

FINAL  
DRAFT

INTERNATIONAL  
STANDARD

ISO/SAE  
FDIS  
21434

ISO/TC 22/SC 32

Secretariat: JISC

Voting begins on:  
**2021-05-12**

Voting terminates on:  
**2021-07-07**

---

---

## Road vehicles — Cybersecurity engineering

*Véhicules routiers — Ingénierie de la cybersécurité*

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/SAE FDIS 21434](https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-fdis-21434)

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-fdis-21434>

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.



Reference number  
ISO/SAE FDIS 21434:2021(E)

© ISO/SAE International 2021

## iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/SAE FDIS 21434

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-fdis-21434>



### **COPYRIGHT PROTECTED DOCUMENT**

© ISO/SAE International 2021

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

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

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

Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

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

# Contents

	Page
<b>Foreword</b> .....	<b>vii</b>
<b>Introduction</b> .....	<b>viii</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms, definitions and abbreviated terms</b> .....	<b>1</b>
3.1 Terms and definitions.....	1
3.2 Abbreviated terms.....	5
<b>4 General considerations</b> .....	<b>5</b>
<b>5 Organizational cybersecurity management</b> .....	<b>7</b>
5.1 General.....	7
5.2 Objectives.....	7
5.3 Inputs.....	8
5.3.1 Prerequisites.....	8
5.3.2 Further supporting information.....	8
5.4 Requirements and recommendations.....	8
5.4.1 Cybersecurity governance.....	8
5.4.2 Cybersecurity culture.....	9
5.4.3 Information sharing.....	10
5.4.4 Management systems.....	10
5.4.5 Tool management.....	11
5.4.6 Information security management.....	11
5.4.7 Organizational cybersecurity audit.....	11
5.5 Work products.....	12
<b>6 Project dependent cybersecurity management</b> .....	<b>12</b>
6.1 General.....	12
6.2 Objectives.....	13
6.3 Inputs.....	14
6.3.1 Prerequisites.....	14
6.3.2 Further supporting information.....	14
6.4 Requirements and recommendations.....	14
6.4.1 Cybersecurity responsibilities.....	14
6.4.2 Cybersecurity planning.....	14
6.4.3 Tailoring.....	15
6.4.4 Reuse.....	15
6.4.5 Component out-of-context.....	17
6.4.6 Off-the-shelf component.....	17
6.4.7 Cybersecurity case.....	17
6.4.8 Cybersecurity assessment.....	17
6.4.9 Release for post-development.....	19
6.5 Work products.....	19
<b>7 Distributed cybersecurity activities</b> .....	<b>20</b>
7.1 General.....	20
7.2 Objectives.....	20
7.3 Inputs.....	20
7.4 Requirements and recommendations.....	20
7.4.1 Supplier capability.....	20
7.4.2 Request for quotation.....	21
7.4.3 Alignment of responsibilities.....	21
7.5 Work products.....	22
<b>8 Continual cybersecurity activities</b> .....	<b>22</b>
8.1 General.....	22

8.2	Objectives.....	22
8.3	Cybersecurity monitoring.....	22
8.3.1	Inputs.....	22
8.3.2	Requirements and recommendations.....	23
8.3.3	Work products.....	23
8.4	Cybersecurity event evaluation.....	24
8.4.1	Inputs.....	24
8.4.2	Requirements and recommendations.....	24
8.4.3	Work products.....	24
8.5	Vulnerability analysis.....	24
8.5.1	Inputs.....	24
8.5.2	Requirements and recommendations.....	25
8.5.3	Work products.....	25
8.6	Vulnerability management.....	25
8.6.1	Inputs.....	25
8.6.2	Requirements and recommendations.....	26
8.6.3	Work products.....	26
<b>9</b>	<b>Concept.....</b>	<b>26</b>
9.1	General.....	26
9.2	Objectives.....	26
9.3	Item definition.....	27
9.3.1	Inputs.....	27
9.3.2	Requirements and recommendations.....	27
9.3.3	Work products.....	27
9.4	Cybersecurity goals.....	28
9.4.1	Inputs.....	28
9.4.2	Requirements and Recommendations.....	28
9.4.3	Work products.....	29
9.5	Cybersecurity concept.....	29
9.5.1	Inputs.....	29
9.5.2	Requirements and recommendations.....	29
9.5.3	Work products.....	30
<b>10</b>	<b>Product development.....</b>	<b>30</b>
10.1	General.....	30
10.2	Objectives.....	31
10.3	Inputs.....	32
10.3.1	Prerequisites.....	32
10.3.2	Further supporting information.....	32
10.4	Requirements and recommendations.....	32
10.4.1	Design.....	32
10.4.2	Integration and verification.....	34
10.5	Work products.....	35
<b>11</b>	<b>Cybersecurity validation.....</b>	<b>36</b>
11.1	General.....	36
11.2	Objectives.....	36
11.3	Inputs.....	36
11.3.1	Prerequisites.....	36
11.3.2	Further supporting information.....	36
11.4	Requirements and recommendations.....	36
11.5	Work products.....	37
<b>12</b>	<b>Production.....</b>	<b>37</b>
12.1	General.....	37
12.2	Objectives.....	37
12.3	Inputs.....	37
12.3.1	Prerequisites.....	37
12.3.2	Further supporting information.....	37

12.4	Requirements and recommendations.....	37
12.5	Work products.....	38
<b>13</b>	<b>Operations and maintenance.....</b>	<b>38</b>
13.1	General.....	38
13.2	Objectives.....	38
13.3	Cybersecurity incident response.....	38
13.3.1	Inputs.....	38
13.3.2	Requirements and recommendations.....	39
13.3.3	Work products.....	40
13.4	Updates.....	40
13.4.1	Inputs.....	40
13.4.2	Requirements and recommendations.....	40
13.4.3	Work products.....	40
<b>14</b>	<b>End of cybersecurity support and decommissioning.....</b>	<b>40</b>
14.1	General.....	40
14.2	Objectives.....	40
14.3	End of cybersecurity support.....	41
14.3.1	Inputs.....	41
14.3.2	Requirements and recommendations.....	41
14.3.3	Work products.....	41
14.4	Decommissioning.....	41
14.4.1	Inputs.....	41
14.4.2	Requirements and recommendations.....	41
14.4.3	Work products.....	41
<b>15</b>	<b>Threat analysis and risk assessment methods.....</b>	<b>41</b>
15.1	General.....	41
15.2	Objectives.....	42
15.3	Asset identification.....	42
15.3.1	Inputs.....	42
15.3.2	Requirements and recommendations.....	43
15.3.3	Work products.....	43
15.4	Threat scenario identification.....	43
15.4.1	Inputs.....	43
15.4.2	Requirements and recommendations.....	44
15.4.3	Work products.....	44
15.5	Impact rating.....	44
15.5.1	Inputs.....	44
15.5.2	Requirements and recommendations.....	44
15.5.3	Work products.....	45
15.6	Attack path analysis.....	45
15.6.1	Inputs.....	45
15.6.2	Requirements and recommendations.....	46
15.6.3	Work products.....	46
15.7	Attack feasibility rating.....	46
15.7.1	Inputs.....	46
15.7.2	Requirements and Recommendations.....	47
15.7.3	Work products.....	48
15.8	Risk value determination.....	48
15.8.1	Inputs.....	48
15.8.2	Requirements and recommendations.....	48
15.8.3	Work products.....	48
15.9	Risk treatment decision.....	49
15.9.1	Inputs.....	49
15.9.2	Requirements and recommendations.....	49
15.9.3	Work products.....	49
<b>Annex A</b>	<b>(informative) Summary of cybersecurity activities and work products.....</b>	<b>50</b>

<b>Annex B</b> (informative) <b>Examples of cybersecurity culture</b> .....	<b>52</b>
<b>Annex C</b> (informative) <b>Example of Cybersecurity interface agreement template</b> .....	<b>54</b>
<b>Annex D</b> (informative) <b>Cybersecurity relevance – example methods and criteria</b> .....	<b>56</b>
<b>Annex E</b> (informative) <b>Cybersecurity assurance levels</b> .....	<b>58</b>
<b>Annex F</b> (informative) <b>Guidelines for impact rating</b> .....	<b>63</b>
<b>Annex G</b> (informative) <b>Guidelines for attack feasibility rating</b> .....	<b>65</b>
<b>Annex H</b> (informative) <b>Examples of application of TARA methods – headlamp system</b> .....	<b>71</b>
<b>BIBLIOGRAPHY</b> .....	<b>79</b>

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

ISO/SAE FDIS 21434

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-fdis-21434>

## 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](http://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](http://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](http://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.

The main changes compared to SAE J3061:2016 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](http://www.iso.org/members.html). Alternatively, to provide feedback on this document, please visit <http://standards.sae.org/PRODCODE>.

## 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.

ITEH STANDARD PREVIEW  
(standards.iteh.ai)

[ISO/SAE FDIS 21434](#)

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-fdis-21434>



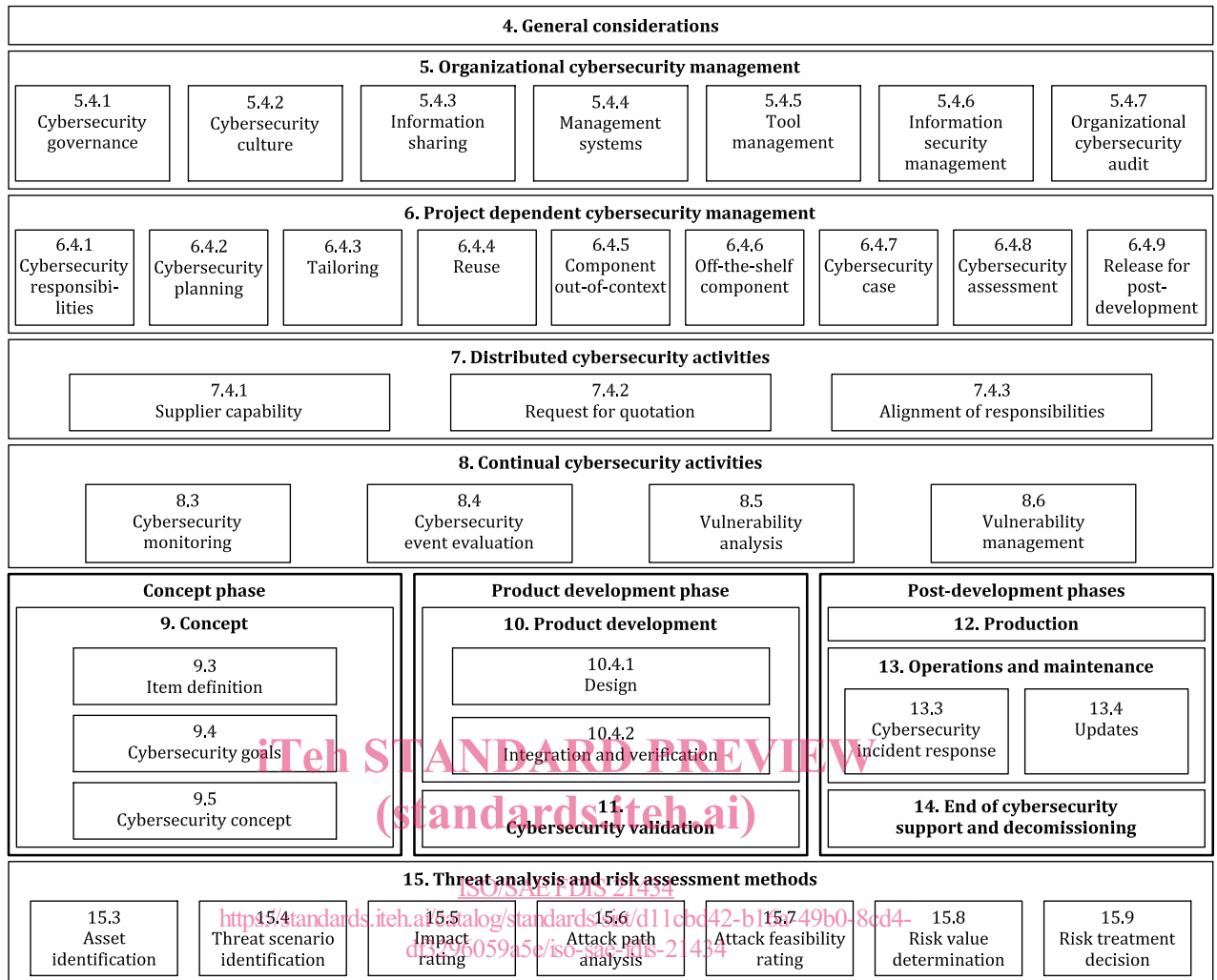


Figure 1 — Overview of this document

[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 for an item cybersecurity risks, cybersecurity goals and cybersecurity requirements.

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

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

## ISO/SAE FDIS 21434:2021(E)

[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 input 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-05-15] refers to the 15th provision in [Clause 5](#), which is a requirement.

(standards.iteh.ai)

ISO/SAE FDIS 21434

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-fdis-21434>

# 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

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-fdis-21434>

### 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 “that is intended for or required by this person or organization” was omitted, 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 for 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” and the note was added. The phrases “to which ISO 26262 is applied” and “or part of a function” have been omitted. The original note was omitted.]

**3.1.26****operational environment**

context considering interactions in operational use

Note 1 to entry: Operational use of an item 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.

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

3.1.32

**tailor**, verb

to omit or perform an activity in a different manner compared to its description in this document

ISO/SAE FDIS 21434  
<https://standards.iteh.ai/catalog/standards/sis/d11c0d42-816a-4960-8cd4-df3296059a5e/iso-sae-fdis-21434>

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) on a vehicle, that is 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