



DPC: 23 / 30456162 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 04 September 2023

Origin: International

Latest date for receipt of comments: 25 October 2023

Project No. 2022/01003

Responsible committee: GEL/9/-/6 Railway Electrotechnical Applications # Standards relating to Cybersecurity, Artificial Intelligence and Machine Learning

Interested committees:

Title: BS EN IEC 63452 Railway applications - Cybersecurity

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 25 October 2023**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **Mr Darren Fitzgerald (BSI)**
Direct tel: **020 3142 5300**
E-mail: **darren.fitzgerald@rssb.co.uk**

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

PROJECT NUMBER: IEC 63452 ED1	
DATE OF CIRCULATION: 2023-09-01	CLOSING DATE FOR COMMENTS: 2023-11-24
SUPERSEDES DOCUMENTS: 9/2810/NP, 9/2835/RVN	

IEC TC 9 : ELECTRICAL EQUIPMENT AND SYSTEMS FOR RAILWAYS	
SECRETARIAT: France	SECRETARY: Mr Denis MIGLIANICO
OF INTEREST TO THE FOLLOWING COMMITTEES: TC 65	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any local regulations or technical reasons that may exist and should be considered should this proposal proceed, recognizing that failure to address such requirements could result in the need for new or existing "In Some Countries" clauses. (See [AC/22/2007](#) or [NEW GUIDANCE DOC](#)).

TITLE:
Railway applications – Cybersecurity

NOTE FROM TC/SC OFFICERS:

Copyright © 2023 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

CONTENTS

FOREWORD	6
INTRODUCTION	8
1 Scope	10
2 Normative references	10
3 Terms and definitions, abbreviated terms and acronyms, taxonomy and terms equivalence	10
3.1 Terms and definitions	10
3.2 Abbreviated terms and acronyms.....	35
3.3 Taxonomy and terms equivalence.....	38
4 Railway system overview	41
4.1 Purpose	41
4.2 Overview.....	41
4.3 [SO-01-01]: Identification of the railway system	41
4.4 [SO-02-01]: Definition of a high-level railway system model	43
4.5 [SO-03-01]: Definition of a high-level railway zone model.....	44
4.6 [SO-04-01]: Specification of shared security services.....	47
5 Overall cybersecurity management	48
5.1 General.....	48
5.2 [CP-01-01] Railway OT cybersecurity program.....	48
5.3 [CP-02-01] Railway OT cybersecurity program coordination	48
5.4 [CP-03-01] Architecture considerations and constraints	49
5.5 [CP-04-01] Supply chain management.....	49
5.6 [CP-05-01] Awareness/training management	50
5.7 [CP-06-01] Inventory management	51
6 Cybersecurity within a railway application lifecycle.....	52
6.1 Purpose	52
6.2 Plan project cybersecurity activities.....	52
6.3 Railway application and product lifecycles	52
6.4 Cybersecurity activities mapping to the IEC 62278-1 lifecycle	53
6.5 Cybersecurity assurance activities.....	60
6.6 Cybersecurity and system development teams relationship	61
6.7 Interaction between cybersecurity and safety.....	62
7 Zoning and risk assessment.....	64
7.1 Purpose and outcome	64
7.2 Overview.....	64
7.3 Identify the SuC and its threat environment	67
7.4 Initial risk assessment.....	69
7.5 Partitioning of the SuC in zones and conduits	71
7.6 Detailed risk assessment.....	72
7.7 Railway duty holder approval.....	82
8 Cybersecurity requirements	83
8.1 Purpose	83
8.2 Input	83
8.3 Output	83
8.4 Outcome	83
8.5 System cybersecurity requirements definition	83
8.6 Requirement breakdown structure for verification.....	107
8.7 Apportionment of cybersecurity requirements	107

8.8	Compensating countermeasures	111
8.9	Shared cybersecurity services system requirements	113
9	Cybersecurity assurance	115
9.1	Purpose	115
9.2	Overview	115
9.3	Installation/Integration	115
9.4	System validation	118
9.5	System acceptance	120
10	Operational, maintenance and disposal requirements	122
10.1	Overview	122
10.2	[OM-01-01] Cybersecurity maintenance	123
10.3	[OM-01-02] Continuous cybersecurity assurance	123
10.4	[OM-02-01] Cybersecurity case update	123
10.5	[OM-03-01] Risk management	124
10.6	[OM-04-01] Vulnerability management	124
10.7	[OM-05-01] Patch management	128
10.8	[OM-06-01] Incident management	130
10.9	[OM-07-01] Business continuity management	132
10.10	[OM-08-01] Operations and maintenance management	132
10.11	[OM-09-01] Security monitoring	135
10.12	[OM-10-01] Decommissioning management	136
Annex A	(informative) Handling conduit	137
A.1	Introduction	137
A.2	Requirement for conduits in IEC 62443	138
A.3	Protection profiles for conduits	138
Annex B	(informative) Handling legacy systems	139
B.1	Introduction	139
B.2	Basic security risks	139
B.3	Basic process activities	140
B.4	Basic security countermeasures	142
Annex C	(informative) Cybersecurity design principles	145
C.1	Introduction	145
C.2	Secure the weakest link	145
C.3	Defence-in-depth	146
C.4	Fail secure	148
C.5	Grant least privilege	149
C.6	Economise mechanism	150
C.7	Authenticate requests	151
C.8	Control access	153
C.9	Assume secrets not safe	154
C.10	Make security usable	155
C.11	Promote privacy	156
C.12	Audit and monitor	157
C.13	Proportionality principle	158
C.14	Precautionary principle	159
C.15	Continuous protection	160
C.16	Secure metadata	161
C.17	Secure defaults	162
C.18	Trusted components	163
Annex D	(informative) Safety and cybersecurity	164

D.1	Introduction	164
D.2	The differences between safety and security	164
D.3	Security from a safety perspective	164
D.4	Co-engineering of safety and security	165
D.5	Quantification of security	166
D.6	The relationship between safety integrity levels and security levels	166
D.7	Responsibility for security	166
Annex E (informative) Risk acceptance methods		167
E.1	Introduction	167
E.2	Example based on IEC 62278-1	167
E.3	Example method – integration service provider	169
E.4	Example method – infrastructure manager	171
E.5	Example method – Product supplier	173
Annex F (informative) Railway system models and zone models		177
F.1	Design Guidance for system models	177
F.2	Magnifications of the high level zone model	179
F.3	Design Guidance for zone models	183
F.4	Train to ground communication	197
Annex G (informative) Cybersecurity deliverables content		198
G.1	Introduction	198
G.2	Cybersecurity management plan	198
G.3	Cybersecurity risk assessment report	199
G.4	Cybersecurity requirement specification	199
G.5	Cybersecurity guidelines	200
G.6	Cybersecurity verification and validation plan	201
G.7	Cybersecurity case	201
G.8	Cybersecurity maintenance plan	202
Annex H (informative) Cybersecurity roles and competence profiles		204
H.1	Purpose	204
H.2	Railway cybersecurity roles and competence profiles	205
Bibliography		219
Figure 1 - Overview of this document		9
Figure 2 - Railway system taxonomy		38
Figure 3 - Segregation between IT and OT		42
Figure 4 - Example of an area-based railway system model		43
Figure 5 - Example of a topology-based railway system model		44
Figure 6 - Example of a high-level railway zone model		46
Figure 7 - Example of shared security service		47
Figure 8 - IEC 62278-1 V-cycle representation		53
Figure 9 - Synchronisation between cybersecurity team and other stakeholders		55
Figure 10 - Relationship Threat Risk Assessment and Security Assurance		61
Figure 11 - Zoning and risk assessment flowchart		65
Figure 12 - Risk assessment flowchart with re-use		66
Figure 13 - Explicit risk evaluation flowchart		77
Figure 14 - Example of workflow of conflict resolution		111
Figure 15 - Handling of SL-C		112

Figure 16 - Overview of assurance activities and applicable requirements during phases 8 through 10 of the RAMS lifecycle.....	115
Figure 17: Overview of operational activities	122
Figure 18: Vulnerability flowchart.....	127
Figure 19 Cybersecurity incident management process	131
Table 1 - IEC 63452 to ISA/IEC 62443 equivalent terms.....	39
Table 2 - Railway system, application, solution and products examples	39

Yellow background marks open points, to dos.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

RAILWAY APPLICATIONS – CYBERSECURITY

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organisation for standardisation comprising all national electrotechnical committees (IEC National Committees). The objective of the IEC is to promote international co-operation on all questions concerning standardisation in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organisations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standards (ISO) in accordance with conditions determined by agreement between the two organisations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC IS 63452 has been prepared by subcommittee PT 63452, of IEC technical committee TC9 “Railway”. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
XX/XX/FDIS	XX/XX/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2:2021, and developed in accordance with ISO/IEC Directives, Part 1:2023 and ISO/IEC Directives, IEC Supplement:2023, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be either:

- Reconfirmed;
- Withdrawn;
- Replaced by a revised edition; or
- Amended.

INTRODUCTION

Purpose

This document addresses cybersecurity within the railway sector. It is an international standard (IS) that applies to all domains within the scope of the IEC TC9, including highspeed lines, mainlines, commuter, heavy and light metros and light rail systems such as tramways and monorails.

Due to digitisation and the need for improved performance and better maintainability, previously isolated industrial systems are now connected to large networks and use standard protocols and commercial components, increasing the potential attack surface and threats of cyber-attacks. Cybersecurity has therefore become a key topic for these industrial systems, including critical systems such as railway systems.

The purpose of this document is to set out requirements and recommendations that, if correctly applied, guarantee that the system under consideration (SuC) is appropriately cyber secured and that the achieved level of cybersecurity is maintained during its operation and maintenance.

This document intends to:

- provide requirements and guidance on cybersecurity activities and deliverables,
- be adaptable and applicable to various system lifecycles,
- be applicable for both safety and non-safety related systems,
- identify interfaces between cybersecurity and other disciplines contributing to railway system lifecycles,
- be compatible and consistent with IEC 62278 when it is applied to the system under consideration,
- separate safety approval and cybersecurity acceptance as much as possible, due to lifecycle differences between safety and cybersecurity,
- identify the key synchronisation points related to cybersecurity between the integration service provider and railway duty holder,
- provide a harmonised and standardised way to express technical cybersecurity requirements,
- provide cybersecurity design principles, promoting simple and modular systems,
- allow the usage of industrial commercial off-the-shelf (COTS) products compliant with the IEC 62443 series of standards without adding any specific railway cybersecurity requirements.

Organisation 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.

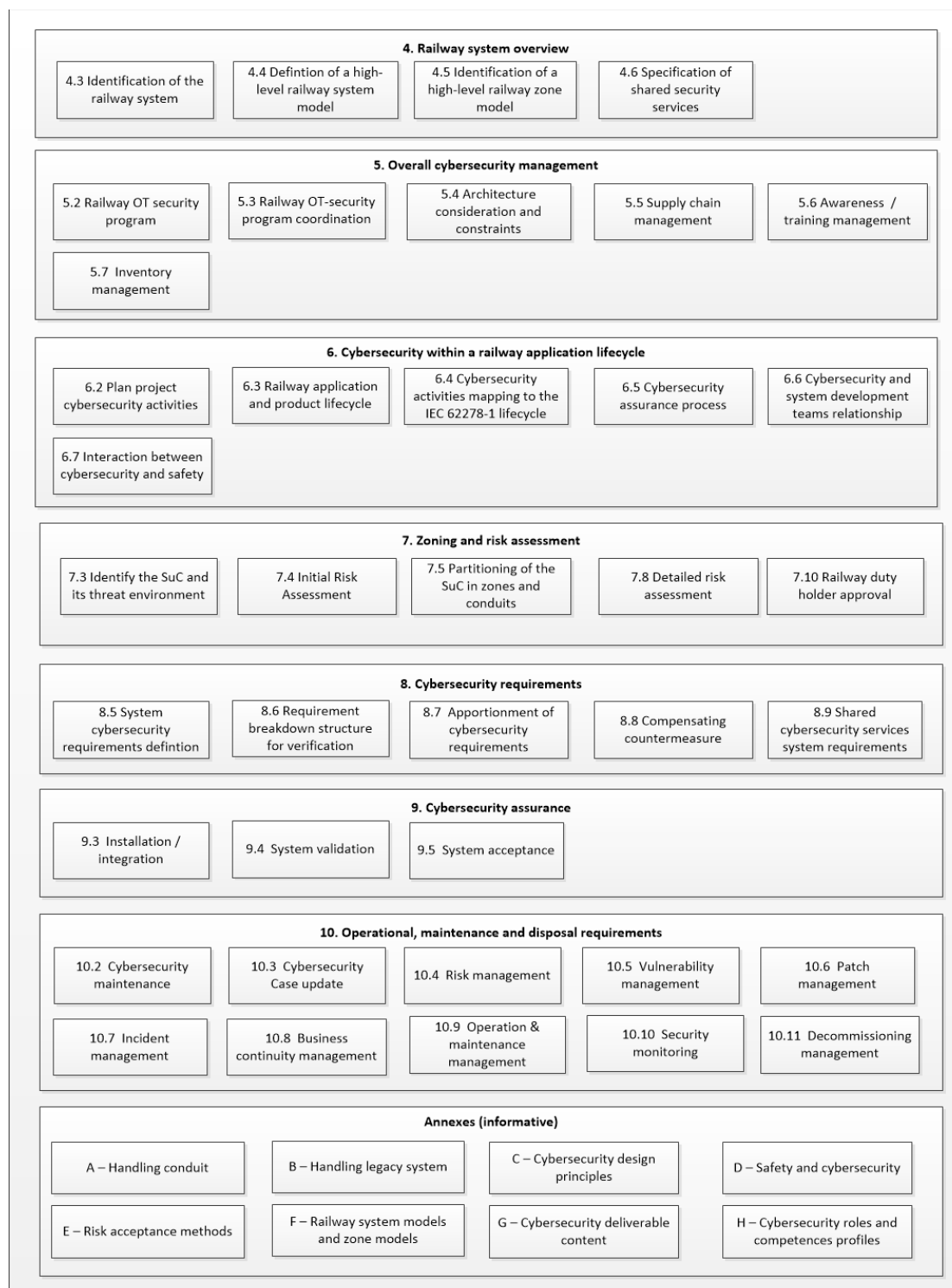


Figure 1 - Overview of this document

RAILWAY APPLICATIONS - CYBERSECURITY

1 Scope

This document provides a consistent approach to the management of the cybersecurity of the railway systems. It applies to all domains within the scope of IEC TC 9.

This document maps and adapts IEC 62443 series standards requirements to the railway application domain and operational environment and details how the requirements are applied in that context. It provides guidance on how the security process can be interfaced with the generic reliability, availability, maintainability and safety (RAMS) life cycle of the IEC 62278 series standards. By doing so, it defines synchronisation points between stakeholders and proposes responsibilities. It presents the underlying security assumptions in a structured manner and the criteria for application to other lifecycles is also provided.

This document is consistent with the application of security management requirements set out in IEC 62443-2-1:2010. It provides security models, security concepts and risk assessment process based on the IEC 62443 series standards and describes the typical expected content for cybersecurity deliverables. This ensures that the residual risks from security threats are identified, supervised and managed to a level that is acceptable to the railway undertaking and/or infrastructure manager.

This document aims to provide support and guidance to ensure a proper protection of the key stakes (such as safety, operation, financial, reputation, regulatory, social) of a railway SuC against cyber-attacks and unintended consequences of configuration or maintenance activities.

This document also provides guidance on the cybersecurity assurance of SuCs during build phase and provides recommendations for security management during operation and maintenance phases.

Finally, this document does not provide any safety requirements nor constraints on safety case for railway systems but provides guidance for relationship between cybersecurity and safety.

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.

IEC 62278:2002 Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS).

IEC 62443-3-2:2020, Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design

IEC 62443-3-3:2019, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

IEC 62443-2-1:2010, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program

3 Terms and definitions, abbreviated terms and acronyms, taxonomy and terms equivalence

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 standardisation at the following addresses:

— IEC Electropedia: available at <http://www.electropedia.org/>

— ISO Online Browsing Platform: available at <http://www.iso.org/obp>

3.1.1**acceptance****<for a product, system or process>**

status achieved by a product, system or process once it has been agreed that it is suitable for its intended purpose

[SOURCE: EN 50126-1:2017, 3.1]

3.1.2**access****<in cybersecurity>**

ability and means to communicate with or otherwise interact with a system in order to use system resources

Note 1 to entry: Access may involve physical access (authorisation to be allowed physically in an area, possession of a physical key lock, PIN code, or access card or biometric attributes that allow access) or logical access (authorisation to log in to a system and application, through a combination of logical and physical means).

3.1.3**access control**

protection of system resources against unauthorised access

[SOURCE: IEC 62443-4-1:2018, 3.1.2]

3.1.4**access point name**

in a network, a point at which the user may connect to the network

[SOURCE: Electropedia]

3.1.5**access control process**

process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy

Note 1 to entry: Access control includes identification and authentication requirements specified in other parts of the IEC 62443 series standards.

[SOURCE: IEC 62443-4-1:2018, 3.1.3 modified, “process” added]

3.1.6**accident**

unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage

[SOURCE: IEC 60050 821:2017, 821-12-02]

3.1.7**achieved security level**

measure of the security level achieved in the deployed security architecture, elsewhere, sometimes referred to as the “as-built” security level

Note 1 to entry: Actual security level will vary over time based on natural degradations, induced events and maintenance of security mechanisms.

3.1.8**air gapped network****<in cybersecurity>**

A network which is physically and logically isolated in a way, that no external unit, e.g. used for a cyber-attack, can address any internal unit of this network.

Note 1 to entry: It might be possible to exchange data with such an air gapped network via a dedicated interface, e.g. mobile storage devices (USB stick).

3.1.9

anti-intrusion

solutions dedicated to detect, notify and deter the access of non-authorised persons

3.1.10

application

software programs executing on the infrastructure that are used to interface with the process of the control system itself

Note 1 to entry: Attributes include executable, typically execute on personal computers (PCs) or embedded controllers

Note 2 to entry: This definition doesn't apply to the term "railway application"

3.1.11

approval

permission for a product or process to be marketed or used for stated purposes or under stated conditions

Note 1 to entry: Approval can be based on fulfilment of specified requirements or completion of specified procedures.

[SOURCE: IEC 60050-902:2013, 902-06-01]

3.1.12

asset

physical or logical object owned by or under the custodial duties of an organisation and having either a perceived or actual value to the organisation

[SOURCE: IEC 62443-2-1:2010, 3.1.3]

3.1.13

asset owner

individual or organisation responsible for one or more railway applications

Note 1 to the entry: In the context of this document, an asset owner is a railway duty holder.

[SOURCE: IEC 62443-4-1:2018, 3.1.6, modified – IACS replaced by railway application, note 1 added to entry]

3.1.14

attack

attempt to gain access to an information processing system or operational technology system in order to produce damage

Note 1 to entry: The damage can be, for example. destruction, disclosure, alteration, disruption, unauthorised use.

[SOURCE: IEC 60050-171:2019, 171-08-12, modified, "or operational technology system" added, "disruption" note added to entry]

3.1.15

attack surface

physical and functional interfaces of a system that can be accessed and, therefore, potentially exploited

Note 1 to entry: The size of the attack surface for a software interface is proportional to the number of methods and parameters defined for the interface. Simple interfaces, therefore, have smaller attack surfaces than complex interfaces.

Note 2 to entry: The size of the attack surface and the number of vulnerabilities are not necessarily related to each other.

[SOURCE: IEC 62443-2-4:2019, 3.1.2]

3.1.16

attack vector

method or means by which an attacker can gain access to the system under consideration in order to deliver a payload or achieve malicious outcome

Note 1 to entry: Attack vectors enable attackers to exploit the vulnerabilities of the system under consideration, including the human element.

Note 2 to entry: Examples of attack vectors include and not limited to USB key, e-mail attachment, wireless connection, compromised credentials, phishing, man in the middle attack, etc.

3.1.17

audit

systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled

[SOURCE: IEC 60050-902:2013, 902-03-04, modified – Note 1 to entry has been removed]

3.1.18

authentication

provision of assurance that a claimed characteristic of an identity is correct

Note 1 to entry: Not all credentials used to authenticate an identity are created equally. The trustworthiness of the credential is determined by the configured authentication mechanism. Hardware or software-based mechanisms can force users to prove their identity before accessing data on a device. A typical example is proving the identity of a user usually through an identity provider.

Note 2 to entry: Authentication is usually a prerequisite to allowing access to resources in a control system.

[SOURCE: IEC 62443-4-1:2018, 3.1.9]

3.1.19

authorization

<in cybersecurity>

right or a permission that is granted to a system entity to access a system resource

[SOURCE: IEC/TR 62443-3-1:2009, 3.1.7]

3.1.20

automatic train operation

ATO

method of operation in which the movement of the train is automatically controlled without the intervention of a driver, who, if provided, exercises only a supervisory function

[SOURCE: Electropedia]

3.1.21

automatic train protection

ATP

safety system that enforces either compliance with or observation of speed restrictions and signal aspects by train

[SOURCE: Subset-023 Glossary of UNISIG Terms and Abbreviations]

3.1.22

availability

<of an item>

ability to be in a state to perform as required

208 [SOURCE: IEC 60050-192:2015, 192-01-23, modified – The notes 1 and 2 to entry have been omitted]

209 **3.1.23**

210 **base transceiver station**

211 **BTS**

212 **<in railway system>**

213 piece of equipment that facilitates wireless communication between train or passenger equipment and a network.

214 Note 1 to entry: Train or passenger equipment are devices like mobile phones, computers with wireless
215 Internet connectivity, cab radio, or antennas mounted on train. The network can be that of any of the wireless
216 communication technologies like GSM, GSMR, CDMA, wireless local loop, Wi-Fi, WiMAX or other wide area
217 network (WAN) technology.

218 **3.1.24**

219 **bridge control system**

220 **<In railway systems>**

221 railway related infrastructure that includes the electronics installed in railway bridges to support bridge specific
222 infrastructure functions (e.g. monitoring systems and lift control)

223 **3.1.25**

224 **central diagnostic system**

225 **<In train>**

226 on-board component that centralises all diagnostic messages and signals from other train devices and sub-systems

227 **3.1.26**

228 **closed-circuit television**

229 **CCTV**

230 television allowing the transmission of images over a relatively short distance, generally by cable, intended for a
231 particular group of users

232 Examples include surveillance of public places or places which are dangerous or difficult to access, tunnels and
233 inside traction sub-stations.

234 [SOURCE: Electropedia, modified “chirurgical operation” replaced by “tunnels, inside traction sub-station”]

235 **3.1.27**

236 **cloud computing**

237 paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with
238 self-service provisioning and administration on-demand

239 [SOURCE: ISO/IEC 17788:2014, 3.2.5]

240

241 **3.1.28**

242 **code of practice**

243 **<in cybersecurity>**

244 written set of rules, that, when correctly applied, can be used to control one or more specific threats

245

246 [SOURCE: CSM Regulation N° 402/2013, modified « hazards » replaced by “threats”]

247

248 **3.1.29**

249 **communication channel**

250 **<in cybersecurity>**

251 specific logical or physical communication link between assets

252 Note 1 to entry: A channel facilitates the establishment of a connection.

253 [SOURCE: IEC 62443-3-3:2019, 3.1.9]

3.1.30**communication path**

physical and logical connection between a source and one or more destinations, which could be devices, physical processes, data items, commands, or programmatic interfaces

Note 1 to entry: The communication path is not limited to wired or wireless networks, but includes other means of communication such as memory, procedure calls, state of physical plant, portable media, and human interactions.

3.1.31**communication system****<in railway system>**

comprises subsystems to communicate with railway equipment (e.g. GSM-R, FRMCS, Wi-Fi), personnel (e.g., Tetra, VoIP) and passengers (e.g., PA).

3.1.32**communication based train control****CBTC**

continuous, automatic train control system utilising high-resolution train location determination, independent of track circuits; continuous, high-capacity, bidirectional train-to-wayside data communications; and trainborne and wayside processors capable of implementing Automatic Train Protection (ATP) functions, as well as optional Automatic Train Operation (ATO) and Automatic Train Supervision (ATS) functions.”

[Source: IEEE 1474:2017]

3.1.33**compensating countermeasure**

countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements

EXAMPLE

— (component-level): locked cabinet around a controller that does not have sufficient cyber access control countermeasures.

— (control system/zone-level): physical access control (guards, gates and guns) to protect a control room to restrict access to a group of known personnel to compensate for the technical requirement for personnel to be uniquely identified by the railway application.

— (component-level): a vendor’s programmable logic controller (PLC) cannot meet the access control capabilities from an end-user, so the vendor puts a hardware-based firewall in front of the PLC and sells it as a system.

[SOURCE: IEC 62443-4-2:2019, 3.1.9, modified, “IACS” replaced by “railway application”, “hardware-based” added]

3.1.34**component**

entity belonging to a railway application that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

[SOURCE: IEC 62443-4-2:2019, 3.1.10, modified “IACS” replaced by “railway application”]

3.1.35**compromise**

violation of the security of a system such that an unauthorised disclosure or modification on sensitive information may have occurred, or unauthorised behaviour of the controlled physical process may have occurred

3.1.36**conduit****<in cybersecurity>**

logical grouping of communication channels, connecting two or more zones, that share common security requirements

300 Note 1 to entry: A conduit is allowed to traverse a zone as long as the security of the channels contained within the
301 conduit is not impacted by the zone.

302 [SOURCE: IEC 62443-4-2:2019, 3.1.11]

303 **3.1.37**

304 **confidentiality**

305 **<in cybersecurity>**

306 assurance that information is not disclosed to unauthorized individuals, processes, or devices

307 Note 1 to entry: When used in the context of a railway application, confidentiality refers to protecting railway
308 application data and information from unauthorised access.

309 [SOURCE: IEC 62443-4-2:2019, 3.1.12, modified, “IACS” replaced by “railway application” in Note 1 to entry]

310 **3.1.38**

311 **connection**

312 **<in cybersecurity>**

313 association established between two or more endpoints which supports the establishment of a session

314 [SOURCE: IEC 62443-4-2:2019, 3.1.13]

315 **3.1.39**

316 **control network**

317 time-critical network that is typically connected to equipment that controls physical processes

318 Note 1 to entry: The control network can be subdivided into zones,

319 Note 2 to entry: there can be multiple separate control networks within one company or site.

320 **3.1.40**

321 **control system**

322 **<in railway application>**

323 Integrated set of hardware and software components of a railway application performing control function within a
324 railway solution

325 Note 1 to entry: control systems can be composed of field devices, embedded control devices, network devices,
326 and host devices (including workstations and servers).

327 **3.1.41**

328 **countermeasure**

329 action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or
330 preventing it, by minimising the harm it can cause, or by discovering and reporting it so that corrective action can
331 be taken

332 Note 1 to entry: The term “control” is also used to describe this concept in some contexts. The term countermeasure
333 has been chosen for this standard to avoid confusion with the term “control” in the context of “process control” and
334 “control system”.

335 [SOURCE: IEC 62443-3-3:2019, 3.1.17]

336 **3.1.42**

337 **cybersecurity**

338 **<in railway application>**

339 set of activities and measures taken with the objective to identify, protect, detect, respond, and recover to
340 unauthorised access or cyberattack which could lead to an accident, an unsafe situation, or railway application
341 performance degradation

342 Note 1 to entry: It is recognised that the term “cybersecurity” has a broader meaning in other standards and
343 guidance, often including non-malevolent threats, human errors, and protection against natural disasters. Those
344 aspects, except human errors degrading security countermeasures, are not included in this document.

3.1.43**cybersecurity case**

documented demonstration that the system under consideration properly address cybersecurity risks and that appropriate design, operation processes and organisation have been implemented to achieve acceptable level of cybersecurity risks

3.1.44**data diode**

network appliance or device allowing data to travel only in one direction

Note 1 to entry: A data diode can be either of the physical or logical type

3.1.45**defence in depth**

approach to defend the system against any particular attack using several independent methods

Note 1 to entry: Defence in depth implies layers of security and detection, even on single systems, and provides the following features:

- is based on the idea that any one layer of protection, may and probably will be defeated;
- attackers are faced with breaking through or bypassing each layer without being detected;
- a flaw in one layer can be mitigated by capabilities in other layers;
- system security becomes a set of layers within the overall network security; and
- each layer should be autonomous and not rely on the same functionality nor have the same failure modes as the other layers.

[SOURCE: IEC 62443-4-1:2018, 3.1.15, modified – defense has been replaced by defence]

3.1.46**demilitarized zone**

common, limited network of servers joining two or more zones for the purpose of controlling data flow between zones

Note 1 to entry: Demilitarized zones (DMZs) are typically used to avoid direct connections between different zones.

[SOURCE: IEC 62443-3-3:2019, 3.1.19]

3.1.47**denial of service**

prevention or interruption of authorised access to a system resource or the delaying of system operations and functions

[SOURCE: IEC/TR 62443-3-1:2009, 3.1.21]

3.1.48**diagnostics system****<in railway system>**

comprises systems dedicated to collecting data from on-ground or on-board sources for monitoring, analysis, and maintenance purposes.

3.1.49**digital signature****<in cybersecurity>**

result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation

[SOURCE: IEC/TR 62443-3-1:2009, 3.1.22]

- 388 **3.1.50**
 389 **digital automatic coupling**
 390 **DAC**
 391 **<in railway system>**
 392 automatic coupling and decoupling the carriages in a freight train both physically as well as digitally (electrical power
 393 and data connection)
- 394 **3.1.51**
 395 **driver advisory system**
 396 **<in railway system>**
 397 system providing the driver with real-time guidance on how to drive the train to arrive on time efficiently
- 398 **3.1.52**
 399 **driver machine interface**
 400 **<in railway system>**
 401 includes all the tech objects used to manage communications between the train and the driver (e.g. screens, buttons
 402 and handles)
- 403 **3.1.53**
 404 **electrical substation**
 405 **<in railway system>**
 406 converts electric power from the form provided by the electrical grid to an appropriate voltage, current type and
 407 frequency to supply railway systems
- 408 **3.1.54**
 409 **encryption**
 410 **<of data>**
 411 transformation of data in order to hide their semantic content using cryptography
- 412 Note 1 to entry: The reverse process is called decryption.
- 413 [SOURCE: IEC 60050-171:2019, 171-08-09]
- 414 **3.1.55**
 415 **energy measurement system**
 416 **<in railway system>**
 417 system that measures the train energy consumptions and regeneration and sends this data to ground for billing and
 418 other purposes
- 419 **3.1.56**
 420 **energy settlement system**
 421 **<in railway system>**
 422 system that receives geo-referenced trains energy data from data collecting systems and associates this data to
 423 consumers and suppliers for billing purposes
- 424 **3.1.57**
 425 **entertainment system**
 426 **<in railway system>**
 427 system that provides train passengers with movies, internet access and other leisure activities
- 428 **3.1.58**
 429 **essential function**
 430 function or capability that is required to maintain health, safety, the environment and availability of the equipment
 431 under control
- 432 Note 1 to entry: Essential functions include, but are not limited to, the safety-related functions, the control functions
 433 and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions
 434 is commonly termed loss of protection, loss of control and loss of view respectively. In some industries additional
 435 functions such as history may be considered essential.

[SOURCE: IEC 62443-3-3:2013, 3.1.22, modified “safety instrumented function (SIF)” replaced by “safety-related function”]

3.1.59

event recording - juridical recording unit

<in railway system>

equipment dedicated to register train events mainly for legal issues in case of an accident; it can be used for diagnostics purposes

3.1.60

facility management system

<in railway system>

supervision system to configure and control railway civil work equipment (lighting, heating, air condition and electric power)

3.1.61

fire protection system

<in railway system>

system detecting smoke and fire and activating extinguishing countermeasures

3.1.62

firewall

functional unit that mediates all traffic between two networks and protects one of them or some part thereof against unauthorised access

[SOURCE: IEC 60050-732:2010, 732-06-01, modified – The notes to entry have been omitted]

3.1.63

future railway mobile communication system

FRMCS

<in railway system>

communication system for rail transport systems developed jointly with the European Union and major companies in the Western European railway industry, successor of global systems for mobile communications – railway (GSM-R) and intended to serve train radio, both for voice and data communication

3.1.64

gateway

<for computer networks>

functional unit that connects two computer networks with different network architectures and protocols

[SOURCE: IEC 60050-732:2010, 732-01-17, modified – The notes to entry have been omitted]

3.1.65

global system for mobile communications railway

GSM-R

international wireless communications standard for railway communication and applications

3.1.66

handover

<in railway>

act of turning a railway solution over to the railway duty holder

Note 1 to entry: Handover effectively transfers responsibility for operations and maintenance of a railway solution from the integration service provider to the railway duty holder and generally occurs after successful completion of system test, often referred to as site acceptance test (SAT).

[SOURCE: IEC 62443-2-4:2019, 3.1.7, modified, “automation solution” replaced by “railway solution”, “asset owner” replaced by “railway duty holder”]

3.1.67

host

<in cybersecurity>

computer that is attached to a communication subnetwork or inter-network and can use services provided by the network to exchange data with other attached systems

3.1.68

host device

<in cybersecurity>

general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers

Note 1 to entry: Typical attributes include filesystem(s), programmable services, no real time scheduler and full HMI (keyboard and mouse)

[SOURCE: IEC 62443-4-2:2019, 3.1.23]

3.1.69

impact

measure of the ultimate loss or harm associated with a consequence

EXAMPLE: The consequence of the incident was a spill. The impact of the spill was a \$100 000 fine and \$25 000 in clean-up expenses.

Note 1 to entry: Impact may be expressed in terms of numbers of injuries and/or fatalities, extent of environmental damage and/or magnitude of losses such as property damage, material loss, loss of intellectual property, lost production, market share loss and recovery costs

[SOURCE: IEC 62443-3-2:2020, 3.1.10]

3.1.70

incident

<in cybersecurity>

event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system

[SOURCE: IEC 62443-3-3:2019, 3.1.28]

3.1.71

integration service provider

service provider that provides integration activities for an railway solution including, design, installation, configuration, testing, commissioning and handover

[SOURCE: IEC 62443-2-4:2019, 3.1.9, modified, “automation solution” replaced by “railway solution”, Note 1 to entry removed]

3.1.72

integrity

<of data>

property that sensitive data has not been modified or deleted in an unauthorised and undetected manner

[SOURCE: IEC 60050-171:2019, 171-08-05, modified – “of data that have not been altered or destroyed” has been replaced with “that sensitive data has not been modified or deleted”]

3.1.73

intercom call

<In railway system>

bidirectional communication between different parts of the train, allowing driver, crew and passengers to communicate even in critical situations

3.1.74**interlocking****<In railway system>**

equipment that controls setting and releasing signals and points to prevent an unsafe condition of the signalling system arising during the passage of trains

Note 1 to entry: Interlockings can be categorised as mechanical, electrical (electro-mechanical or relay-based), or electronic/computer-based (called CBI or computer based interlocking)

3.1.75**internet of things****IoT**

infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world

[SOURCE: ISO/IEC 20924:2018, 3.2.1]

3.1.76**internet on board****<In railway system>**

Internet access for train passengers

3.1.77**intrusion****<in cybersecurity>**

A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorisation to do so

[SOURCE: RFC 4949 Internet Security Glossary, Version 2]

3.1.78**intrusion detection**

security service that monitors and analyses system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorised manner

3.1.79**least privilege**

basic principle that holds that users (humans, software processes or devices) should be assigned the fewest privileges consistent with their assigned duties and functions

Note 1 to entry: Least privilege is commonly implemented as a set of roles in a railway application.

[SOURCE: IEC 62443-4-2:2019, 3.1.28, modified “IACS” replaced by “railway application”]

3.1.80**legacy system****<in railway cybersecurity>**

existing system that is already in use and meets the needs it was originally designed for but which does not have the required native cybersecurity capabilities and which update cost of implementation is not acceptable or technically not feasible.

Note 1 to entry: Legacy does not necessarily imply that the system has reached its end of life. The vendor may still support it. Legacy systems are common in Operational Technology as these have lifetime of over 20 years. An issue is outdated and unmanaged components.

3.1.81**level crossing****<In railway system>**

crossing of a railway and a road at the same level

- 574 **3.1.82**
 575 **lighting system**
 576 **<in railway system>**
 577 system including the electronics dedicated to ensure correct illumination of railway cars both internally and
 578 externally (a special case of external lighting are headlights) as well are on-ground location such as station, depots,
 579 control rooms and tunnels
- 580 **3.1.83**
 581 **life time buy**
 582 purchase of a part in quantities enough for the remaining life time of the product or system where the part is used.
 583 It is a risk mitigation approach to the part obsolescence.
- 584 **3.1.84**
 585 **likelihood**
 586 **<of occurrence>**
 587 weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given
 588 vulnerability or a set of vulnerabilities
- 589 [SOURCE: NIST SP 800-30: September 2012]
- 590 **3.1.85**
 591 **maintenance and diagnostic system**
 592 **<In railway system>**
 593 system ensuring the analysis of the field data/status, assessing maintenance needs and planning and logging of
 594 maintenance activities
- 595 **3.1.86**
 596 **maintenance service provider**
 597 **<In railway system>**
 598 service provider that provides support activities for a railway solution after handover
- 599 Note 1 to entry: Maintenance is often considered to be distinguished from operation (e.g. in common colloquial
 600 language it is often assumed that an railway solution is either in operation or under maintenance). Maintenance
 601 service providers can also perform cybersecurity related support activities during operations, e.g. managing user
 602 accounts, security monitoring, and security assessments.
- 603 [SOURCE: IEC 62443-2-4:2019 3.1.10, modified “Automation Solution” replaced by “railway solution”]
- 604 **3.1.87**
 605 **mobile communication gateway**
 606 **<in railway system>**
 607 train-side sub-system providing on-board to on-ground communication services for the on-board end devices
- 608 **3.1.88**
 609 **network management centre**
 610 **<in railway system>**
 611 entity in charge to control the railway network, to analyse traffic, to record call with drivers and to ensure
 612 configuration control, fault detection and diagnosis and maintenance.
- 613 **3.1.89**
 614 **network management system**
 615 **<in railway system>**
 616 system in charge to monitor and administrate communication networks
- 617 **3.1.90**
 618 **non-repudiation**
 619 **<in cybersecurity>**
 620 ability to prove the occurrence of a claimed event or action and its originating entities

621 Note 1 to entry: The purpose of non-repudiation is to resolve disputes about the occurrence or non-occurrence of
622 the event or action and involvement of entities in the event.

623 [SOURCE: IEC 62443-3-3:2019, 3.1.33]

624 **3.1.91**

625 **on-board multimedia and telematics**

626 **OMTS**

627 **<in railway system>**

628 multimedia and telematics subsystems identified as video surveillance/CCTV, driver and crew orientated services,
629 passenger orientated services and train operator and maintainer orientated services.

630 **3.1.92**

631 **operational technology**

632 **OT**

633 programmable digital systems or devices that interact (i.e. detect or cause a direct change) of the physical
634 environment or manage devices that interact with the physical environment

635 Note 1 to entry: examples include transportation systems, interlocking, signalisation systems, physical control
636 access systems, physical environment monitoring systems and physical environment measurement systems

637 **3.1.93**

638 **passenger alarm system**

639 **<in railway system>**

640 mechanism that passengers can manually activate in case of immediate danger conditions to alert the on-board
641 staff or the driver and eventually stop the train

642 **3.1.94**

643 **passenger information system**

644 **<in railway system>**

645 system informing passengers about train departure time, platforms, etc.

646 Note 1 to entry: may also be referred to as customer information system

647 **3.1.95**

648 **passenger counting system**

649 **<in railway system>**

650 on-board system, usually installed over a door, which are able to count incoming and outcoming passengers and
651 to communicate the balance to a control unit.

652 **3.1.96**

653 **patch management**

654 area of systems management that involves monitoring, acquiring, testing, scheduling and installing software
655 patches (code change) to a product

656 Note 1 to entry: See IEC TR 62443-2-3 for additional information.

657 Note 2 to entry: Patch management also applies to the process of keeping included 3rd party libraries current before
658 releasing a product.

659 [SOURCE: IEC 62443-4-1:2018, 3.1.21]

660 **3.1.97**

661 **platform screen doors**

662 system of automated doors synchronised with the train doors which are provided at the platform edge to isolate
663 passengers on platform from track

664 **3.1.98**

665 **penetration**

666 successful unauthorised access to a protected system resource

3.1.99

penetration testing

process where a known person or group of person tries to penetrate the security defences in a system, in order to identify and characterize security-related issue via tests that focus on discovering and exploiting security vulnerabilities.

Note 1 to entry: Many companies specialize in penetration testing for traditional IT systems. It may be more difficult to find a group that understands the special requirements of a railway solution.

3.1.100

privilege

authorisation or set of authorisations to perform specific functions, especially in the context of a computer operating system

Note 1 to entry: Examples of functions that are controlled using privilege include acknowledging alarms, changing set points and modifying control algorithms.

3.1.101

point heating

device using electric or gas heating, clipped to the rails to heat a set of points, to prevent ice forming and keep the switch blades moving

3.1.102

point machine

electromechanical device which sets points/switches to left or right position according to the route setting for a train

3.1.103

protection profile

<in cybersecurity>

generic implementation-independent cybersecurity requirement specification for a class or type of components or specific configuration setting of different components which is typically created by an user or an user community

Note 1 to entry: A protection profile document is a combination of threats, security objectives, assumptions, security functional requirements, security assurance requirements and rationales.

3.1.104

public address

system informing passengers and railway personnel about actual situation via audio path

3.1.105

purdue model

model that was adopted from the Purdue Enterprise Reference Architecture (PERA) model by ISA-99, and used as a concept model for industrial control system (ICS) network segmentation

Note 1 to entry: It is an industry adopted reference model that shows the interconnections and interdependencies of all the main components of a typical ICS.

3.1.106

radio block center

RBC

device used at European train control system (ETCS) Level 2 and Level 3 acting as a centralised safety unit, which, using radio connection via GSM-R, receives train position information and sends movement authority and further information required by the train for its movement

3.1.107

railway application

collection of personnel, hardware, software, procedures and policies involved in the operation of the railway service and that can affect or influence its safe, secure and reliable operation.

Note 1 to entry: It corresponds in the railway domain to the IEC 62443 term “IACS” of IEC 62443.

714 [SOURCE: IEC 62443 4-1:2018 3.1.20, modified – “IACS” replaced by “railway application”, <industrial process>
715 replaced with <railway service>, Note 1 added]

716 **3.1.108**

717 **railway duty holder**

718 body with the overall accountability for operating a railway system within the legal framework

719 Note 1 to entry: Railway duty holder accountabilities for the overall system or its parts and lifecycle activities are
720 sometimes split between one or more bodies or entities. For example:

721 — the owner(s) of one or more parts of the system assets and their purchasing agents;

722 — the operator of the system;

723 — the maintainer(s) of one or more parts of the system;

724 Note 2 to entry: Typically, the railway duty holders are railway undertakings and the infrastructure managers. Such
725 splits are based on either statutory instruments or contractual agreements. Such responsibilities are defined at the
726 earliest stages of a system lifecycle.

727 [SOURCE: EN 50126-1:2017, 3.48]

728 **3.1.109**

729 **railway operator**

730 organisation responsible for the operation of the railway system or sub-system

731 **3.1.110**

732 **railway solution**

733 control system and any complementary hardware and software components that have been installed and configured
734 to operate in a railway application

735 Note 1 to entry: railway solution deliverables include the cybersecurity case and security guidelines.

736 [SOURCE: IEC 62443-2-4:2017 3.1.3, modified – <IACS> replaced with <railway application>. Note 1 added]

737 **3.1.111**

738 **railway system**

739 overall railway system that consists of multiple railway applications

740 Note 1 to entry: Besides railway applications, it may also include other associated systems and components
741 depending on the mission of the railway duty holder.

742 **3.1.112**

743 **reference model**

744 structure that allows the modules and interfaces of a system to be described in a consistent manner

745 [SOURCE (for IACS): IEC/TS 62443-1-1:2009, 3.2.81]

746 **3.1.113**

747 **remote access**

748 access to a control system by any user (human, software process or device) communicating from outside the
749 perimeter of the zone being addressed

750 [SOURCE: IEC 62443-3-3:2019, 3.1.35]

751 **3.1.114**

752 **residual risk**

753 **<in cybersecurity>**

754 risk that remains after existing countermeasures are implemented (such as, the net risk or risk after
755 countermeasures are applied)

756 [SOURCE: IEC 62443-3-2:2020, 3.1.13]

757 **3.1.115**

758 **risk**

759 **<in cybersecurity>**

760 expectation of loss expressed as the likelihood that a particular threat will exploit a potential vulnerability with a
761 particular consequence

762 [SOURCE: IEC 62443-3-2:2020, 3.1.14, modified “particular” replaced by “potential”]

763 **3.1.116**

764 **risk assessment**

765 **<in cybersecurity>**

766 process that systematically identifies potential vulnerabilities to valuable system resources and threats to those
767 resources, evaluates loss exposures and consequences based on likelihood of occurrence, and (optionally)
768 recommends how to allocate resources to countermeasures to minimize total exposure

769 Note 1 to entry: Types of resources include physical, logical and human.

770 Note 2 to entry: Risk assessments are often combined with vulnerability assessments to identify vulnerabilities and
771 evaluate the associated risk. They are carried out initially and periodically to reflect changes in the organisation's
772 risk tolerance, vulnerabilities, procedures, personnel and technological changes.

773 [SOURCE: IEC 62443-1-1:2009, 3.2.88, modified, “quantifies” replaced by “evaluates”, “probability” replaced by
774 “likelihood”]

775 **3.1.117**

776 **risk matrix**

777 tool used in risk management to qualitatively determine the level of risk by assessing the likelihood of an incident
778 occurring and the impact of the consequence should the incident occur;

779 Note 1 to entry: A risk matrix presents likelihood on one axis and impact on the second axis. The intersections
780 between likelihood and impact establish the risk level.

781 Note 2 to entry: The intersection between the lowest likelihood and lowest severity yields the lowest risk level.
782 Whereas the intersection between the highest likelihood and highest severity yields the highest risk level. The
783 intersections are typically colour-coded to indicate increasing risk level with green typically being the lowest and red
784 typically being the highest.

785 Note to entry: While always 2-dimensional, risk matrices vary in size (for example, 3 x 3, 4 x 4, 3 x 5, 5 x 5)
786 depending on the number of categories in the likelihood and severity scales.

787 **3.1.118**

788 **risk mitigation**

789 prioritising, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended
790 from the risk management process

791 **3.1.119**

792 **role**

793 A set of connected behaviours, privileges and obligations associated with all users (humans, software processes
794 or devices) of a railway application

795 Note 1 to entry: The privileges to perform certain operations are assigned to specific roles.

796 [SOURCE: IEC 62443-3-3:2019, 3.1.36, modified “IACS” replaced by “railway application”]

797 **3.1.120**

798 **safety**

799 freedom from unacceptable risk

800 Note 1 to entry: Risk related to human health or to the environment.

[SOURCE: IEC 60050-903:2013, 903-01-19, modified – Note 1 to entry has been added]

3.1.121

safety lighting

Emergency lighting refers to battery-backed or otherwise independently powered light sources that are designed to activate when a power outage creates low-visibility conditions in a rail environment.

3.1.122

safety-related system

system used to implement functional safety

[SOURCE: IEC 62443 2-4:2015 / AMD 1:2017, 3.1.14, modified – all notes removed]

3.1.123

safety tunnel earthing system

integrated automatic system that allows the safe management of the power disconnectors and the earthing of overhead line in the tunnel.

3.1.124

sandbox

system that allows an untrusted application to run in a highly controlled environment where the application's permissions are restricted to an essential set of computer permissions

Note 1 to entry: In particular, an application in a sandbox is usually restricted from accessing the file system or the network.

3.1.125

security information event management

SIEM

monitoring system for real-time analysis of security alerts generated by applications, host computers and network components

3.1.126

security operation centre

SOC

A combination of people, processes and technology protecting the information and/or operation systems of an organisation through proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and minimising damage from unwanted effects

3.1.127

secret

condition of information being protected from being known by any system entities except those intended to know it

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.98]

3.1.128

security

<in cybersecurity>

condition of system resources being free from unauthorised access and from unauthorised or accidental change, destruction or loss

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.99]

3.1.129

security architecture

<in cybersecurity>

plan and set of principles describing the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the services, and the performance levels required in the elements to deal with the threat environment

848 Note 1 to entry: In this context, security architecture would be an architecture to protect the control network from
849 intentional or unintentional security events.

850 [SOURCE: IEC/TS 62443-1-1:2009, 3.2.100]

851 **3.1.130**

852 **security assurance**

853 **<in cybersecurity>**

854 grounds for confidence that the set of intended security controls/countermeasures in an railway application are
855 effective in their application and that an entity meets its security objectives

856 [SOURCE: NIST SP 800-39, amended, “information system” replaced by “railway application”]

857 **3.1.131**

858 **security device**

859 **<in cybersecurity>**

860 device that performs a protective or detective security function

861 **3.1.132**

862 **security event**

863 **<in cybersecurity>**

864 event that may have a cybersecurity impact on the operations, (e.g. a login attempt)

865 **3.1.133**

866 **security incident**

867 **<in cybersecurity>**

868 security compromise that is of some significance to the asset owner or failed attempt to compromise the system
869 whose result could have been of some significance to the asset owner

870 Note1 to entry: The term “of some significance” is relative to the environment in which the security compromise is
871 detected. For example, the same compromise may be declared as a security incident in one environment and not
872 in another. Triage activities are often used by asset owners to evaluate security compromises and identify those
873 that are significant enough to be considered incidents.

874 Note 2 to entry: In some environments, failed attempts to compromise the system, such as failed login attempts,
875 are considered significant enough to be classified as security incidents.

876 [SOURCE: IEC 62443-2-4:2019, 3.1.16]

877 **3.1.134**

878 **security level**

879 **SL**

880 **<in cybersecurity>**

881 measure of confidence that the SuC, zone, conduit or a component is free from vulnerabilities and functions in the
882 intended manner

883 Note 1 to entry: Vulnerabilities can either be designed into the SuC, inserted at any time during its lifecycle or result
884 from changing threats. Designed-in vulnerabilities may be discovered long after the initial deployment of the SuC,
885 e.g. an encryption technique has been broken or an improper policy for account management such as not removing
886 old user accounts. Inserted vulnerabilities may be the result of a patch or a change in policy that opens a new
887 vulnerability.

888 [SOURCE: IEC 62443-3-3:2019, 3.1.38, modified]

889 **3.1.135**

890 **security objective**

891 **<in cybersecurity>**

892 aspect of security whose purpose is to use certain mitigation measures, such as confidentiality, integrity, availability,
893 user authenticity, access authorisation and accountability.

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.109]

3.1.136

security patch

<in cybersecurity>

A software patch that is relevant to the security of a software component

Note 1 to entry: For the purpose of this definition, firmware is considered software.

Note 2 to entry: Software patches may address known or potential vulnerabilities, or simply improve the security of the software component, including its reliable operation.

[SOURCE: IEC 62443-2-4:2019, 3.1.17]

3.1.137

security perimeter

boundary (logical or physical) of the domain in which a security policy or security architecture applies, i.e. the boundary of the space in which security services protect system resources

[SOURCE: IEC 62443-1-1:2010, 3.2.110]

3.1.138

security policy

A set of rules that specify or regulate how a system or organisation provides security services to protect its assets

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.112]

3.1.139

security program

<in cybersecurity>

A portfolio of security services, including integration services and maintenance services, and their associated policies, procedures, and products that are applicable to the railway application

Note 1 to entry: The security program for railway application service providers refers to the policies and procedures defined by them to address security concerns of the railway application.

[SOURCE: IEC 62443-2-4:2019, 3.1.18, modified “IACS” replaced by “railway application”]

3.1.140

security-related application condition

SecRAC

<in cybersecurity>

those conditions which need to be met in order for a system to be securely integrated and securely operated

Note 1 to entry: Application conditions can be, for example, operational restrictions (such as access control process), operational rules, maintenance rules (such as antimalware update periodicity) or environmental conditions (such as external public key infrastructure (PKI))

3.1.141

security services

<in cybersecurity>

mechanisms used to provide confidentiality, data integrity, authentication, or no repudiation of information

3.1.142

sensitive data

data that is likely to cause to its owner some adverse impact if either it becomes known to others when not intended or it is modified without consent of the affected stakeholder. It thus requires protection from unauthorised disclosure or modification.

- 937 **3.1.143**
 938 **service provider**
 939 **<in cybersecurity>**
 940 individual or organisation (internal or external organisations) that provides a specific support service and associated
 941 supplies in accordance with an agreement with the asset owner
- 942 Note 1 to entry: This term is used in place of the generic word “vendor” to provide differentiation.
- 943 Note 2 to entry: The service provider can be an organisation within the asset owner’s organisation.
- 944 [SOURCE: IEC 62443-2-4:2019, 3.1.19, modified Note 2 added]
- 945 **3.1.144**
 946 **session**
 947 semi-permanent, stateful, interactive information interchange between two or more communicating devices
- 948 Note 1 to entry: Typically, a session has a clearly defined start process and end process.
- 949 [SOURCE: IEC 62443-3-3:2019, 3.1.40]
- 950 **3.1.145**
 951 **shared cybersecurity service**
 952 A subsystem providing common security functions to the assets of a railway application, such as user identification
 953 and authentication, log service, identity and access management, time service, backup and restore and intrusion
 954 detection.
- 955 **3.1.146**
 956 **signal**
 957 **<in railway context>**
 958 device informing the train driver about the allowance to entry a track section and the allowed speed of the route
- 959 **3.1.147**
 960 **software-defined wide area network**
 961 **SD-WAN**
 962 wide area network that uses software-defined network technology, such as communicating over the internet using
 963 overlay tunnels which are encrypted when destined for internal organisation locations.
- 964 **3.1.148**
 965 **spoke network**
 966 **<in virtual private cloud context>**
 967 virtual network peered with the central service (hub) to enable cross-virtual network communication.
- 968 **3.1.149**
 969 **supervisory control and data acquisition system**
 970 **SCADA system**
 971 monitoring and control system including computers, networked data communications and graphical user interfaces
 972 (GUI) for high-level process supervisory management, while also including other peripheral devices like
 973 programmable logic controllers (PLC) and ICS to interface with process systems such as rolling stock, interlocking,
 974 energy and buildings, or machinery.
- 975 **3.1.150**
 976 **system integrator**
 977 person or company that specialises in bringing together component subsystems into a whole and ensuring that
 978 those subsystems perform in accordance with project specifications
- 979 [SOURCE: IEC 62443-4-1:2018, 3.1.34]

3.1.151**system under consideration****SuC**

collection of assets that are needed to provide complete a railway application including any relevant network infrastructure assets

Note 1 to entry: A SuC consists of one or more zones and related conduits. All assets within a SuC belong to either a zone or conduit.

[SOURCE: IEC 62443-3-2:2020, 3.1.19, modified, “automation solution” replaced by “railway solution”]

3.1.152**threat****<in cybersecurity>**

circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorised access, destruction, disclosure, modification of data and/or denial of service

[SOURCE: IEC 62443-3-3:2019, 3.1.44]

3.1.153**threat environment****<in cybersecurity>**

environment summary of information about threats, such as threat sources, threat vectors and trends, that have the potential to adversely impact a defined target (for example a company, facility or SuC)

[SOURCE: IEC 62443-3-2:2020, 3.1.19]

3.1.154**threat source****<in cybersecurity>**

intent and method targeted at the intentional exploitation of a vulnerability, or a situation and method that may accidentally trigger a vulnerability

Note 1 to entry: the term threat agent is sometime used instead of threat source

[SOURCE: IEC 62443-3-2:2020, 3.1.20]

3.1.155**threat vector****<in cybersecurity>**

path or means by which a threat source can gain access to an asset

[SOURCE: IEC 62443-3-2:2020, 3.1.21]

3.1.156**Ticketing system****<in railway context>**

system for ordering, sales and validation of tickets

3.1.157**track supervision**

ground based system that can monitor certain conditions of tracks (such as avalanche detection and air speed indication)

3.1.158**traction system****<in railway context>**

onboard system responsible to supply the necessary force to move the train

- 1025 **3.1.159**
 1026 **traction mains**
 1027 **<in railway context>**
 1028 trackside systems for the conversion and supply of traction power
- 1029 **3.1.160**
 1030 **traffic management system**
 1031 **<in railway context>**
 1032 system controlling the route setting for trains based on timetables and short-term needs
- 1033 **3.1.161**
 1034 **train communication network**
 1035 **TCN**
 1036 communication backbone on vehicles and trains
- 1037 **3.1.162**
 1038 **train control monitoring system**
 1039 **TCMS**
 1040 train-borne distributed control system, comprised of computer devices software, human-machine interfaces, digital
 1041 and analogue input/ output (I/O) capability and the data networks to connect all these together in a secure and fault-
 1042 resistant manner to operate the train.
- 1043 **3.1.163**
 1044 **train detection sensor**
 1045 device detecting if a given track section is free or occupied by a train (or coach)
- 1046 **3.1.164**
 1047 **train supervision**
 1048 ground system for supervision of trains
- 1049 **3.1.165**
 1050 **tunnel control system**
 1051 **<in railway context>**
 1052 components installed in railway tunnels to support tunnel specific infrastructure functions (for example ventilation,
 1053 alarm systems, fire and smoke detectors and fire extinguishers)
- 1054 **3.1.166**
 1055 **vehicle control unit**
 1056 **VCU**
 1057 core component of train control and management system (TCMS) that manages and controls vehicles
- 1058 **3.1.167**
 1059 **validation**
 1060 confirmation, through the provision of objective evidence, that the requirements for a specific intended use or
 1061 application have been fulfilled
- 1062 Note 1 to entry: The term “validated” is used to designate the corresponding status.
- 1063 Note 2 to entry: The use conditions for validation can be real or simulated.
- 1064 Note 3 to entry: In design and development, validation concerns the process of examining an item to determine
 1065 conformity with user needs.
- 1066 Note 4 to entry: Validation is normally performed during the final stage of development, under defined operating
 1067 conditions, although it may also be performed in earlier stages.
- 1068 Note 5 to entry: Multiple validations may be carried out if there are different intended uses.
- 1069 [SOURCE: ISO 9000:2005, 3.8.5, modified – Notes 3, 4 and 5 have been added]

- 1070 **3.1.168**
1071 **verification**
1072 confirmation, through the provision of objective evidence, that specified requirements have been fulfilled
- 1073 Note 1 to entry: The term “verified” is used to designate the corresponding status.
- 1074 Note 2 to entry: Design verification is the application of tests and appraisals to assess conformity of a design to the
1075 specified requirement.
- 1076 Note 3 to entry: verification is conducted at various lifecycle stages of development, examining the systems and its
1077 constituents to determine conformity to the requirements specified at the beginning of that lifecycle stage.
- 1078 [SOURCE: ISO 9000:2005, 3.8.4, modified – Note 2 has been modified and Note 3 has been added]
- 1079 **3.1.169**
1080 **virtual private network**
1081 **VPN**
1082 mechanism for creating a secure connection between a computing device and a computer network, or between two
1083 networks, using an insecure communication medium such as the public Internet.
- 1084 **3.1.170**
1085 **virtual routing and forwarding**
1086 **VRF**
1087 technology that allows in IP-based computer networks multiple instances of a routing table to co-exist within the
1088 same router at the same time.
- 1089 Note 1 to entry: One or more logical or physical interfaces may have a VRF and these VRFs do not share routes
1090 therefore the packets are only forwarded between interfaces on the same VRF.
- 1091 Note 2 to entry: Technology predominantly used for software defined networks in data centres
- 1092 **3.1.171**
1093 **voice for critical operation**
1094 **<in railway context>**
1095 train-to-ground voice communication system through dedicated radio systems (such as a cab radio) or ground to
1096 ground voice communication system, both for critical operation
- 1097 **3.1.172**
1098 **vulnerability**
1099 flaw or weakness in a system's design, implementation, or operation and management that could be exploited to
1100 violate the system's integrity or security policy
- 1101 [SOURCE: IEC 62443-3-2:2020, 3.1.24]
- 1102 **3.1.173**
1103 **web application firewall**
1104 provides centralised protection of web applications from common exploits and vulnerabilities.
- 1105 **3.1.174**
1106 **wireless local area network**
1107 **WLAN**
1108 network that allows devices to connect and communicate wirelessly.
- 1109 **3.1.175**
1110 **zone**
1111 grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational
1112 function, physical or logical location, required access (for example, least privilege principles) or responsible
1113 organisation

1114 Note 1 to entry: Collection of logical or physical assets that represents partitioning of a system under
1115 consideration on the basis of their common security requirements, criticality (such as high financial, health, safety
1116 or environmental impact), functionality, logical and physical (including location) relationship.

1117 [SOURCE: IEC 62443-3-2:2020, 3.1.25]

1118 3.2 Abbreviated terms and acronyms

1119 The list below defines the abbreviated terms and acronyms used in this document:

ANSSI	agence nationale de la sécurité des systèmes d'information
API	application programming interface
APN	access point name
ATO	automatic train operation
ATP	automatic train protection
ATS	automatic train supervision
CBTC	communication based train control
CCTV	closed-circuit television
CEF	common event format
CERT	computer emergency response team
CIA	confidentiality, integrity, and availability
CISA	Cybersecurity and Infrastructure Security Agency
CISO	chief information security officer
CMDB	configuration management database
COTS	commercial off the shelf
CPU	central processing unit
CR	component requirement
CRS	cybersecurity requirements specification
CSIRT	computer security incident response team
CSMS	cybersecurity management system
CVE	common vulnerabilities and exposures
CVSS	common vulnerability scoring system
DAC	digital automatic coupling
DAS	driver advisory system
DC	data confidentiality
DRA	detailed risk assessment
DMI	driver machine interface
DMZ	demilitarized zone
DoS	denial of service
EMS	energy management system
ENISA	European Network and Information Security Agency
EPSS	exploit prediction scoring system
ERA	European Railway Agency
ER-ISAC	European Railway Information Sharing and Analysis Center
ERP	enterprise resource planning
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EU NIS	European Union Directive on Security of Network and Information Systems
EVC	European Vital Computer
FIRST	Forum of Incident Response and Security Teams
FR	foundational requirement

FRMCS	future railway mobile communication system
HMAC	hash-based message authentication code
HVAC	heating, ventilation and air-conditioning
HW	hardware
IAC	identification and authentication control
IACS	industrial automation and control system(s)
IAM	identity access management
ICS	industrial control systems
ID	identifier
IDS	intrusion detection system
IEC	International Electrotechnical Commission
I/O	input/output
IOB	Internet on board
IP	internet protocol
ISAC	information sharing and analysis centre
ISDN	Integrated services digital network
ISMS	information security management system
ISO	international organisation for standardization
IT	information technology
IoT	Internet of things
IXL	interlocking
KEV	known exploited vulnerabilities
LAN	local area network
MAC	media (or medium) access control
MCG	mobile communication gateway
MMS	maintenance management system
MVB	multifunction vehicle bus
NDR	network device requirement
NIDS	network intrusion detection system
NIS	network and information systems
NIST [US]	national institute of standards and technology
NMS	network management system
NVD	national vulnerability database
OMTS	onboard multimedia and telematic subsystem
OSI	open systems interconnect
OT	operational technology
PACIS	Public Address and Customer Information System
PAS	public address system
PIN	personal identification number
PIS	passenger information system
PKI	public key infrastructure
PLC	programable logic controller
RA	resource availability

RAM	reliability availability maintainability
RAMS	reliability availability maintainability safety
RBC	radio block centre
RDF	restricted data flow
RFC	request for comments
SAT	site acceptance test
SBOM	software bill of materials
SecRAC	security-related application condition
SCADA	supervisory control and data acquisition
SG	security gateway
SIEM	security information and event management
SIL	safety integrity level
SL	security level
SL-A	achieved security level
SL-C	capability security level
SL-T	target security level
SMS	safety management system
SOC	security operations centre
SR	system requirement
STES	safety tunnel earthing system
SuC	system under consideration
SW	software
SDWAN	software defined wide area network
TCMS	train control management system
TCN	train communication network
TMS	traffic management system
TRA	threat risk assessment
TRE	timely response to events
TS	technical specification
TSI	technical specification for interoperability (from ERA)
T&C	test & commissioning
USB	universal serial bus
VPN	virtual private network
VRF	virtual routing and forwarding
V&V	verification & validation
WLAN	wireless local area network

1120
1121

3.3 Taxonomy and terms equivalence

The railway system taxonomy used in this document is shown in Figure 2.

The scope covers railway system (see 3.1.111), railway application (see 3.1.107) and railway solution (see 3.1.110).

The ISA/IEC life cycle of the products below the dotted line in Figure 2 is out-of-scope of this document, (see 6.3 Railway application and product lifecycles). The interface between the product life cycle and the railway application life cycle (supplier management), represented by the dotted line, is considered in this standard.

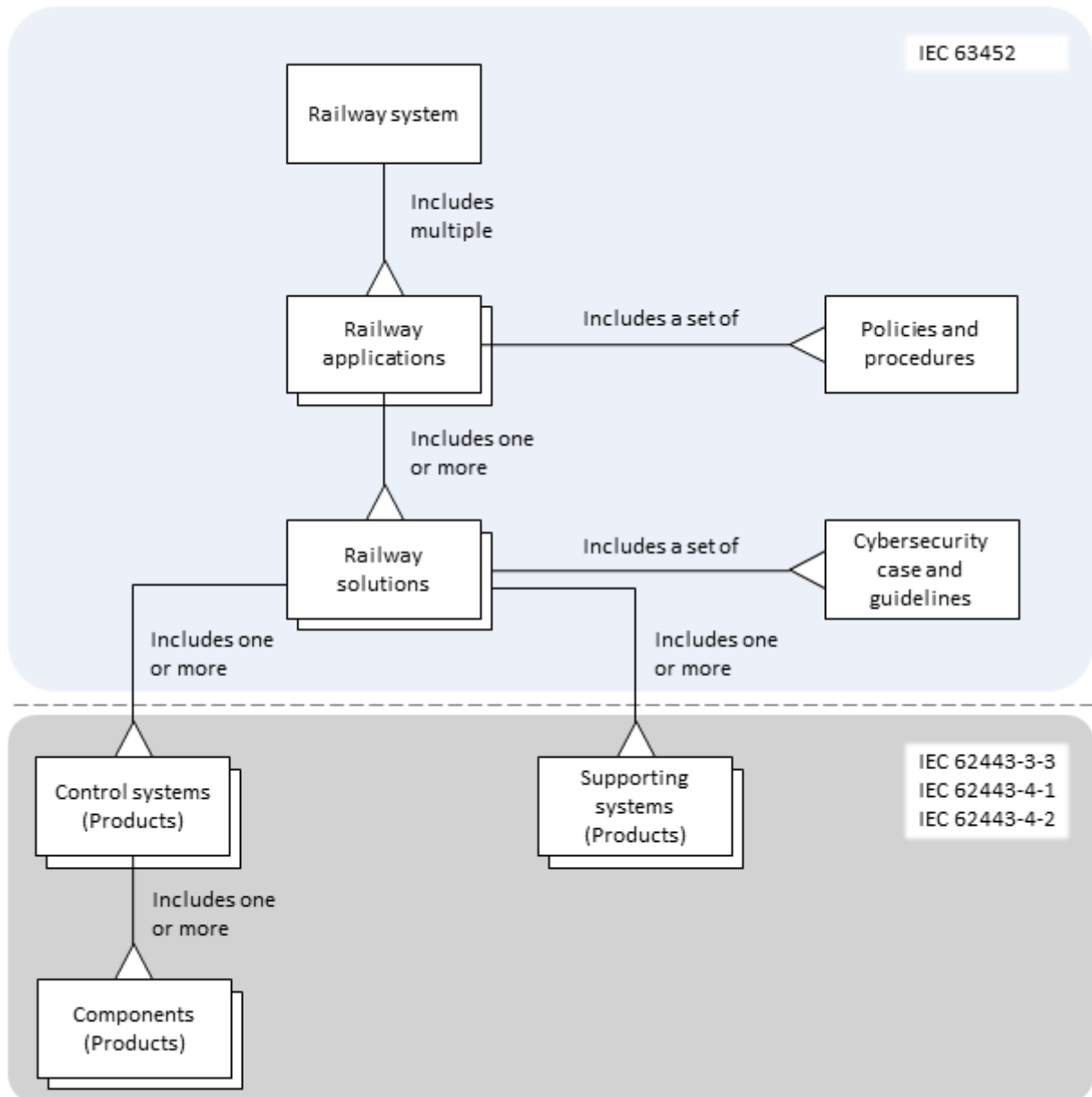


Figure 2 - Railway system taxonomy

Note 1: Figure 2 is based on the Figure 3 – System Taxonomy from ISA-62443-1-1 (D11E1), April 2022

The term system under consideration (SuC) is used with the same meaning as in the IEC 62443 series (see 3.1.148). It is used to define the scope of the railway solution to be provided and on which the cybersecurity Risk Assessment is to be performed.

To ease the adaption and integration of the terms, system taxonomy and roles defined in ISA/IEC 62443-1-1 within railway business, the terms' definitions in Table 1 have been added or adapted and are used throughout the IEC 63452 standard.

1137

Table 1 - IEC 63452 to ISA/IEC 62443 equivalent terms

IEC 63452 term	IEC 63452 Definition reference	ISA/IEC 62443 equivalent term
railway system	3.1.111	<none>
railway application	3.1.107	industrial automation and control system (IACS)
railway solution	3.1.110	automation solution
control system (product)	3.1.40	control system (product)
component (product)	3.1.34	component (product)
safety related system	3.1.122	safety instrumented system (SIS)
legacy system	3.1.80	<none>
railway duty holder	3.1.108	asset owner
integration service provider	3.1.71	integration service provider
maintenance service provider	3.1.86	maintenance service provider

1138 Besides the fact that a railway application can include one or more railway solutions handed over by
 1139 the integration service provider to the railway duty holder, the main difference between them is that a
 1140 railway application is operational and includes the personnel, policies and procedures required for its
 1141 operation, maintenance and decommission.

1142 Note 2: In the IEC 62443 series, it is described that automation solutions are installed in asset owner sites whereas
 1143 in this standard, railway solutions like trains and other rolling stock sub-systems are usually integrated and installed
 1144 by the integration service providers at their sites. Example of railway solutions includes trains, interlocking,
 1145 passenger information systems and automatic train supervision (see Figure 4).

1146 The Table 2 provide some non-exhaustive examples of usage of this taxonomy.

1147

Table 2 - Railway system, application, solution and products examples

IEC 63452 term	Examples
railway system	• A single metro or tramway line (with tracks, signalling, trains, stations and OCC) if not connected with any other lines • The whole metro system of a city if the lines are connected each other • A single railway line (with tracks, signalling, trains, stations and OCC) if not connected with other railway lines • The whole railway system of a country or a region (with tracks, signalling, trains, stations and OCC) when lines are connected each other
railway application	• A train fleet in operation, with their associated personnel, policies and procedures. • A signalling system in operation with its associated personnel, policies and procedures • A railway network (and relevant elements including traffic management, tracking and navigation systems) in operation with their associated security policy and procedure • A train video surveillance/CCTV subsystem and relevant elements in operation with their associated personnel, policies and procedures
railway solution	• manufactured train with relevant subsystems, elements, devices and components designed, installed, and configured to operate in a railway system • Electrification system, (including overhead lines and the trackside electricity consumption measuring and charging system); designed, manufactured, installed, and configured to operate (in a railway system)

	• On-board and trackside equipment required to ensure safety and to command and control movements of trains as well as other functional operations; designed, manufactured, installed, and configured to operate in a railway system • Platform screen doors subsystem with relevant elements, devices and components on both station and train designed, manufactured, installed, and configured to operate (in a railway system)
control system (product)	• Passenger Information System (PIS) • Automatic Train Protection (ATP) • Automatic Train Operation (ATO) • Interlocking (IXL)
component (product)	• Vital computer • Signal, point machine • Camera • Switch, gateway • Train doors controller • closed-circuit television (CCTV)

1148
1149
1150

4 Railway system overview

4.1 Purpose

This clause provides requirements and guidance to the railway duty holder to create a comprehensive description of a railway system for projects where cybersecurity is relevant. This clause is intended to be read in conjunction with IEC TS 62443-1-1, Clause 5.9.

The completeness and quality of information about the railway system is crucial for the effectiveness of projects where cybersecurity is relevant. By adopting the models and procedures in this clause to describe the railway system and its security needs, the following goals can be achieved:

- understandable, complete, and maintainable system documentation
- the capability to align the interpretation of the high-level security needs
- easier derivation of the SuC as a part of the overall railway system
- easier integration of final SuC descriptions into the original railway system description.

Cybersecurity experts and railways stakeholders can benefit from a unique and common description of the SuC. By using the same description, less time will be taken to understand the SuC, which can remove conflicts arising due to different interpretations of the SuC.

4.2 Overview

A railway system description can be established in the following three steps:

- a) Creating a description of the railway system from a cybersecurity perspective to identify all systems belonging to the overarching railway system, as detailed in Subclause 4.3
- b) Identifying the subsystems that compose the railway system and to their topological or physical distribution, as detailed in Subclause 4.4
- c) Describing a high-level railway zone model that comprises all assets of the railway system, as detailed in Subclause 4.5.

Subclause 4.6 deals with the applicability of shared security services within the railway system.

NOTE: This clause uses the terms “railway system”, “railway application”, and “railway duty holder” according to the taxonomy and terms equivalence as described in Clause 3.3.

4.3 [SO-01-01]: Identification of the railway system

4.3.1 Requirement

The railway duty holder shall identify the scope of its railway system and railway application, identifying the OT (operational technology) systems and subsystems, segregating them from the IT (Information Technology) systems.

The railway duty holder shall, where no clear assignment to IT or OT is apparent, decide if the subsystem is to be considered as IT or OT and inform the stakeholder in charge of IT cybersecurity.

4.3.2 Rationale and supplemental guidance

Railway cybersecurity protects railway system essential functions, including if they are threatened by malicious attackers. Cybersecurity of a railway system is effective when no hardware or software assets contributing to essential functions can be exfiltrated, modified, corrupted or deleted by unauthorised people or processes. Since the modification of data or processes may force systems to malfunction, a lack of cybersecurity can result in operational interruptions, damage of assets or, even worse, injury and death of human beings.

Describing the SuC is the first step in understanding the applicability of this standard (and the associated referred 62443 standards) to this SuC.

At minimum, the railway system scope should include the following systems:

- Signalling
- Fixed installation
- Rolling Stock

1195 The railway duty holder can manage the subsystems as different railway applications, for example they can specify
1196 separate security programs for signalling and rolling stock or combine all or some of them as one single railway
1197 application.

1198 Figure 3 shows the segregation of an enterprise's IT systems in an industrial environment as proposed by the IEC
1199 62443 series standards. A key element of this architecture is the segregation of IT and OT by technical means such
1200 as a demilitarised zone (DMZ) or data diode for data exchange between business systems and operational systems,
1201 as well as procedural means which includes different user management policies in the business and operations
1202 context.

1203 In the area of operations or systems management, IT and OT systems can overlap or coexist. This requires careful
1204 consideration towards which policies and related standards are relevant for the individual systems.

1205 The railway duty holder should also consider the application of Internet of Things (IoT) or Industrial IoT (IIoT)
1206 technology in the railway system and manage it according to this standard.

1207 IoT has recently found its way into the railway domain, for example in predictive diagnostics or environmental
1208 monitoring such as avalanche detection. Since this technology can be adapted very quickly to the respective needs
1209 due to its flexible connectivity, special attention should be paid to cybersecurity. These connectivity standards,
1210 which are very often based on radio transmission, are easier to access for potential attackers than traditional railway
1211 components. On the other hand, they may be based on cloud technology, which can ensure the maintenance of
1212 cybersecurity through continuous monitoring and networked maintenance management.

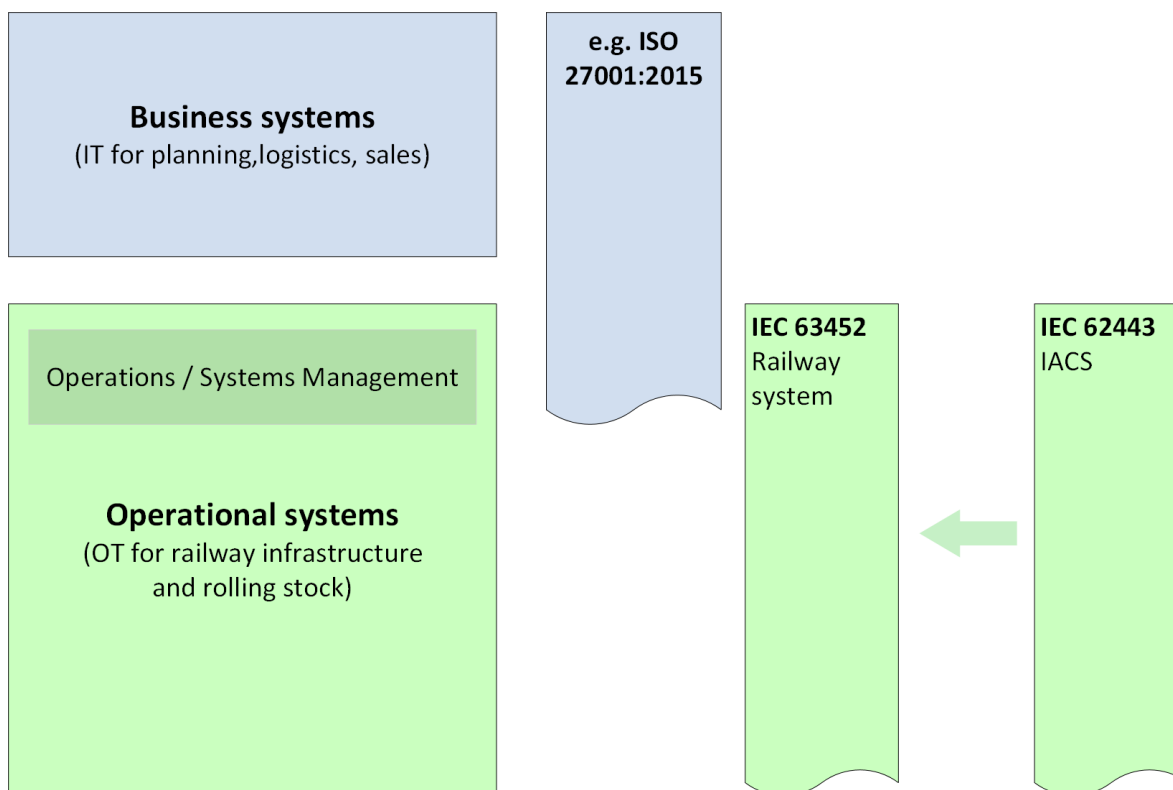


Figure 3 - Segregation between IT and OT

1215 The low cost of technology is leading to the substitution of pyramidal or hierarchical structures of automation of
1216 control systems with more flexible and adaptable architectures, which span over multiple locations and independent
1217 organisations, with very different responsibilities and competences.
1218

4.4 [SO-02-01]: Definition of a high-level railway system model

4.4.1 Requirement

The railway duty holder shall set out a high-level system model of the railway system.

4.4.2 Rationale and supplemental guidance

Subsystems should be divided in groups taking the following aspects into account:

- physical location, such as trackside-onboard, stations, tracks and data centres
- functional criticality level, such as signalling, command and control, auxiliary, comfort and public (see Figure 4)
- organisational context, such as responsible entities including operators and maintainers.

The resulting model can be used as a basis to define SuC for different railway applications, for example a traffic management system.

Subclauses 4.4.2.1 and 0 give examples how to create the high-level railway system model.

4.4.2.1 Area-based approach

Figure 4 shows an example of an area-based railway system model. Subsystems are allocated in three areas to show their corresponding physical area. Each subsystem is identified by its functional name, for example the “traffic management system”, and coloured to indicate the subsystem group. Subsystems of the same group have similar criticality or type of function, and are more likely to be interconnected, though they are often separated in different virtual or physical networks. Nevertheless, there are also logical connections between different subsystems of different criticality or group, for instance, between a traffic management system and an interlocking.

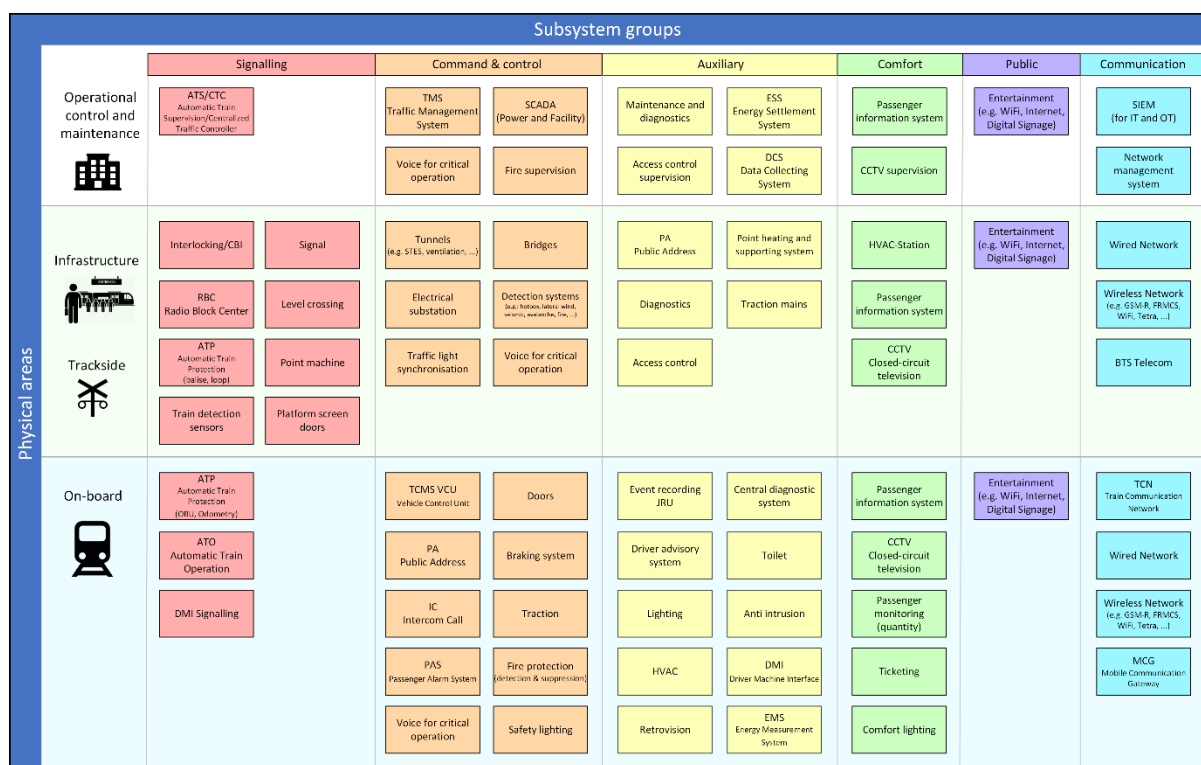


Figure 4 - Example of an area-based railway system model

NOTE: In addition to the subsystems and functionalities shown in Figure 2, there are many of network devices, such as switches and routers, spread all over the railway system (including trains) that are also regarded as assets to be protected from cybersecurity attacks. These components should be considered either as part of the security zone or as a part of the subsystem for which they deliver the network service.

Annex F.1 provides a guidance on how to build an area-based high level-railway system model.

4.4.2.2 Topology-based approach

One of the main challenges of the railway system is its large extent, ranging from a few kilometres up to several thousand kilometres. Therefore, the network types used range from local area networks up to wide area networks and can also include the use of public network connections.

Furthermore, many subsystems include a variety of products and communication protocols demanding the creation of a comprehensive network architecture of the railway system.

Figure 5 shows an example of a topology-based view of the railway system.

From a cybersecurity perspective, the distributed locations of the different components and subsystems as well as their physical security features should be considered, especially in risk analysis.

For instance, assets located along the track are likely to be more prone to a direct physical attack than assets in a control centre. On the other hand, a traffic management system, may have interfaces to the enterprise environment such as Enterprise Resource Planning (ERP) systems, mail servers, and other office systems which may be prone to a denial-of-service (DoS) attack or other threats such as ransomware in the IT domain.

Railway duty holders and integration service providers can identify the network-oriented connections between the components of the SuC in the topology-based model.

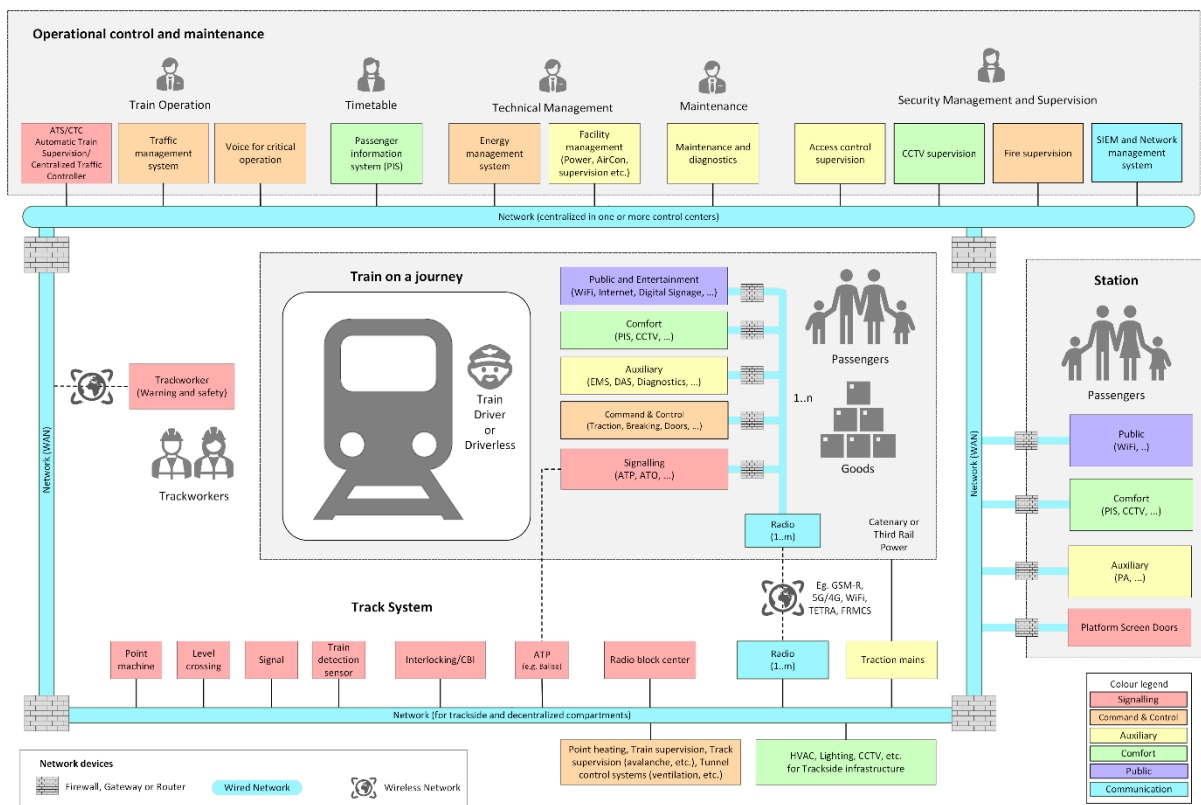


Figure 5 - Example of a topology-based railway system model

NOTE: The terms 1..m and 1..n mean that there can be one or more communication channels on-board and/or between train and ground. Further explanations of train to ground communication can be found in Annex F.4.

Annex F.1 provides guidance on how to build a topology-based high-level railway system model.

4.5 [SO-03-01]: Definition of a high-level railway zone model

4.5.1 Requirement

The railway duty holder shall set out a high-level railway zone model of the railway system. The railway zone model is the grouping of assets in different zones and criticality.

4.5.2 Rationale and supplemental guidance

By the railway duty holder setting out a high-level railway system zone model when applying this standard, a structure to the systems and subsystems according to their criticality for railway operation will be provided.

- 1272 This subclause references the design principles of IEC 62443-1-1 and uses zones in a generic way. With reference
1273 to IEC 62443-1-1, the term zone is used as a synonym for a security zone.
- 1274 The high-level railway zone model will be used in cybersecurity relevant projects as an input for the identification of
1275 the SuC, the initial risk assessment and zoning activities.
- 1276 The definition of zones includes measures for encapsulation of functionality to keep a particular service alive in the
1277 case of a security incident in another zone; the same as the capability to isolate an incident by closing gateways to
1278 an infected zone.
- 1279 The combination of zones, conduits, subsystems and zone priorities results in a generic zone model including
1280 communication rules (see Annex F.3). Figure 6 shows an example of a high-level railway zone model according to
1281 the design principles of IEC 62443-1-1, which supports the risk-based approach in IEC 62443-3-2.
- 1282 The railway duty holder zone model depends on existing systems and zones, of the result of the threat risk
1283 assessment and of the specific architecture of its railway system.
- 1284 Following principles are part of the zoning concept:
- 1285 – The communication and human interactions in high criticality zones should be monitored, logged,
1286 and stored for forensics at least at the subsystem boundaries (see also IEC 62443-3-3, SR 2.8).
 - 1287 – Security devices between zones with different criticality that protect the zone with the higher
1288 criticality should be managed by the responsible organisation of the higher criticality zone (see
1289 also IEC 62443-3-2, ZCR 3.1).
 - 1290 – The higher criticality zone should consider inputs from the lower zone as potentially hostile
 - 1291 – The data flow between rolling stock and land-based subsystems should be reduced to a minimum
1292 of conduits (without impacting the availability of the communication) to control and detect
1293 unallowed data flow and malware by security devices.
- 1294 The principles are further described in Annex F.3, that contains also practical examples how to
1295 evaluate the criticality of systems to build security zones.

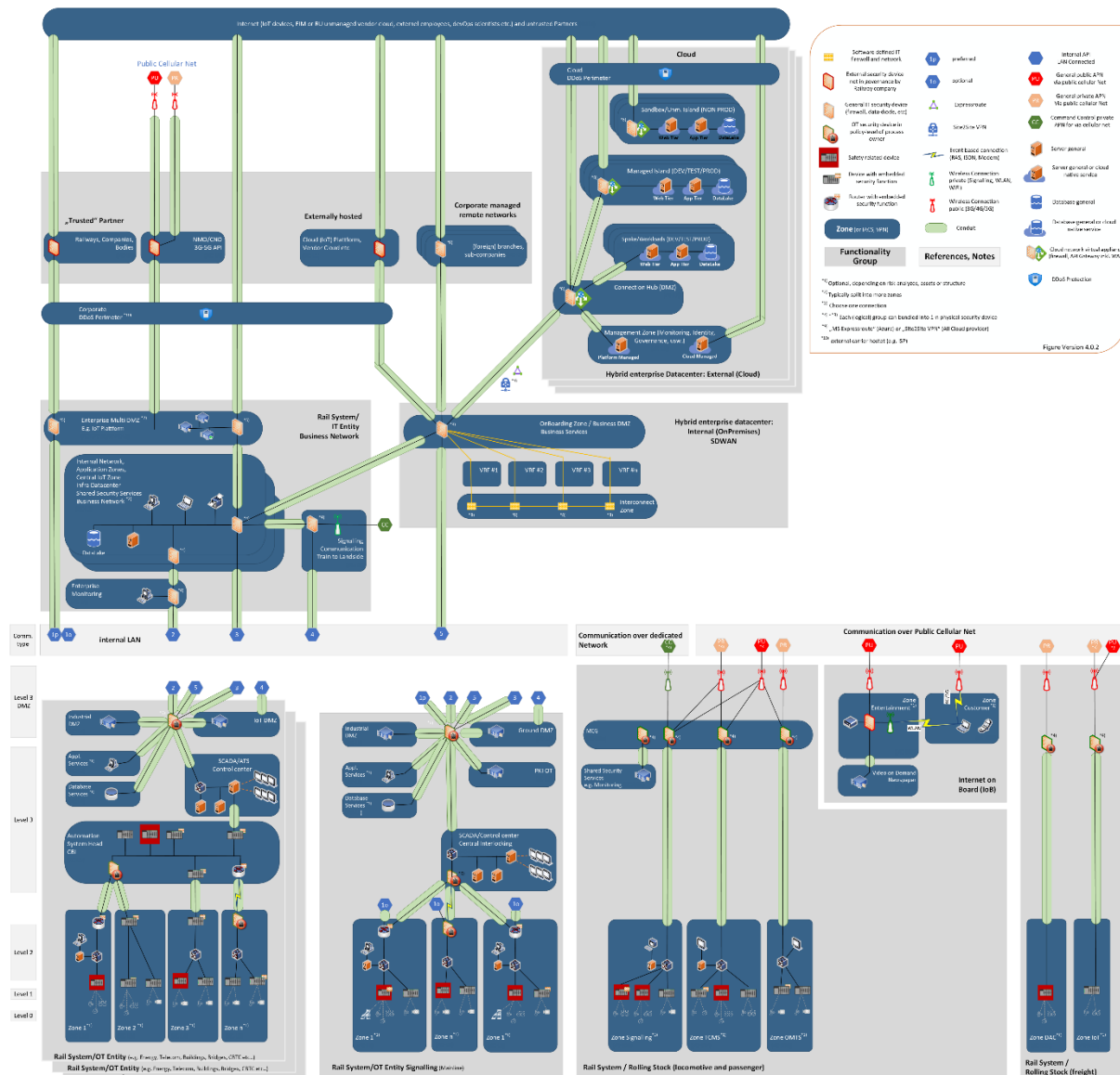


Figure 6 - Example of a high-level railway zone model

NOTE 1: The levels on the left side are based on the Purdue Enterprise Reference Architecture (PERA).

NOTE 2: For magnified sections of Figure 6 see Annex F.2.

NOTE 3: Some technical publications differentiate zones in network zones, security zones or communication zones. Network zones represent the wide area communication which normally is not under control of the railway duty holder. Security zones represents group of assets with similar security requirements. Communication zones are special zones without any operational components. They represent the communication and are terminated with a security device on each edge.

NOTE 4: The aim of defining zones and conduits is to group systems or components that have the same requirements from the security perspective, due to similar threats and possible impacts.

As an alternative, the zones and conduits can be defined based on the predefined protection requirements. The integration and application of the zone model is highly dependent on the railway duty holders SuC, also due to legacy systems or processes.

This methodology supports cybersecurity risk analysis and the definition of measures on system and component level. Corresponding security zones can exist in multiple locations but are connected by conduits meeting the appropriate security requirements.

In contrast, a conduit or a network zone should separate different areas to ensure communication between zones of common security requirements. A network zone can be a measure to support security but is not a complete security solution.

See also Annex A (Handling conduits).

4.6 [SO-04-01]: Specification of shared security services

4.6.1 Requirement

The railway duty holder shall specify which shared security services shall be provided centrally by the railway system and which shared security services shall be provided as an inherent capability of the SuC itself.

4.6.2 Rationale and supplemental guidance

To efficiently comply with several security requirements, it is recommended that some security functions are implemented as shared services amongst components.

Figure 7 provides an example a set of security functions that, according to research and practice, can be shared.

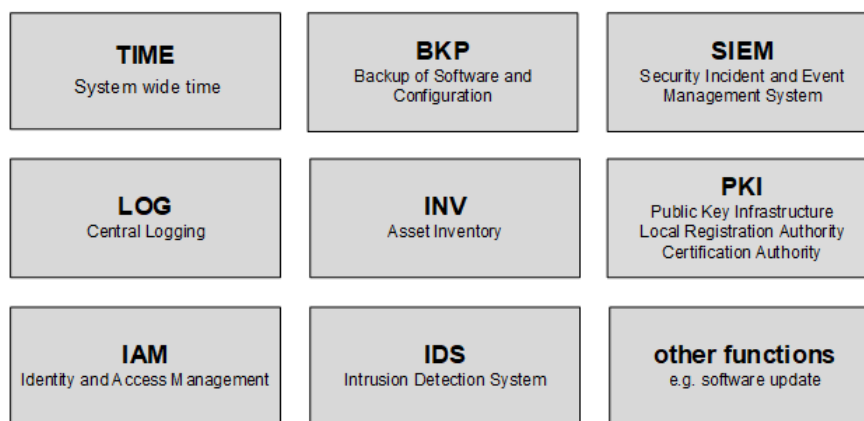


Figure 7 - Example of shared security service

The security functions as shown in Figure 7 can be integrated into one or more security services or provided by several services, such as multiple time servers. Since these services require a lot of effort regarding implementation and operation, it is recommended to share them for systems or subsystems.

For example, some services could be implemented and operated centrally for the whole railways system, as might be the case for TIME or Security Incident and Event Management (SIEM) systems. Alternatively, they can be implemented on subsystem level, for example PKI for the trackside signalling of one infrastructure operator.

The functions in Figure 7 are described in Clause 8 (Security requirements), where they are further referenced to the corresponding system requirements of IEC 62443-3-3.

5 Overall cybersecurity management

5.1 General

The following subclauses deal with requirements on processes and procedures for the cybersecurity management of railway applications. These activities are not related to a specific SuC lifecycle. They are to be managed globally at an organisational level and they are to be applied before, during and after any SuC lifecycle and they are required to be in place independent of a given SuC for the railway duty holder, integration service provider and maintenance service provider.

EXAMPLE: Training and awareness management

5.2 [CP-01-01] Railway OT cybersecurity program

5.2.1 Requirement

An railway OT cybersecurity program shall be established before the development of a new railway application, approved by management and shall include the programme's objectives, scope, and responsibilities.

The railway OT cybersecurity program is located at organisational level independent of any SuC.

Within the railway OT cybersecurity program, the following capabilities shall be implemented:

- OT governance management,
- Architecture management,
- Supply chain management,
- Awareness / training management,
- Inventory management,
- Risk management,
- Vulnerability management,
- Patch management,
- Incident management,
- Business continuity management,
- Operations/maintenance management,
- Cybersecurity monitoring,
- Decommissioning management.

5.2.2 Rationale and supplemental guidance

Management approval is essential to the Railway OT cybersecurity program as it requires the allocation of resources (personnel and financial) to apply a process across functional disciplines. Once the handover of the SuC has taken place, the railway duty holder addresses several topics for the operational lifecycle of the SuC, where the majority the SUC's lifecycle is conducted and maybe operational for decades. An Railway OT cybersecurity program ensures a structured and systematic approach to meeting the operational requirements.

NOTE: Refer to IEC 62443-2-1 (ORG 1.2, 1.3, 2.4) and NIST SP 800-82 for further guidance on OT cybersecurity programs.

5.2.3 Output

A documented Railway OT cybersecurity program.

5.3 [CP-02-01] Railway OT cybersecurity program coordination

5.3.1 Requirement

The Railway OT cybersecurity program shall be aligned with existing management systems. These can be one or more of the following:

- Information security management systems (ISMS); or
- Cybersecurity management system (CSMS); or
- Safety management system (SMS); or