INTERNATIONAL STANDARD

ISO/SAE 21434

First edition
2021-08

Road vehicles — Cybersecurity engineering

Véhicules routiers — Ingénierie de la cybersécurité

Reference number
ISO/SAE 21434:2021(E)

COPYRIGHT PROTECTED DOCUMENT

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

Email: copyright@iso.org
Website: www.iso.org

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

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

Foreword

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

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

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

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

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

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

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

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

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

The main changes are as follows:

— complete rework of contents and structure.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html. Alternatively, to provide feedback on this document, please visit https://www.sae.org/standards/content/ISO/SAE 21434/.

Introduction

Purpose of this document

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

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

— define cybersecurity policies and processes;

— manage cybersecurity risk; and

— foster a cybersecurity culture.

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

Organization of this document

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

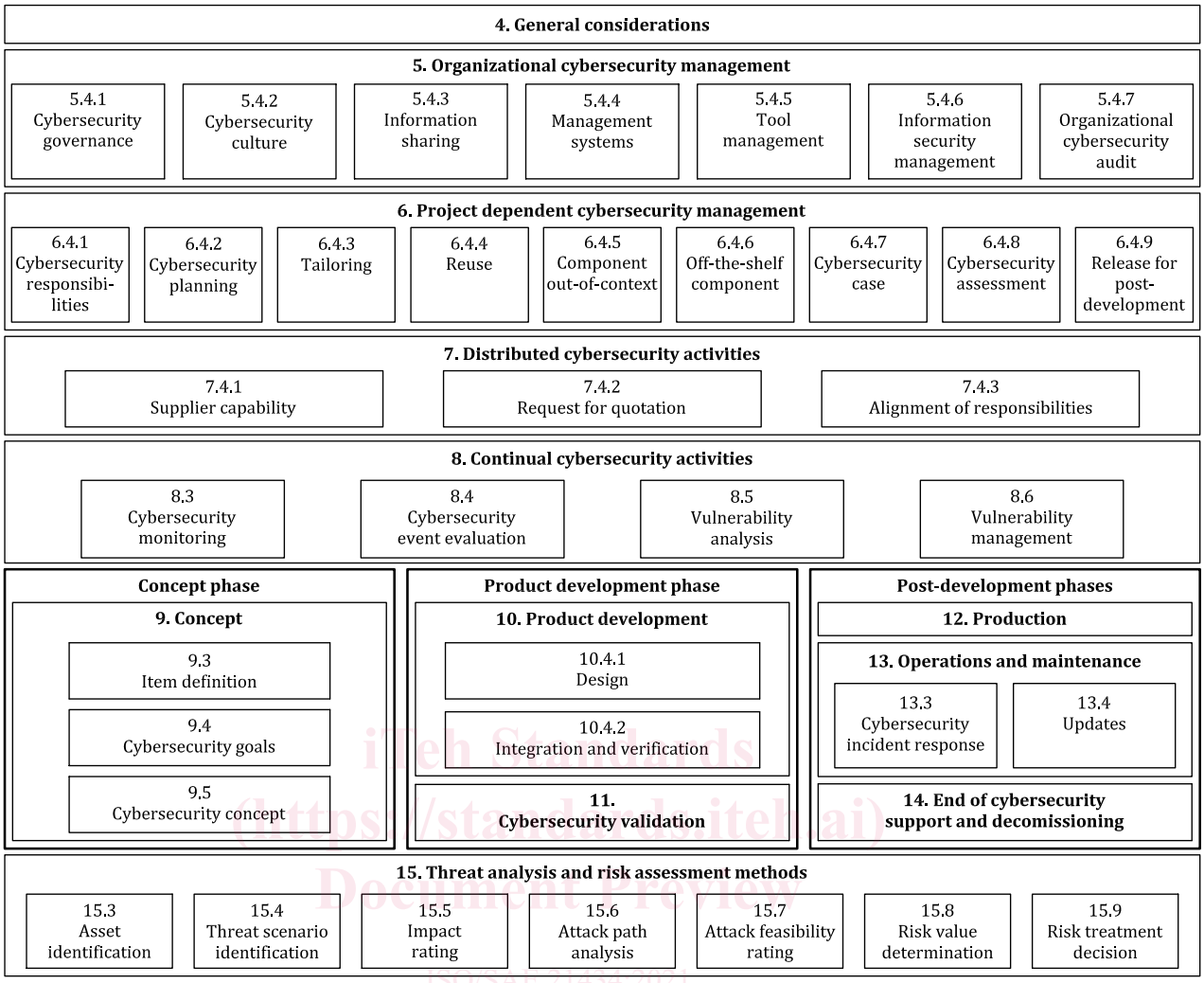

Figure 1 — Overview of this document

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Road vehicles — Cybersecurity engineering

1 Scope

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

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

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

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

2 Normative references

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

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

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

ISO Online browsing platform: available at https://www.iso.org/obp

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

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

3.1.2
asset
object that has value, or contributes to value

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

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

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

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

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

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

3.1.7
component
part that is logically and technically separable

3.1.8
customer
person or organization that receives a service or product

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

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

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

3.1.10
cybersecurity assessment
judgement of *cybersecurity* (3.1.9)

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

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

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

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

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

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

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

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

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

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

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

3.1.20
cybersecurity property
attribute that can be worth protecting

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

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

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

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

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

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

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

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

3.1.26
operational environment
context considering interactions in operational use

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

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

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

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

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

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

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

3.1.31
road user
person who uses a road

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

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

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

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

3.1.35
trigger
criterion for *triage* (3.1.34)

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

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

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

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

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

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

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

3.1.40
weakness
defect or characteristic that can lead to undesirable behaviour

EXAMPLE 1 Missing requirement or specification.

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

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

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

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

3.2 Abbreviated terms

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

4 General considerations

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

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

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

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

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

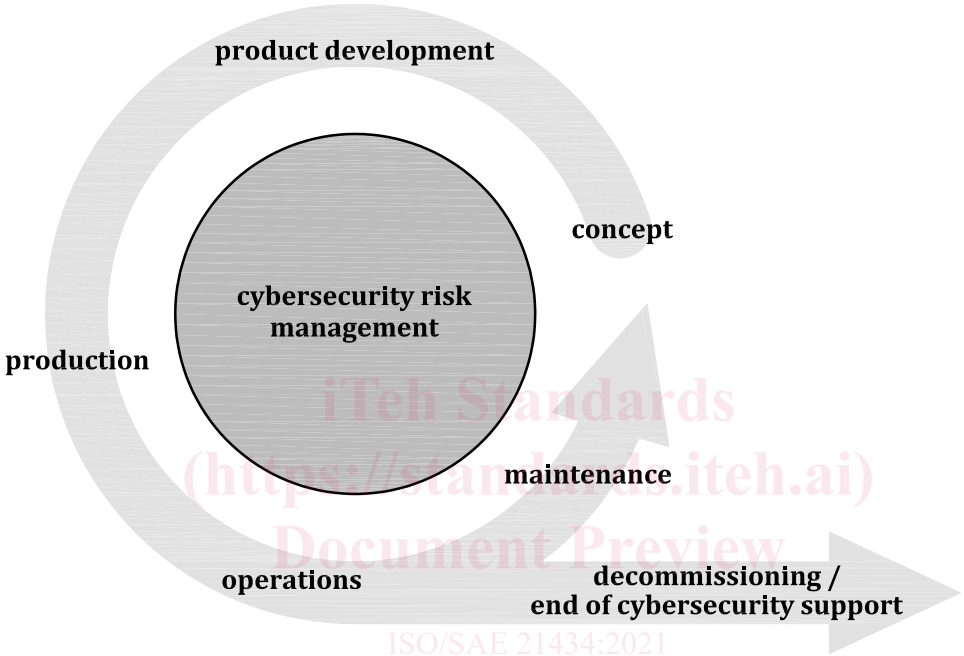

Figure 2 — Overall cybersecurity risk management

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

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

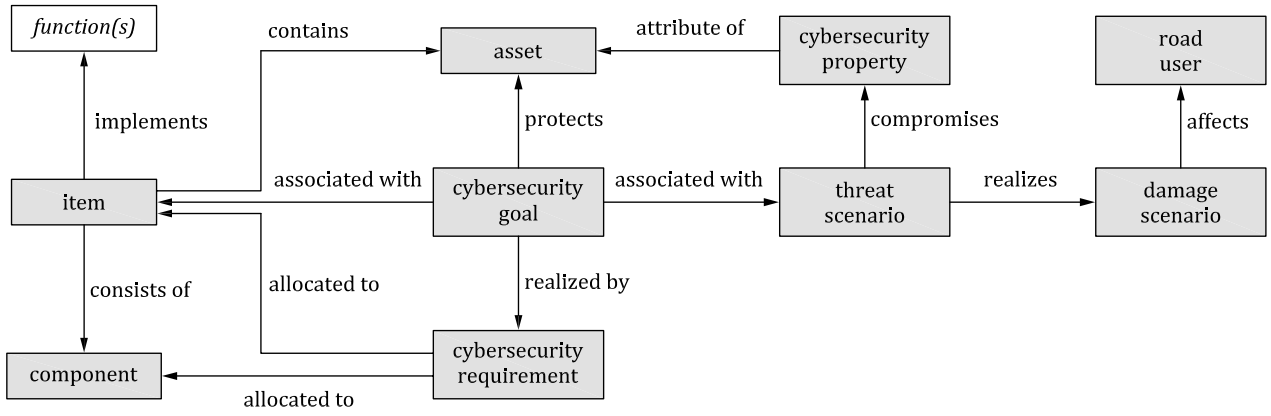

Figure 3 — Relationship between item, function, component and related terms

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

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

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

5 Organizational cybersecurity management

5.1 General

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

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

5.2 Objectives

The objectives of this clause are to:

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

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

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

d) manage the cybersecurity risk;

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

f) support and manage the sharing of cybersecurity information;

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

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

i) perform an organizational cybersecurity audit.

5.3 Inputs

5.3.1 Prerequisites

None.

5.3.2 Further supporting information

The following information can be considered:

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

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

5.4 Requirements and recommendations

5.4.1 Cybersecurity governance

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

a) acknowledgement of road vehicle cybersecurity risks; and

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

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

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

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

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

b) support the execution of the corresponding activities.

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

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

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

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

---

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

