 risks.

NOTE 1: Links to the organization's objectives and other policies can be included in the cybersecurity policy.

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 organization-specific 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 definition, technical rules, guidelines, methods and templates.

NOTE 3: These rules and processes cover concept, development, production, operation, maintenance, and decommissioning, including cybersecurity risk management, information sharing, vulnerability disclosure, cybersecurity monitoring, incident response, and triggers (see 3.1.33).

NOTE 4: The rules and processes regarding vulnerability disclosure can be specified in accordance with ISO 29147[2].

NOTE 5: See Figure 4.

DRAFT

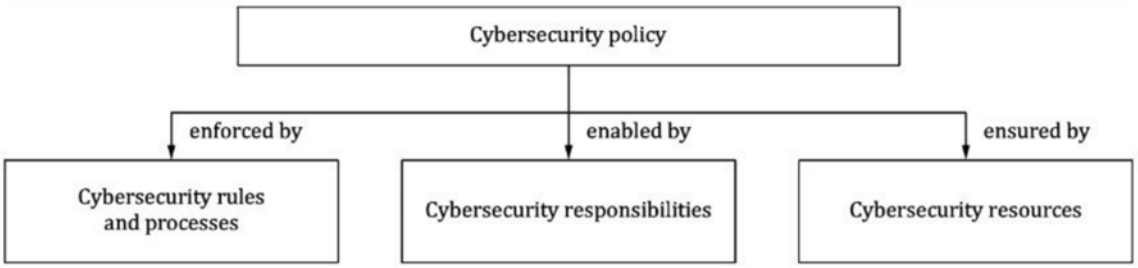


Figure 4 - Cybersecurity governance

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

NOTE 6: This relates to the organizational as well as to the project dependent activities.

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

NOTE 7: Resources include the persons responsible for cybersecurity risk management, development, and incident management.

EXAMPLE 2: Appropriate resources might include public affairs or a red team.

[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 8: Disciplines include information technology security, functional safety, data protection, and privacy.

NOTE 9: Relevant information includes threat scenarios and hazard information, cybersecurity goals and safety goals, or where a cybersecurity requirement might conflict or compete with a safety requirement.

NOTE 10: Coordination includes the identification of shared cybersecurity services and the reuse of cybersecurity strategies and tools between disciplines.

[RQ-05-06] The organization shall define the risk values (1 to 5) in a risk matrix in accordance with 8.8.

NOTE 11: See Annex J for guidance and examples.

5.4.2 Cybersecurity Culture

[RQ-05-07] The organization shall foster and maintain a cybersecurity culture.

NOTE 1: Those responsible for cybersecurity engineering lead by example such that others trust and follow them.

NOTE 2: See Annex B for examples.

[RQ-05-08] The organization shall ensure the persons within the organization that are involved in cybersecurity have the competences and awareness to fulfil their responsibilities.

DRAFT

EXAMPLE: Experience, awareness and training programs consider areas, such as:

- 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-05-09] The organization shall institute and maintain a continuous improvement process, such as:

a) learning from previous cybersecurity experiences, including experiences gathered by field monitoring and observation of internal and external information;

b) learning from information obtained regarding products of similar application in the field;

c) deriving improvements to be applied during subsequent cybersecurity activities;

d) communicating lessons learned to the appropriate persons; and

e) checking the adequacy of its rules and processes in accordance with [RQ-05-02].

NOTE 3: Lessons learned applies to activities of all phases (e.g., risk management, cybersecurity monitoring, and vulnerability management).

5.4.3 Cybersecurity Risk Management

[RQ-05-10] Cybersecurity risk management shall be in accordance with ISO 31000.

[PM-05-01] The organization may align its cybersecurity risk management and its corporate risk management.

NOTE: New and evolving cybersecurity risks after the release for post-development are managed with cybersecurity monitoring and vulnerability management and, if applicable, incident management.

EXAMPLE: During the development phase an assumption is made that a specific cryptographic algorithm is secure, but in the field it is discovered via cybersecurity monitoring that the algorithm is no longer secure. Vulnerability management and incident response are used to manage this issue.

5.4.4 Organizational Cybersecurity Audit

[RQ-05-11] A cybersecurity audit shall be performed to independently judge whether the organizational processes achieve the objectives of this document.

NOTE 1: Such a cybersecurity audit can be included in, or combined with, an audit according to a quality management system standard.

EXAMPLE: IATF 16949[16] in conjunction with ISO 9001[3].

NOTE 2: Independence can be based on, for example, IATF 16949[16] in conjunction with ISO 9001[3], or ISO 26262[1].

NOTE 3: The person that performs the audit can be internal or external to the organization.

DRAFT

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

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

5.4.5 Information Sharing

[RQ-05-12] The organization shall define the circumstances under which sharing is required, permitted, and prohibited, within and outside of the organization.

NOTE: This can include:

a) a list of the types of cybersecurity information that can be shared;

b) approval process for sharing;

c) requirements for redacting and sanitizing information;

d) rules for source attribution; and

e) consultation and types of communications permitted.

5.4.6 Management Systems

[RQ-05-13] The organization shall institute and maintain a quality management system in accordance with international standards, or equivalent, to support cybersecurity engineering, including:

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.

EXAMPLE 1: 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.

EXAMPLE 2: IATF 16949[16] in conjunction with ISO 9001[3]; ISO 10007[5], Automotive SPICE ®1, the ISO/IEC 33000 series of standards[13], ISO/IEC/IEEE 15288[14], ISO/IEC 12207[4].

[RQ-05-14] The configuration information regarding the cybersecurity of the products in the field shall remain available until the end of their support.

EXAMPLE 3: Bill of materials, binaries.

[RC-05-01] A cybersecurity management system for the manufacturing processes should be established.

EXAMPLE 4: IEC 62443 2-1[19], ISO/IEC 27001[10].

---

[1] Automotive SPICE® (refer to [27]) 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.

5.4.7 Tool Management

[RQ-05-15] Tools that can impact the cybersecurity of an item, system, 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:

- correct usage of the tool based on a user manual including errata;
- protection against unintended usage or action;
- access control for the tool users; or
- authentication of the tool.

[RC-05-02] An appropriate environment to support remediation actions for the cybersecurity incident response (see 13.3) should be reproducible until the end of support for the product.

EXAMPLE 4: Testing environment for reproducing the vulnerability.

EXAMPLE 5: Forensic methods.

5.4.8 Information Security Management

[RC-05-03] The relevant information security properties of the work products required by the cybersecurity plan should be managed by an information security management system.

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

5.5 Work Products

[WP-05-01] Cybersecurity policy, rules and processes, resulting from the requirements of 5.4.1, 5.4.3 and 5.4.5.

[WP-05-02] Evidence of competence management, awareness management and continuous improvement, resulting from the requirements of 5.4.2.

[WP-05-03] Organizational cybersecurity audit report, resulting from the requirements of 5.4.4.

[WP-05-04] Evidence of the organization's management systems, resulting from the requirements of 5.4.6.

[WP-05-05] Evidence of tool management, resulting from the requirements of 5.4.7.

DRAFT

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 and the planning of the cybersecurity activities. This document defines requirements in a generic fashion such that it can be applied to a variety of items and components, including new developments. In addition, tailoring can be applied (see 6.4.3) that is based on a rationale and is defined in the cybersecurity plan (see [WP-06-01]). Examples of when tailoring can be used include:

a) reuse (see 6.4.4);

b) out of context development (see 6.4.5); or

c) use of an off the shelf component (see 6.4.6).

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, such as an evolution of attack techniques, newly emerged vulnerabilities (e.g., learned from information sharing (see 5.4.5)), or a change of the assets since the original development. If the original item or component was developed according to this document, the reuse is specified based on the existing work products. If the item or component was not originally developed according to this document, the reuse can be based on the existing documentation with a rationale.

A component can be developed based on an assumed context (i.e., out of 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 can be used without customization (e.g., a third-party software library or an open source software component). Such a component can be integrated as part of the development. It might or might not have been developed in accordance with this document.

The cybersecurity case provides a structured argument for the achieved degree of cybersecurity (see 6.4.7). The cybersecurity case is a structured document that provides a basis for judgement and confidence of cybersecurity. The purpose of the cybersecurity case is to provide a clear, comprehensible and defensible rationale, supported by evidence and documentation, that an item or component achieves a sufficient degree cybersecurity for a specific application in a specific environment. As such, it is an input to a cybersecurity assessment and the release for post-development.

A cybersecurity assessment (see 6.4.8) independently judges the achieved degree of cybersecurity of an item or component and its report includes a recommendation for acceptance, conditional acceptance, or rejection. It can be based on a judgement of whether the objectives of this document are achieved. Multiple skills, knowledge, and experience are relevant to carry out a cybersecurity assessment (see also 5.4.2).

Finally, the cybersecurity case and the cybersecurity assessment, if applicable, provide input for the decision to 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 that provides the argument for the achieved degree of cybersecurity;

d) perform a cybersecurity assessment that judges the achieved degree of cybersecurity, if applicable; and

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

6.3 Inputs

6.3.1 Prerequisites

The following information shall be available:

- organizational policy, rules and processes (see [WP-05-01]); and

- organizational cybersecurity audit report (see [WP-05-03]), if an organizational audit is already performed.

6.3.2 Further Supporting Information

The following information can be considered:

- the relevant bills of materials.

NOTE: The corresponding bills of materials support the management of the identified cybersecurity vulnerabilities, including the applicable configurations.

6.4 Requirements and Recommendations

6.4.1 Cybersecurity Responsibilities and Their Assignment

[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 providing that this is communicated and there is a handover of pertinent information.

6.4.2 Cybersecurity Planning

[RQ-06-02] An analysis shall be performed to determine:

a) whether the item or component is cybersecurity relevant; and

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

b) whether the item or component is a new development or a reuse.

NOTE 2: If the item or component is reused, a reuse analysis in accordance with 6.4.4 is performed. A reuse can be applied with or without modification to the item, component or environment.

NOTE 3: If the item or component is determined as not being cybersecurity relevant, there are no relevant cybersecurity activities thus cybersecurity planning is not initiated.

[RQ-06-03] The responsibilities for 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-06-04] 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.

DRAFT

NOTE 4: The cybersecurity plan can incorporate cross-references to other information under configuration management.

[RQ-06-05] The cybersecurity plan shall specify the activities that are required to comply with the requirements of this document associated with the concept phase and product development phases (see Clauses 9, 10, and 11).

NOTE 5: The cybersecurity plan can be refined in incremental steps during development and integration.

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

a) the objective of an activity;

b) the dependencies on other activities or information;

c) the person responsible for performing an activity;

d) the required resources for performing an activity;

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

f) the identification of the work products.

NOTE 6: The extent of the cybersecurity activities defined in the cybersecurity plan can be updated (e.g., depending on the results of the risk determination) (see Clause 8).

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

[RQ-06-08] The work products required by the cybersecurity plan shall be maintained and updated during the development phases so as to provide an adequate representation of the item or component, until and at the release for post-development.

[RQ-06-09] When cybersecurity activities are distributed, both the customer and the supplier shall define a cybersecurity plan regarding their respective cybersecurity activities and interfaces in accordance with Clause 15.

[RQ-06-10] The cybersecurity plan, as well as the work products resulting from the cybersecurity activities defined in the cybersecurity plan, shall be subject to configuration management, change management, requirements management, and documentation management, in accordance with 5.4.6.

6.4.3 Tailoring of the Cybersecurity Activities

[PM-06-01] A cybersecurity activity may be tailored.

[RQ-06-11] If a cybersecurity activity is tailored, then a rationale shall be provided that includes why the tailoring is adequate and sufficient to achieve the relevant objectives of this document.

NOTE 1: An activity is tailored if it is omitted or performed in a different manner compared to its description in this document.

NOTE 2: Activities that are not performed because they are performed by another entity in the supply chain are not considered as tailored, but as distributed activities (see Clause 15).

DRAFT

6.4.4 Reuse

[RQ-06-12] A reuse analysis of an existing item or component shall be carried out if it is reused with or without modification; i.e., if:

a) it has been developed, but modifications are planned;

b) it is reused in another operational environment; and/or

c) it is planned to be reused without modification and the information concerning the item or component has changed relevantly, such as a change in the known attacks and vulnerabilities, or a change of the assets.

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.

NOTE 1: Modifications can include design modifications and/or implementation modifications:

- Design modifications can result from requirements modification (e.g., functional or performance enhancement).

- Implementation modifications can result from corrections of software, or the use of new production or maintenance tools (e.g., model based development). These modifications might not affect the specification or performance of the existing item or component, but only the implementation features.

NOTE 2: A modification to configuration data or calibration data is considered as a modification if it impacts the functional behavior or the assets and cybersecurity properties of the existing item or component.

[RQ-06-13] The reuse analysis of an existing item or component shall:

a) identify the modifications to the operational context, including the modifications to the item or component as well as modifications of its environment;

b) analyze the implication of the modifications regarding cybersecurity, including the impact on the validity of cybersecurity claims and previously made assumptions;

c) identify the affected or missing work products and determine the activities necessary to comply with this document; and

NOTE 3: This includes an analysis of the existing threat analysis and risk assessment; e.g., considering new assets, threat scenarios or risk determination compared to when the existing item or component was developed.

d) specify the cybersecurity activities in the cybersecurity plan, based on this reuse analysis, in accordance with 6.4.2.

EXAMPLE 2: A modification can have one or more implications on:

- the cybersecurity requirements;

- the design and implementation;

- operational environments and operating modes;

- maintenance;

- cybersecurity controls;

- susceptibility to known attacks and exposure of known vulnerabilities; or

- the assets.

DRAFT

[RQ-06-14] The reuse analysis of an existing component shall:

a) evaluate whether, with or without modifications, the reused component is able to comply with the allocated cybersecurity requirements that result from the item, or component, in which it is to be integrated; and

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

6.4.5 Component Out of Context

[RQ-06-15] If cybersecurity activities are tailored in accordance with 6.4.2 because a component is developed out of context, then:

a) assumptions on the new intended use and context, including the external interfaces, shall be documented in the corresponding work products;

b) the out of context development shall be based on cybersecurity requirements that are derived from the assumptions; and

c) for the out of context component integration, the cybersecurity claims and assumptions of the out of context development shall be validated.

6.4.6 Off-the-Shelf Component

[RQ-06-16] When integrating an off-the-shelf component in accordance with 6.4.6, the cybersecurity-relevant information shall be gathered and analyzed to determine whether:

a) the allocated cybersecurity requirements can be complied with;

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

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

NOTE: The integration and test activities are documented in the work products related to integration and testing.

[RQ-06-17] If the existing documentation is insufficient to support the integration of the off-the-shelf component, then the cybersecurity activities to comply with this document shall be identified and performed.

EXAMPLE: Insufficient documentation concerning vulnerabilities of the off-the-shelf component.

6.4.7 Cybersecurity Case

[RQ-06-18] A cybersecurity case shall be created to provide the argument, supported by work products, for the achieved degree of cybersecurity.

NOTE: The argument can be implicit (i.e., if the argument is evident from the compiled set of work products an explicit argument can be omitted). In this scenario, the cybersecurity case contains the list of work products required by the cybersecurity plan (see [WP-06-01]).

6.4.8 Cybersecurity Assessment

[RQ-06-19] A judgement based on a rationale shall be made to decide whether a cybersecurity assessment is performed for an item or component.

NOTE 1: The judgement of whether to perform a cybersecurity assessment or not can be based on the results of the risk determination in accordance with Clause 8, supported by a rationale.

DRAFT

[RQ-06-20] The rationale of [RQ-06-19] shall be independently reviewed.

NOTE 2: The corresponding independence scheme regarding the review of the rationale can be based on IATF 16949[16] in conjunction with ISO 9001[3], or ISO 26262[1].

[RQ-06-21] The cybersecurity assessment shall judge whether the available evidence provides confidence that the achieved degree of cybersecurity of the item or component is sufficient.

NOTE 3: The available evidence is provided by the documented results of the cybersecurity activities (i.e., the work products) (see Annex A).

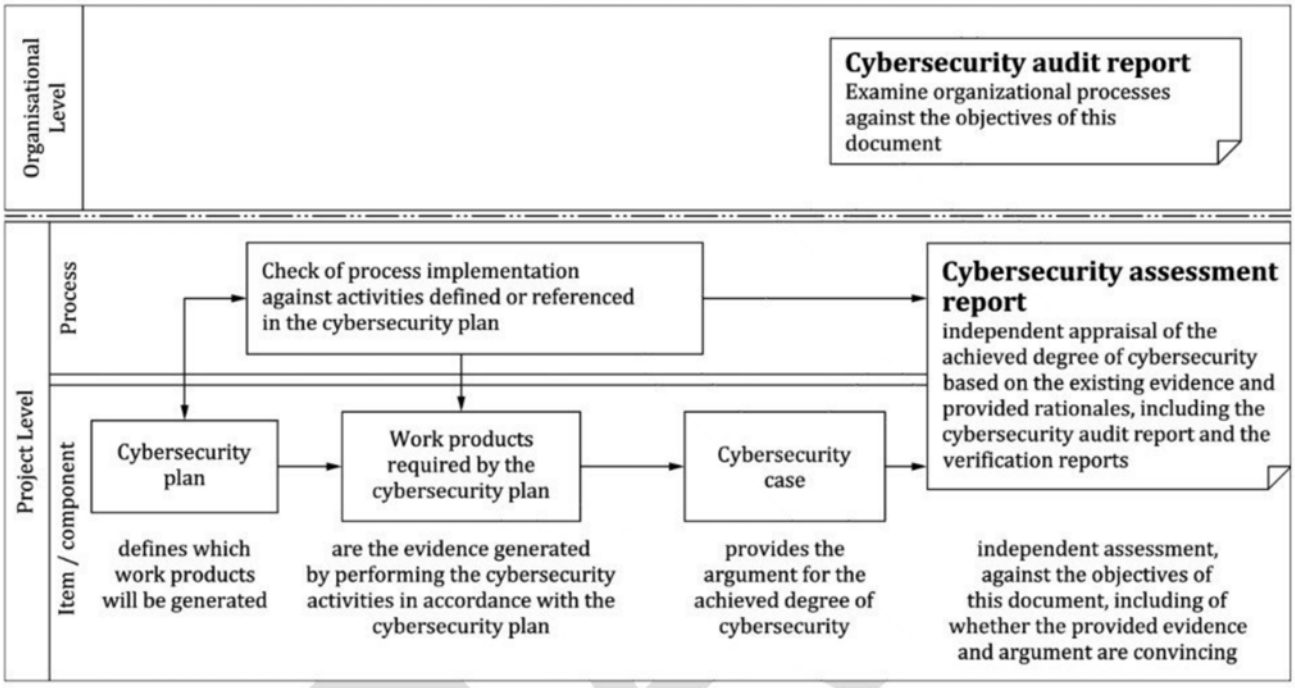


Figure 5 - Project cybersecurity assessment in relation to other activities

NOTE 4: The cybersecurity assessment can be performed in incremental steps to facilitate an early resolution of identified issues.

NOTE 5: The assessment can be repeated or supplemented; e.g., due to a change, when the previous assessment provided a negative recommendation, or when a vulnerability is discovered.

[RQ-06-22] The cybersecurity assessment report shall be made available prior to the release for post-development.

NOTE 6: The scope of the cybersecurity assessment report at the release for post-development can include the performed cybersecurity activities and the cybersecurity requirements for post-development (see [WP-10-02]).

[RQ-06-23] The person responsible to plan and independently perform the cybersecurity assessment shall be appointed in accordance with [RQ-05-08] and [RQ-06-01], supported by [RQ-05-03] and [RQ-05-04].

NOTE 7: The independence scheme can be based on IATF 16949[16] in conjunction with ISO 9001[3], or ISO 26262[1].

EXAMPLE: A person of a quality assurance department within the organization, a person from a different team or department, or a person from an independent third party.

[RQ-06-24] A person who carries out a cybersecurity assessment shall have access to the relevant information, tools and the cooperation of the personnel responsible for performing the cybersecurity activities.

[PM-06-02] A cybersecurity assessment may be based on a judgement of whether the project related objectives of this document are achieved.

[RQ-06-25] The scope of a cybersecurity assessment shall include:

a) the cybersecurity plan and all work products required by the cybersecurity plan;

NOTE 8: The activities and work products are summarized in Annex A.

b) the appropriateness and effectiveness of the implemented or performed cybersecurity technical or process controls;

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

c) the rationales, if provided, that demonstrate the achievement of the relevant objectives of this document;

NOTE 10: The person(s) responsible for the creation of a work product can provide a rationale as to why the objectives of this document are achieved in order to facilitate a cybersecurity assessment, considering [PM-06-02].

NOTE 11: Compliance with all the corresponding requirements is a sufficient rationale for having achieved an objective of this document.

d) the rationales for the treatment of the cybersecurity risks, in accordance with 8.9; and

e) the cybersecurity requirements for post-development (see [WP-10-02]).

[RQ-06-26] A cybersecurity assessment report shall include a recommendation for acceptance, conditional acceptance, or rejection of the achieved degree of cybersecurity of the item or component.

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

[PM-06-03] A cybersecurity assessment report may include a recommendation for conditional acceptance.

[RQ-06-27] If a recommendation for conditional acceptance in accordance with [PM-06-03] is made, then the cybersecurity assessment report shall include the conditions for acceptance.

6.4.9 Release for Post-Development

[RQ-06-28] The following work products shall be available prior to the release for post-development:

- the cybersecurity case in accordance with 6.4.7;
- if applicable, the cybersecurity assessment report in accordance with 6.4.8; and
- the cybersecurity requirements for post-development (see [WP-10-02].(

[RQ-06-29] The release for post-development of the item or component shall be approved if both of the following conditions are fulfilled:

a) sufficient evidence of the achieved degree of cybersecurity is provided by the cybersecurity case; and if applicable the judgement included in the cybersecurity assessment report; and

b) the cybersecurity requirements for the post-development phase are identified and reviewed.

NOTE: Changes to the cybersecurity claims (see [WP-09-05]) can result in repeating the release for post-development.

DRAFT

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. CONTINUOUS CYBERSECURITY ACTIVITIES

7.1 General

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

Cybersecurity monitoring (see 7.3) collects cybersecurity information on potential threats, vulnerabilities, and possible mitigations for items and components to avoid known issues and to address new threats, and can serve as the input for vulnerability management and cybersecurity incident response activities.

Cybersecurity event assessment (see 7.4) determines the criticality of a cybersecurity event and launches corresponding activities.

Vulnerability analysis (see 7.5) examines weaknesses and assesses if a particular weakness can be exploited to launch an attack.

Vulnerability management (see 7.6) tracks and oversees the treatment of vulnerabilities.

7.2 Objectives

The objectives of this clause are:

a) to collect relevant cybersecurity information;

b) to triage collected cybersecurity information using triggers;

c) to assess cybersecurity events;

d) to identify and analyze cybersecurity vulnerabilities; and

e) to manage identified cybersecurity vulnerabilities.

7.3 Cybersecurity Monitoring

7.3.1 Inputs

7.3.1.1 Prerequisites

The following information shall be available:

- configuration information regarding the cybersecurity of the products in the field in accordance with [RQ-05-14]; and
- criteria, including triggers, for the triage of cybersecurity information included in [WP-05-01].

DRAFT

7.3.1.2 Further Supporting Information

None.

7.3.2 Requirements and Recommendations

[RQ-07-01] Internal and external sources shall be monitored for collection of cybersecurity information.

EXAMPLE 1: External sources for cybersecurity information can include:

- researchers;
- commercial or non-commercial sources;
- organization's supply chain;
- customers of the organization; and/or
- government sources.

EXAMPLE 2: Internal sources for cybersecurity information can include:

- results of vulnerability analyses;
- information received from the field (e.g., vulnerability scanning reports, repair information, consumer usage information); and/or
- configuration information such as a hardware or software bill of materials.

[RQ-07-02] Triage shall be based on defined triggers and applied to cybersecurity information to determine if cybersecurity information becomes one or more cybersecurity events.

EXAMPLE 3: Criteria for the triage that can be used to define the trigger thresholds can include:

- whether cybersecurity information comes from a known trusted source;
- the determined risk of the threat scenarios of the item resulting from the activity in [RQ-09-05]; and/or
- the type of information obtained (e.g., an active attack or proof of concept).

7.3.3 Work Products

[WP-07-01] List of sources for cybersecurity monitoring, resulting from [RQ-07-01].

[WP-07-02] Results from the triage of cybersecurity information, resulting from [RQ-07-02].

7.4 Cybersecurity Event Assessment

7.4.1 Inputs

7.4.1.1 Prerequisites

The following information shall be available:

- results from the triage of cybersecurity information (see [RQ-07-02]); and
- cybersecurity requirements for post development (see [WP-10-02]), if applicable.

DRAFT

7.4.1.2 Further Supporting Information

The following information can be considered:

- vulnerability analysis reports from product development (see [WP-10-04]).

7.4.2 Requirements and Recommendations

[RQ-07-03] A cybersecurity event shall be analyzed to determine if the cybersecurity event affects an item or component based on a vulnerability analysis in accordance with 7.5.

NOTE 1: If the cybersecurity event assessment determines that the item or component is unaffected by the cybersecurity event, the organization can decide to cease further activities.

NOTE 2: A cybersecurity vulnerability identified as a result of [RQ-07-03] is handled in accordance with 7.6.

[PM-07-01] Based on the risk treatment decision from 8.9, the cybersecurity incident response process in accordance with 13.3 may be applied in post-development phases.

NOTE 3: The organization can define the criteria for invoking incident response.

EXAMPLE: Risk treatment from 7.6 affects items or components in post-development phases.

NOTE 4: If the cybersecurity incident response process is applied, then the cybersecurity event becomes a cybersecurity incident.

7.4.3 Work Products

[WP-07-03] The cybersecurity event assessment, resulting from [RQ-07-03].

7.5 Vulnerability Analysis

7.5.1 Inputs

7.5.1.1 Prerequisites

The following information shall be available:

- item definition (see [WP-09-01]).

7.5.1.2 Further Supporting Information

The following information can be considered:

- cybersecurity event assessments (see [WP-07-03]);
- past vulnerability analysis documentation (see [WP-07-04]);
- attack paths for the item or component (see [WP-08-05]);
- verification reports (see [WP-10-05] and [WP-10-06]); and
- cybersecurity incident response information [WP-13-02]).

7.5.2 Requirements and Recommendations

[RQ-07-04] Weaknesses and/or cybersecurity events shall be analyzed to identify vulnerabilities.

NOTE 1: Weaknesses can be inherent to the item or component or caused by human mistakes or errors during concept or development.

DRAFT

EXAMPLE: Weaknesses include:

- missing requirements or specifications;
- architectural or design weaknesses, including incorrect design of security protocols;
- implementation weaknesses, including hardware and software bugs, incorrect implementation of security protocols;
- weaknesses in the operational processes and procedures, including misuse and inadequate user-training; and/or
- use of outdated or deprecated functions, including cryptographic algorithms.

NOTE 2: Relevance of the weakness for the item can be assessed through an analysis of the architecture or invocation of attack path analysis.

NOTE 3: A root cause analysis can be performed to determine the underlying causes of vulnerability, including possible methods of exploitation as it relates to the instance of the cybersecurity event.

[RC-07-01] Attack paths should be analyzed in accordance with 8.6 to map the discovered vulnerabilities to specific attack paths.

[RC-07-02] Attack feasibility rating in accordance with 0 should be determined for the discovered vulnerabilities.

7.5.3 Work Products

[WP-07-04] Vulnerability analysis, resulting from [RQ-07-04].

7.6 Vulnerability Management

7.6.1 Inputs

7.6.1.1 Prerequisites

The following information shall be available:

- cybersecurity event assessment (see [WP-07-03]), if applicable; and
- reports of vulnerability analyses from product development (see [WP-10-04]), if applicable.

7.6.1.2 Further Supporting Information

None.

7.6.2 Requirements and Recommendations

[RQ-07-05] Identified vulnerabilities shall be managed based on a rationale such that the corresponding risk is treated.

EXAMPLE: Rationales can include arguments such as the following:

- verification report that shows the vulnerability is eliminated;
- analysis, risk determination and risk treatment of the vulnerability.

[RQ-07-06] The risk treatment shall be based on:

a) the results of a vulnerability analysis in accordance with [WP-07-04]; and

b) the results of the risk determination in accordance with 8.8.

NOTE 1: An organization can consider several factors in determining the treatment, such as impact rating (see 8.5) or attack feasibility rating (see 0).

DRAFT

[RQ-07-07] Risk treatment for vulnerabilities shall be performed in accordance with 8.9, and Clauses 9 and 10.

NOTE 2: Risk acceptance is a possible risk treatment. In this case, the rationale for acceptance is documented.

NOTE 3: If the risk treatment results in a change to an item or component, change management is applied in accordance with [RQ-05-13].

NOTE 4: Information about identified vulnerabilities can be shared in accordance with 5.4.5.

[RQ-07-08] If cybersecurity information becomes available that invalidates the existing rationale, the vulnerability shall no longer be considered as managed.

7.6.3 Work Products

[WP-07-05] Rationale for the managed vulnerability, resulting from [RQ-07-05].

8. RISK ASSESSMENT METHODS

8.1 General

The purpose of this clause is to describe the methods that organizations can use to determine the extent to which a stakeholder can be impacted by a threat scenario. For this clause, a stakeholder is defined as a road user, with the option for the business to include additional entities.

All work products listed in this clause are documented as work products in other clauses.

The risk assessment methods defined in this clause make use of the following generic modules that can be called systematically, and from any point in the lifecycle:

- Asset Identification (see 8.3): Identification of damage scenarios and assets of an item or component.

  NOTE 1: Assets are contained within an item or component. The item or component itself can be one of the identified assets.

  NOTE 2: See Annex G for an illustration with a practical example.

- Threat Scenario Identification (see 8.4): The identification of threat scenarios to the cybersecurity properties of the assets under analysis.

- Impact Rating (see 8.5): Estimation of the magnitude of damage or physical harm associated with a damage scenario.

  NOTE 3: The impact of a damage scenario is the same regardless of:

  - the attack path that leads to the damage; or

  - a particular threat agent.

- Attack Path Analysis (see 8.6): Identification and linking of potential attack paths to one or more threat scenarios.

  NOTE 4: Attack paths form the basis for the assessment of attack feasibility. They are also used for the refinement of cybersecurity goals to cybersecurity requirements and to support the selection of appropriate controls.

- Attack Feasibility Rating (see 0): The rating of the feasibility of attack paths based on the ease of exploitation.

  NOTE 5: It is intended to be able to handle information at different abstraction levels during an attack feasibility rating. A high-level attack path description might be available from the concept phase, and a more concrete attack path description might be available in the later phases. An attack feasibility rating is possible in both cases.

- Risk Determination (see 8.8): The determination of the risk value of a threat scenario.

DRAFT

- Risk Treatment Decision (see 8.9): Addressing identified risks by selecting a suitable risk treatment option.

The aforementioned modules are not connected to a particular process phase of the lifecycle and can be used in the order most appropriate for the organization.

8.2 Objectives

The objectives of this clause are to:

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

b) identify threat scenarios;

c) rate the impact of the identified damage scenarios;

d) identify and/or update the attack paths that realize a threat scenario;

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

f) determine the risk value of a threat scenario; and

g) select the appropriate risk treatment options.

8.3 Asset Identification

8.3.1 Inputs

8.3.1.1 Prerequisites

The following information shall be available:

- item definition (see [WP-09-01]).

8.3.1.2 Further Supporting Information

Existing information regarding the item or component can be considered.

EXAMPLE: architectural design

8.3.2 Requirements and Recommendations

[RQ-08-01] Damage scenarios shall be identified.

[RQ-08-02] Assets with cybersecurity properties whose compromise leads to a damage scenario shall be enumerated.

NOTE: The enumeration of relevant assets can be based on various methods, including:

- performing an impact rating;
- deriving assets from threat scenarios; and
- 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 messages received by the braking function and its cybersecurity property is integrity. The damage scenario is unintended full braking when the vehicle is travelling at high speed resulting from the loss of integrity.

DRAFT

8.3.3 Work Products

[WP-08-01] Damage scenarios, resulting from [RQ-08-01].

[WP-08-02] Identified assets and cybersecurity properties, resulting from [RQ-08-02].

8.4 Threat Scenario Identification

8.4.1 Inputs

8.4.1.1 Prerequisites

The following shall be available:

- item definition (see [WP-09-01]).

8.4.1.2 Further Supporting Information

The following information can be considered:

- architectural design, if available;
- damage scenarios (see [WP-08-01]); and
- identified assets and cybersecurity properties (see [WP-08-02]).

8.4.2 Requirements and Recommendations

[RQ-08-03] Threat scenarios shall be identified.

NOTE 1: See Annex G for an illustration with a practical example.

NOTE 2: The method for threat scenario identification can use brainstorming-based approaches.

EXAMPLE 1:

- misuse-case elicitation;
- taxonomy mnemonic-based approaches (e.g., STRIDE); or
- a combination of the above.

NOTE 3: A threat scenario can include:

- the targeted asset;
- the compromised cybersecurity property; and
- the action to accomplish a damage scenario.

EXAMPLE 2: Spoofing of CAN (controller area network) messages for the powertrain ECU (electronic control unit) leads to loss of integrity of the CAN messages (and thereby to loss of integrity of the acceleration function) potentially causing uncontrollable acceleration of the vehicle and possible harm.

NOTE 4: Relations and dependencies between assets can be relevant in the identification of threat scenarios.

NOTE 5: If more information about a threat scenario is available, such as the threat agent who initiates action, the method, tools, and entry points, it can be documented to provide further information to the risk assessment process (e.g., attack path analysis, attack feasibility).

DRAFT

NOTE 6: One damage scenario can correspond to multiple threat scenarios (see Figure 6).

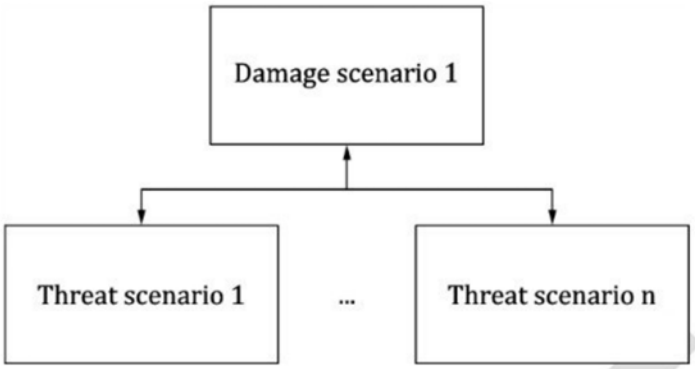


Figure 6 - Relationship between damage scenario and threat scenario

8.4.3 Work Products

[WP-08-03] Threat scenarios, resulting from [RQ-08-03].

8.5 Impact Rating

8.5.1 Inputs

8.5.1.1 Prerequisites

The following shall be available:

- damage scenarios (see [WP-08-01]).

8.5.1.2 Further Supporting Information

The following information can be considered:

- item definition (see [WP-09-01]); and
- identified assets and cybersecurity properties (see [WP-08-01]).

8.5.2 Requirements and Recommendations

[RQ-08-04] The damage scenarios shall be assessed against potential adverse consequences for stakeholders in the independent impact categories of safety, financial, operational, and privacy (S, F, O, P).

[RQ-08-05] If further impact categories are considered beyond S, F, O and P, then those categories shall be documented.

NOTE 1: S, F, O, P are the core impact categories that are used to rate the impact on road users. This document makes provision for the extension of the core categories with additional categories that could help assess the impact on other stakeholders, for example the business or the performing organization. Example categories are loss of intellectual property, financial losses to business, loss of brand image or reputation.

NOTE 2: If distributed development in accordance with Clause 15 is used, then the rationale and explanation of these parameters can be forwarded in the supply chain.

DRAFT

[RQ-08-06] The impact rating of the damage scenario shall be determined to be one of the following:

- Severe;
- Major;
- Moderate; or
- Negligible.

NOTE 3: Financial, operational and privacy related impacts can be rated in accordance with tables given in Annex H.

[RQ-08-07] Safety related impacts shall be derived from ISO 26262-3:2018, 6.4.3 Classification of hazardous events.

NOTE 4: Table H.1 in Annex H can be used for mapping safety impacts.

8.5.3 Work Products

[WP-08-04] Impact rating, including the associated impact categories of the damage scenarios, resulting from [RQ-08-04] to [RQ-08-07].

8.6 Attack Path Analysis

8.6.1 Inputs

8.6.1.1 Prerequisites

The following information shall be available:

- item definition (see [WP-09-01]); and
- threat scenarios (see [WP-08-03]).

8.6.1.2 Further Supporting Information

The following information can be considered:

- known vulnerabilities from common public sources (e.g., common vulnerabilities and exposures);
- architectural design, if available;
- previously identified attack paths (see [WP-08-05]), if available; and
- vulnerability analysis (see [WP-07-04]).

8.6.2 Requirements and Recommendations

[RQ-08-08] The threat scenarios shall be analyzed to describe possible attack paths.

[RQ-08-09] The attack path analysis approach applied shall be documented.

NOTE 1: An attack path analysis approach can be based on (see Figure 7):

a) Top-down approaches such as attack trees, attack graphs, taxonomy mnemonic-based approaches (e.g., STRIDE):

   i. In top-down (deductive) approach, attack paths are deduced (i.e., theorized, inferred, reasoned, conjectured) for the item or component based on historical knowledge of vulnerabilities in similar systems and components.

   ii. Top-down approach is useful in the concept and development phases when implementation of the current item or component is not available, or when effort is directed toward building attack hypotheses or attack path models.

DRAFT

b) Bottom-up approaches (e.g., the output of vulnerability analysis):

i. In a bottom-up (inductive) approach, attack paths are built for the item or component from the cybersecurity vulnerabilities identified. Each action in the attack path is based on an "exploitable weakness."

ii. The bottom-up approach is most commonly used when an implementation of the item or component is available, or when hypotheses or attack model are to be confirmed.

c) A combination of these approaches.

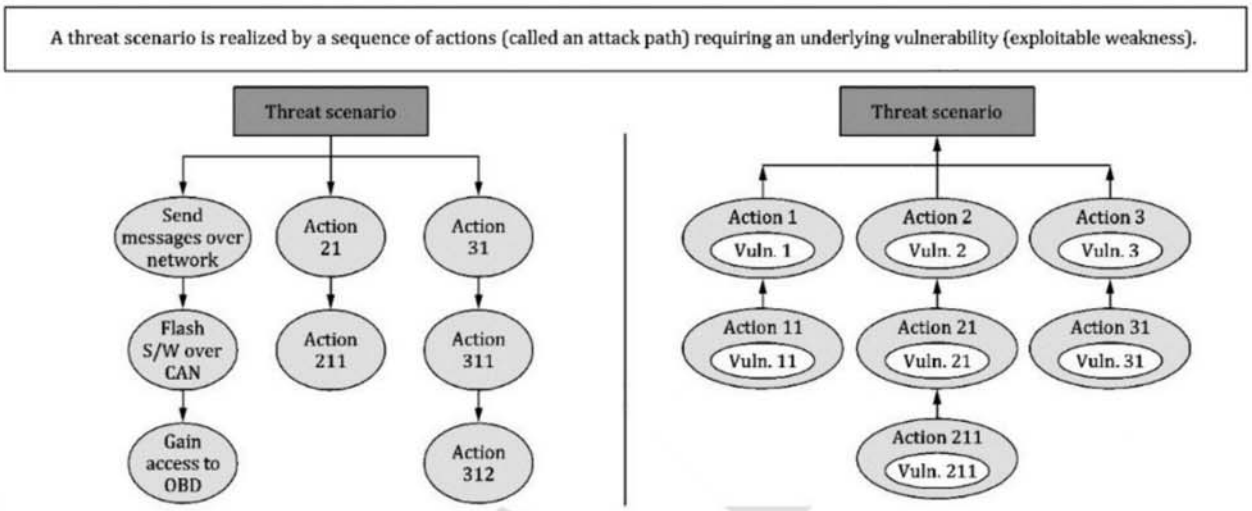


Figure 7 - Methods for determining attack paths

NOTE 2: If attack path analysis reveals that a partial attack path does not accomplish the threat scenario, this partial attack path can be truncated, and the analysis can be stopped at that point.

[RC-08-01] The attack path description should include a reference to the threat scenarios that can be realized by the attack path.

NOTE 3: If a bottom-up approach is used, the following information can be included:

a) vulnerabilities or weaknesses that could be exploited; and

b) how the vulnerabilities could be leveraged in an attack to realize the threat scenario.

NOTE 4: In the early stages of product development the attack paths are often incomplete or imprecise as specific implementation details are not yet known in sufficient detail to be able to identify specific vulnerabilities. During the lifecycle, the attack paths could be updated with additional detail as more information becomes available (e.g., after a vulnerability analysis).

EXAMPLE:

- Threat Scenario: Spoofing of CAN (Controller Area Network) messages for the braking ECU (Electronic Control Unit), causing uncontrollable arbitrary braking of the vehicle leading to loss of passenger safety causing physical harm to the vehicle user.

- Attack Path: The telematics ECU is compromised via the cellular interface, then Gateway ECU is compromised via CAN communication, next the gateway ECU forwards malicious torque request signals, resulting in spoofing of acceleration torque requests.

8.6.3 Work Products

[WP-08-05] Identified attack paths, resulting from [RQ-08-08] and [RC-08-01].

8.7 Attack Feasibility Rating

8.7.1 Inputs

8.7.1.1 Prerequisites

The following information shall be available:

- identified attack paths (see [WP-08-05]).

8.7.1.2 Further Supporting Information

The following information can be considered:

- architectural design; and
- vulnerability analysis (see [WP-07-04]).

8.7.2 Requirements and Recommendations

[RQ-08-10] For each attack path the attack feasibility rating shall be determined as one of the following:

- high;
- medium;
- low; or
- very low.

NOTE 1: Annex I provides guidelines on determining attack feasibility rating.

[RC-08-02] The defined rating method should be based on one of the following assessment approaches:

a) attack potential-based approach;

b) CVSS[2] based approach; or

c) attack vector-based approach.

NOTE 2: Selection of the rating approach can depend upon the phase in the lifecycle and available information.

[RC-08-03] If an attack potential-based approach is used, it should be determined based on core factors including elapsed time, specialist expertise, knowledge of the item or component, window of opportunity, and equipment.

NOTE 3: The core attack potential factors can be derived from ISO/IEC 18045[8].

NOTE 4: I.3 provides guidelines on determining attack feasibility based on attack potential.

[RC-08-04] If a CVSS based approach is used, it should be determined based on the exploit metrics group of the base metrics, including attack vector, attack complexity, privileges required, and user interaction.

NOTE 5: I.4 provides guidelines on determining attack feasibility based on a CVSS based approach.

[RC-08-05] If an attack vector based approach is used, it should evaluate the predominant attack vector (cf. CVSS) of the attack path.

---

[2] Refer to [25].

NOTE 6: I.5 provides guidelines on determining attack feasibility based on an attack vector based approach.

NOTE 7: Attack feasibility can be estimated qualitatively using an attack vector based approach during the early stages of product development, when there is insufficient detailed information to identify specific attack paths.

8.7.3 Work Products

[WP-08-06] Attack feasibility rating, resulting from [RQ-08-10].

8.8 Risk Determination

8.8.1 Inputs

8.8.1.1 Prerequisites

The following information shall be available:

- impact rating (see [WP-08-04]); and
- attack feasibility rating (see [WP-08-06]).

8.8.1.2 Further Supporting Information

None.

8.8.2 Requirements and Recommendations

[RQ-08-11] The risk value of a threat scenario shall be determined from the impact of the associated damage scenario and the attack feasibility of the associated attack paths.

NOTE 1: The value 1 is the lowest risk and value 5 is the highest risk, see Annex J.

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

8.8.3 Work Products

[WP-08-07] Risk value, resulting from [RQ-08-11].

8.9 Risk Treatment Decision

8.9.1 Inputs

8.9.1.1 Prerequisites

The following information shall be available:

- item definition (see [WP-09-01]);
- impact categories from impact rating (see [WP-08-04]);
- threat scenarios (see [WP-08-03]);
- identified attack paths (see [WP-08-05]); and
- corresponding risk values (see [WP-08-07]).

DRAFT

8.9.1.2 Further Supporting Information

The following information can be considered:

- previous risk treatment decisions of the item or component, or of similar items or components;
- attack feasibility rating (see [WP-08-06]).

8.9.2 Requirements and Recommendations

[RQ-08-12] A risk treatment option shall be determined, considering impact categories, attack paths and the results from risk determination.

NOTE 1: Options for treating risk can involve:

a) avoiding the risk by removing the risk sources, or deciding not to start or continue with the activity that gives rise to the risk;

b) reducing the risk;

c) sharing or transferring the risk (e.g., through contracts, buying insurance); and/or

d) accepting or retaining the risk.

NOTE 2: Risk treatment options are not mutually exclusive or appropriate in all circumstances.

[PM-08-01] For threat scenarios of risk value 1, determined from an analysis in accordance with 8.8, compliance with 9.5, and with Clauses 10 and 11 of this document may be omitted.

NOTE 3: These threat scenarios can have consequences with regards to cybersecurity and if so, the corresponding risks are treated, albeit potentially with less rigor than defined in this document.

NOTE 4: The sufficiency of the treatment of such risks can be argued based on a rationale defined in the cybersecurity case, for example assurance based on compliance with a quality management standard, such as IATF 16949[16] in conjunction with ISO 9001[3], in combination with additional measures, such as cybersecurity awareness assurance and cybersecurity training of quality personnel and the existence of cybersecurity specific aspects or measures defined in the corporate quality management system.

NOTE 5: For risk acceptance and risk transfer, the corresponding rationales are recorded as cybersecurity claims and subject to monitoring and vulnerability management in accordance with Clause 7.

8.9.3 Work Products

[WP-08-08] Risk treatment decision per threat scenario, resulting from [RQ-08-12].

9. CONCEPT PHASE

9.1 General

In this clause, the item and its environment are defined (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). For this purpose, cybersecurity risks of the item are assessed. This is done by using the methods of Clause 8 (for an informational overview see Figure G.1). Cybersecurity requirements applied to an item and assumptions made about the operational environment can reduce the risk of an item. Cybersecurity goals are identified as top-level cybersecurity requirements. Cybersecurity claims are used to explain why the risk treatment is deemed adequate.

From the cybersecurity goals, the cybersecurity concept is derived (see 9.5). The cybersecurity concept describes the realization of the cybersecurity goals in terms of cybersecurity requirements that are allocated to the components of the preliminary architectural design or to the operational environment. Furthermore, the cybersecurity concept provides rationales for the achievement of the cybersecurity goals through the cybersecurity requirements.

DRAFT

9.2 Objectives

The objectives of this clause are to:

a) define the item, the operational environment and its interaction with other items in the context of cybersecurity;

b) specify cybersecurity goals and cybersecurity claims according to risk assessment results; and

c) specify cybersecurity requirements and allocate them to the item and/or the operational environment.

9.3 Item Definition

9.3.1 Inputs

9.3.1.1 Prerequisites

None.

9.3.1.2 Further Supporting Information

Existing information regarding the item and the operational environment can be considered.

EXAMPLE:

- in-vehicle E/E system architecture including in-vehicle network;
- networks external to the vehicle;
- functions of the item; and/or
- reference model(s) and the documentation of earlier developments/lessons learned.

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 environment. The description of the item boundary can include interfaces with other item and components internal and/or external to the vehicle.

b) function; and

NOTE 2: The description of the item function can include the intended behavior independent from implementation and architecture. The function of the item includes the operational vehicle functionality that is realized by the item, and all other functions that are intended during the lifecycle phases of the item, such as: product development (testing), production, operations and maintenance, and decommissioning.

c) preliminary architecture.

NOTE 3: The description of preliminary architecture can include:

- internal components and their connections in the item;
- data flow with other objects outside of the item;
- physical aspects; and
- logical aspects.

DRAFT

[RQ-09-02] The relevant information about the operational environment of the item with regard to cybersecurity shall be described.

NOTE 4: The description of the operational environment of the item can include the aspects that allow the identification and analysis of relevant threat scenarios and attack paths.

NOTE 5: The item definition and in particular the item boundary for the processes as described in this document can differ from the scope and item boundary of the item definition from another process such as functional safety in accordance with ISO 26262[1].

[RQ-09-03] Constraints and compliance needs shall be identified.

EXAMPLE 1: This can include:

- functional constraints;
- technical constraints; and/or
- standards.

[RQ-09-04] Assumptions about the item and the operational environment of the item shall be identified.

NOTE 6: Some attacks might not be feasible under the assumptions on the operational environment.

NOTE 7: If the item is being reused after its development was completed, the assumptions of [RQ-09-04] for the original item are validated with respect to the operational environment for the re-use (see 6.4.4).

NOTE 8: Development of a component out of context can include a definition of an assumed (generic) item and description of the functions of the component within the item.

EXAMPLE 2: Assumptions on physical aspects can include:

- the item will be placed in an anti-tamper enclosure.

EXAMPLE 3: Assumptions on connectivity aspects can include:

- every PKI certificate authority that the item relies on are appropriately managed.

9.3.3 Work Products

[WP-09-01] Item definition, resulting from [RQ-09-01] to [RQ-09-04].

9.4 Cybersecurity Goals

9.4.1 Inputs

9.4.1.1 Prerequisites

The following information shall be available:

- item definition (see [WP-09-01]).

9.4.1.2 Further Supporting Information

None.

DRAFT

9.4.2 Requirements and Recommendations

[RQ-09-05] In order to identify cybersecurity goals, an analysis of the item shall be performed that involves:

a) asset identification in accordance with 8.3;

NOTE 1: The list of assets with cybersecurity properties (as part of the result of asset identification) can be consolidated for easier reference by the cybersecurity requirements.

b) threat scenario identification in accordance with 8.4;

c) impact rating in accordance with 8.5;

d) attack path analysis in accordance with 8.6;

NOTE 2: In the concept phase information about potential attacks can vary in granularity and depth, from an abstract classification in terms of remote, adjacent, local, and/or physical attacks (i.e., the attack vector according to CVSS[25]) to a detailed description of distinct attack actions (e.g., an attack path). This can lead to a corresponding level of granularity for the subsequent risk determination and for the potential cybersecurity goals.

NOTE 3: Assumptions considering the attack path analysis enable the exclusion of attack paths that are infeasible and clarify the rationale for the determined attack feasibility. If the assumptions are later shown to be is false, the excluded attack paths are retroactively identified and analyzed.

NOTE 4: To estimate attack feasibility in the concept phase, the attack feasibility rating method described in I.5 can be used.

e) attack feasibility rating in accordance with 0; and

f) risk determination in accordance with 8.8.

[RQ-09-06] For the identified threat scenarios and their associated risks, a risk treatment decision shall be performed in accordance with 8.9.

NOTE 5: A risk can be reduced by a cybersecurity requirement allocated to the item or to the operational environment of the item.

NOTE 6: If the risk is addressed by assumptions on the operational environment, the cybersecurity claim explains why this is adequate.

NOTE 7: Avoiding a risk by removing the risk source means changing the item and subsequently to a re-iteration of the concept phase process starting at item definition.

[RQ-09-07] If the risk treatment decision for a threat scenario involves reducing the risk, then one or more corresponding cybersecurity goals shall be specified.

NOTE 8: The statement of the cybersecurity goal can include the protection of cybersecurity properties of assets whose compromise can lead to the associated damage scenario.

NOTE 9: If applicable, a CAL can be derived for cybersecurity goals (see Annex E).

NOTE 10: Cybersecurity goals can be defined for operations and maintenance, and decommissioning. This includes the cybersecurity implications of service and repair in the design and development of their products.

NOTE 11: Cybersecurity goals can be combined.

DRAFT

[RQ-09-08] Cybersecurity claims shall be stated for the following cases:

a) an assumption on the operational environment leads to a reduction of the risk of a threat scenario so that the risk becomes acceptable; or

b) the risk treatment involves sharing or transferring the risk.

NOTE 12: Cybersecurity claims are subject to monitoring.

[RQ-09-09] The activities to specify cybersecurity goals and cybersecurity claims shall be verified to:

a) confirm consistency of the analysis of [RQ-09-05];

b) confirm consistency of the risk treatment decisions [RQ-09-06];

c) confirm consistency and completeness of the cybersecurity goals of [RQ-09-07] with respect to the threat scenarios; and

d) consistency between different cybersecurity goals.

9.4.3 Work Products

[WP-09-02] Threat analysis and risk assessment, resulting from [RQ-09-05].

[WP-09-03] Risk treatment decisions, resulting from [RQ-09-06].

[WP-09-04] Cybersecurity goals, resulting from [RQ-09-07].

[WP-09-05] Cybersecurity claims, resulting from [RQ-09-08].

[WP-09-06] Verification report, resulting from [RQ-09-09].

9.5 Cybersecurity Concept

9.5.1 Inputs

9.5.1.1 Prerequisites

The following information shall be available:

- item definition [WP-09-04](see [WP-09-01]); and
- cybersecurity goals (see [WP-09-04]).

9.5.1.2 Further Supporting Information

The following information can be considered:

- threat analysis and risk assessment (see [WP-09-02]); and
- cybersecurity claims (see [WP-09-05]).

DRAFT

9.5.2 Requirements and Recommendations

[RQ-09-10] Cybersecurity requirements shall be specified for the cybersecurity goals, including a rationale for the achievement of the cybersecurity goals.

NOTE 1: Cybersecurity requirements can specify which threat scenarios are controlled.

NOTE 2: If available, additional information about potential attack paths that can lead to a violation of the cybersecurity goals, can be considered for the derivation of the cybersecurity requirements.

NOTE 3: The type of asset protection can be specified as an intermediate step, which supports traceability between cybersecurity goals and cybersecurity requirements and can identify and resolve potential conflicts.

EXAMPLE 1: Types of asset protection include combinations of:

- prevention, reduction, detection, correction, or monitoring of losses or compromise; and/or
- restoring or recovery from damage.

NOTE 4: The cybersecurity requirements can depend on or include update capabilities of the item.

[RQ-09-11] The cybersecurity requirements shall be allocated to one or more components of the item or to the operational environment.

[RQ-09-12] The cybersecurity requirements and their allocation shall be verified to confirm:

a) consistency with the cybersecurity goals;

b) completeness with respect to the cybersecurity goals; and

c) consistency and compatibility with the functionality of the item.

EXAMPLE 2: A potential compatibility issue can be: performance of the item affected by cybersecurity requirements.

NOTE 5: If applicable, conformance with the cybersecurity goals includes effectiveness of the mitigation or capabilities for handling of cyber security events (e.g., over the air update).

9.5.3 Work Products

[WP-09-07] Cybersecurity concept, resulting from [RQ-09-10] and [RQ-09-11].

[WP-09-08] Verification report of cybersecurity concept, resulting from [RQ-09-12].

10. PRODUCT DEVELOPMENT

10.1 General

Firstly, this clause describes the specification of the cybersecurity requirements and of the architectural design (see 10.4.1), which corresponds to the left leg of the V-model (see Figure 10).

Secondly, this clause describes integration and verification activities (see 10.4.2), which corresponds to the right leg of the V-model.

These cybersecurity activities are applied to the different levels of abstraction or architecture; e.g., in development of a system, hardware component, or software component. This corresponds to incremental refinement of the cybersecurity specification (i.e., the cybersecurity requirements and the architectural design) and incremental integration of components and items into “higher levels of architectural abstraction” (hereinafter, referred to as just "higher level"), and finally into a target vehicle.

DRAFT

Given software development includes additional specification, design, implementation and verification steps, requirements specific to cybersecurity engineering activities for software development are provided in 0). These requirements can also apply when components are created using a process similar to software development, for example creation of a hardware component using a hardware description language.

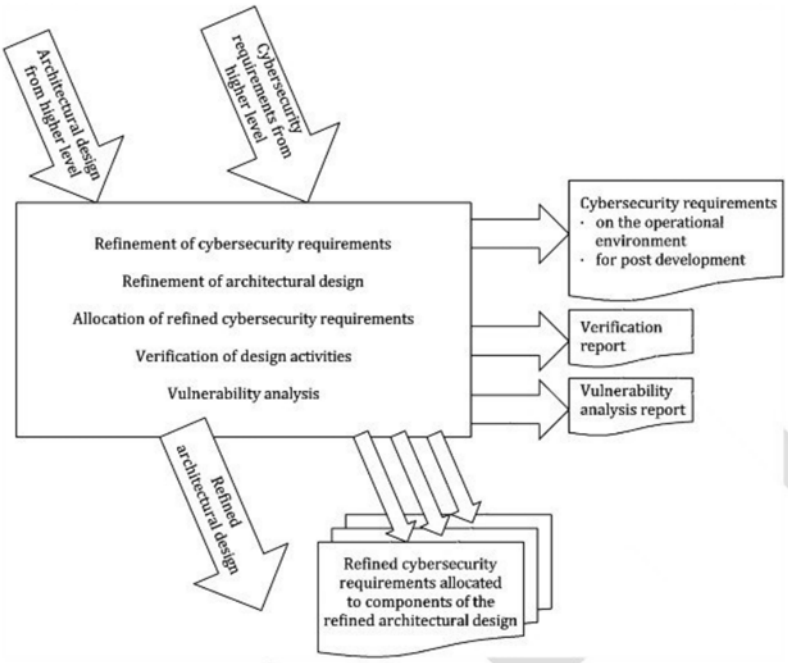
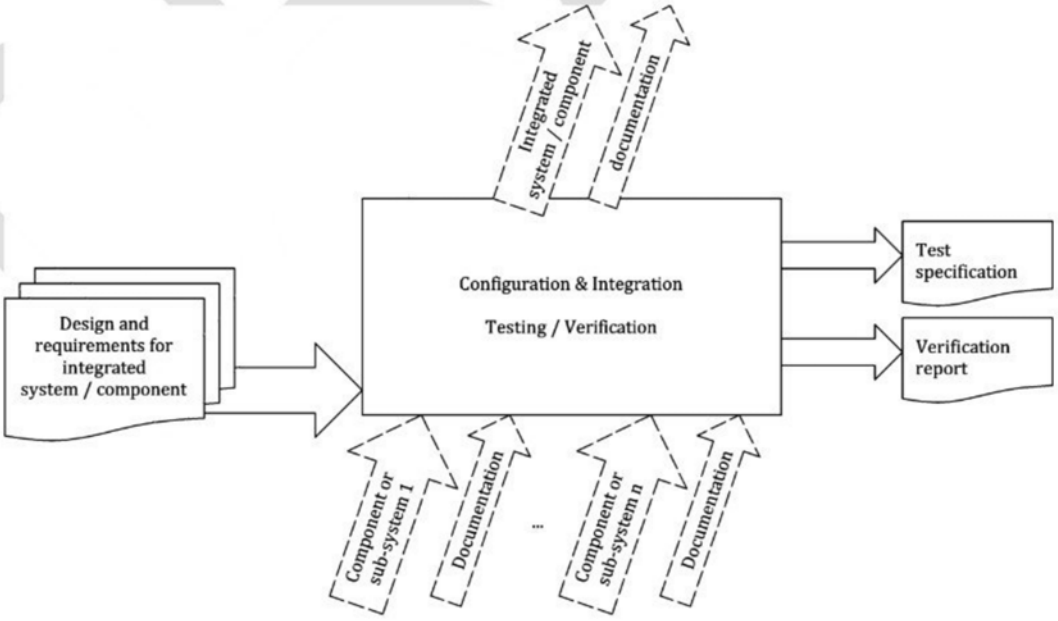


Figure 8 - Refinement of cybersecurity requirements and architectural design

The cybersecurity engineering activities regarding refinement of cybersecurity requirements and architectural design, as illustrated in Figure 8, include:

- understanding and complying with the cybersecurity requirements from a higher level;
- preventing the introduction of new vulnerabilities; and
- identifying and managing known vulnerabilities, if applicable.



NOTE: Dashed shapes refer to work products not specified in this document.

Figure 9 - Integration and verification

The cybersecurity engineering activities regarding integration and verification (see Figure 9) include:

- configuration and integration of the system or component for secure operation (e.g., correct configuration of cybersecurity functionality);
- verification of the fulfilment of the cybersecurity requirements allocated to the system or component;
- verification that identified vulnerabilities have been successfully managed; and
- searching for previously unidentified vulnerabilities and managing these.

Figure 10 describes the workflow that correspond with this clause. It addresses an item for which the cybersecurity plan has specified a work breakdown structure of one or more systems, and a system composed of hardware and software components.

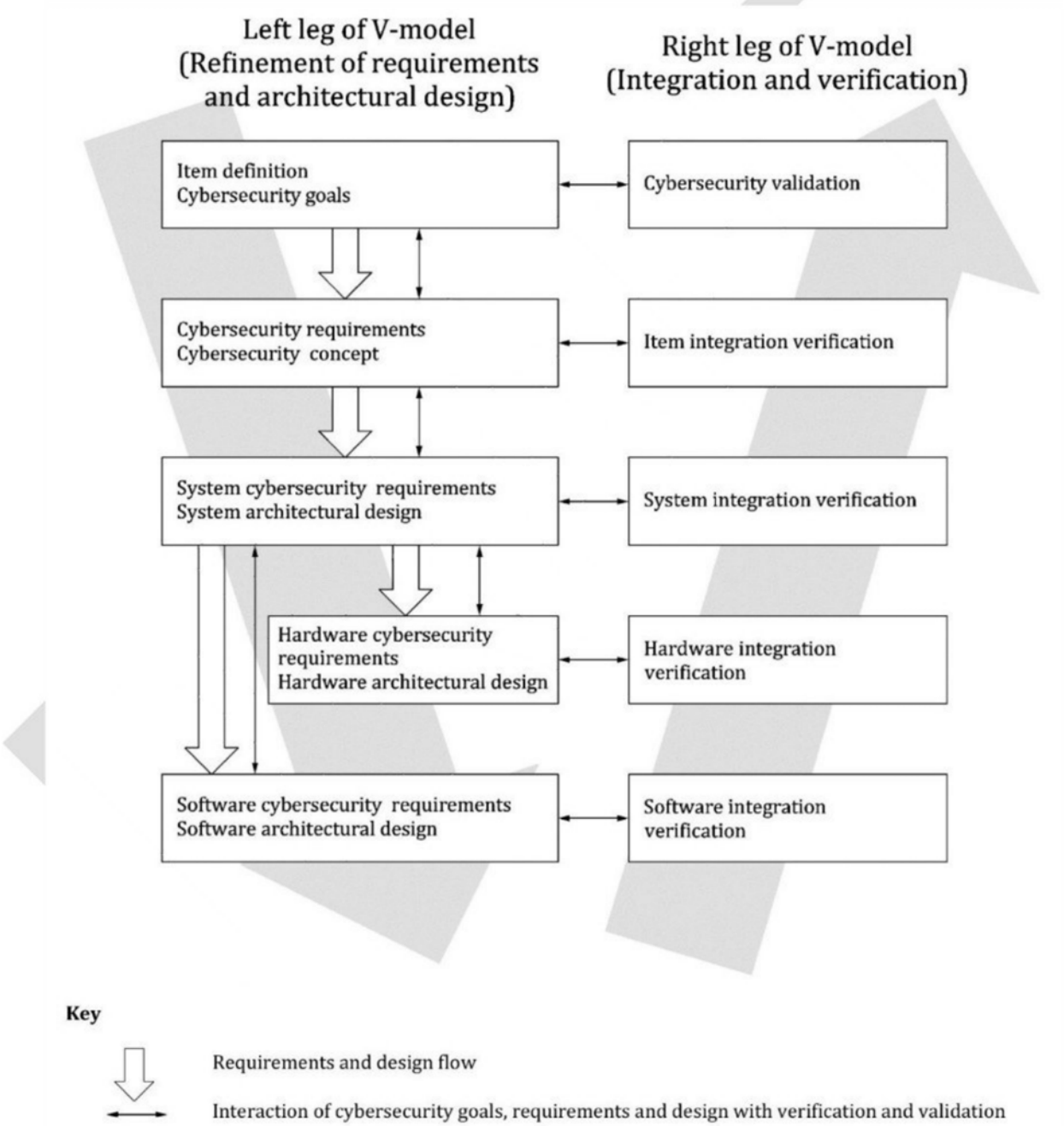


Figure 10 - Example workflow for product development

Validation examines whether the cybersecurity goals are adequate and are achieved and is described in Clause 11.

Verification examines:

a) whether the implementation and realization fulfil the requirements; and

b) whether the design and analysis activities are performed correctly, including their completeness and consistency.

NOTE: See Annex F for further guidance.

Development approaches or methods that differ from the V-model; e.g., agile software development, can be applied if the achievement of the objectives of this clause is demonstrated. In such situations, tailoring can be applied (see 6.4.3).

10.2 Objectives

The objectives of this clause are to:

a) specify refined cybersecurity requirements and architectural design;

NOTE: This can include the specification of cybersecurity related components, including software units, not present in the initial architectural design.

b) verify that the refined cybersecurity requirements and architectural design comply with the cybersecurity requirements from higher level of abstraction;

c) identify vulnerabilities in the design and manage accordingly; and

d) provide evidence that the component complies with the cybersecurity specification and does not contain undesired functionality regarding cybersecurity.

10.3 Inputs

10.3.1 Prerequisites

The following information shall be available:

- cybersecurity specification from a higher level.

NOTE 1: Cybersecurity specification includes cybersecurity requirements and architectural design.

EXAMPLE: Cybersecurity concept for top-level system development of an item, system level cybersecurity specification for hardware and software design.

NOTE 2: Architectural design includes interface specifications between components.

NOTE 3: Architectural design from higher level includes information of the operational environment of the component under development.

NOTE 4: For top-level system development of an item, architectural design can be substituted by corresponding architectural or interface information of the item definition (e.g., the preliminary architecture described in [RQ-09-01]).

DRAFT

10.3.2 Further Supporting Information

The following information can be considered:

- initial architectural design;
- cybersecurity architecture;

NOTE 1: Cybersecurity architectures are not defined in this document.

- already established cybersecurity solutions;

EXAMPLE 1: Prescribed cybersecurity algorithms and components.

- results of vulnerability analysis from higher level ([WP-10-04]);

NOTE 2: For top-level system development of an item, the results of attack path analysis and attack feasibility rating (see [RQ-09-05]) can be applied.

- known weaknesses and vulnerabilities from reused subsystems, hardware and software components, operational environment, and, if applicable, target environment;
- guidelines and/or rules for secure design and implementation; and

EXAMPLE 2: Secure coding guidelines.

- organizational rules for the application of development and verification methods, and their extent, depth and rigor (see [RQ-05-02]).

EXAMPLE 3: Rules based on CAL (see Annex E).

10.4 Requirements and Recommendations

10.4.1 Refinement of Cybersecurity Requirements and Architectural Design

[RC-10-01] Cybersecurity controls should be selected based on the cybersecurity requirements allocated from higher level and on the architectural design from higher level.

EXAMPLE 1: For system or hardware development: use of a separate microcontroller with an embedded hardware trust anchor for secure key store functionalities, and isolation of the trust anchor regarding non-secure external connections.

EXAMPLE 2: Use of catalogues and standard solutions that are traceable to national, international or industry standards.

NOTE 1: Cybersecurity controls are effective if their implementation achieves or supports the fulfilment of the cybersecurity requirements from higher level allocated to the component under development.

[RQ-10-01] Cybersecurity requirements shall be refined based on:

a) cybersecurity requirements allocated from higher level;

NOTE 2: This can include cybersecurity requirements allocated to the component under development and cybersecurity requirements allocated to its operational environment.

b) architectural design from higher level; and

c) cybersecurity controls from [RC-10-01], if applicable.

DRAFT

NOTE 3: This can include the cybersecurity requirements refined according to the refined architectural design of [RQ-10-02].

NOTE 4: In order to ensure proper functioning of a cybersecurity control, additional requirements can be provided with regard to secure and appropriate use of the cybersecurity controls.

EXAMPLE 3: Anomaly detection with respect to the functioning of the cybersecurity control.

EXAMPLE 4: A system with secure event logging mechanism imposes implementation of a secure communication with external systems for log data collection.

NOTE 5: Technical realizations for cybersecurity requirements from higher level imposed from external sources can also be included in the refined cybersecurity requirements.

[RQ-10-02] Architectural design shall be refined for the development level based on:

a) the initial architectural design, if applicable;

b) the cybersecurity controls from [RC-10-01], if applicable;

c) the refined cybersecurity requirements;

d) the higher level architectural design; and

e) the operational environment.

EXAMPLE 5: Interface specifications between hardware and software.

NOTE 6: The architectural design can include the static design aspects and the dynamic design aspects.

NOTE 7: Information for correct integration and initialization of cybersecurity controls can be included in the architectural design.

[RC-10-02] The refined architectural design should apply architectural design principles to avoid or minimize the introduction of weaknesses.

NOTE 8: Examples of design principles for architectural design for cybersecurity are given in NIST SP 800-1600, appendix F.1.

NOTE 9: Design principles can be achieved by applying and enforcing design and modelling guidelines.

[RQ-10-03] The refined cybersecurity requirements shall be allocated to components of the refined architectural design.

[RQ-10-04] Interfaces between components of the refined architectural design related to the fulfillment of the refined cybersecurity requirements shall be identified and described, and include the following:

a) purposes and usage; and

b) parameters.

NOTE 10: Parameters are explicit inputs to and outputs from an interface that controls the behavior of interfaced component.

EXAMPLE 6: Allowed range of data in the interface.

EXAMPLE 7: The interface between hardware and software is defined or refined in order to allow for the correct usage of cybersecurity control.

NOTE 11: Interfaces are a potential entry point for cybersecurity attacks. The interface specification can serve as an input to vulnerability analysis of [RQ-10-09].

DRAFT

[RQ-10-05] During the refinement of cybersecurity requirements, the cybersecurity implications of post-development phases shall be considered.

[RQ-10-06] If specific procedures are required to ensure cybersecurity in post-development phases, these cybersecurity requirements shall be specified and allocated to the relevant entities of the operational environment.

EXAMPLE 8: Table 1 provides example requirements and procedures to ensure cybersecurity in post-development phases including their allocation.

Table 1 - Example cybersecurity requirements for post-development

Requirement	During	Allocated to
secured management of the key store	production	system production
	maintenance	service and maintenance facilities/instructions
deactivation of debug interfaces	production	hardware production
deactivation of development functions	production	deployment finalization for software
procedures to delete personally identifiable information	operations	user manual

[RQ-10-07] The refined cybersecurity requirements shall be verified to ensure:

a) completeness, correctness, and adequacy with the cybersecurity requirements from higher level; and

b) consistency with the architectural design from higher level.

[RQ-10-08] The refined architectural design shall be verified to ensure:

a) compliance with the refined cybersecurity requirements;

b) compliance with the architectural design from higher level; and

c) for software development: compatibility with the target environment.

NOTE 12: The target environment includes architectural constraints.

EXAMPLE 9: Verification methods can include:

- review;
- analysis;
- simulation; and
- prototyping.

NOTE 13: If CAL is used, then Annex E (Table E.3) provides methods of verification and criteria for applicability.

[RQ-10-09] Vulnerability analysis in accordance with 7.5 shall be performed to identify vulnerabilities associated with the refined architectural design and refined cybersecurity requirements, including the interactions between components that could impair the fulfilment of the refined cybersecurity requirements.

[RQ-10-10] Identified vulnerabilities shall be managed according to 7.6.

NOTE 14: Vulnerabilities can be handled with additional cybersecurity requirements and components in the architectural design.

DRAFT

EXAMPLE 10: Treatment of vulnerabilities in development can include:

- isolation of functions;
- use of encryption;
- secure storage; and/or
- anonymization of personal information.

[RQ-10-11] The vulnerability analysis of [RQ-10-09] shall be verified.

10.4.2 Integration and Verification

[RQ-10-12] Verification activities shall be performed to confirm that the implementation of the design and the integration of the components are compliant with:

a) the refined cybersecurity requirements (result of [RC-10-01] to [RQ-10-01]); and

b) the refined architectural design (result of [RQ-10-02] to [RQ-10-04]).

NOTE 1: This can include the vehicle integration and verification at system level.

NOTE 2: The results of the hardware and software verification activities can be considered at system level.

NOTE 3: Verification activities can include regression testing for updates and changes and re-testing for patching of a discovered vulnerability.

NOTE 4: Verification methods as part of standard engineering per a quality management system can be used as a baseline. Additional verification types or activities specific for cybersecurity can be used.

EXAMPLE 1: Methods for verification can include:

- requirements-based test;
- interface test;
- resource usage evaluation;
- verification of the control flow and data flow; and
- static analysis; for software: static code analysis.

NOTE 5: If CAL is used, then Annex E (Table E.4) provides methods of verification and criteria for applicability.

[RQ-10-13] The integration and verification specification for the verification activities of [RQ-10-12] shall be defined considering:

a) the refined architectural design;

NOTE 6: This includes assumptions on reused components.

EXAMPLE 2: The hardware-software interface can require specific consideration.

b) the refined cybersecurity requirements;

c) the vulnerability analysis of [RQ-10-09] and the results of vulnerability management of [RQ-10-10];

d) configurations and/or calibration processes intended for production, if applicable;

DRAFT

e) dependencies that are relevant for integration; and

f) sufficient resources to support the functionality specified in refined cybersecurity requirements.

NOTE 7: The verification specification initiated during system development can be further refined during hardware and software development.

[RQ-10-14] If testing is used for the verification activities of [RQ-10-12], test cases shall be specified that include pass/fail criteria.

EXAMPLE 3: Methods of test case specification can include:

- analysis of requirements;
- generation and analysis of equivalence classes;
- boundary values analysis; and/or
- error guessing based on knowledge or experience.

NOTE 8: If CAL is used, then Annex E (Table E.5) provides methods of test case specification and criteria for applicability.

[RQ-10-15] Test coverage by test cases shall be determined for the completeness of testing activities using a defined test coverage metric relevant for cybersecurity.

NOTE 9: Test coverage can be determined by the use of appropriate software tools.

NOTE 10: A target value below full test coverage can be sufficient if a rationale is provided.

NOTE 11: Test coverage is only useful for determining whether all requirements were transcribed into implementation and realization; e.g., software code in the case of software development, and whether the implementation matches the requirements.

NOTE 12: Some weaknesses go beyond the fact that all possible control flows are evaluated. For example, improper sequence of operations, insufficient authentication. As a consequence, a review of the coverage of common weaknesses by the tests can complement this activity.

NOTE 13: Analysis of test coverage can reveal shortcomings in requirements-based test cases, inadequacies in requirements, dead code, deactivated code or unintended functionality.

EXAMPLE 4: Structural coverage metrics at the software unit level can include:

- statement coverage; and/or
- branch coverage.

NOTE 14: For software development, if instrumented code is used to determine the degree of structural coverage, it can be necessary to provide evidence that the instrumentation has no effect on the test results. This can be done by repeating representative test cases with non-instrumented code.

EXAMPLE 5: Structural coverage at the software architectural level can include:

- function coverage; and/or
- call coverage.

NOTE 15: If CAL is used, then Annex E (Table E.6 and Table E.7) provide methods and criteria for applicability.

DRAFT

[RQ-10-16] A verification that components do not contain any unspecified functionality shall be performed.

NOTE 16: Unspecified functionality is not explicitly described in the architecture design specification but is implemented for any reason.

EXAMPLE 6: For software development, code used for debugging or instrumentation.

NOTE 17: If the unspecified function is deactivated, this can be an acceptable control.

NOTE 18: If the unspecified function is encapsulated in a separate zone outside of the trust boundary, this can be an acceptable control.

[RQ-10-17] If testing is used for the verification activities of [RQ-10-12], the test environment shall be suitable for achieving the test objectives.

EXAMPLE 7: Test environments can include:

- hardware-in-the-loop;
- electronic control unit network environments; and/or
- vehicles.

NOTE 19: In software development, the target environment can be considered. Depending on the scope of the tests and the hierarchical level of integration, the appropriate test environments for the execution of the software components can be used. Such test environments can be the target processor for final integration, a processor emulator or a development system for the previous integration steps.

NOTE 20: In software development, if the integration testing is not carried out in the target environment, the differences between the test environment and the target environment can be analyzed in order to specify additional tests in the target environment during the subsequent test phases.

NOTE 21: In software development, differences between the test environment and the target environment can arise in the source or object code, for example, due to different bit widths of data words and address words of the processors.

[RC-10-03] Component testing should be performed to search for unidentified vulnerabilities.

EXAMPLE 8: Test methods to search for vulnerabilities can include:

- penetration testing;
- vulnerability scanning; and/or
- fuzz testing.

NOTE 22: If CAL is used, then Annex E (Table E.8) provides test methods and criteria for applicability.

NOTE 23: In software development, different weaknesses can exist in the test environment and the target environment, and their triggering into vulnerabilities depends on the functionality or code that executes on them. Thus, the studied differences between the test environment and the target environment encompass also existing weaknesses and how they can or cannot be triggered by the functionality or code that executes on them.

[RQ-10-18] If testing of [RC-10-03] identifies weaknesses and/or vulnerabilities from, these shall be managed according to 7.6.

EXAMPLE 9: An additional cybersecurity control is implemented to achieve a cybersecurity requirement, or a cybersecurity requirement is reworked and subsequently complied with.

DRAFT

10.4.3 Specific Requirements for Software Development

[RQ-10-19] When selecting a design, modelling or programming language the following shall be considered:

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; and

d) support for the use of secure design and coding techniques.

EXAMPLE 1: Community or provider support for the language itself.

[RQ-10-20] Criteria for suitable modelling, design or programming languages for cybersecurity (see [RQ-10-19]) that are not sufficiently addressed by the language itself shall be covered by coding guidelines, or by the development environment.

EXAMPLE 2: Use of MISRA C:2012 3rd edition, 1st Revision or CERT C for secure coding in the "C" programming language.

EXAMPLE 3: Criteria for suitable design, modelling and programming languages for cybersecurity can include:

- use of language subsets;
- enforcement of strong typing; and/or
- use of defensive implementation techniques.

EXAMPLE 4: User input (e.g., input field, data import, APIs) is validated and sanitized.

NOTE 1: If CAL is used, then Annex E (Table E.9) provides topics and criteria for applicability.

[RC-10-04] Design principles for software unit design and implementation at the source code level should be applied to achieve the following characteristics:

a) correct order of execution of subprograms and functions within the software units, based on the software architectural design;

b) consistency of the interfaces between the software units;

c) correctness of data flow and control flow between and within the software units;

d) low complexity;

e) readability and comprehensibility;

f) robustness;

EXAMPLE 5: Methods to prevent use of tainted data.

g) suitability for software modification (unless ease of software modification runs contrary to the cybersecurity requirements); and

h) verifiability.

NOTE 2: These characteristics can be achieved by applying and enforcing coding guidelines.

NOTE 3: Coding guidelines can cover aspects such as safety and overall code quality as well as the required cybersecurity properties.

DRAFT

[RQ-10-21] The software unit design and the implemented software unit shall be verified to provide evidence for compliance with the coding guidelines of [RQ-10-20], if applicable.

10.5 Work Products

[WP-10-01] Refined cybersecurity specification, resulting from [RC-10-01] to [RQ-10-04].

[WP-10-02] Cybersecurity requirements for post-development, resulting from 0 and [RQ-10-06].

[WP-10-03] Verification report for the refined cybersecurity specification, resulting from [RQ-10-07] and [RQ-10-08].

[WP-10-04] Vulnerability analysis report, resulting from [RQ-10-09] to [RQ-10-11].

[WP-10-05] Integration and verification specification, resulting from [RQ-10-13].

[WP-10-06] Integration and verification reports, resulting from the requirements of [RQ-10-12] and [RQ-10-14] to [RQ-10-18].

NOTE: This work product includes results from 0 in software development.

[WP-10-07] Documentation of the modelling, design or programming languages and coding guidelines, if applicable, resulting from [RQ-10-19] to [RQ-10-20].

[WP-10-08] Software unit design and software unit implementation, if applicable, resulting from [RC-10-04].

11. CYBERSECURITY VALIDATION

11.1 General

This clause describes activities for cybersecurity validation of the item at the vehicle level. These activities are performed after the integration of its components is completed. The item is considered in its operational environment at the vehicle level and with the configuration intended for production and operational vehicle use (i.e., all end-of-line test features disabled).

EXAMPLE: Integration of the item into a partially assembled vehicle.

11.2 Objectives

The objectives of this clause are:

a) to validate the cybersecurity goals and cybersecurity claims;

b) to confirm that the item satisfies the cybersecurity goals; and

c) to confirm that the residual risks of the item are acceptable.

11.3 Inputs

11.3.1 Prerequisites

The following information shall be available:

- item definition (see [WP-09-01]);
- cybersecurity claims, if applicable (see [WP-09-04]);
- cybersecurity goals (see [WP-09-05]); and
- work products from product development (see 10.5).

DRAFT

11.3.2 Further Supporting Information

None.

11.4 Requirements and Recommendations

[RQ-11-01] Validation activities shall be performed to confirm:

a) the adequacy of the cybersecurity goals;

b) the completeness, consistency, correctness and adequacy of:

   i. the item and

   ii. the cybersecurity requirements on the operational environment

   to achieve the cybersecurity goals of the item; and

c) if applicable, the validity of the cybersecurity claims.

[RQ-11-02] A validation specification for the validation activities of [RQ-11-01] shall be defined considering the configurations intended for production.

[RC-11-01] Penetration testing should be performed to validate the cybersecurity goals as part of the validation activities of [RQ-11-01].

NOTE: The extent of penetration testing can be defined based on risk considerations.

[RQ-11-03] Vulnerabilities revealed during the validation activities of [RQ-11-01] shall be managed in accordance with 7.6.

[PM-11-01] If the residual risk is unacceptable, activities from 10 or, 9.4 and 9.5 may be re-performed.

[RQ-11-04] The validation of the item shall confirm that all the risks identified during the concept and product development phases are accepted or have been treated such that they are accepted, based on a rationale.

11.5 Work Products

[WP-11-01] Validation specification, resulting from [RQ-11-02].

[WP-11-02] Validation report, resulting from [RQ-11-01] and [RC-11-01] to [RQ-11-04].

12. PRODUCTION

12.1 General

Production covers the fabrication, assembly and/or configuration of an item or component. 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 the item or component cannot be exploited during production and additional vulnerabilities cannot be added during production.

12.2 Objectives

The objectives of this clause are to:

a) apply the cybersecurity requirements for post-development to the item or component; and

b) prevent the introduction of vulnerabilities in the item or component during production.

DRAFT

12.3 Inputs

12.3.1 Prerequisites

The following information shall be available:

- release for post-development report (see [WP-06-04]); and
- cybersecurity requirements for post-development (see [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 and includes:

a) the cybersecurity requirements for post-development allocated to production;

b) an outline of the necessary installation procedures to achieve a);

NOTE 1: To manufacture an item or component and install the hardware and software, the production process can use privileged access. Such access can be used to introduce vulnerabilities in the item or component if used in an unauthorized manner after production.

EXAMPLE 1: Removal of production access once the item or component is produced.

c) description of protection measures for components to prevent unauthorized alteration; and

NOTE 2: The protection measures can cover physical access and logical access.

EXAMPLE 2: Physical measure that prevents physical access to production servers holding software.

EXAMPLE 3: Logical measure that applies cryptographic techniques and/or access controls.

EXAMPLE 4: Protected components can include:

- microcontrollers and processors;
- control units;
- systems;
- low-level programs;
- bootloaders;
- application software; and/or
- cryptographic material.

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

NOTE 3: Methods can include verification, validation, inspection or configuration and calibration checks.

NOTE 4: Methods can be conducted at the component level to give assurance, and to reduce testing at the integrated item level.

NOTE 5: The production control plan can be included as part of an overall production plan.

DRAFT

12.5 Work Products

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

13. OPERATIONS AND MAINTENANCE

13.1 General

This clause describes cybersecurity incident response and updates.

Cybersecurity incident response occurs when an organization responds to a cybersecurity event. If a cybersecurity event does not rise to the level of a cybersecurity incident, it is managed according to 7.6.

Updates are changes made to the hardware or software of an item or component during post-development and can include additional data and information, such as technical specifications and integration or user manuals. Organizations can issue updates for various reasons; for example, cybersecurity vulnerabilities, functional improvements or safety issues.

Modifications of items or components that are in the concept, development or production phases can be covered by change management (see 5.4.6) instead of this clause.

13.2 Objectives

The objectives of this clause are to:

a) handle cybersecurity events that become a cybersecurity incident; and

b) preserve cybersecurity during and after updates to items or components post-production.

13.3 Cybersecurity Incident Response

13.3.1 Inputs

13.3.1.1 Prerequisites

The following information shall be available:

- cybersecurity event assessment (see [WP-07-03]).

13.3.1.2 Further Supporting Information

The following information can be considered:

- cybersecurity information related to the cybersecurity event (see 7.4).

13.3.2 Requirements and Recommendations

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

a) remediation actions for the cybersecurity incident;

NOTE 1: Remediation actions are determined under vulnerability management in 7.6.

b) a communication plan;

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

NOTE 3: A communication plan can include identification of internal and external communication partners (e.g., development, researchers, the public, authorities) and communication packages for various 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 process, communications, purchasing, legal); and/or
- decision authority.

d) a method for determining progress; and

EXAMPLE 1: Procedures to determine the progress criteria during the remediation actions can include:

- percentage of affected items or components that are covered within a defined timeframe; and/or
- percentage of items or components affected by remediation actions.

e) criteria for closure and actions upon closure.

[RQ-13-02] The status of cybersecurity incident remediation shall be tracked.

[RQ-13-03] Relevant information for a cybersecurity incident shall be associated with the cybersecurity incident.

EXAMPLE 2: Relevant information can come from various sources and can include:

- assets affected (e.g., part number, system description, number of assets affected);
- related incidents and vulnerabilities;
- forensic data such as logging data; crash sensor data; and/or
- end-user complaints.

13.3.3 Work Products

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

[WP-13-02] Cybersecurity incident response information, resulting from [RQ-13-03].

13.4 Updates

13.4.1 Inputs

13.4.1.1 Prerequisites

The following information shall be available:

- cybersecurity incident response plan (see [WP-13-01]), if the update is issued because of cybersecurity incident response; and
- release for post-development report (see [WP-06-04]).

13.4.1.2 Further Supporting Information

The following information can be considered:

- cybersecurity requirements for post-development (see [WP-10-02]).

DRAFT

13.4.2 Requirements and Recommendations

[RQ-13-04] Updates and related capabilities shall be developed in accordance with Clauses 9 and 10.

NOTE 1: Capabilities can include the update capability within the vehicle.

NOTE 2: Cybersecurity of updates and capabilities can be achieved by considering cybersecurity properties (confidentiality, integrity and availability) and risk-based approaches.

[RQ-13-05] Cybersecurity implications of recovery options for updates shall be considered in accordance with 0.

NOTE 3: Recovery options can negatively affect the cybersecurity of the item or component.

EXAMPLE 1: Recovery options can include:

- rollback of the update to restore the item or component to its previous state; and/or
- replacement/repair of the item or component.

[RQ-13-06] A procedure shall be created to communicate to customers when an organization decides to end cybersecurity support for an item or component.

NOTE 4: These communications can be handled under contract requirements.

EXAMPLE 2: Timeframes for communication, method of communication.

13.4.3 Work Products

[WP-13-03] Procedures to communicate end of cybersecurity support, resulting from [RQ-13-06].

14. DECOMMISSIONING

14.1 General

Decommissioning is a part of the lifecycle of an item or component and is considered in the concept and product development phases.

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

14.2 Objectives

The objective of this clause is to ensure that the item or component can be decommissioned in a secure manner.

14.3 Inputs

14.3.1 Prerequisites

None.

14.3.2 Further Supporting Information

None.

DRAFT

14.4 Requirements and Recommendations

[RQ-14-01] The cybersecurity implications of decommissioning shall be considered in accordance with Clauses 9 and 10.

14.5 Work Products

None.

15. DISTRIBUTED CYBERSECURITY ACTIVITIES

15.1 General

This clause specifies requirements for distributed cybersecurity activities and applies to:

a) items and components developed in a distributed activity;

b) the interaction on all levels of the customer-supplier relationship; and

c) all phases where an agreement is applicable.

For example, a Tier-1 can be a supplier for an OEM in the development and in another contractual relationship the Tier-1 can be a customer of a Tier-2 for a component. This is illustrated in Figure 11.

Key
C Customer
S Supplier
CIAD Cybersecurity Interface Agreement for Development

Figure 11 - Use cases for customer-supplier relationships along the supply chain

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

15.2 Objectives

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

15.3 Inputs

15.3.1 Prerequisites

None.

15.3.2 Further Supporting Information

None.

15.4 Requirements and Recommendations

15.4.1 Demonstration and Evaluation of Supplier Capability

[RQ-15-01] For distributed activities, the capability of the considered supplier, to develop and, if applicable, perform post-development activities according to this document shall be evaluated.

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

DRAFT

[RC-15-01] To support the customer's evaluation of supplier capability, the supplier should provide a cybersecurity record of capability.

NOTE 2: The supplier's record of capability can include:

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

b) evidence of continuous cybersecurity activities in accordance with Clause 7;

c) summary of previous cybersecurity assessments;

d) organizational audit results, if available;

e) evidence of an information security management system; and

f) evidence of the organization's management systems in accordance with 5.4.6.

NOTE 3: An organization can outsource parts of running a management system.

15.4.2 Request for Quotation

[RQ-15-02] When cybersecurity activities are distributed, a request for quotation from the customer to the candidate supplier shall include:

a) a formal request to comply with this document;

b) the expectation of cybersecurity responsibilities taken by the supplier in accordance with 15.4.3; and

c) the cybersecurity goals or the set of relevant cybersecurity requirements, including their attributes, depending on what the supplier is quoting for.

EXAMPLE: Technical specification for integrating message authentication.

15.4.3 Alignment of Responsibilities

[RQ-15-03] The customer and the supplier shall specify the distributed cybersecurity activities in a cybersecurity interface agreement including:

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

b) if applicable, a joint tailoring of the cybersecurity activities in accordance with 6.4.2;

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

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

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

NOTE 1: The supplier, the customer or a third party can perform the cybersecurity assessment concerning the components or work products developed by the supplier.

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

DRAFT

d) the information and the work products to be shared, including distribution, reviews and feedback mechanisms in the case of a cybersecurity issue;

EXAMPLE 3: The shared information can include:

- information sharing strategy (see 5.4.5);
- information exchange procedures for cybersecurity vulnerability and findings regarding cybersecurity risks;
- 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;
- the definition of roles, the way of communicating and documenting changes, and potentially a re-iteration of the risk determination;
- alignment on a tool for requirements management;
- process of reporting known vulnerabilities in a customer released product; and/or
- results of cybersecurity assessments.

e) the target milestones regarding the cybersecurity activities of the customer and the supplier; and

f) the definition of the end of cybersecurity support for the items or components.

NOTE 3: Activities can be omitted if they are performed by the other party.

[RC-15-02] The cybersecurity interface agreement should be concluded between the customer and the supplier by the start of the distributed activities.

EXAMPLE 4: Cybersecurity interface agreement for development, cybersecurity interface agreement for production.

[RQ-15-04] If a vulnerability report in accordance with 7.5 requires actions, the customer and the supplier shall agree the actions required and who performs them.

[RQ-15-05] When there is a risk of not conforming to the agreed cybersecurity planning, or a risk concerning cybersecurity, the other party shall be informed and both parties shall agree on a resolution.

[RQ-15-06] A party shall notify the other if there are conflicts concerning cybersecurity requirements between cybersecurity and related disciplines (see [RQ-05-05]) such that appropriate action and decision can take place.

[RQ-15-07] If the customer's cybersecurity requirements are unclear or not feasible, the supplier shall consult the customer to come to a mutual understanding.

[RC-15-03] The definition of responsibilities should be specified in a matrix of responsibility assignment.

EXAMPLE 5: Template in Annex C.

15.5 Work Products

[WP-15-01] Cybersecurity interface agreement, resulting from the requirements of 15.4.3.

DRAFT

ANNEX A
(INFORMATIVE)
SUMMARY OF CYBERSECURITY ACTIVITIES AND WORK PRODUCTS

Table A.1 provides a summary of the cybersecurity activities and their corresponding work products. This can help with the organization and oversight of these activities to ensure coverage and to help understand potential workload. The work products generated during the concept and product development phases highlight the cybersecurity activities that are defined in the cybersecurity plan and are thus in the scope of a cybersecurity assessment.

Table A.1 - Activities and work products of this document

Activities		Work Products	
Organization Culture			
Cybersecurity Management	5. Overall Cybersecurity Management	[WP-05-01]	Cybersecurity policy, rules and processes
		[WP-05-02]	Evidence of competence management, awareness management and continuous improvement
		[WP-05-03]	Organizational cybersecurity audit report
		[WP-05-04]	Evidence of the organization's management systems
		[WP-05-05]	Evidence of tool management
	6. Project Dependent Cybersecurity Management	[WP-06-01]	Cybersecurity plan
		[WP-06-02]	Cybersecurity case
		[WP-06-03]	Cybersecurity assessment report
		[WP-06-04]	Release for post-development report
Continuous Cybersecurity Activities			
Continuous Cybersecurity Activities	7.3 Cybersecurity Monitoring	[WP-07-01]	List of sources for cybersecurity monitoring
		[WP-07-02]	Results from the triage of cybersecurityinformation
	7.4 Cybersecurity Event Assessment	[WP-07-03]	Cybersecurity event assessment
	7.5 Vulnerability Analysis	[WP-07-04]	Vulnerability analysis
	7.6 Vulnerability Management	[WP-07-05]	Rationale for the managed vulnerability
Concept and Product Development Phases			
Risk Assessment Methods	8.3 Asset Identification	[WP-08-01]	Damage scenarios
		[WP-08-02]	Identified assets and cybersecurity properties
	8.4 Threat Scenario Identification	[WP-08-03]	Threat scenarios
	8.5 Impact Rating	[WP-08-04]	Impact rating, including the associated impact categories of the damage scenarios
	8.6 Attack Path Analysis	[WP-08-05]	Identified attack paths
	8.7 Attack Feasibility Rating	[WP-08-06]	Attack feasibility rating
	8.8 Risk Determination	[WP-08-07]	Risk value
	8.9 Risk Treatment Decision	[WP-08-08]	Risk treatment decision per threat scenario
Concept Phase	9.3 Item Definition	[WP-09-01]	Item definition
	9.4 Cybersecurity Goals	[WP-09-02]	Threat analysis and risk assessment
		[WP-09-03]	Risk treatment decisions
		[WP-09-04]	Cybersecurity goals
		[WP-09-05]	Cybersecurity claims
		[WP-09-06]	Verification report
	9.5 Cybersecurity Concept	[WP-09-07]	Cybersecurity concept
		[WP-09-08]	Verification report of cybersecurity concept

DRAFT

Product Development Phases	10.4.1 Refinement of Cybersecurity Requirements and Architectural Design	[WP-10-01] [WP-10-02] [WP-10-03]	Refined cybersecurity specification Cybersecurity requirements for post-development Verification report for the refined cybersecurity specification
	10.4.2 Integration and Verification	[WP-10-04] [WP-10-05] [WP-10-06]	Vulnerability analysis report Integration and verification specification Integration and verification reports
	10.4.3 Specific Requirements for Software Development	[WP-10-07] [WP-10-08]	Documentation of the modelling, design, or programming languages and coding guidelines Software unit design and software unit implementation
	11. Cybersecurity Validation of the Item at Vehicle Level	[WP-11-01] [WP-11-02]	Validation specification Validation report
Post-Development phases			
	12. Production	[WP-12-01]	Production control plan
	13.3 Cybersecurity Incident Response	[WP-13-01] [WP-13-02]	Cybersecurity incident response plan Cybersecurity incident response information
	13.4 Updates	[WP-13-03]	Procedures to communicate end of cybersecurity support
	14. Decommissioning	None	
Supporting Processes			
	15. Distributed Cybersecurity Activities	[WP-15-01]	Cybersecurity interface agreement

DRAFT

ANNEX B
(INFORMATIVE)
EXAMPLES OF CYBERSECURITY CULTURE

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

Table B.1 - Examples of poor and strong cybersecurity culture

Examples Indicative of a Poor 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 and schedule always take precedence over cybersecurity.	Cybersecurity and safety have the highest priority regarding the design and development decisions.
The reward system favors 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.
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 the integral processes (cybersecurity, verification, validation and configuration management).
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; - managements react only when there is a cybersecurity incident in production, the field or high 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 in the case of a vulnerability or incident in the field.
The required resources are not planned or allocated in a timely manner.	The required resources are allocated. Skilled resources have the competence commensurate with the activity assigned.
"Groupthink" confirmation bias "Stacking the deck" when forming review groups to prevent potential dissention Dissenter is ostracized or labelled as "not a team player" Dissent reflects negatively on performance reviews "Minority dissenter" is labelled or treated as a "troublemaker", "not a team player" or a "whistle-blower" Concerned employees fear repercussion	The process uses diversity to advantage: - Intellectual diversity is sought, valued and integrated in all processes. - Behavior which counters the use of diversity is discouraged and penalized. Supporting communication and decision-making channels exist and the management encourages their usage: - Self-disclosure is encouraged. - Disclosure of discovery by anyone (internally and externally) else is encouraged. - The discovery and resolution process continue in the field, manufacturing and development of other products.
No systematized 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 process are followed.

DRAFT

ANNEX C
(INFORMATIVE)
CYBERSECURITY INTERFACE AGREEMENT TEMPLATE EXAMPLE

C.1 PURPOSE

How Cybersecurity Interface Agreement is communicated is important to prevent misunderstandings of agreement such as responsibilities, level of disclosure of information, level of achievement for each milestone, between different organizations participating in a distributed cybersecurity activity.

This annex provides an example (see Figure C.1) of a Cybersecurity Interface Agreement template related to work sharing to illustrate how responsibilities of cybersecurity activities performed by the customer and by the supplier are identified in accordance with [RQ-15-03]. The template uses RASIC to demonstrate the assignment of responsibilities for specific work products between organizations.

Other information is also addressed, such as point of contact, level of disclosure of information sharing, target milestones, methods or tools for the collaborations.

C.2 EXAMPLE TEMPLATE

The entries of column in this example template are:

- Phase: Phase of this document;
- Work product: Work products of this document that are related to the interface of the distributed activities;
- Doc Ref: Relevant clauses of this standard;
- Supplier: Supplier responsibilities by RASIC;
- Customer: Customer responsibilities by RASIC;

NOTE: RASIC can be used as follows:

- R (responsible): The organization that is responsible for getting the activity done;
- A (approval): The organization that has the authority to approve or deny the activity once it is complete;
- S (support): The organization that a will help the organization responsible for the activity;
- I (inform): The organization that is informed of the progress of the activity and any decisions being made; and
- C (consult): The organization that offers advice or guidance but does not actively work on the activity.

DRAFT

- Level of confidentiality: Supplier and customer agree on the confidentiality of each work product; and

  NOTE: 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 external parties; and
  - Public: The work product can be shared without any restrictions.

- Comment: Additional information concerning results of negotiation and discussion.

Phase	Work product	Doc ref.	Supplier					Customer					Level of confidentiality	Comment
			R	A	S	I	C	R	A	S	I	C		
Concept	Item definition													
	Threat 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 METHOD AND CRITERIA

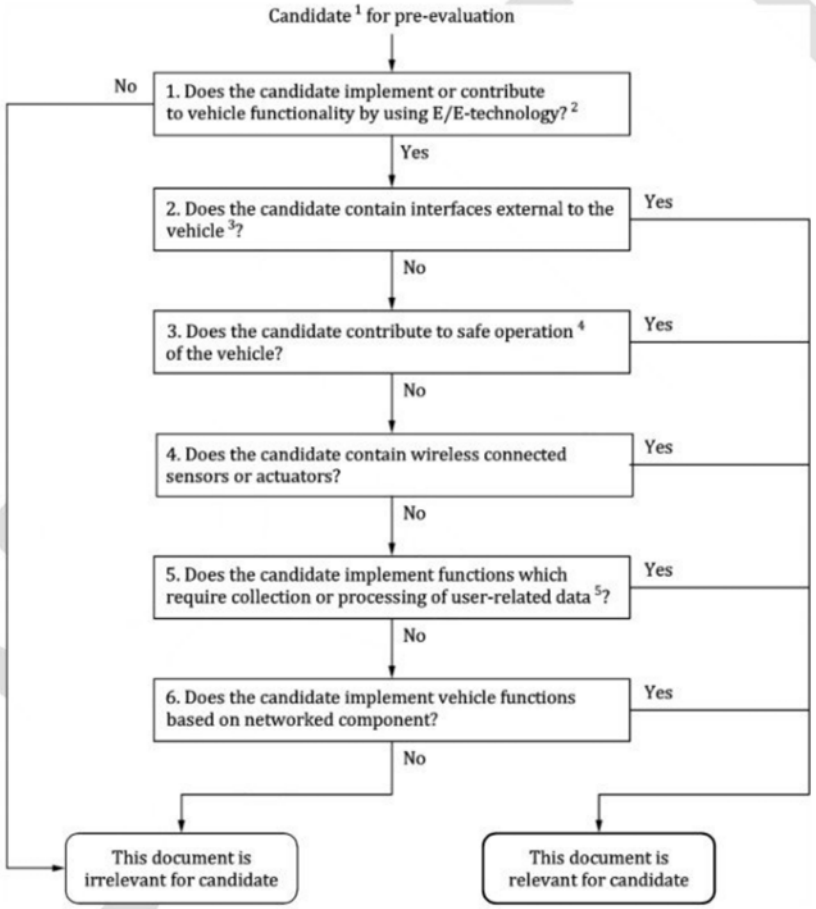
D.1 PURPOSE

Not all items and their components that are installed in road vehicles are cybersecurity relevant. This annex provides an example of an approach to determine if an item or a component is cybersecurity relevant. This can help to avoid irrelevant application of this document.

D.2 METHOD

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

Cybersecurity relevance can also be determined by holding a brainstorming session utilizing experience and expert judgment.



NOTE:
[1] item or component.
[2] This can also consider previous developments.
[3] EXAMPLE 1: Function interface to backend server; 4G cellular telecommunications network.
[4] EXAMPLE 2: Candidate implements or contributes to:
- networked functions for longitudinal or lateral vehicle control;
- networked functions for active or passive safety of the vehicle.
[5] EXAMPLE 3: Data related to drivers or passengers, or to potentially sensitive information such as location data.

Figure D.1 - Cybersecurity relevance example method and criteria

ANNEX E
(INFORMATIVE)
CYBERSECURITY ASSURANCE LEVELS

E.1 GENERAL

This annex describes a Cybersecurity Assurance Level (CAL) classification scheme that can be used to help provide assurance that the assets of an item or component are adequately protected against the relevant threat scenarios.

A CAL can be used to specify a set of assurance requirements, in terms of levels of rigor or effort to provide confidence that the protection of the assets is adequate. The CAL does not specify technical requirements for cybersecurity measures. The CAL can be used to drive the cybersecurity engineering, providing a common language for communicating cybersecurity assurance requirements among organizations involved.

A CAL can be determined by the organization developing an item or assumed by an organization developing a component out of context. 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 support, for example parameters based on the assets of the item and their criticality. The relationship between CAL and risk is illustrated in Figure E.1.

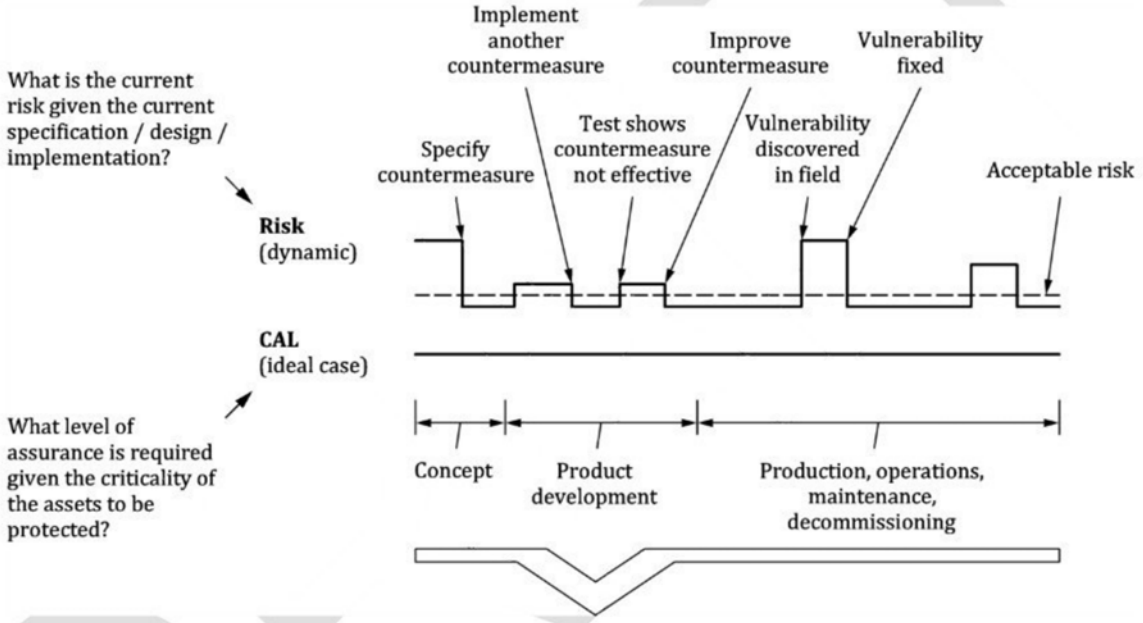


Figure E.1 - Relationship between CAL and risk

The determined or assumed CAL can then be used to drive subsequent cybersecurity activities 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 can be determined based on consideration of the identified threat scenarios (see 8.4). The following Table E.1 gives an example based on four CALs, each corresponding to an increasing level of assurance or confidence in the cybersecurity engineering methods used.

EXAMPLE: The CAL can be assigned based on the maximum impact, and the attack vector of the relevant threat scenarios, as shown in Table E.1.

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

		Attack Vector			
		Physical	**Local**	**Adjacent**	**Network**
Impact	Negligible	---[1]	---[1]	---[1]	---[1]
	Moderate	CAL1	CAL1	CAL2	CAL3
	Major	CAL1	CAL2	CAL3	CAL4
	Severe	CAL2	CAL3	CAL4	CAL4

[1] NOTE: See [PM-08-01].

Documenting the rationale for the determination of a CAL can improve communication within the supply chain and assist with traceability. A CAL can also be part of the interface agreement between customer and supplier.

NOTE: A single CAL can be assigned to all cybersecurity goals of an item or different CALs can be assigned to each cybersecurity goal. Similar cybersecurity goals can be combined into a single one in accordance with 0, NOTE 11, and the highest of the individual CALs assigned to the combined goal.

E.3 USAGE OF THE CYBERSECURITY ASSURANCE LEVEL

E.3.1 General Considerations

The CAL can be used to determine with which level of rigor cybersecurity activities are performed.

The CAL can affect:

- the number, scope and extent of the specified activities;
- the content of the specified work products;
- the methods used for development and testing:
  - requirements management;
  - methods for design and verification;
  - testing methods for specific verification and validation activities including depth of testing; and
  - vulnerability analysis and testing methods.

For each increasing CAL, the corresponding requirements represent a meaningful increase in the assurance of the item or component by the design, verification, and other cybersecurity activities in which the methods are used.

An example for the number of CALs and guidance for the concept and the product development phases is given in Table E.2.

DRAFT

Table E.2 - Example number of CALs and expected rigor in cybersecurity assurance measures

Level	Description	Philosophy	Difference from Previous Level
CAL1	Developers or users require a low to moderate level of independently assured cybersecurity.	Functionally and structurally tested.	Requiring developer testing, and a vulnerability analysis.
CAL2	Developers or users require a moderate level of independently assured cybersecurity and require a thorough investigation of the item without substantial re-engineering.	Methodically tested and checked. It provides assurance through the use of development environment controls.	Procedures that provide moderate confidence that the item will not be tampered with during development.
CAL3	Developers or users require a moderate to high level of independently assured cybersecurity in conventional commodity items and are prepared to incur additional security-specific engineering costs.	Methodically designed, tested, and reviewed (resistance to penetration attackers with an enhanced-basic attack potential).	Requiring more design description, the implementation representation for the security functions, and improved mechanisms and/or procedures that provide confidence that the item will not be tampered with during development.
CAL4	Developers or users require the highest-level rigor.	Advanced methodically designed, tested, and reviewed.	Independent tested and reviewed (for example add an independent vulnerability analysis).

E.3.2 Concept Phase

This subclause provides an example on the usage of CAL to adapt the rigor 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, the CAL can be used as follows as an extension to [RQ-09-11]:

a) Cybersecurity requirements derived from a cybersecurity goal inherit the CAL from that cybersecurity goal.

b) If several cybersecurity requirements with CAL inherited from multiple cybersecurity goals are allocated to an architectural component, the highest CAL is selected from those cybersecurity requirements as the CAL of the architectural component if isolation from the other components cannot be confirmed in the preliminary architecture.

c) If redundant cybersecurity requirements are allocated to isolated components then the CAL assigned to such requirements can be tailored, based on a rationale.

E.3.3 Product Development

An application of CAL 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 the other components cannot be confirmed, then the components can be developed in accordance with the highest CAL for those cybersecurity requirements.

The example methods in Clause 10 can be applied as shown in Table E.3 through Table E.9, where "✔" indicates "recommended". If there is no check mark, there is no particular recommendation of the method or measure for achievement of that particular CAL.

DRAFT

1932 ***Table E.3 - Verification methods of architectural design ([RQ-10-08])***

Methods	CAL			
	1	2	3	4
Review	✔	✔	✔	✔
Analyses	✔	✔	✔	✔
Simulation			✔	✔
Prototyping			✔	✔

1933 ***Table E.4 - Methods for verification of integration ([RQ-10-12])***

Topics	CAL			
	1	2	3	4
Requirements-based test [a]	✔	✔	✔	✔
Interface test	✔	✔	✔	✔
Resource usage evaluation [b, c]	✔	✔	✔	✔
Verification of the control flow and data flow			✔	✔
Static code analysis; for software: static code analysis [d]	✔	✔	✔	✔

[a] The refined cybersecurity requirements allocated to the architecture are the basis for this requirements-based test.
[b] In software development: to ensure the fulfilment of requirements influenced by the hardware architectural design with sufficient tolerance, properties such as average and maximum processor performance, minimum or maximum execution times, storage usage (e.g., RAM for stack and heap, ROM for program and data) and the bandwidth of communication links (e.g., data buses) have to be determined. This method applies to interfaces, values approaching and crossing the boundaries and out of range values.
[c] Some aspects of the resource usage evaluation can only be performed properly when the integration tests are executed on the target environment or if the emulator for the target processor adequately supports resource usage tests.
[d] In software development: static analyses are a collective term which includes analysis such as architectural analyses, analyses of resource consumption and searching the source code text or the model for patterns matching known faults, common weakness patterns or compliance with modelling or coding guidelines, if not already verified at the unit level.

1934 ***Table E.5 - Methods for deriving test cases ([RQ-10-14])***

Topics	CAL			
	1	2	3	4
Analysis of requirements	✔	✔	✔	✔
Generation and analysis of equivalence classes [a]			✔	✔
Boundary values analysis [b]			✔	✔
Error guessing based on knowledge or experience [c]				

[a] Equivalence classes can be identified based on the division of inputs and outputs, such that a representative test value can be selected for each class.
[b] This method applies to parameters or variables, values around (below, equal or above) boundary values, values altering the behavior of the software (as evidenced by prior data flow analysis).
[c] Error guessing tests can be based on data collected through lessons learned, expert judgment, shared between vendors in a consortium or publicly disclosed.

1935

DRAFT

1936 ***Table E.6 - Structural coverage metrics at the software unit level ([RQ-10-15])***

Topics	CAL			
	1	2	3	4
Statement coverage	✔	✔		
Branch coverage			✔	✔

1937 ***Table E.7 - Structural coverage at the software architectural level ([RQ-10-15])***

Topics	CAL			
	1	2	3	4
Function coverage [a]			✔	✔
Call coverage [b]			✔	✔

[a] Method 1 refers to the percentage of executed software sub-programs or functions in the software (for definition refer to IEC 61508-7:2010, C.5.8).
[b] Method 2 refers to the percentage of executed software sub-programs or function with respect to each implemented call of these sub-programs or functions in the software.

1938 ***Table E.8 - Component testing methods ([RC-10-03])***

Methods	CAL			
	1	2	3	4
Vulnerability scanning	✔	✔	✔	✔
Penetration testing (Basic Level Attack potential: see I.3)	✔	✔		
Penetration testing (Enhanced-Basic Level Attack potential: see I.3)			✔	✔

1939 ***Table E.9 - Topic list (0)***

Topics	CAL			
	1	2	3	4
Use of language subsets [a]	✔	✔	✔	✔
Enforcement of strong typing [b]	✔	✔	✔	✔
Use of defensive implementation techniques [c]			✔	✔

[a] The objectives of method 1 are avoidance of:
- Execution of ambiguously defined language constructs which can be interpreted differently by different modelers, programmers, code generators or compilers.
- Execution of language constructs which from experience easily lead to mistakes, for example assignments in conditions of identical naming of local and global variables.
- Execution of language constructs which could result in unhandled run-time errors.
- Execution of language constructs which could introduce weaknesses (see for instance Common Weakness Enumeration: https://cwe.mitre.org/).

[b] Variables are globally defined once in a central place. Type castings are restricted to the minimal necessary amount.
[c] The techniques used by attackers are taken into account while programming in order to avoid weaknesses that has been already exploited.

DRAFT

ANNEX F
(INFORMATIVE)
VERIFICATION AND VALIDATION

F.1 GENERAL

Clause 3 defines in 3.1.34 validation as “confirmation, through the provision of objective evidence, that the cybersecurity goals of the item are adequate and are achieved”. 3.1.35 defines verification as “confirmation, through the provision of objective evidence, that specified requirements have been fulfilled”.

Validation and verification address two similar but different questions. Validation addresses the question “are we building the right product?”, and verification addresses the question “are we building the product right?”. Verification and validation both examine whether certain requirements have been fulfilled, and they can use the same technique (e.g., testing, to obtain objective evidence). However, verification and validation differ from each other in the following aspects:

1. The type of requirements that are examined:
    a. validation examines the cybersecurity goals;
    b. verification examines the cybersecurity requirements; and
    c. verification examines that the design activities are performed correctly.
2. The integration level of the product on which the activity is performed:
    a. generally, at the item level it is validation; and
    b. generally, at the component level it is verification.
3. The stage at which the activity is performed:
    a. validation is performed close to the end of the product development phase and before the release for post-development; and
    b. verification is performed during the concept phase and the product development phase.

Verification can be accomplished through review, analysis or by testing methods. Validation is typically performed using analysis and by testing.

F.2 EXAMPLE METHODS

F.2.1 Review

Review is a verification method in which a peer or another party checks a document or work product against certain objectives and criteria. Typically, checklists are used for formal reviews and inspections, following a particular review process.

DRAFT

F.2.2 Analysis

Analysis is a systematic and methodical means to research one or more aspects of a work product or of an item or component. Analysis checks for inherent weaknesses, human errors, known and visible system flaws, observable artefacts under the scenario of operation, and overall consistency, correctness and completeness with respect to cybersecurity requirements specifications.

Techniques can include industry standardized or best practice leading tools for identifying known vulnerabilities and weaknesses.

EXAMPLE: Static software code analysis tools that check against MISRA-C and CERT-C.

F.2.3 Simulation

Simulation is an approximation of the operation of an item or component. Simulation can be used to confirm the consistency, correctness, and completeness of requirements or design specifications. Simulation can be used when a system or component is being designed but not yet built. It can also be used when a system or component does not exist, and only a model is available.

F.2.4 Prototyping

A prototype is an early sample or physical mock-up of an item or component. Prototyping is a method that uses a prototype to confirm the consistency, correctness, and completeness of the requirements or design specifications.

F.2.5 Testing

F.2.5.1 General

Testing is a means to dynamically evaluate an item or component (i.e., by exercising stimuli to an item or component and observing its responses to these stimuli; e.g., external outputs or internal nodes). Testing can be done on the actual item or component or can be based on a model.

F.2.5.2 Functional Testing

Functional testing is applied to an item or component, possibly integrated in a test environment, to determine whether the functionality meets the requirements.

F.2.5.3 Interface Testing

Interface testing is performed by applying functional testing to verify all inputs and outputs to and from the item or component meet the requirements.

F.2.5.4 Penetration Testing

Penetration testing is a group of testing methods used to find vulnerabilities present in a system that can be exploited by an adversary to take control, gain privileged access, expose privileged data, or simply cause system malfunction. Penetration testing can be performed with different levels of knowledge about the system (i.e., black, grey, and white box testing). The output of the penetration testing helps to identify cybersecurity requirements and controls to harden items or components against potential threats.

Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual adversaries. Penetration testing often involves looking for the combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability, see [21].

DRAFT

F.2.6 Vulnerability Scanning

Vulnerability scanning is a suite of techniques where the exploitation risk of the vulnerability is assessed and quantified. Vulnerability scanning can be performed via passive scanning (e.g., looking for coding errors that can be exploited) or active scanning for access to for example host processes, network protocols, file systems, or memory. Vulnerability scanning can also be applied to hardware and system architecture in a similar manner using checklists of known vulnerabilities at these levels. Vulnerability scanning can be used as a technique for penetration testing or analysis.

F.2.7 Fuzz Testing

Fuzz testing is a type of testing where large amounts of random data are provided (usually in an automated or semi-automated fashion) as the input to a system to look for weaknesses and vulnerabilities (e.g., failures and coding errors). If the system crashes or departs from the normal defined behavior, the output is reported as an error. Fuzz testing can be done at the system or interface level, or more exhaustively by listing every variable in the software under test and fuzzing random values for each software variable in the code. In the latter approach, the testing is typically highly automated. Fuzz testing can be used to discover, for example, overflows, segmentation and heap errors that have cybersecurity implications. Fuzz testing can be applied to hardware inputs. Fuzz testing can be used as a technique for penetration testing.

DRAFT

ANNEX G
(INFORMATIVE)
EXAMPLE USE CASE AND WORK PRODUCTS: HEADLAMP SYSTEM

G.1 GENERAL

This annex is intended to aid understanding of activities of this document through examples. This annex shows an example use case for the development of a headlamp system, by two fictional companies A and B to illustrate different scenarios with different levels of architectural granularity. The system is simplified and abstracted in order to illustrate activities of this document. The contents of this annex is limited to the concept phase and product development at the system level. In particular it addresses:

a) item definition;

b) derivation of cybersecurity goals and statement of cybersecurity claims;

c) refinement of cybersecurity specification; and

d) integration and verification.

The above includes the respective risk assessment methods.

The example and its work products in this annex are provided for illustrative purposes only and are not intended to imply any particular approach for practical use.

G.2 OVERVIEW OF GENERAL INTERACTIONS BETWEEN CLAUSES

This clause provides an overview of various interactions between clauses. Figure G.1 takes the concept phase point of view, Figure G.2 takes the product development point of view, and Figure G.3 takes the continuous cybersecurity activities point of view.

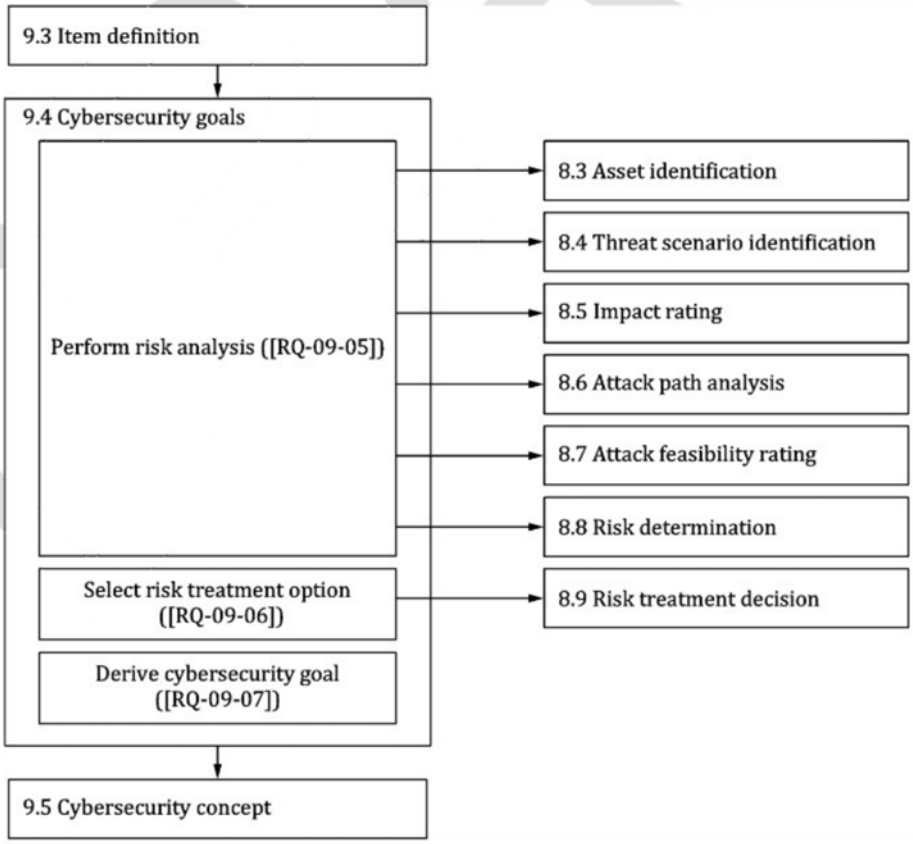


Figure G.1 - General interactions in the concept phase

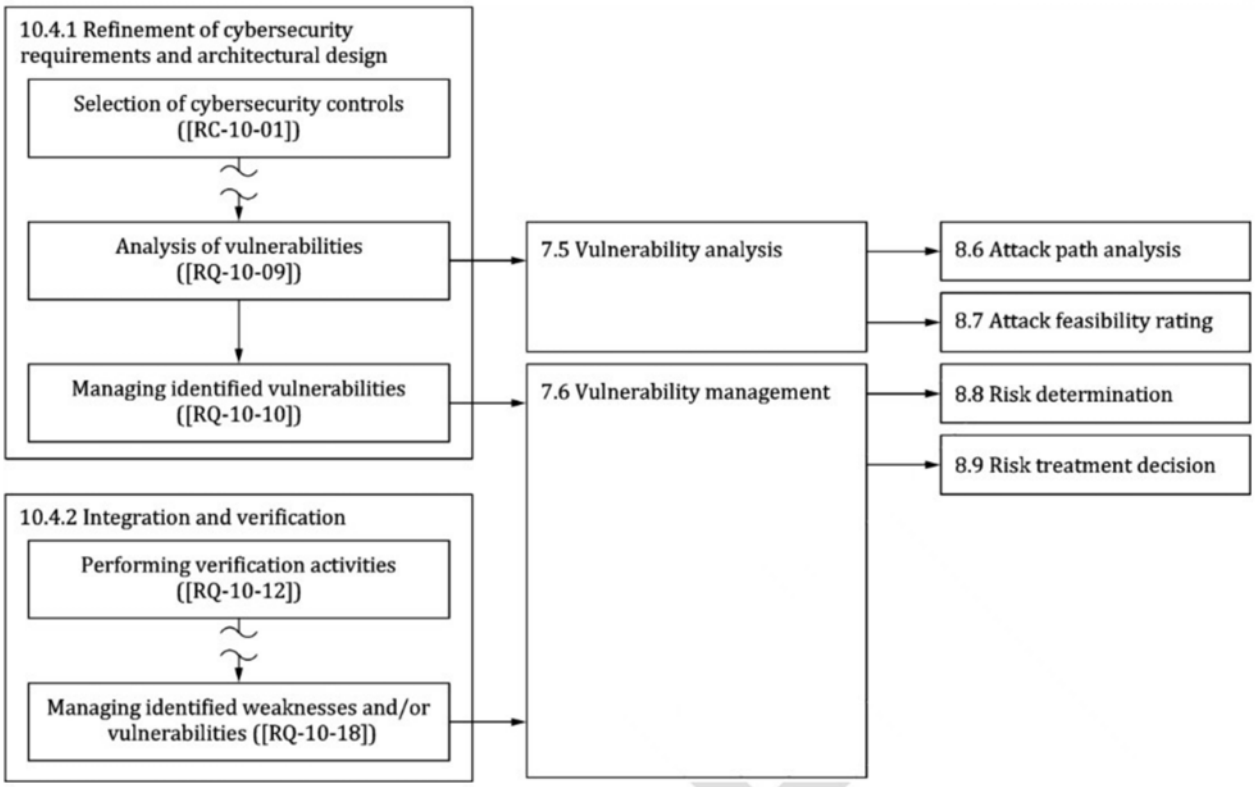


Figure G.2 - General interactions in product development

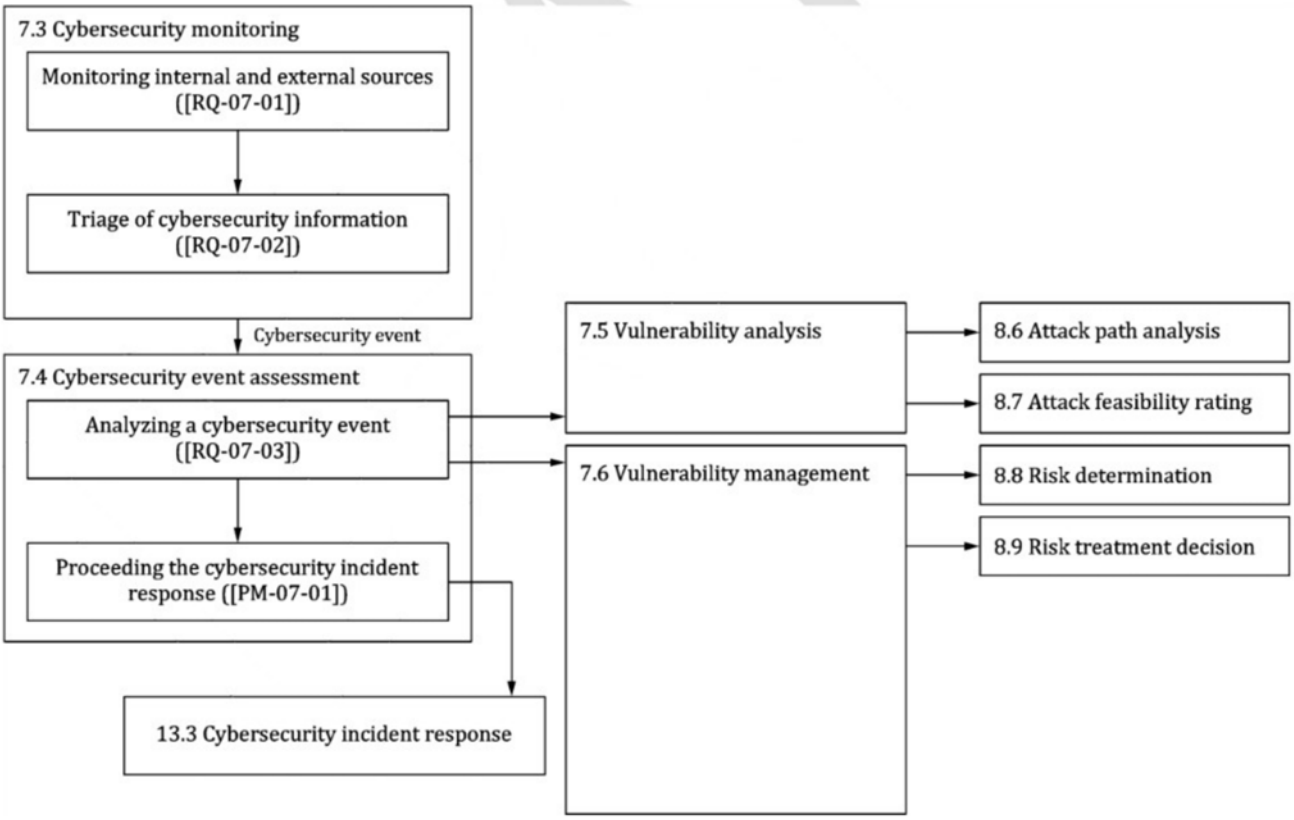


Figure G.3 - General interactions in continuous cybersecurity activities

G.3 USE CASE OF A HEADLAMP SYSTEM

G.3.1 Concept Phase

G.3.1.1 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. The Headlamp item includes the Headlamp system, the Navigation ECU and the Gateway ECU.

- Item Boundary
  - This is described in Figure G.4.
- Functions
  - Functional overview of the item: The Headlamp system turns on/off the headlamp according to 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. And it returns automatically the headlamp 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.
- Preliminary Architecture
  - This is described in Figure G.4.

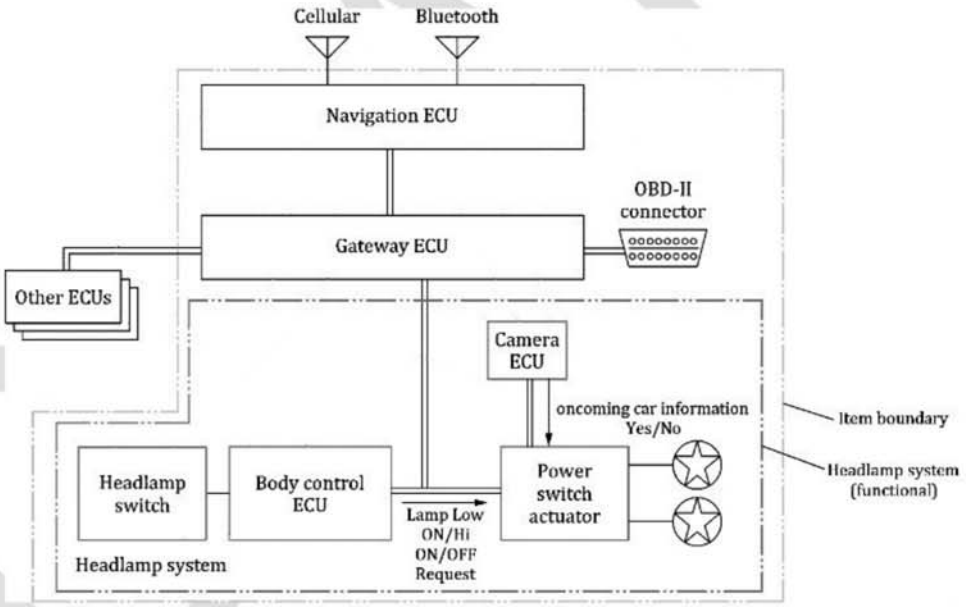


Figure G.4 - Example of item boundary and preliminary architecture of the headlamp

Table G.1 shows example assumptions identified in accordance with [RQ-09-04].

Table G.1 - Example assumptions

Assumptions No.	Description
A.1	The item is physically protected by anti-tamper enclosures, which is an assumption on the operational environment.
:	:

G.3.1.2 Cybersecurity Goals

G.3.1.2.1 Asset Identification

[RQ-09-05] calls asset identification in accordance with 8.3 to identify assets of the item and their damage scenarios. An example format for damage scenario description is as follows:

<SFOP impact or damage including its condition (if relevant)> resulting from loss of <**security property**> of <**asset**>.

Example: **Unintended Headlamp's turn off during night driving** resulting from loss of **integrity** of **CAN signal**
Table G.2 and Table G.3 show example results of asset identification in accordance with 8.3.

Table G.2 - Example of a list of assets and damage scenarios created by Company A

Component/ Message	Function	Asset	Cyber Security Property			Damage Scenario No.	Damage Scenario	Identified Asset for Safety
			C	I	A			
Navigation ECU	…	N/A	…	…	…	N/A	N/A	
Gateway ECU	…	N/A	…	…	…	N/A	N/A	
Body Control ECU	Power switch control function	Firmware	-	X	X	…	…	
	CAN message transmission function	CAN Frame	-	X	X	xx	Unintended headlamp's turn off during IGN switch's turn off, resulting from loss of integrity of CAN signal	X
						D.x	Unintended headlamp's turn off during night driving resulting from loss of integrity of CAN signal	X
						:	:	
	…	…	…	…	…	…	…	
Power Switch Actuator	Headlamp control function	Firmware	…	…	…	…	…	X
	CAN message transmission function	CAN Frame	…	…	…	…	…	X
	……	…	…	…	…	…	…	
Camera ECU	Oncoming car information	…	…	…	…	…	…	
	…	…	…	…	…	…	…	
CAN Message	Oncoming car information Yes/No	CAN Frame	-	X	X	xx	Unintended low beam of headlamp…	
						xx	Unintended fixing of high beam…	
CAN Message	Lamp low ON/HI ON/OFF Request	CAN Frame	-	X	X	xx	Unintended headlamp's turn off during IGN switch's turn off, resulting from loss of integrity of CAN signal	X
						xx	Unintended headlamp's turn off during night driving resulting from loss of integrity of CAN signal)	X
…	…	…	…	…	…		…	

DRAFT

Table G.3 - Example of a list of assets and damage scenarios created by Company B

Asset	Security Property (C/I/A)	Damage Scenario
Lamp switch off request	I	Unexpected loss of head light
	A	Unable to switch off head light
Lamp switch on request	I	Unexpected gain of head light
	A	Unable to switch on head light
…	…	…
	…	…
	…	...

G.3.1.2.2 Impact Rating

[RQ-09-05] also calls impact rating in accordance with 8.5 to rate the impact of damage scenarios. Table G.4 and Table G.5 show example results of impact rating in accordance with 8.5.

Table G.4 - Example of impact ratings for damage scenarios created by Company A

Component/ Message	Function/ Message	Asset	Damage Scenario No.	Damage Scenario	Impact Category	Impact Level	Impact
Body Control ECU	…	…	…	…	…	…	…
	…	…	…	…	…	…	…
	CAN message transmission function	CAN Frame	xx	Unintended headlamp's turn off during IGN switch's turn off, resulting from loss of integrity of CAN signal	F:-	-	-
					S:-	-	-
					O:	Moderate	Since the headlamp turns off when the driver turns off IGN switch, there is no serious impact on the operation of the vehicle
					P:-	-	-
			D.x	Unintended headlamp's turn off during night driving resulting from loss of integrity of CAN signal	F:-	-	-
					S:S3	Severe	A crash against a street tree poses a fatal injury
					O:	-	-
					P:-	-	-
			:	:	:	:	:
	…	...		...	...	...	...
	...	...		...	...	...	...
CAN Message	Oncoming car information Yes/No	CAN Frame	xx	Unintended low beam of headlamp	F:-	-	-
					S:-	Negligible	...
					O:	Moderate	Since the headlamp turns off when the driver turns off IGN switch, there is no serious impact on the operation of the vehicle
					P:-	-	-

DRAFT

			xx	Unintended fixing of high beam	F:-	-	-
					S:-	Negligible	...
					O:	Negligible	Since the headlamp turns off when the driver turns off IGN switch, there is no serious impact on the operation of the vehicle
					P:-	-	-
CAN Message	Lamp low ON/HI ON/OFF request	CAN Frame	xx	Unintended headlamp's turn off during IGN switch's turn off, resulting from loss of integrity of CAN signal	F:-	-	-
					S:-	Negligible	...
					O:	Negligible	Since the headlamp turns off when the driver turns off IGN switch, there is no serious impact on the operation of the vehicle
					P:-	-	-
			xx	Due to loss of integrity of CAN signal, headlamp turn off unintentionally during night driving and leading to collision	F:-	-	-
					S:S3	Severe	A crash against a street tree poses a fatal injury
					O:	Negligible	...
					P:-	-	-
…	...	...		...	...	...	...

2089

DRAFT

Table G.5 - Example of impact ratings for damage scenarios created by Company B

Asset	Security Property (C/I/A)	Damage Scenario	Impact Category				
			S	F	O	P	Justification
Lamp switch off request	I	Unexpected loss of head light	Major	Negligible	Major	Negligible	Unexpected loss of your lamps during adverse conditions during driving may cause a crash, severe safety impact and degradation of functionality, but survival is likely
	A	Unable to switch off head light	Negligible	Negligible	Major	Negligible	Serious impact to functionality as you can't turn the lamps off, but no impact to safety
Lamp switch on request	I	Unexpected gain of head light	Negligible	Negligible	Major	Negligible	Serious impact to functionality as you can't turn the lamps off, but no impact to safety
	A	Unable to switch on head light	Moderate	Negligible	Major	Negligible	This is not sudden. It's expected that you're in park or are driving and it's getting dark, but not as severe as driving at night and a sudden turning off of the lamps. Loss of functionality is serious.
…	…	…	…	…	…	…	…

G.3.1.2.3 Threat Scenario Identification

[RQ-09-05] also calls threat scenario identification in accordance with 8.4. Table G.6 and Table G.7 show example results of threat scenario identification in accordance with 8.4.

Table G.6 - Example of a list of threat scenarios created by Company A

Damage Scenario No.	Damage Scenario	Threat Scenario	Threat Scenario No.
:	:	:	:
D.x	Unintended headlamp's turn off during night driving resulting from loss of integrity of CAN signal	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU potentially causing unintended headlamp's turn off during night driving resulting from loss of integrity of CAN signal	T.x
		Tampering of a signal sent by Body Control ECU leads to ….	T.y
		….	…
:	:	:	:

DRAFT

Table G.7 - Example of a list of threat scenarios created by Company B

Damage Scenario	Threat Scenario
Unexpected loss of head light	The lamp switch off request message could be spoofed.
Unable to switch off head light	The CAN bus could be flooded with higher priority messages, so that the lamp switch off request may be processed with significant delay.
Unexpected gain of head light	The lamp switch on request message could be spoofed.
Unable to switch on head light	The CAN bus could be flooded with higher priority messages, so that the lamp switch on request may be processed with significant delay.
…	…

G.3.1.2.4 Attack Path Analysis

[RQ-09-05] also calls attack path analysis in accordance with 8.6. Table G.8 and Table G.9 show example results of attack path analysis in accordance with 8.6. Figure G.5 shows an example of attack path analysis by attack tree analysis.

Analysis of attack paths can take into account assumptions. For example, attack paths that use physical access to the item can be omitted according to the assumption A.1 as shown in Table G.1.

Table G.8 - Example of a list of attack paths for each threat scenario created by Company A

Threat Scenario No.	Threat Scenario	Attack Path No.	Attack Path
T.x	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	AP.x	An attacker compromise Navigation ECU from Cellular interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		AP.y	An attacker compromise Navigation ECU from Bluetooth interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		AP.z	An attacker sends malicious control signals from OBD2 connector
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		:	:
:	:	:	:

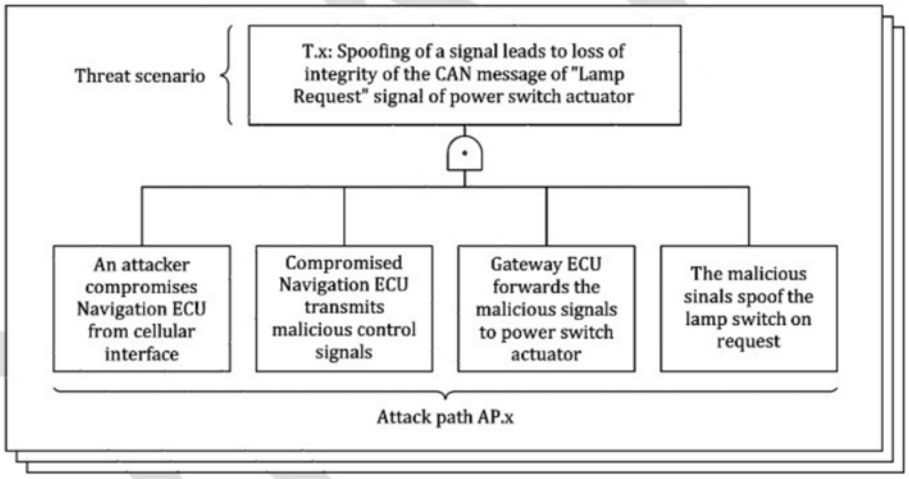
NOTE: Attack paths that require physical access to the item were omitted according to the assumption A.1.

DRAFT

2105 ***Table G.9 - Example of a list of attack paths for each threat scenario created by Company B***

Threat Scenario	Attack Path
The lamp switch off request message could be spoofed.	Since the authentication code is essentially non-existent, an attacker can deliver malicious payload through **OBD-II connector** interface compromising the integrity of the Gateway ECU enabling the injection of spoofed lamp switch off requests.
	Since the authentication code is essentially non-existent, an attacker can deliver malicious payload through C**ellular** interface compromising the integrity of the Gateway ECU enabling the injection of spoofed lamp switch off requests.
	Since the authentication code is essentially non-existent, an attacker can deliver malicious payload through **Bluetooth** interface compromising the integrity of the Gateway ECU enabling the injection of spoofed lamp switch off requests.
The CAN bus could be flooded with higher priority messages, so that the lamp switch off request may be processed with significant delay.	Malicious payload delivered through OBD-II connector, cellular or **Bluetooth** interfaces compromises the integrity of the Gateway ECU enabling the flooding of the bus used for lamp switch-off requests.
The lamp switch on request message could be spoofed.	Since the authentication code is essentially non-existent, an attacker can deliver malicious payload through OBD-II connector, cellular or **Bluetooth** interfaces compromises the integrity of the Gateway ECU enabling the injection of spoofed lamp switch on requests.
The CAN bus could be flooded with higher priority messages, so that the lamp switch on request may be processed with significant delay.	Malicious payload delivered through OBD-II connector, cellular or Bluetooth interfaces compromises the integrity of the Gateway ECU enabling the flooding of the bus used for lamp switch-off requests.
…	…

2106



2107

2108 ***Figure G.5 - Example of an attack path derived by attack tree analysis***

2109

G.3.1.2.5 Attack Feasibility Rating by Attack Vector and Attack Potential Based Approaches

[RQ-09-05] also calls attack feasibility rating for each attack path in accordance with 8.7. Table G.10 and Table G.11 show example results of attack feasibility rating in accordance with 8.7.

Table G.10 - Example of a list of attack feasibility levels rated by attack vector based approach created by Company A

Threat Scenario No.	Threat Scenario	Attack Path No.	Attack Path	Attack Feasibility Level According to the Attack Vector Based Approach
T.x	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	AP.x	An attacker compromise Navigation ECU **from Cellular interface**	High
			Compromised Navigation ECU transmits malicious control signals	
			Gateway ECU forward the malicious signals to Power Switch Actuator	
			The malicious signals spoof the lamp switch on request	
		AP.y	An attacker compromise Navigation ECU **from Bluetooth interface**	Medium
			Compromised Navigation ECU transmits malicious control signals	
			Gateway ECU forward the malicious signals to Power Switch Actuator	
			The malicious signals spoof the lamp switch on request	
		AP.z	An attacker sends malicious control signals **from OBD2 connector**	Low
			Gateway ECU forward the malicious signals to Power Switch Actuator	
			The malicious signals spoof the lamp switch on request	
		:	:	:
	:	:	:	:

NOTE: 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.

DRAFT

Table G.11 - Example of a list of attack feasibility levels rated by attack-potential based approach created by Company B

Threat Scenario	Attack Path	Attack Feasibility Assessment						
		Elapsed Time	Specialist Expertise	Knowledge of the item (or component)	Window of Opportunity	Equipment	Value	Attack Feasibility
The lamp switch off request message could be spoofed.	Since the authentication code is essentially non-existent, an attacker can deliver malicious payload through OBD-II connector interface compromising the integrity of the Gateway ECU enabling the injection of spoofed lamp switch off requests	4	6	3	4	4	21	Low
	Since the authentication code is essentially non-existent, an attacker can deliver malicious payload through Cellular interface compromising the integrity of the Gateway ECU enabling the injection of spoofed lamp switch off requests	4	8	3	0	4	19	Medium
	…	…	…	…	…	…	…	…

DRAFT

G.3.1.2.6 Risk Determination

[RQ-09-05] also calls risk determination for each threat scenario in accordance with 8.8. Table G.12 and Table G.13 show example results of risk determination in accordance with 8.8.

Table G.12 - Example of a list of determined risk values created by Company A

Threat Scenario No.	Threat Scenario		Attack Path No.	Attack Path	Attack Feasibility Level	Aggregated Attack Feasibility Level	Damage Scenario	Impact Level	Risk Value
T.1	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU		AP.x	…	High	High	…	Severe	5
			AP.y	…	Medium				
			AP.z	…	Low				
			:	:	:				
:	:		:	:	:	:	:	:	:

Table G.13 - Example of a list of determined risk values created by Company B

Threat Scenario	Attack Path	Aggregated Attack Feasibility Level	Risk Value			
			S	F	O	P
The lamp switch off request message could be spoofed.	Since the authentication code is essentially non-existent, an attacker can deliver malicious payload through **OBD-II connector** interface compromising the integrity of the Gateway ECU enabling the injection of spoofed lamp switch off requests	Medium	4	1	4	1
	Since the authentication code is essentially non-existent, an attacker can deliver malicious payload through **Bluetooth** interface compromising the integrity of the Gateway ECU enabling the injection of spoofed lamp switch off requests					
	…					
The CAN bus could be flooded with higher priority messages, so that the lamp switch off request may be processed with significant delay.	Malicious payload delivered through OBD-II connector, cellular or **Bluetooth** interfaces compromises the integrity of the Gateway ECU enabling the flooding of the bus used for lamp switch-off requests	Medium	1	1	4	1
…	…	…	…	…	…	…

DRAFT

G.3.1.2.7 Selection of Treatment Option

[RQ-09-06] requires to select treatment options in accordance with 8.9. Table G.14 and Table G.15 show example results of risk treatment decision in accordance with 8.9.

Table G.14 - Example result of selection of risk treatment option created by Company A

No.	Threat Scenario	Attack Path No.	Attack Path	Attack Feasibility Level	Aggregated Attack Feasibility Level	Impact Level	Risk Value	Risk Treatment Option
T.x	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	AP.x	...	High	High	Severe	5	Reducing the risk
		AP.y	...	Medium				
		AP.z	...	Low				
		:	:	:				
:	:	:	:	:	:	:	:	:
T.z	...	...	...	...	Low	Moderate	...	sharing
:	:	:	:	:	:	:	:	:

Table G.15 - Example result of selection of risk treatment option created by Company B

Threat Scenario	Aggregated Attack Feasibility Level	Risk Value				Risk Treatment Option
		S	F	O	P	
The lamp switch off request message could be spoofed.	Medium	4	1	4	1	Reducing the risk
...	...	...	...	...	...	

DRAFT

G.3.1.2.8 Derivation of Cybersecurity Goals

[RQ-09-07] specifies cybersecurity goals for the threat scenarios with treatment option in accordance with 8.9 selected as "reducing the risk". Table G.16 shows an example result of cybersecurity goals stated on each treatment option selected as "reducing the risk".

Table G.16 - Example of cybersecurity goals created by Company A

No.	Threat Scenario	Attack Path No.	Attack Path	Attack Feasibility Level	Aggregated Attack Feasibility Level	Damage Scenario	Impact Level	Risk Value	Risk Treatment Option	Cyber Security Goal
T.x	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	AP.x	…	High	High	…	Severe	5	Reducing the risk	"Lamp switch on request integrity shall be protected against spoofing."
			…							
			…							
			…							
		AP.y	…	Medium						
			…							
			…							
			…							
		AP.z	…	Low						
			…							
			…							
		:	:	:						
	:	:	:	:	:	:	:	:	:	:
T.z	…	…	…	…	Low	…	Moderate	…	sharing	n/a
	:	:	:	:	:	:	:	:	:	:

CALs can be derived for cybersecurity goals. Table G.17 shows an example of CAL derivation according to Table E.1 in Annex E.

Table G.17 - Example of CAL derivation

No.	Threat Scenario	Attack Path No.	Attack Path	Impact Level	Cybersecurity Goal	Attack Vector	CAL
T.x	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	AP.x	An attacker compromise Navigation ECU **from Cellular interface**	Severe	"Lamp switch on request integrity shall be protected against spoofing."	network	CAL4
			Compromised Navigation ECU transmits malicious control signals				
			Gateway ECU forward the malicious signals to Power Switch Actuator				
			The malicious signals spoof the lamp switch on request				
		AP.y	…				
		AP.z	…				
		:	:				
	:	:	:	:	:	:	:

G.3.1.2.9 Statement of Cybersecurity Claims

[RQ-09-08] specifies cybersecurity claims for the risks for which cybersecurity goals are not derived and for assumptions. Table G.18 shows an example of cybersecurity claims.

Table G.18 - Example of cybersecurity claims created by Company A

Related Threat Scenario or Related Assumption	Cybersecurity Claim
T.z: … Treatment option: sharing	Risk of T.z is transferred to insurance. It is adequate because its impact level is low, and its aggregated attack feasibility is moderate. If the insurance does not match to the risk, its risk treatment is re-considered.
:	:
A.1 Assumption on the operational environment: …	Assumption A.1 (see Table G.1) is satisfied. If the assumption is failed to be satisfied, risks related to the assumption are (identified and) managed.
:	:

G.3.1.3 Cybersecurity Concept

G.3.1.3.1 Specifying Cybersecurity Requirements and Their Allocation

Subclause 9.5 specifies cybersecurity requirements and allocates them to the item or the operational environment. Attack paths can be considered to derive cybersecurity requirements for related cybersecurity goals. Table G.19 an shows example of cybersecurity requirements and their allocation in accordance with [RQ-09-10] and [RQ-09-11].

Table G.19 - Example of cybersecurity requirements and their allocation including CAL created by Company A

No.	Threat Scenario	Attack Path No.	Attack Path	Cyber Security Goal	CAL (Opt)	Cybersecurity Requirement		CAL Allocation (Opt)
						Description	Allocation	
T.x	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	AP.x	An attacker compromise Navigation ECU from Cellular interface	"Lamp switch on request integrity shall be protected against spoofing."	CAL4	Verify the received data if it is sent from valid entity	Navigation ECU	-
						Prevent unauthenticated entities from accessing to the cellular network.	Cellular network (operational environment)	-
			Compromised Navigation ECU transmits malicious control signals			Detect malicious control signals, and prevent them from being transmitted	Navigation	-
			Gateway ECU forward the malicious control signals to Power Switch Actuator			Detect malicious control signals and drop them.	Gateway	CAL4
			The malicious signals spoof the lamp switch on request			Detect spoofing "Lamp switch on request" by verifying its MAC and drop it.	Power Switch	-
						Generate a MAC for a "Lamp switch on request" and send it with its MAC.	Body Control ECU	-

DRAFT

		AP.y	…			…	…	…
		AP.z	…			…	…	…
		:	:			:	:	:
	:	:	:	:	:	:	:	:

G.3.2 Product Development

This subclause shows examples of product development in accordance with Clause 10 focusing on the Gateway ECU in the item as shown in Figure G.6. Example cybersecurity requirements for the Gateway ECU is shown in Table G.20.

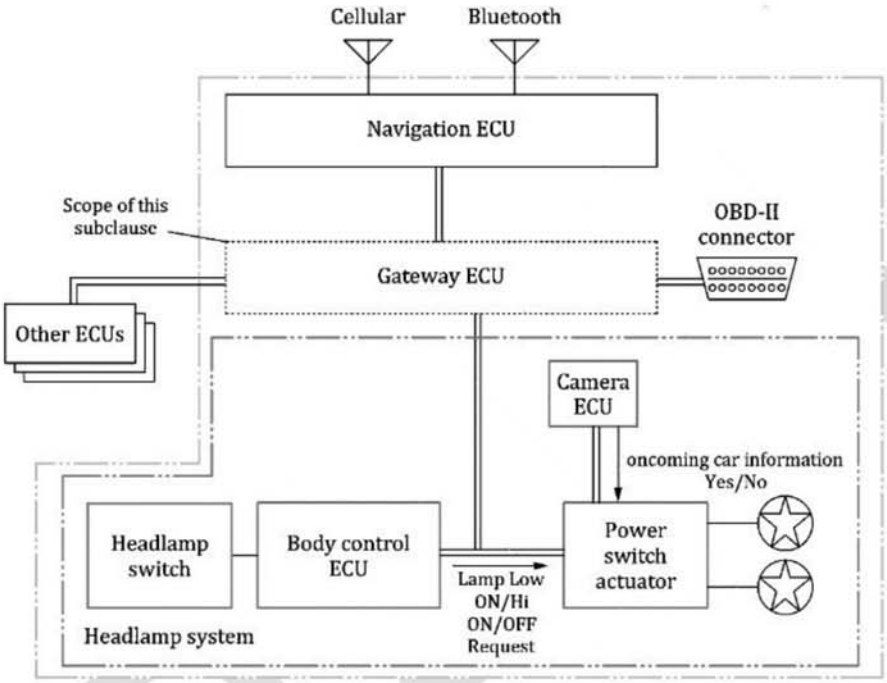


Figure G.6 - Scope of the subclause G.3.2

Table G.20 - Example cybersecurity requirements for the Gateway ECU

Example Cybersecurity Requirement	CAL Allocation (Opt)
Detect malicious control signals and drop them.	CAL4
:	:

G.3.2.1 Refinement of Cybersecurity Requirements and Architectural Design

Cybersecurity requirements and architectural design are refined in accordance with 10.4.1. In order to comply with the cybersecurity requirements allocated to the gateway ECU (see Table G.20), filtering by a white list is selected as a cybersecurity control. The refined cybersecurity requirement in consideration of the cybersecurity control is as follows:

- "Any signals from the Navigation ECU to the Headlamp system except for signals in a white list shall not be transferred. (CAL4)"

Architectural design is refined in consideration of this refined cybersecurity requirement and the preliminary architecture defined in concept phase. In this use case, this refined cybersecurity requirement is allocated to LUT (Look up table) that is a component of the gateway ECU as shown in Figure G.7.

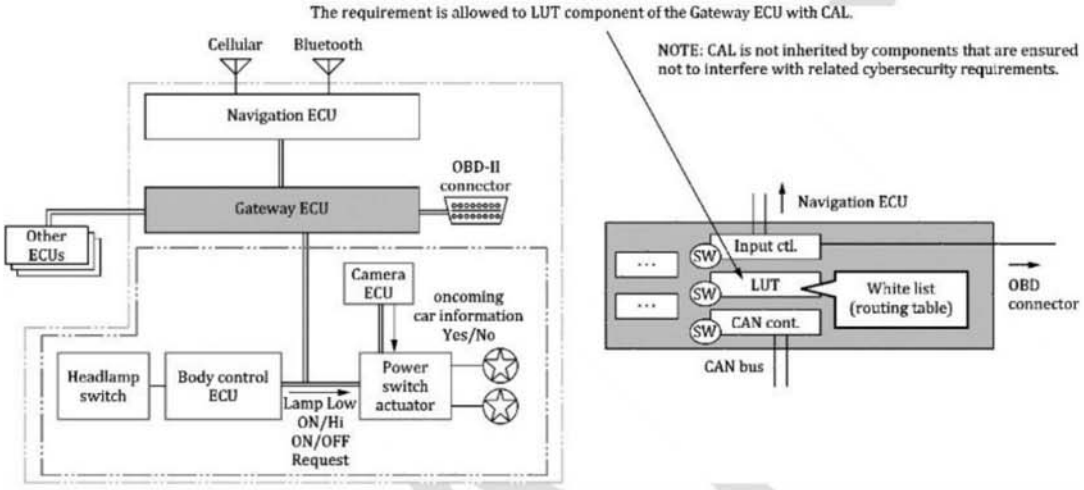


Figure G.7 - Architecture of gateway ECU and allocation of a cybersecurity requirement

The architectural design is verified by the method indicated in Table E.3 CAL4. In this example, no vulnerabilities are found by the vulnerability analysis.

G.3.2.2 Integration and Verification

The Gateway ECU is integrated and verified in accordance with 10.4.2. The implementation of the design and the integration of the Gateway ECU is verified using the methods and/or criteria indicated by Table E. through Table E.8 in Annex E for CAL4, which is the CAL of the Gateway ECU. In this example, a vulnerability is found by penetration testing indicated by Table E.8 for CAL4. After finding the vulnerability, vulnerability management is performed in accordance with 7.6. In this example, based on 7.6, attack path analysis in accordance with 8.6 and attack feasibility rating in accordance with 0 are performed. Table G.21 shows the example result of attack feasibility rating in accordance with I.3.

Table G.21 - Example result of attack feasibility rating based on attack potential-based approach

Parameters	Value
Elapsed Time	4
Specialist Expertise	3
Knowledge of the item (or component)	3
Window of Opportunity	4
Equipment	4
Total	18

According to I.3, the total value is mapped to attack feasibility: Medium. Then vulnerability management is continued.

ANNEX H
(INFORMATIVE)
IMPACT RATING FOR SAFETY, FINANCIAL, OPERATIONAL AND PRIVACY DAMAGE

H.1 PURPOSE

This annex gives examples of criteria for impact rating (see 8.5) for damage scenarios involving safety, financial, operational and privacy damage. The tables (see Table H.1 through Table H.4) in this annex can be used for impact rating for the road user as the primary stakeholder.

H.2 IMPACT RATING FOR SAFETY DAMAGE

Table H.1 - 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

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

Controllability according to ISO 26262-3:2018 can also be considered for calculating impact on safety, if a rationale is provided.

H.3 IMPACT RATING FOR FINANCIAL DAMAGE

Table H.2 - Financial impact rating criteria

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

H.4 IMPACT RATING FOR OPERATIONAL DAMAGE

Table H.3 - Operational impact rating criteria

Impact Rating	Criteria for Operational Impact Rating
Severe	The operational damage leads to a vehicle not working, from non-intended operation up to the vehicle being non-operational.
Major	The operational damage leads to the loss of a vehicle function.
Moderate	The operational damage leads to partial degradation of a vehicle function or performance.
Negligible	The operational damage leads to no effect or indiscernible degradation of a vehicle function or performance.

DRAFT

H.5 IMPACT RATING FOR PRIVACY DAMAGE

Table H.4 - 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. In this case, 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. In this case, 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 significant inconveniences to the road user. In this case, 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 can create few inconveniencies to the road user. In this case, the information regarding the road user is not sensitive and difficult to link to a PII principal.

Personally identifiable information (PII) and PII principal are according to ISO/IEC 29100[12].

DRAFT

ANNEX I
(INFORMATIVE)
GUIDELINES FOR DETERMINING ATTACK FEASIBILITY RATING

I.1 PURPOSE

Subclause 8.7 defines four levels for attack feasibility, which are further described in I.2.

This annex also provides guidelines on how the following approaches can be used for attack feasibility rating (see [RC-08-02]):

- attack potential based;
- CVSS based; and
- attack vector based.

I.2 ATTACK FEASIBILITY LEVELS AND THE RESPECTIVE CRITERIA

Table I.1 provides criteria related to each attack feasibility level.

Table I.1 - Attack feasibility levels and the respective criteria

Level	Description
High	**Highly feasible utilizing minimal effort:** It is easy or almost certain to accomplish the attack path.
Medium	**Quite feasible utilizing moderate effort:** It is feasible and not unusual to accomplish the attack path.
Low	**Conceivably feasible utilizing significant effort:** It is feasible to accomplish the attack path.
Very low	**Mostly infeasible utilizing reasonable effort:** It is difficult or almost never possible to accomplish the attack path.

I.3 GUIDELINE FOR THE ATTACK POTENTIAL-BASED APPROACH

Attack potential, as defined in ISO/IEC 18045[8], is 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, expertise, equipment, knowledge of the item or component, window of opportunity. This section gives examples of the customization and example mappings to attack feasibility.

I.3.1 Example of Adaptation of the Parameters

I.3.1.1 Example of Customization of Elapsed Time

The elapsed time scale 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 I.2.

Table I.2 - Elapsed time

< 1 week
< 1 month
<= 6 months
<= 3 years
> 3 years

DRAFT

I.3.1.2 Example of Customization of Expertise

The expertise is related to the capabilities of the attacker, relative to their skill and experience, see Table I.3.

Table I.3 - Expertise

Layman: Unknowledgeable compared to experts or proficient persons, with no particular expertise. EXAMPLE: Ordinary person using step-by-step descriptions of an attack that is publicly available.
Proficient: Knowledgeable in that they are familiar with the security behavior of the product or system type. EXAMPLE: 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 behavior, 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: Experienced technician or engineer.
Multiple Experts: is introduced to allow for a situation, where different fields of expertise are required at an Expert level for distinct steps of an attack. EXAMPLE: Multiple highly experienced engineers who have expertise in different fields, and which are required at an expert level for distinct steps of an attack.

I.3.1.3 Example of Customization of Knowledge of the Item or Component

The knowledge of the item or component is related to the amount of information the attacker has acquired about the item or component, see Table I.4.

Table I.4 - Knowledge of the item or component

Public information: Public information concerning the item or component (e.g., as gained from the Internet). EXAMPLE: Information and documents published on the product homepage or on an internet forum.
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: 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: 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: Customer specific calibrations or memory maps documented internally by the manufacturer and/or supplier.

DRAFT

I.3.1.4 Example of Customization of Window of Opportunity

The window of opportunity is related to the possible success when mounting 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 countermeasures, etc.; see Table I.5.

Table I.5 - 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: Attack is carried out remotely (e.g., vehicle-to-anything or cellular interfaces) without need for any preconditions.
Easy: High availability and limited access time. Remote access without physical presence, as well as limited physical access to the item or component. EXAMPLE: Attacker enters an unlocked car and got access to exposed physical interface, e.g., physical access via on-board diagnostic port, or a 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: Physically opening screws of an ECU to access deep internals to manipulate flash memory.
Difficult Very low availability of the item or component. Impractical level of access to the item or component to perform the attack. EXAMPLE: There are typically (statistically) no sufficient opportunity window to perform the attack.

I.3.1.5 Example of Customization of Equipment

The equipment is related to the tools the attacker has available to execute the attack, see Table I.6.

Table I.6 - Equipment

Standard: Equipment is readily available to the attacker, either for the identification of a vulnerability or to mount an attack. This equipment may 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 analyzer or simple attack scripts). EXAMPLE: Laptop, CAN adapter, on-board diagnostic dongles, 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: Specialized hardware debugging device, in-vehicle communication devices (e.g., hardware in the loop test rig, high-grade oscilloscope, signal generator, special chemicals).
Bespoke: Equipment is not readily available to the public (e.g., black market) as it may need to be specially produced (e.g., very sophisticated software), or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive. EXAMPLE: 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.

DRAFT

I.3.2 Guideline for Mapping Between Attack Potential and Attack Feasibility

For each parameter, numerical values can be defined. Based on the ISO/IEC 18045[8], the following scales are proposed based on the adaptation presented above, see Table I.7.

Table I.7 - 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 week	0	Layman	0	Public	0	Unlimited	0	Standard	0
< 1 month	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
< 6 months	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
<= 3 years	10	Multiple experts	8	Strictly Confidential	11	Difficult/None	10	Multiple bespoke	9
> 3 years	19								

According to ISO/IEC 18045[8], attack potential corresponds to the addition of all parameters. Attack feasibility is mapped according to Table I.8:

Table I.8 - Example attack potential mapping

Values	Attack Feasibility
0 - 9	High
10 - 13	
14 - 19	Medium
20 - 24	Low
=> 25	Very low

I.4 GUIDELINE FOR THE CVSS BASED APPROACH

To rate information technology security vulnerabilities, the CVSS maintained by the Forum of Incident Response and Security Teams (FIRST) can be used. Within the so-called base metrics group, the exploitability metrics of version 3 can be used to rate threat and attack feasibility. Other CVSS metrics like the impact metrics are covered by aspects of this document like damage scenarios and impact assessment.

The exploitability metrics are:

a) attack vector;

b) attack complexity;

c) privileges required; and

d) user interaction.

They are described by FIRST, refer to [25]. 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 (refer to [25], CVSS 3.0, 8.1):

$$E = 8.22 \times V \times C \times P \times U$$

DRAFT

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 qualitative mapping of CVSS exploitability values to attack feasibility, according to 0 is given in Table I.9. This is an example of equidistant exploitability steps.

Table I.9 - Example CVSS exploitability mapping

CVSS Exploitability Value	Qualitative Exploitability/ Attack Feasibility Rating	Attack Feasibility
0.12 - 1.05	Very low	1
1.06 - 1.99	Low	2
2.00 - 2.95	Medium	3
2.96 - 3.89	High	4

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 according to this document the missing Impact metric can be compensated by the impact metrics of this document, see 8.5 and Annex H.

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.

If changes to the metrics values are made, a rationale is provided.

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

I.5 GUIDELINE FOR THE ATTACK VECTOR-BASED APPROACH

This metric 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 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 I.10.

DRAFT

Table I.10 - Attack vector based approach

Attack Feasibility Rating	Determination Criteria
High	**Network**: Potential attack path is bound to network stack without any limitation. EXAMPLE: Potential attack surface is a cellular network connection.
Medium	**Adjacent:** Potential attack path is bound to network stack; however, the connection is limited physically or logically. EXAMPLE: Bluetooth interfaces, virtual private network connections.
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: Universal serial bus mass storage devices, memory cards.
Very low	**Physical**: Threat agents require physical access to realize the attack path.

DRAFT

ANNEX J
(INFORMATIVE)
MATRICES FOR RISK DETERMINATION

J.1 PURPOSE

The determination of risk values described in this document is compatible with IEC 31010[17]. This document uses an ordinal scale of risk values of 1, 2, 3, 4, and 5, where 1 represents minimal risk and 5 the highest risk. The mapping of the associated impact and attack feasibility for a threat scenario to a risk value is up to the organization (e.g., via risk matrix).

J.2 APPLICATION SCENARIOS

A risk matrix is a representation of a mapping of levels of impact and attack feasibility respectively on given scales to risk values. For example, risk matrices see Table J.1 through Table J.3.

The purpose of the determination of a risk value can be one of the following:

- to support criteria for decisions on risk treatment, incl. selection of controls;
- prioritization of risks for treatment;
- report to stakeholders; and
- monitoring of risk.

The organization can define appropriate risk matrices according to their specific needs and purposes (e.g., different matrices for different damage categories).

NOTE: The determination of a risk value does not immediately imply an evaluation concerning the acceptability of the risk. This can be influenced by further aspects that might not be represented in the assignment of the risk value as such for example specific constraints, or trade-offs with respect to other risks.

J.3 EXAMPLE RISK MATRICES

Table J.1 - Risk matrix example (symmetric)

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

DRAFT

Table J.2 - Risk matrix example (asymmetric)

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

Table J.3 - Risk matrix example (low risk profile)

		Attack Feasibility			
		Very Low	Low	Medium	High
Impact	Severe	**1**	**2**	**3**	**3**
	Major	**1**	**2**	**2**	**3**
	Moderate	**1**	**1**	**2**	**2**
	Negligible	**1**	**1**	**1**	**1**

DRAFT

BIBLIOGRAPHY

[1] ISO 26262 (all parts), *Road vehicles - Functional safety*

[2] ISO 29147, *Information technology - Security techniques - Vulnerability disclosure*

[3] ISO 9001, *Quality management systems - Requirements*

[4] ISO 12207, *Systems and software engineering - Software life cycle processes*

[5] ISO 10007, *Quality management - Guidelines for configuration management*

[6] ISO/IEC 2382:2015, *Information technology - Vocabulary* [online]. Available at: https://www.iso.org/obp/ui#iso:std:iso-iec:2382:ed-1:v1:en

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

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

[9] ISO/IEC 27000, *Information technology - Security techniques - Information security management systems - Overview and vocabulary*

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

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

[12] ISO/IEC 29100, *Information technology - Security techniques - Privacy framework*

[13] ISO/IEC 33001, *Information technology - Process assessment - Concepts and terminology*

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

[15] ISO/IEC/IEEE 26511:2011, *Systems and software engineering - Requirements for managers of user documentation*

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

[17] IEC 31010, *Risk management - Risk assessment techniques*

[18] IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures*

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

[20] NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments* [online]. Available at: http://dx.doi.org/10.6028/NIST.SP.800-30r1

[21] NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* [online]. Available at: https://doi.org/10.6028/NIST.SP.800-115

[22] NIST SP 800-150, *Guide to Cyber Threat Information Sharing* [online]. Available at: https://doi.org/10.6028/NIST.SP.800-150

[23] NIST SP 800-160 Vol.1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [online]. Available at: https://doi.org/10.6028/NIST.SP.800-160v1

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

[25] FIRST Common Vulnerability Scoring System (CVSS), *Common Vulnerability Scoring System,* [online]. Available at https://www.first.org/cvss/

[26] FIRST Traffic Light Protocol (TLP), *FIRST Standards Definitions and Usage Guidance - Version 1.0*, [online]. Available at: https://www.first.org/tlp/

[27] Automotive SPICE, *Process Reference Model, Process Assessment Model, Version 3.0* [online]. Available at: http://www.automotivespice.com/fileadmin/software-download/Automotive_SPICE_PAM_30.pdf

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

DRAFT