



BSI Standards Publication

Railway applications — Cybersecurity

National foreword

This Published Document is the UK implementation of CLC/TS 50701:2021.

The UK participation in its preparation was entrusted to Technical Committee GEL/9, Railway Electrotechnical Applications.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 539 05296 1

ICS 35.030; 45.020

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 July 2021.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English Version

Railway applications - Cybersecurity

Applications ferroviaires - Cybersécurité

Bahnanwendungen - IT-Sicherheit

This Technical Specification was approved by CENELEC on 2021-05-11.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents	Page
European foreword	6
Introduction	7
1 Scope	8
2 Normative references	8
3 Terms, definitions and abbreviations	8
3.1 Terms and definitions.....	8
3.2 Abbreviations	24
4 Railway system overview	26
4.1 Introduction	26
4.2 Railway asset model	27
4.3 Railway physical architecture model.....	28
4.4 High-level railway zone model	29
5 Cybersecurity within a railway application lifecycle	31
5.1 Introduction	31
5.2 Railway application and product lifecycles	31
5.3 Activities, synchronization and deliverables	31
5.4 Cybersecurity context and cybersecurity management plan	35
5.5 Relationship between cybersecurity and essential functions	35
5.5.1 General	35
5.5.2 Defence in depth	35
5.5.3 Security-related application conditions	36
5.5.4 Interfaces between the safety and the cybersecurity processes	37
5.6 Cybersecurity assurance process.....	38
6 System definition and initial risk assessment	39
6.1 Introduction	39
6.2 Identification of the system under consideration	40
6.2.1 Definition of the SuC.....	40
6.2.2 Overall functional description	41
6.2.3 Access to the SuC	41
6.2.4 Essential functions.....	41
6.2.5 Assets supporting the essential functions	42
6.2.6 Threat landscape	42
6.3 Initial risk assessment	42
6.3.1 Impact assessment.....	42
6.3.2 Likelihood assessment	43
6.3.3 Risk evaluation	44
6.4 Partitioning of the SuC	45

6.4.1	Criteria for zones and conduits breakdown	45
6.4.2	Process for zones and conduits breakdown	45
6.5	Output and documentation	46
6.5.1	Description of the system under consideration	46
6.5.2	Documentation of the initial risk assessment	46
6.5.3	Definition of zones and conduits	46
7	Detailed risk assessment	47
7.1	General aspects	47
7.2	Establishment of cybersecurity requirements	48
7.2.1	General	48
7.2.2	Threat identification and vulnerability identification	49
7.2.3	Vulnerability identification	51
7.2.4	Risk acceptance principles	51
7.2.5	Derivation of SL-T by explicit risk evaluation	53
7.2.6	Determine initial SL	55
7.2.7	Determine countermeasures from EN IEC 62443-3-3	56
7.2.8	Risk estimation and evaluation	56
7.2.9	Determine security level target	58
7.2.10	Cybersecurity requirements specification for zones and conduits	58
8	Cybersecurity requirements	59
8.1	Objectives	59
8.2	System security requirements	59
8.3	Apportionment of cybersecurity requirements	74
8.3.1	Objectives	74
8.3.2	Break down of system requirements to subsystem level	75
8.3.3	System requirement allocation at component level	75
8.3.4	Specific consideration for implementation of cybersecurity requirement on components	76
8.3.5	Requirement breakdown structure as verification	76
8.3.6	Compensating countermeasures	77
9	Cybersecurity assurance and system acceptance for operation	78
9.1	Overview	78
9.2	Cybersecurity case	79
9.3	Cybersecurity verification	80
9.3.1	General	80
9.3.2	Cybersecurity integration and verification	80
9.3.3	Assessment of results	82
9.4	Cybersecurity validation	82
9.5	Cybersecurity system acceptance	83
9.5.1	Independence	83
9.5.2	Objectives	83
9.5.3	Activities	83

9.5.4 Cybersecurity handover	83
10 Operational, maintenance and disposal requirements	83
10.1 Introduction	83
10.2 Vulnerability management	84
10.3 Security patch management	85
10.3.1 General	85
10.3.2 Patching systems while ensuring operational requirements	86
Annex A (informative) Handling conduits	89
Annex B (informative) Handling legacy systems	92
Annex C (informative) Cybersecurity design principles	98
Annex D (informative) Safety and security	127
Annex E (informative) Risk acceptance methods	131
Annex F (informative) Railway architecture and zoning	140
Annex G (informative) Cybersecurity deliverables content	158
Bibliography	161

Figures

Figure 1 — Segregation of IT and OT	27
Figure 2 — Railway asset model (example)	28
Figure 3 — Railway physical architecture model (example)	29
Figure 4 — Generic high-level railway zone model (example)	30
Figure 5 — Defence in depth with example of measures	36
Figure 6 — Relationship TRA and SA	39
Figure 7 — Initial risk assessment flowchart	40
Figure 8 — Detailed risk assessment flowchart	49
Figure 9 — Explicit risk evaluation flowchart	54
Figure 10 — Handling of SL-C	77
Figure 11 — Cybersecurity assurance	78
Figure 12 — Cybersecurity case concept	79
Figure 13 — Cybersecurity assurance during integration and validation activities	81
Figure 14 — General vulnerability handling flowchart	85
Figure 15 — Vulnerability and outage time during system update (maintenance phase) [example]	87
Figure 16 — Vulnerability and outage time during system update with observation phases [example]	88
Figure A.1 — Zones and conduits example	90
Figure D.1 — Security as an environmental condition for safety	128
Figure F.1 — Adopted generic high-level railway zone model (example)	148
Figure F.2 — Example of a railway system zone model	149

Tables

Table 1 — Security-related activities within a railway application lifecycle (EN 50126-1)	32
Table 2 — Examples of function related supporting assets in regard to the defence in depth layers	36
Table 3 — Qualitative Impact Assessment example	43
Table 4 — Likelihood assessment matrix – Example	44
Table 5 — Risk matrix example	44
Table 6 — System Security Requirements and Foundational Classes	61
Table E.1 — Risk acceptance categories acc. EN 50126-1	131
Table E.2 — Mapping severity categories acc. EN 50126-1 to cybersecurity severity	132
Table E.3 — Likelihood assessment criteria	132
Table E.4 — Mapping Likelihood to accessibility and Probability	133
Table E.5 — Impact assessment matrix – Example 2	134
Table E.6 — Likelihood assessment matrix – Example 2	135
Table E.7 — Risk acceptance matrix – Example 2	136
Table E.8 — Impact assessment matrix – Example 3	137
Table E.9 — Likelihood assessment matrix – Example 3	138
Table E.10 — Likelihood conversion table – Example 3	138
Table E.11 — Risk acceptance matrix – Example 3	138
Table E.12 — Risk Severity / Mitigation matrix – Example 3	139
Table F.1 — Railway system glossary	140
Table F.2 — Example – Evaluating groups of criticalities for landside-landside communication	143
Table F.3 — Example – Zone criticality definition for landside-landside communication	144
Table F.4 — Example – Landside-landside communication matrix basic structure	145
Table F.5 — Example – Communication matrix - landside to landside	146
Table F.6 — Example – Rolling stock zone model	150
Table F.7 — Example – Communication matrix - rolling stock to rolling stock	151
Table F.8 — Example – Communication matrix - landside to rolling stock	154
Table F.9 — Example – Communication matrix - rolling stock to landside	155

European foreword

This document (CLC/TS 50701:2021) has been prepared by CLC/TC 9X “Electrical and electronic applications for railways”.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Introduction

The aim of this document is to introduce the requirements as well as recommendations to address cybersecurity within the railway sector.

Due to digitization and the need for more performance and better maintainability, previously isolated industrial systems are now connected to large networks and increasingly use standard protocols and commercial components. Because of this evolution, cybersecurity becomes a key topic for these industrial systems, including critical systems such as railway systems.

The purpose of this document is that, when a railway system is compliant to this document, it can be demonstrated that this system is at the state of the art in terms of cybersecurity, that it fulfils its targeted Security Level and that its security 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 EN 50126-1 when it is applied to the system under consideration
- due to lifecycle differences between safety and cybersecurity, separate safety approval and cybersecurity acceptance as much as possible
- identify the key synchronization points related to cybersecurity between system integrator and asset owner
- provide harmonized and standardized way to express technical cybersecurity requirements
- provide cybersecurity design principles promoting simple and modular systems
- allow the usage of market products such as industrial COTS compliant with the 62443 series.

1 Scope

This document provides the railway operators, system integrators and product suppliers, with guidance and specifications on how cybersecurity will be managed in the context of EN 50126-1 RAMS lifecycle process. This document aims at the implementation of a consistent approach to the management of the security of the railway systems. This document can also be applied to the security assurance of systems and components/equipment developed independently of EN 50126-1:2017.

This document applies to Communications, Signalling and Processing domain, to Rolling Stock and to Fixed Installations domains. It provides references to models and concepts from which requirements and recommendations can be derived and that are suitable to ensure that the residual risk from security threats is identified, supervised and managed to an acceptable level by the railway system duty holder. It presents the underlying security assumptions in a structured manner.

This document does not address functional safety requirements for railway systems but rather additional requirements arising from threats and related security vulnerabilities and for which specific measures and activities need to be taken and managed throughout the lifecycle. The aim of this document is to ensure that the RAMS characteristics of railway systems / subsystems / equipment cannot be reduced, lost or compromised in the case of intentional attacks.

The security models, the concepts and the risk assessment process described in this document are based on or derived from IEC/EN IEC 62443 series standards. This document is consistent with the application of security management requirements contained within IEC 62443-2-1 which in turn are based on EN ISO/IEC 27001 and EN ISO 27002.

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.

EN 50126-1:2017, *Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process*

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

EN IEC 62443-3-3:2019¹, *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, definitions and abbreviations

3.1 Terms and definitions

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

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

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online Browsing Platform: available at <http://www.iso.org/obp>

NOTE The correspondence of the terms IACS, Solution and System used in EN IEC 62443 series with the terms in this document can need further clarification in future issues of the TS. Particularly, when using EN IEC 62443

¹ Document impacted by EN IEC 62443-3-3:2019/AC:2019-10.

definitions and requirements, the term “IACS” is to be understood and replaced by, “railway application” or “railway system” as relevant in the context.

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 (authorization 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 (authorization to log in to a system and application, through a combination of logical and physical means).

3.1.3

access control

<control>

protection of system resources against unauthorized access

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

3.1.4

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.

[SOURCE: EN IEC 62443-4-1:2018, 3.1.3]

3.1.5

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]

3.1.6

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.

3.1.7

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"

3.1.8

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]

3.1.9

asset

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

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

3.1.10

asset owner

individual or organization responsible for one or more IACS

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

[SOURCE: EN IEC 62443-4-1:2018, 3.1.6, modified – Note 1 to entry has been added]

3.1.11

attack

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

Note 1 to entry: The damage can be e.g. destruction, disclosure, alteration, unauthorized use.

[SOURCE: IEC 60050-171:2019, 171-08-12]

3.1.12

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: EN IEC 62443-2-4:2019, 3.1.2]

3.1.13**attack vector**

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

3.1.14**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]

3.1.15**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: EN IEC 62443-4-1:2018, 3.1.9]

3.1.16**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]

3.1.17**boundary**

software, hardware, or other physical barrier that limits access to a system or part of a system

3.1.18**boundary device**

communication security asset, within a zone or conduit, that provides a protected interface between a zone and a conduit

3.1.19**communication channel****<in cybersecurity>**

specific logical or physical communication link between assets

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

[SOURCE: EN IEC 62443-3-3:2019¹, 3.1.9]

3.1.20

communication path

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.

3.1.21

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 IACS.

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

[SOURCE: EN IEC 62443-4-2:2019, 3.1.9]

3.1.22

compromise

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

3.1.23

conduit

<in cybersecurity>

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

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

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

3.1.24

confidentiality

<in cybersecurity>

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

Note 1 to entry: When used in the context of an IACS, confidentiality refers to protecting IACS data and information from unauthorized access.

[SOURCE: EN IEC 62443-4-2:2019, 3.1.12]

3.1.25**connection****<in cybersecurity>**

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

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

3.1.26**control network**

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

Note 1 to entry: The control network can be subdivided into zones, and there can be multiple separate control networks within one company or site.

3.1.27**control system****<in industrial automation and control system>**

hardware and software components of an IACS

Note 1 to entry: Control systems are composed of field devices, embedded control devices, network devices, and host devices (including workstations and servers).

[SOURCE: EN IEC 62443-3-3:2019¹, 3.1.16, modified – Note 1 to entry has been added]

3.1.28**countermeasure**

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

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

[SOURCE: EN IEC 62443-3-3:2019¹, 3.1.17]

3.1.29**cybersecurity****<in railway application>**

set of activities and measures taken with the objective to prevent, detect, react to unauthorized access or cyberattack which could lead to an accident, an unsafe situation, or railway application performance degradation

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

3.1.30**data diode**

boundary device which ensures that data between two separate networks is only transmitted in one direction

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

3.1.31

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

3.1.32

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: EN IEC 62443-3-3:2019¹, 3.1.19]

3.1.33

denial of service

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

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

3.1.34

digital signature

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]

3.1.35

encryption

<of data>

transformation of data in order to hide their semantic content using cryptography

Note 1 to entry: The reverse process is called decryption.

[SOURCE: IEC 60050-171:2019, 171-08-09]

3.1.36**essential function**

function or capability that is required to maintain health, safety, the environment and availability for the equipment under control

Note 1 to the entry: Essential functions include, but are not limited to, the safety instrumented function (SIF), the control function and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control and loss of view respectively. In some industries additional functions such as history may be considered essential.

[SOURCE: EN IEC 62443-4-2:2019, 3.1.20]

3.1.37**firewall**

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

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

3.1.38**gateway****<for computer networks>**

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

[SOURCE: IEC 60050-732:2019, 732-01-17, modified – The notes to entry have been omitted]

3.1.39**handover****<from system integrator to asset owner>**

act of turning a railway solution over to the asset owner

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

3.1.40**host computer****host**

in a computer network, a computer that provides end users with services such as computation and data base access and that may perform network control functions

[SOURCE: IEC 60050-732:2010, 732-01-14]

3.1.41**impact**

evaluated consequence of a particular event

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: EN IEC 62443-3-3:2019¹, 3.1.27, modified – Note 1 to entry has been added]

3.1.42

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: EN IEC 62443-3-3:2019¹, 3.1.28]

3.1.43

integration service provider

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

Note 1 to entry: Integration service providers are often referred to as integrators or Main Automation Contractors (MAC).

[SOURCE: EN IEC 62443-2-4:2019, 3.1.9]

3.1.44

integrity

<of data>

property that sensitive data has not been modified or deleted in an unauthorized 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”]

3.1.45

intrusion

<in cybersecurity>

unauthorized act of compromising a system

Note 1 to entry: See “attack”.

3.1.46

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 unauthorized manner

3.1.47

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 an IACS.

[SOURCE: EN IEC 62443-4-2:2019, 3.1.28]

3.1.48

legacy system

any kind of system which is already in operation

3.1.49

likelihood

<of occurrence>

weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities

[SOURCE: NIST SP 800-30: September 2012]

3.1.50**non-repudiation****<in cybersecurity>**

ability to prove the occurrence of a claimed event or action and its originating entities

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

[SOURCE: EN IEC 62443-3-3:2019¹, 3.1.33]

3.1.51**patch management**

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

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

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

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

3.1.52**penetration**

successful unauthorized access to a protected system resource

3.1.53**privilege**

authorization or set of authorizations 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 setpoints and modifying control algorithms.

3.1.54**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 a user or 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.

3.1.55**Purdue model**

model that was adopted from the Purdue Enterprise Reference Architecture (PERA) model by ISA-99, and used as a concept model for 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.

3.1.56

railway application

part of a running railway system which consists of a technical system with its organizational and procedural measures

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

[SOURCE (for IACS): IEC/TS 62443-1-1:2009, 3.2.57]

3.1.57

railway duty holder

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

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

- the owner(s) of one or more parts of the system assets and their purchasing agents;
- the operator of the system;
- the maintainer(s) of one or more parts of the system;

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

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

3.1.58

reference model

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

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

3.1.59

remote access

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

[SOURCE: EN IEC 62443-3-3:2019¹, 3.1.35]

3.1.60

residual risk

<in cybersecurity>

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

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

3.1.61

risk

<in cybersecurity>

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

[SOURCE: EN IEC 62443-3-2:2020, 3.1.14]

3.1.62**risk assessment****<in cybersecurity>**

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

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

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

3.1.63**risk mitigation**

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

3.1.64**role**

set of connected behaviours, privileges and obligations associated with all users (humans, software processes or devices) of an IACS

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

[SOURCE: EN IEC 62443-3-3:2019¹, 3.1.36]

3.1.65**safety**

freedom from unacceptable risk

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]

3.1.66**safety-related application condition**

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

Note 1 to entry: Application conditions can be e.g.: operational restrictions (e.g. speed limit, maximum duration of use), operational rules, maintenance restrictions (e.g. requested maintenance intervals) or environmental conditions.

[SOURCE: EN 50126-1:2017, 3.75]

3.1.67**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]

3.1.68

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]

3.1.69

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

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

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

3.1.70

security assurance

<in cybersecurity>

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

[SOURCE: NIST SP 800-39, amended]

3.1.71

security incident

<in cybersecurity>

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

Note 1 to entry: The term ‘of some significance’ is relative to the environment in which the security compromise is detected. For example, the same compromise may be declared as a security incident in one environment and not in another. Triage activities are often used by asset owners to evaluate security compromises and identify those that are significant enough to be considered incidents.

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

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

3.1.72

security level

<in cybersecurity>

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

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

[SOURCE: EN IEC 62443-3-3:2019¹, 3.1.38, modified]

3.1.73**security objective****<in cybersecurity>**

aspect of security whose purpose is to use certain mitigation measures, such as confidentiality, integrity, availability, user authenticity, access authorization, accountability, etc

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

3.1.74**security patch****<in cybersecurity>**

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: EN IEC 62443-2-4:2019, 3.1.17]

3.1.75**security policy**

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

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

3.1.76**security program****<in cybersecurity>**

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

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

[SOURCE: EN IEC 62443-2-4:2019, 3.1.18]

3.1.77**security-related application condition****<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 e.g.: operational restrictions (e.g. access control usage), operational rules, maintenance rules (antimalware update periodicity) or environmental conditions (e.g. external PKI infrastructure)

3.1.78**security services****<in cybersecurity>**

mechanisms used to provide confidentiality, data integrity, authentication, or non repudiation of information

3.1.79**sensitive data**

data that is likely to cause 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 unauthorized disclosure or modification

3.1.80

service provider

<in cybersecurity>

individual or organization (internal or external organization, manufacturer, etc.) that provides a specific support service and associated supplies in accordance with an agreement with the asset owner

Note 1 to entry: This term is used in place of the generic word “vendor” to provide differentiation.

[SOURCE: EN IEC 62443-2-4:2019, 3.1.19]

3.1.81

session

semi-permanent, stateful, interactive information interchange between two or more communicating devices

Note 1 to entry: Typically, a session has a clearly defined start process and end process.

[SOURCE: EN IEC 62443-3-3:2019¹, 3.1.40]

3.1.82

system integrator

person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications

[SOURCE: EN IEC 62443-4-1:2018, 3.1.34]

3.1.83

system under consideration

collection of assets that are needed to provide and operate 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: EN IEC 62443-3-2:2020, 3.1.19, modified to be adapted to railway context]

3.1.84

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 unauthorized access, destruction, disclosure, modification of data and/or denial of service

[SOURCE: EN IEC 62443-3-3:2019¹, 3.1.44]

3.1.85

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 (e.g. company, facility or SuC)

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

3.1.86**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

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

3.1.87**threat vector****<in cybersecurity>**

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

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

3.1.88**verification**

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

Note 1 to entry: The term “verified” is used to designate the corresponding status.

Note 2 to entry: Design verification is the application of tests and appraisals to assess conformity of a design to the specified requirement.

Note 3 to entry: Verification is conducted at various lifecycle phases of development, examining the system and its constituents to determine conformity to the requirements specified at the beginning of that lifecycle phase.

[SOURCE: EN 50126-1:2017, 3.83, modified – “life cycle” has been replaced by lifecycle]

3.1.89**vulnerability**

flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy

[SOURCE: EN IEC 62443-3-2:2020, 3.1.24]

3.1.90**zone**

grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access (e.g. least privilege principles) or responsible organization

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

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

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply:

ANSSI	agence nationale de la sécurité des systèmes d'information
API	application programming interface
APN	access point name
ATP	automatic train protection
CCTV	closed-circuit television
CIA	confidentiality, integrity, and availability
CISO	chief Information security officer
COTS	commercial off the shelf
CPU	central processing unit
CR	component requirement
CRS	cybersecurity requirements specification
CVE	common vulnerabilities and exposures
DAS	driver advisory system
DC	data confidentiality
DMI	driver machine interface
DMZ	demilitarized zone
DoS	denial of service
EMS	energy management system
ENISA	European Network and Information Security Agency
ERA	European Railway Agency
ERP	enterprise resource planning
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EVC	European Vital Computer
FR	foundational requirement
HVAC	heating, ventilation and air-conditioning
HW	Hardware
IAC	identification and authentication control
IACS	industrial automation and control system(s)
ICS	industrial control systems
ID	identifier
IDS	intrusion detection system
IEC	International Electrotechnical Commission
I/O	input/output

IP	internet protocol
ISO	international organization for standardization
IT	information technology
IXL	Interlocking
LAN	local area network
MAC	media (or medium) access control
MCG	mobile communication gateway
NDR	network device requirement
NIDS	network intrusion detection system
NIS	network and information systems
NIST [US]	national institute of standards and technology
NMS	network monitoring system
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
RA	resource availability
RAM	reliability availability maintainability
RAMS	Reliability Availability Maintainability Safety
RBC	radio block centre
RDF	restricted data flow
SAT	site acceptance test
SecRAC	security-related application condition
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
SR	system requirement
SRAC	safety-related application condition
STES	safety tunnel earthing system

SuC	system under consideration
SW	software
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)
USB	universal serial bus
VPN	virtual private network
WLAN	wireless local area network

4 Railway system overview

4.1 Introduction

This Clause describes the railway system covered by this document. There might be deviations in different countries where the NIS directive is applied; or even between different railway operators. The 'system under consideration' (SuC) referred in several parts of this document is always a part of the railway system.

The following figure shows the segregation of an enterprise IT in an industrial environment as proposed by the IEC 62443 series. A key element of this architecture is the segregation of IT (information technology) and OT (operation technology) by technical (e.g. DMZ for data exchange between the business zone and the control zone) as well as procedural means (e.g. different user management policies in the two zones). In this document the railway system is defined as the equivalent to the control zone in IEC/TS 62443-1-1. The proposed segregation of IT and OT in the railway system is shown in Figure 1.

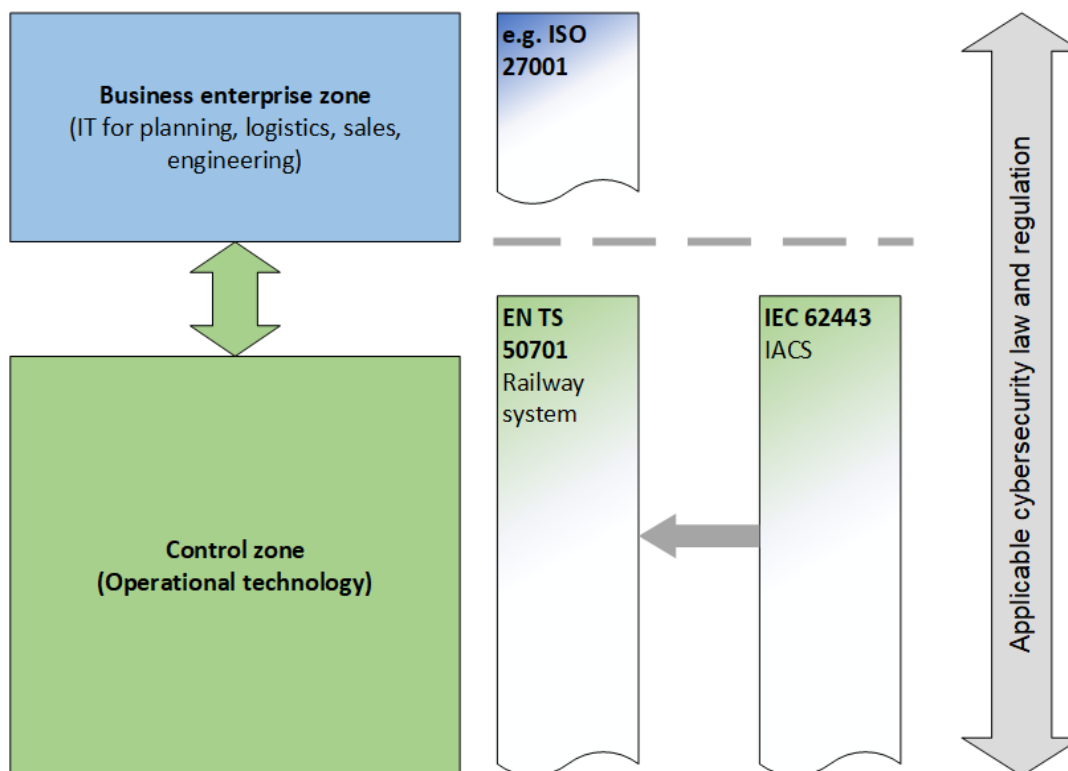


Figure 1 — Segregation of IT and OT

The continuous lowering of the cost of modern solutions is leading to the substitution of the classic pyramidal or hierarchical structure of automation and control systems with more flexible and adaptable architectures, which span over multiple locations and independent organizations, with very different responsibilities and competences. The reference model in Figure 1 thus is only used to match the definition of 'Industrial Automation and Control Systems' to the 'Railway system', which is described in this Clause.

The main goal of railway cybersecurity is to protect railway system essential functions, even in the case they are threatened by some malicious attackers. In other words, cybersecurity of a railway is effective when no hardware or software assets contributing to essential functions can be exfiltrated, modified, corrupted or deleted by unauthorized people or processes. Since modification of data or processes may force systems to malfunction, lack of cybersecurity can result in operational interruptions, damage of assets or, even worse, death and injuries of human beings.

4.2 Railway asset model

The railway operator shall define an asset model of its railway system. Assets shall be divided in groups corresponding to physical areas and functional criticality level (e.g. signalling, command and control, auxiliary, comfort, public). The resulting model is an input to define the SuC.

Figure 2 shows an informative example of an railway asset model. Assets are divided in four groups in order to show their physical area. Each asset is identified by its functional name (e.g. "Traffic management system") and coloured using a five-colour scheme to indicate their function classes. Assets of the same function class are more likely to be interconnected, though they are often separated in different virtual or physical networks (i.e. public network, comfort network, auxiliary network, command and control network, signalling network in trains). Nevertheless, there are also logical connections between different functional classes; for instance, between a Traffic management system and an interlocking.

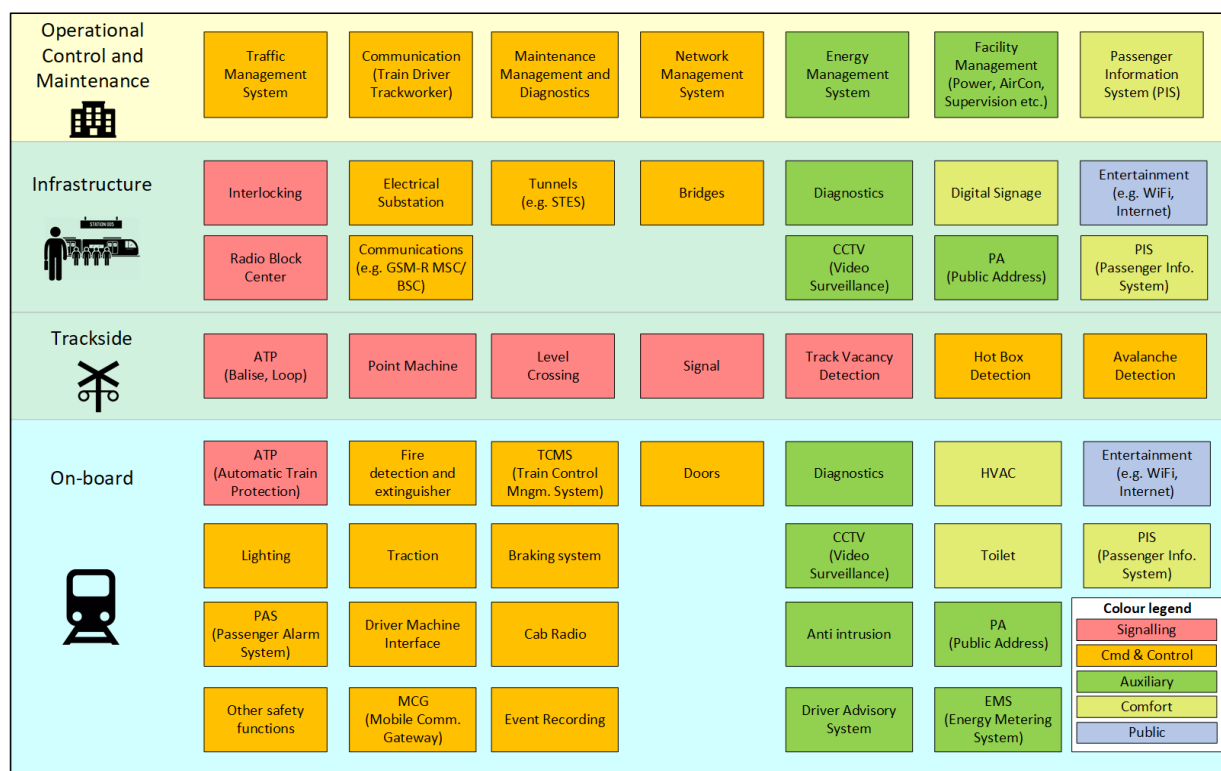


Figure 2 — Railway asset model (example)

Railway operators can identify the scope - or the assets - of a specific SuC as a subset in the Railway asset model shown in Figure 2 or a similar documentation.

Annex F.1 includes a description of the functionality of the assets in short terms.

NOTE Beside the assets shown in Figure 2 there are a lot of network devices (switches, routers, etc.) spread all over the railway system (including trains) that are also regarded as assets to be protected from cybersecurity attacks. These components can be considered either as part of the communications domain or as a part of the specific system (i.e. signalling systems). For example, the MCG in Figure 2 that is shown as a part of 'Cmd and control' could also be regarded as part of the communication domain that provides conduits for application with different criticality.

4.3 Railway physical architecture model

One of the main challenges of the railway system is its large geographical 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 a thorough network architecture of the railway system.

Figure 3 shows exemplarily a domain-oriented view of the railway system within the scope of the technical specification.

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

For instance, assets located along the track are more prone to a direct physical attack than assets in a control centre. On the other hand, a traffic management system, that may have interfaces to the enterprise world (ERP systems, mail servers and other office systems), may be more exploitable by a Denial-of-Service attack or other threats (e.g. ransomware CryptoLocker) in the IT domain.

Railway operators and system integrators can identify the network-oriented connections between the components of the SuC in the Railway physical architecture model.

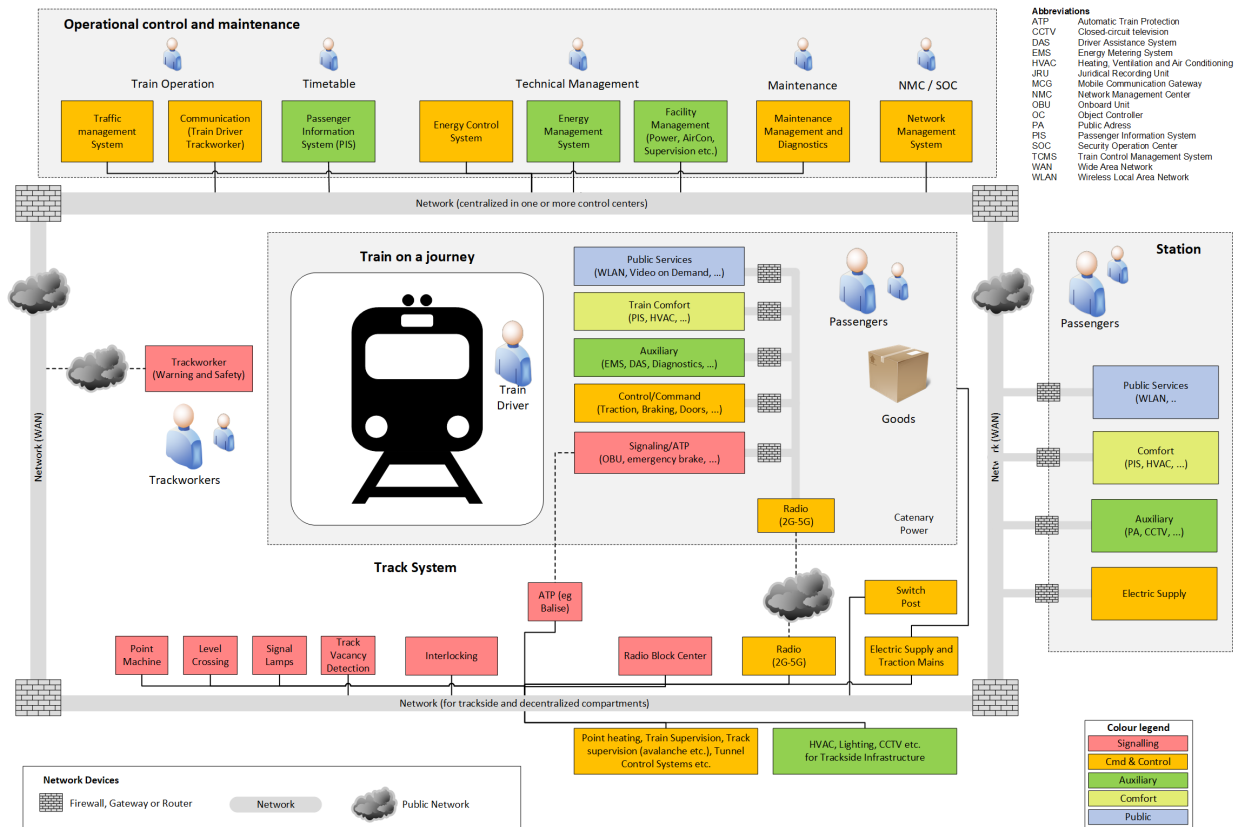


Figure 3 — Railway physical architecture model (example)

Concerning the 'Train to ground' communication, the security level attributed to related subsystems depends on the supported application (e.g. signalling, public services). The set of security measures (e.g. private APN, secured exchange between train to ground over a public network, hardening of exposed components, etc.) should fulfil the security needs of the supported applications.

4.4 High-level railway zone model

The railway operator should establish a high-level railway zone model to be used as input for the SuC identification, initial risk assessment and SuC zoning activities. The zoning principles used should be similar to the one described in Clause 6.

The definition of zones includes measures for encapsulation of functionality to keep a particular service alive in case of an incident in another zone; the same way as capabilities to isolate an incident by closing the gateways to the infected zone.

The combination of zones, conduits, subsystems and zone priorities results in a generic zoning model including communication rules (see F.2). Figure 4 shows the generic railway zoning reference according to the design principles of IEC/TS 62443-1-1:2019, the zoning principles of EN IEC 62443-3-2:2020 and the risk-based approach.

Data flow between rolling stock and land-based subsystems should be reduced to a minimum of conduits to control and detect unallowed data flow and malware by security devices.

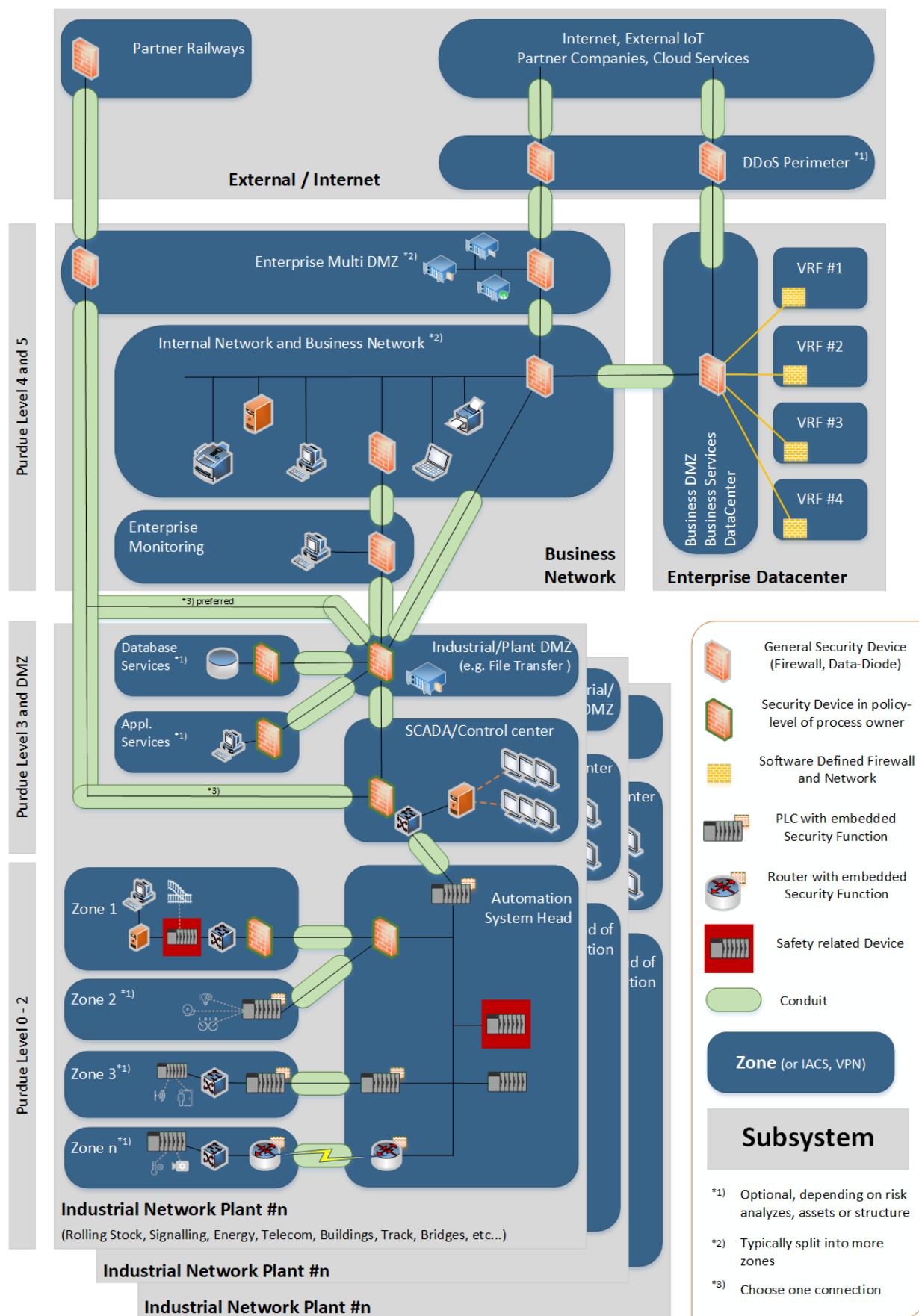


Figure 4 — Generic high-level railway zone model (example)

The final zone model depends on existing systems and zones, the result of the threat risk assessment and the target architecture of each railway operator.

Following two topics are part of the zoning concept:

- Communication and human interactions in high criticality zones should be monitored, logged and stored for forensics at least at the subsystem boundaries (see also EN IEC 62443-3-3 / SR 2.8).
- security devices between zones with different criticality that protect the zone with the higher criticality should be managed by the responsible organization of the higher criticality zone (see also EN IEC 62443-3-2, ZCR 3.1).

F.2 contains a practical example of how to evaluate the criticality of a zone.

5 Cybersecurity within a railway application lifecycle

5.1 Introduction

This Clause provides an overview of the cybersecurity activities to be carried out during the lifecycle of a railway application. It is given within the framework of the lifecycle described in EN 50126-1, but different lifecycles can be applied depending on the system under consideration (SuC).

To comply with this Clause when a different lifecycle is used for an entire SuC or parts of it, the cybersecurity activities as presented in this Clause shall be undertaken and deliverables shall be exchanged during defined synchronization points.

5.2 Railway application and product lifecycles

In the IEC 62443 framework, which is the basis of this document, the lifecycle of an Industrial Automation and Control System (IACS) can be distinguished from the lifecycle of products that are integrated into the system under consideration during the Integration phase. For the purpose of this document, the IACS is to be understood as the system under consideration of the railway application.

The integration of products designed and possibly certified in accordance with different cybersecurity standards is an important option to ensure flexibility and cost-effectiveness of the railway SuC.

Thus, product lifecycle (EN IEC 62443-4-1) is not in the scope of this document, and therefore no synchronization points or deliverables are prescribed for the corresponding lifecycle phases (6 and 7) of EN 50126-1.

5.3 Activities, synchronization and deliverables

The following table provides an overview of:

- Basic descriptions of the security activities relevant to the lifecycle of the railway SuC
- Necessary synchronization points required to achieve coordination between the security activities and all the stakeholders: system engineering, safety, RAM, V&V, T&C activities.
- Deliverables to be exchanged.

Many activities in the table below include references to subsequent clauses of this document. Within the referenced clauses, additional guidance and rationale is provided for the corresponding activities, including roles and responsibilities.

In Table 1, the relevant security-related activities as well as synchronization points and corresponding deliverables are allocated along the lifecycle phases of EN 50126-1. To reach conformity with this Clause, the listed activities need to be performed, synchronization points checked, and deliverables exchanged, independently of the lifecycle to be applied. In order to allow for the use of pre-developed cybersecurity components, no synchronization points or deliverables are prescribed in phases 6 and 7.

Table 1 — Security-related activities within a railway application lifecycle (EN 50126-1)

Phase (EN 50126-1)		Synchronization points and deliverables	Cybersecurity activities
0	Prerequisites		— Railway operator's security program is established — Manufacturer's and integrator's secure development process is established — Legal and regulatory framework is identified
1	Concept	<u>SuC Identification:</u> → Operational environment incl. existing security-related controls and High-Level zone model (see Clause 4) → Applicable security standards → Purpose and scope ← Project cybersecurity management plan (incl. cybersecurity context, goals and lifecycle activities (see Annex G, G.2))	— Review of the level of security achieved up to now — Analysis of the project's security implication and context (incl. generic threats) (see 5.4) — Alignment with railway operator / asset owner and stakeholder's security goals — Consideration of security lifecycle aspects (patch management, monitoring, etc.) (see Clause 10) — Plan cybersecurity-related activities
2	System definition and operational context	<u>System definition:</u> → System boundaries → Initial system architecture, incl. list of functions, interfaces and generic systems → Logical and physical network plans ← Logical and physical network plans review <u>Operational context and criticality:</u> → Essential functions ← Initial risk analysis results ← Zones and Conduits	— Review of the logical and physical network plans — * <i>Initial Risk Assessment for the SuC</i> (see 6.3) — * <i>Partitioning of the SuC into zones and conduits</i> (see 6.4) — * <i>Documentation of components, interfaces and characteristics for each zone and conduit</i> (see 6.5) *: This activity and the corresponding synchronization point may also be conducted in phase 3.
3	Risk analysis and evaluation	<u>DRA:</u> → Functional Requirements (linked to essential functions) ← Initial Threat Log ← Potential Updates (Zones and Conduits, network plans)	— Detailed Risk Assessment (DRA) (see Clause 7): - Derive technical (e.g. SL-T), physical and organizational countermeasures or assumptions for zones and conduits — Consider business continuity aspects (incl. incidence response and recovery) for the SuC

Phase (EN 50126-1)		Synchronization points and deliverables	Cybersecurity activities
4	Specification of system requirements	<u>CRS release:</u> ← System Cybersecurity Requirements Specification incl. security-related application conditions	— SuC-specific refinement of normative requirements (see Clause 8) — Definition of organizational and physical requirements — Definition of security-related application conditions (see Clause 7)
5	Architecture and apportionment of system requirements	<u>CRS breakdown:</u> → System architecture breakdown to components, incl. SuC inventory ← Subsystem Cybersecurity Requirements Specification incl. security-related application conditions, technical and organizational compensating countermeasures	— DRA update, incl. assessment of the SL-C for components and definition of compensating countermeasures including security-related application condition (see 8.3) — Assigning the technical security requirements to components (see 8.3) — Assigning responsibilities for the organizational and physical requirements for the railway operator/maintainer or asset owner — Establish third party management for security aspects, including supplier security capabilities and support contracts
6	Design and implementation	No synchronization	— Follow product lifecycle (EN IEC 62443-4-1 and 4-2 or other adequate cybersecurity standards) — Consider and prevent potential conflicts between component cybersecurity functionality and functional architecture
7	Manufacture or Procurement	No synchronization	— Follow product lifecycle (EN IEC 62443-4-1 and 4-2 or other adequate cybersecurity standards) — Consider and prevent potential conflicts between component cybersecurity functionality and functional architecture
8	Integration	<u>Component integration:</u> ← Qualification of security components → Integration test documentation including SuC environment information	— Review of logical and physical network plans, list of systems and installed applications after implementation — Qualification of security components and functions from test integration results, penetration testing and vulnerability scanning (see 9.3) — Check and ensure removal of unnecessary software, hardware and services

Phase (EN 50126-1)		Synchronization points and deliverables	Cybersecurity activities
			— Update of threat risk assessment based on the results of phases 6 “Design & implementation” to 8 “Integration”
9	System Validation	<u>Cybersecurity validation:</u> ← Cybersecurity case incl. security-related application conditions ← Security guidelines	— Verification of security guidelines — Validation of configuration and security functionality (see 9.4) — Applicability verification of organizational requirements and security-related application conditions (see 9.4)
10	System acceptance	<u>Cybersecurity acceptance:</u> ← Cybersecurity case updated incl. security-related application conditions ← Security guidelines updated	— Finalization of cybersecurity case and security-related guidelines (see 9.2 and 9.5) — Security Handover between System Integrator and railway operator — Review of business continuity aspects (incl. incidence response and recovery) for the SuC.
11	Operation, maintenance and performance monitoring	<u>Cybersecurity case updates:</u> ← Continuous updates of the cybersecurity case based on vulnerabilities, incidents and changes including security patches	— Maintenance of the logical and physical network plan and also the list of IT systems and installed applications — Perform security and vulnerability monitoring and risk-based incidence response including risk analysis updates. (see Clause 10) — Perform patch and/or configuration management (see Clause 10) — Perform data backup and auditing procedures to enable data recovery — Maintenance of restrictive access authorizations — If applicable, prepare and perform security (compliance) audits
12	Decommissioning	<u>Secrets Disposal:</u> ← Disposal report	— Disposal of components taking security criteria into account (will be addressed later in Clause 10)
Key → Information to be provided by all stakeholders contributing to the development, delivery, operation, maintenance and disposal of the SuC (e.g. System Engineering, Safety, RAM, V&V, etc.) to the cybersecurity process ← Information to be provided by the cybersecurity process to the other stakeholders Underlined text are synchronization points			

NOTE all inputs provided during one phase are by default available for the following phases.

The railway operator security program shall be consistent with the application of security management requirements contained within the IEC 62443-2-1 and which are based on EN ISO/IEC 27001.

5.4 Cybersecurity context and cybersecurity management plan

Asset owners shall define the applicable cybersecurity context, they:

- a) shall develop and document an understanding of their cybersecurity threats, which includes identifying threat sources, systems, architectures of systems, organizational structures and interfaces relevant to cybersecurity, and legal and regulatory requirements (Cybersecurity context)
- b) shall communicate the cybersecurity context to their senior managers and board members and ensure they are informed about cybersecurity risk
- c) should regularly (at least annually) review the threat context to detect and highlight any emerging trends that can change the risk context that the asset owner operates in;
- d) shall implement a systematic methodology for the identification, evaluation and management of cyber threats. Any risk assessment framework satisfying these requirements may be selected, e.g. ISO 27005, NIST SP 800-30, ANSSI (EBIOS 2010 and EBIOS RM).

The system integrator shall define its cybersecurity management plan with the applicable security context and the risk assessment framework.

See informative Annex G, G.2 for typical content of the cybersecurity management plan.

5.5 Relationship between cybersecurity and essential functions

5.5.1 General

For a railway application to operate in a safe and fully functional manner, its essential functions need to be protected. Essential functions are defined as functions or capabilities which are required to maintain the safety (including health and environment) and availability of the system. For railway applications, a loss of protection, loss of control or loss of view would be considered as a loss of essential functions. Since attacks on the system can lead to losses of either of these properties, security countermeasures need to be implemented to provide appropriate protection without affecting these functions negatively.

In contrast to the engineering domain of functional safety, the availability of railway applications needs to be ensured at the same level of priority when considering security functions. While losses of availability for trains or railway networks might be considered safe in the scope of functional safety, continuous operation is one of the primary goals of security. Civil unrest as well as public relations and financial damage to the operating entity due to loss of availability all need to be considered as part of the scope of security.

5.5.2 Defence in depth

“Defence in depth” is one of the guiding principles to provide appropriate security for the essential functions of all systems. At its core, it reduces the susceptibility of systems to attacks by eliminating single points of failure within the systems’ protections. Layered security mechanisms increase the security of the system as a whole, since attacks that successfully cause one mechanism to fail, still need to penetrate one or several remaining mechanisms.

The principle of defence in depth is illustrated in Figure 5 below. When applying defence in depth to railway essential functions, integrity and availability are to be considered with the highest priority.

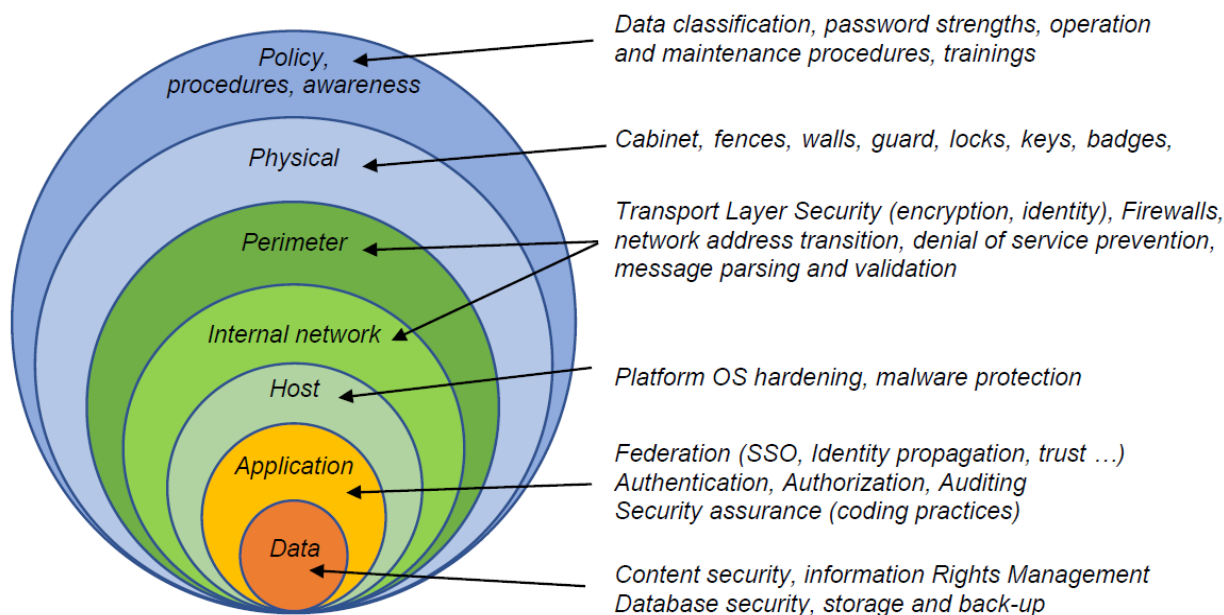


Figure 5 — Defence in depth with example of measures

The table below provide examples of areas concerned by each layer of the defence in depth for PACIS and ERTMS.

Table 2 — Examples of function related supporting assets in regard to the defence in depth layers

	PACIS (Information for Passengers on board)	ERTMS Control and Command
Policy	Maintenance procedure of the PACIS	Organizational procedure for management of keys
Physical	Cabinets for server; Physical ports not exposed to outside for Displays or HMI	Equipment Room, RBC cabinet, On-board cabin for EVC
Perimeter	Firewall with others Ethernet On-Board Network	Segregation of critical networks
Internal Network	Ethernet On-Board PACIS Network	RBC network
Host	On-Board Server; Displays; HMI	Vital computer (RBC, EVC)
Application	Information for Passenger SW (PIS)	ETCS SW
Data	Packmedia (including pictures, text, etc.)	Movement Authority

5.5.3 Security-related application conditions

Security-related application conditions (SecRACs) are a set of conditions that need to be satisfied to fulfil the cybersecurity requirements.

In the case a zone, conduit or SuC cannot meet the targeted security requirements inherently, compensating countermeasures shall be defined. If their implementation takes place externally to the considered SuC, they are exported as security-related application conditions (SecRACs).

Security-related application conditions (SecRACs) can be either:

— Technical countermeasures introduced outside of the considered SuC.

or

— Organisational and procedural countermeasures.

NOTE IEC 62443-2-1 and EN IEC 62443-2-4 are possible sources.

or

— Any combination of these.

For secure operation, it is necessary for the asset owner to be compliant with the security-related application conditions.

SecRACs to be fulfilled by the end user (railway duty holders) shall be documented in the cybersecurity case of the SuC as primary document and in the security guidelines as secondary documents. Security guidelines for installation, operation, maintenance and disposal of the SuC shall be referenced by the Security Case and handed over during the SuC Handover phase

SecRACs are an essential part of the cybersecurity case (refer to Clause 9 and Annex G, G.2).

It is important, that SecRACs are communicated to stakeholders of essential functions. Particularly, SecRACs may be used as a basis for the coordination of the cybersecurity and safety process.

5.5.4 Interfaces between the safety and the cybersecurity processes

5.5.4.1 Principles

To ensure the necessary stability and viability of safety-related documentation and approval, it is advisable to separate cybersecurity and safety issues as far as possible and coordinate them adequately in order to decouple the different lifecycles and the approval processes. Otherwise, each change affecting the security of the system may trigger a new safety approval.

However, communication and interaction between safety and cybersecurity teams should be implemented throughout the lifecycle and appropriate review processes and intervals should be maintained.

Particularly, the safety process shall inform the cybersecurity process about the safety-related functions or assets to be protected. This information shall be documented and serves as an input for the cybersecurity risk assessment.

The cybersecurity process deals with the risks stemming from attacks and malicious interventions, implementing cybersecurity requirements in the SuC or exporting some security-related application conditions (SecRAC).

If cybersecurity threats have potential impacts on the safety of the system, the cybersecurity case shall include or refer evidence on how security threats with the potential to affect safety-related functions have been evaluated and how protection against the adverse influence has been achieved.

The cybersecurity case and its SecRACs shall be communicated to the Safety management. If Safety management considers SecRACs to potentially impact safety-related functions, they can then be considered as SRACs.

5.5.4.2 Possible implementation through high level cybersecurity objectives

One possible solution to achieve the necessary levels of separation and coordination between cybersecurity and safety processes is to define only a limited number of coordinated cybersecurity objectives on a high level. These objectives need to be fulfilled through security requirements or security-related application conditions.

EXAMPLE 1 For safety-critical communication, the high-level cybersecurity objective could be “The safety-critical messages has to be protected against manipulation”.

EXAMPLE 2 The high-level cybersecurity objectives can also be related to a safety-critical item list. In this case, the high-level cybersecurity objective could be “The functions of the safety-critical items has to be protected against manipulation.”

The fulfilment of the high-level cybersecurity objectives is demonstrated as part of the cybersecurity case. Either they are fulfilled by the cybersecurity functions or under certain security conditions and assumptions (SecRAC).

The cybersecurity case shall be maintained and updated regularly. If the cybersecurity functions are changed, it has to be demonstrated that the safety-related cybersecurity objectives still hold (including the exported SecRAC). If necessary, the cybersecurity case can be assessed and certified according to the relevant cybersecurity standards.

As a result of this documentation structure, the documentation regarding functional safety can be considered stable and viable so long as the cybersecurity process is properly adapted to changing threat scenarios. Hence, while the security documentation may be subject to frequent updates as a result of the volatile threat landscape, the safety approval can remain valid.

5.6 Cybersecurity assurance process

The cybersecurity assurance and acceptance process for railway applications has the goal to successfully validate security functions implemented and complete the handover process from the System Integrator to the asset owner. It is based on the confidence placed in implemented countermeasures required by the cybersecurity requirements specification (CRS) for the SuC. The evidence delivered to the asset owner is the cybersecurity case (incl. cybersecurity validation report). More detailed information and guidance on the structure and handling of the cybersecurity case can be found in Clause 9.

A generic overview of the relationship between the threat risk assessment (TRA) and the system cybersecurity assurance is shown in Figure 6 below. Identification of threats and vulnerabilities during the TRA considers technical, organisational as well as physical aspect of the SuC. The CRS defines security countermeasures, which enables the achievement of an acceptable level of residual risk, as demonstrated by the detailed risk assessment (DRA). The CRS, once implemented has to be verified. This is achieved by applying assurance techniques. In the next step, system cybersecurity validation is performed assuring the SuC is fulfilling the requirements demanded by the operational environment where it is implemented (configuration). The documented results of all these verification and validation activities are documented in the cybersecurity case.

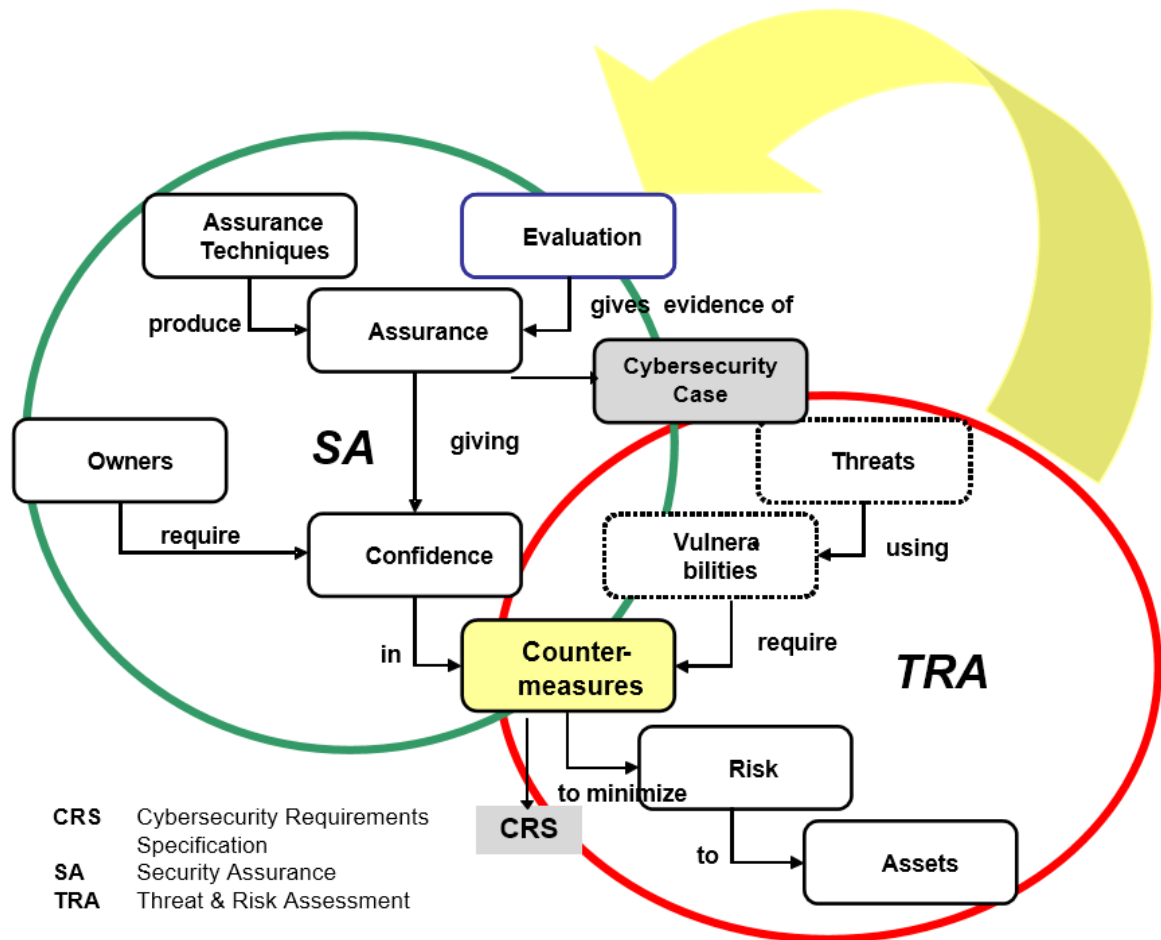


Figure 6 — Relationship TRA and SA

6 System definition and initial risk assessment

6.1 Introduction

This Clause provides the overview of the system definition and its scope. It defines the rules and the process how to handle cybersecurity activities on system level with the aim to identify:

- the system under consideration (SuC)
- the essential functions of the SuC
- the assets supporting the essential functions
- possible threats for the given SuC
- initial risk assessment of the unmitigated cybersecurity risks
- the separation into zones and conduits.

Figure 7 illustrates the different steps to be applied to perform the initial risk assessment and to derive a security architecture in “zones and conduits” (see also the lifecycle phase 2 in Clause 5). The process corresponds to EN IEC 62443-3-2 and the references relate to the zone and conduit requirements (ZCR) defined there.

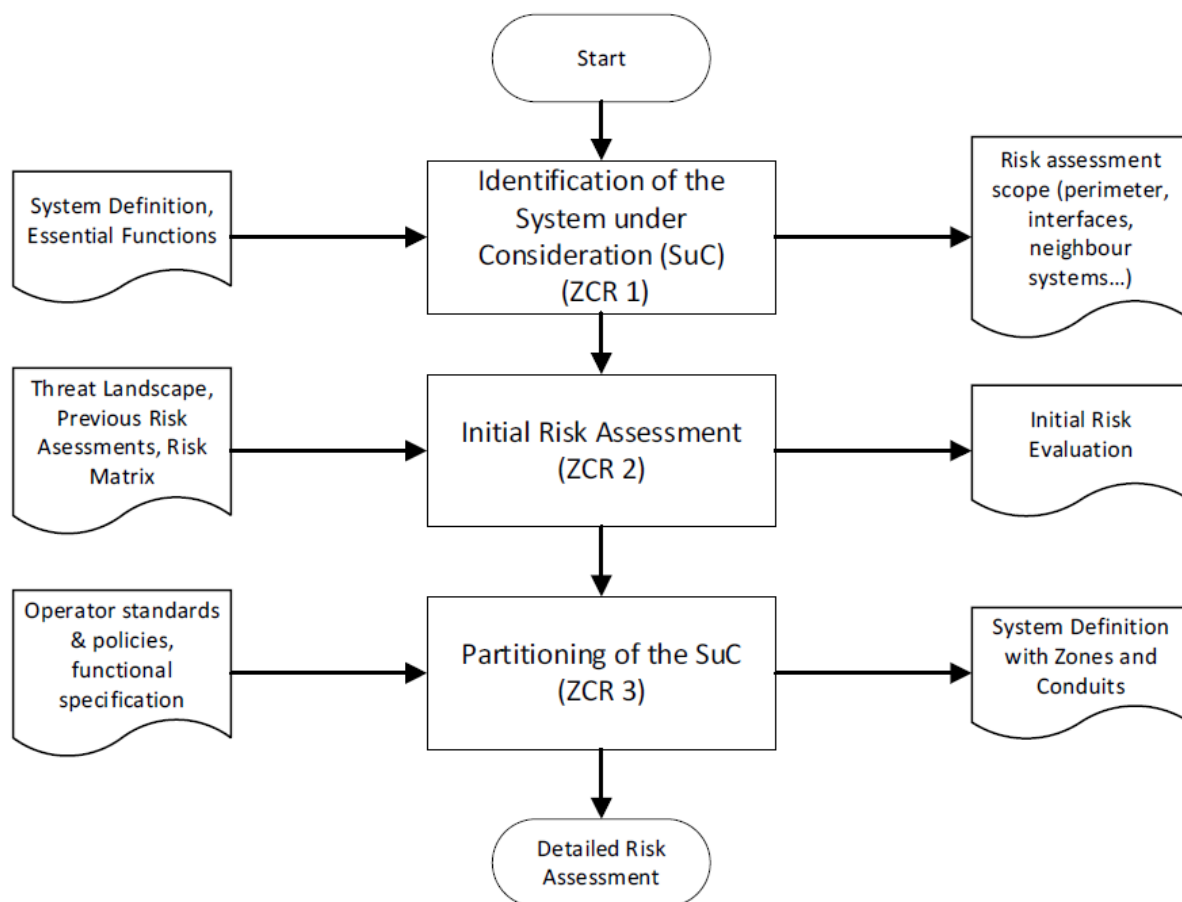


Figure 7 — Initial risk assessment flowchart

6.2 Identification of the system under consideration

6.2.1 Definition of the SuC

The system under consideration (SuC) is a constituent part of the railway system (see Clause 4), which can be understood as a system of nested systems, each comprising subsystems and components, which together provide the required functionality. Cybersecurity threats may endanger the correct execution of this functionality as well as the integrity of safety-related functions and therefore endanger the secure behaviour of the system with potential impact on safety, finance or system availability. The identification of these cybersecurity threats (ref. subclause 6.2.) needs a description of the SuC, the functions this SuC provides and all interfaces of the SuC. The following rules apply for the description of the SuC:

- The definition of the SuC shall contain the scope and boundary of the system, which is to be developed and assessed.
- The SuC is part of an operational system to control railway related technical systems.
- The functional and architectural description of the SuC should follow the hierarchical approach given in EN 50126-1:2017, 5.2 to identify it exactly including borders and external interfaces

NOTE Generally, a draft of the SuC is expected to be supplied by the overall system engineering process (see phase 2 in 5.2).

6.2.2 Overall functional description

The location of the SuC within the railway architecture model (see Clause 4) shows to which kind of system the SuC belongs (i.e. rolling stock, signalling, infrastructure etc.) and which main functions are supported. The cybersecurity threat identification of the SuC (including known vulnerability identification) shall be based on a SuC, in which the functions, the system boundaries and the provided functionality are defined. Therefore, this identification of the main functions should be detailed by giving information related to:

- a) the objective (intended purpose) and the mission profile of the SuC comprising the definition of the system functions, the system borders and the interfaces
- b) the operational scenarios, which define, how the SuC will be used, and which actors are interfering or interfacing with the SuC
- c) the context of implementation and use
- d) the planned lifetime and therefore possibly necessary system updates in HW and SW
- e) maintenance plans and concepts for the SuC
- f) constraints by the environment which integrates the SuC.

6.2.3 Access to the SuC

Compromising the SuC is possible via access to the SuC (e.g. through interfaces, where an access is possible). Such access includes human-machine interfaces as well as technical interfaces which enable a rogue device to be added to the system and communication interfaces via a network. A complete list of the SuC interface should be provided with the definition of:

- Function for which the interface is used
- Protocol for the transmission via networks (if already available)
- Functional data being used
- Impact (loss of confidentiality, integrity or availability)
- Function of neighbouring systems
- Organizational interfaces.

6.2.4 Essential functions

The essential functions of the SuC are the key functions needed for the operation of the railway application. They include, but are not limited to, functions related to safety, availability or control. For example, these may include traction and braking, door control, signalling, passenger information and communication functions.

If the essential functions are compromised, this normally means loss of protection, loss of confidential data, loss of control, loss of data integrity and status or loss of connection to the device.

NOTE The security functions protect the essential functions.

Knowing the essential functions of the SuC is crucial to protect them and to avoid imposing security requirements that could limit or even compromise them. The essential functions shall be identified by the overall system engineering process and shall be provided as input for the cybersecurity process (see phase 2 in 5.2). The essential functions may be identified by requirements from the system engineering process that are labelled with the appropriate properties e.g. safety-related.

6.2.5 Assets supporting the essential functions

Assets supporting the essential functions of the SuC shall be clearly identified in the system definition with their relationship to their corresponding essential function.

6.2.6 Threat landscape

To build an appropriate cybersecurity strategy, shared between all the stakeholders, the first step is to identify and agree on a consistent list of generic cybersecurity threats that could jeopardize the railway application. Agreement on threat landscape is crucial as discrepancies in the set of considered threats by the different stakeholders will lead to risk underestimation and lack of control measure implementation. Hence, all stakeholders should participate in a process to agree on a generally accepted threat landscape. The threat landscape should be based on recognized and accepted threat library or reports and built with a high-level approach providing an overview of the threats applicable to the railway sector.

Threat libraries and reports like the following should be taken as inputs:

- ENISA Threat Landscape Yearly report
- ISO/IEC 27005
- NIST SP 800-30.

Finally, the threat landscape should:

- be defined or at least approved by the asset owner
- be updated at least once a year (or according to contractual requirements)
- provide mapping to the input threat libraries or reports
- provide rationale for not considered threats.

It should be noted that natural hazards are out of scope of this threat landscape.

If the stakeholders agree that a detailed risk assessment is necessary then in the initial risk assessment the threats can be grouped into classes of generic threats, e.g. threats on integrity. All identified threats shall be entered into the threat log (usually created in lifecycle phase 3). The threat landscape is the most important input to be extended in the detailed threat identification (see 7.2.1).

6.3 Initial risk assessment

6.3.1 Impact assessment

The first step of the initial risk assessment consists in the impact assessment: for each asset supporting the essential functions of the SuC, the consequences of losing the integrity, availability or confidentiality of the asset shall be evaluated.

The impact evaluation in the initial risk assessment shall measure the worst global impact in case of loss of the asset properties. The global impact shall be evaluated not only at the business level, but also at the environmental, societal and human impact levels.

To enable a consistent approach for threat risk assessment between asset owners, system integrator and product suppliers, it is important that all the stakeholders share same impact assessment reference.

For the railway application, at least the following criteria should be considered:

- Human health and safety
- Operational availability
- Financial impact

Table 3 is given as an example for qualitative impact assessment (see Annex E for more examples).

Table 3 — Qualitative Impact Assessment example

Impact	Human health and safety	Operational availability	Financial impact
A	One or several fatalities	Most of operations disturbed during more than 1 week	Could lead to organization bankrupt
B	Several severe or critical injuries	Most of operation disturbed between 1 day and 1 week. Important operation disturbed during more than 1 week	Impact in a significant way the organization annual budget (>10 % of revenue)
C	One severe injury or several injuries requiring hospitalization	Most of operation disturbed between 1 h and 1 day Important operation disturbed between 1 day and 1 week	Impact in a significant way the organization annual benefits.
D	One injury requiring hospitalization or several light injuries (not requiring any hospitalization)	Important operation disturbed less than 1 day.	Impact not visible on annual basis

In the initial risk assessment, the worst-case consequence shall be used to determine the considered impact for each asset property.

6.3.2 Likelihood assessment

The threat landscape may change suddenly, and experience is of limited use for cybersecurity. Therefore, likelihood can be evaluated only on a qualitative or semiquantitative scale. Because of that, asset owners shall make use of intelligence reports and other information sources to determine the potential attackers that they might be targeted by.

Likewise, this information should be shared with the system integrators before performing any threat risk assessment since it will have a direct impact in the cybersecurity requirements of the final product.

For a railway SuC, at least the following aspects should be considered when estimating the likelihood of a threat:

- The exposure of the asset to be attacked depending e.g. of its ease of informational or physical access
- The physical location of the asset
- Capability needed to perform the attack, e.g. sophistication and effort

The choice of the factors, that influence likelihood, should be justified (see Annex E for examples). Subjective factors as well as highly dependent or correlated factors should be avoided.

As an example likelihood could be estimated from scales based on exposure and vulnerability of the asset (see Table 4). In this example the resulting likelihood L is calculated from Exposure and Vulnerability by $L = EXP + VUL - 1$.

Table 4 — Likelihood assessment matrix – Example

Rating	Exposure (EXP)	Vulnerability (VUL)
1	Highly restricted logical or physical access for attacker, e.g. — highly restricted network and physical access, or — product or components cannot be acquired by attacker or only with high effort	— Successful attack is only possible for a small group of attackers with high hacking skills (high capabilities needed) — Vulnerability is only exploitable with high effort, and if strong technical difficulties can be solved, non-public information about inner workings of system is required — State of the art security measures to counter the threat — High chance for attacker to be traced and prosecuted
2	Restricted logical or physical access for attacker, e.g. — internal network access required, or — restricted physical access, or — product or components can be acquired by attacker with medium effort	— Successful attack is feasible for an attacker with average hacking skills (medium capabilities needed) — Vulnerability is exploitable with medium effort, requiring special technology, domain or tool knowledge — Some security measures to counter the threat — Medium chance for attacker to be traced and prosecuted
3	Easy logical or physical access for attacker, e.g. — Internet access sufficient, or — public physical access, or — attacker has access as part of daily work, operation, or maintenance activities, or — product or components can be acquired by attacker with low effort	— Successful attack is easy to perform, even for an unskilled attacker (little capabilities needed) — Vulnerability can be exploited easily with low effort, since no tools are required, or suitable attack tools freely exist. — No or only weak security measures to counter the attack caused by the threat — Low chance for attacker to be traced and prosecuted

In the initial risk assessment, for each asset the worst-case result (i.e. the highest likelihood without any cybersecurity countermeasure) shall be used to determine the likelihood of the occurrence of a threat.

6.3.3 Risk evaluation

The risk evaluation may be determined by a risk matrix in which the likelihood and the impact of the threat are related. The risk acceptance criteria shall be defined or at least approved by the asset owner.

The risk matrix in Table 5 is a general example. It should be calibrated, justified and agreed with the asset owner. Detailed examples can be found in Annex E.

Table 5 — Risk matrix example

Risk matrix example		Likelihood				
		1	2	3	4	5
Threat impact	D	Low	Low	Low	Medium	Significant
	C	Low	Low	Medium	Significant	High
	B	Low	Medium	Significant	High	High
	A	Medium	Significant	High	High	Very high

The initial risk evaluation shall be performed for each asset supporting the essential functions of the SuC as defined by the system definition considering the mission profile and the identified threat landscape. It is permitted to concentrate the initial risk evaluation depending on the most critical property lost by the asset (Integrity, Availability or Confidentiality). In the initial risk assessment, the risk ranking of the assets

is determined by the risk matrix, because in the initial risk assessment the evaluation is performed as a worst-case evaluation without any countermeasures.

6.4 Partitioning of the SuC

6.4.1 Criteria for zones and conduits breakdown

On the basis of the output of the initial risk assessment, the assets shall be assigned to consistent security zones connected by conduits. This means all assets in the same zone and all data sent by the same conduit share the same or similar cybersecurity requirements.

NOTE 1 In case of a pre-existing system, it is possible to reuse as input the result of previous security analyses.

The following criteria should be used to partition the SuC into Zones and Conduits:

- a) Risk of the assets, in terms of Integrity, Availability and Confidentiality
- b) Type of interfaces or connection to the other parts of the SuC (e.g. wireless)
- c) Physical or logical location
- d) Access requirements
- e) Operational function
- f) Organization responsibilities for each asset
- g) Safety aspect
- h) Technology lifecycle, e.g. product lifecycle, obsolescence.

In the railway framework, “risk”, “physical location” and “safety aspect” are commonly used criteria to break down the SuC into Zones and Conduits.

NOTE 2 In the railway context, examples of operational functions are braking, traction control, doors open/close, train control, diagnostic, maintenance.

6.4.2 Process for zones and conduits breakdown

The objective followed by grouping the assets into zones and conduits is to identify the assets that share common cybersecurity requirements and to group them to share the mitigation means.

The following aspects shall be considered according to EN IEC 62443 for the process to define zones and conduits:

- a) The business assets (IT) and control assets (OT) shall be separated in different zones.

Refer to EN IEC 62443-3-2 ZCR-3.2.

- b) Safety-related assets shall be grouped in dedicated zones which are logically or physically separated from zones which are not safety related. However, if non-safety assets are allocated to a such zone, the complete zone is considered as safety related.

Refer to EN IEC 62443-3-2 ZCR-3.3.

- c) Temporarily connected devices should be included in zones separated from assets that are intended to be permanently connected.

Refer to EN IEC 62443-3-2 ZCR-3.4.

- d) Wireless devices should be included in zones separated from the ones with the wired devices.

Refer to EN IEC 62443-3-2 ZCR-3.5.

- e) (Remote) Devices that are permitted to make connections to the SuC via networks external to the SuC should be grouped into a separate zone or zones.

Refer to EN IEC 62443-3-2 ZCR-3.6.

- f) Zones shall contain the security device protecting the perimeter at conduit edges.

Refer to EN IEC 62443-3-3, SR 5.2.

Exceptions from the above requirements shall be justified by risk analysis.

As a refinement according to the rules above, the following design rules should be considered for maintenance application:

- Direct (maintenance) access from business zones to control zones without control by a security device or similar (e.g. proxy server) should not be allowed.
- External maintenance access (e.g. via Internet) should be grouped in a separate zone.

6.5 Output and documentation

6.5.1 Description of the system under consideration

A high-level description of the SuC shall include the name, a high-level description of the function and the intended usage of the SuC, as well as, a description of the equipment or process under control as it is known at the stage of Initial Risk Assessment.

At later stage, during the Detailed Risk Assessment, this SuC description should be completed to achieve a detailed description of all assets (reference and version).

6.5.2 Documentation of the initial risk assessment

The documentation shall include at least

- Threat Landscape
- Risk Matrix
- Risk Evaluation.

6.5.3 Definition of zones and conduits

The following items shall be identified and documented for each defined zone and conduit:

- a) Name and/or unique identifier indicating also the type (zone or conduit)
- b) Accountable organization(s)
- c) Definition of logical boundary
- d) Definition of physical boundary, if applicable
- e) Safety designation
- f) List of all logical access points

- g) List of all physical access points, if applicable
- h) List of data flows associated with each access point
- i) Connected zones or conduits
- j) List of assets and their risk classification and business value.

7 Detailed risk assessment

7.1 General aspects

Clause 7 describes the detailed risk assessment, which should be performed for each zone and each conduit (or cluster of zones and conduits) resulting in the definition of the cybersecurity requirements specification, as the central outcome of this activity.

NOTE 1 It is assumed that for railway applications a detailed risk assessment is almost always necessary. In the event that the outcome from the initial risk assessment is that all risks are sufficiently mitigated without any additional countermeasures (e.g. because there is very strong physical and organisational protection, see ZCR4 of EN IEC 62443-3-2), the detailed risk assessment could be skipped but for the documentation of the cybersecurity requirements, see 7.2.5.

In EN IEC 62443-3-2 ZCR 5.6 different approaches for the derivation of SL-T are described. The first is based directly on the need of protection against a particular kind of attacker (e.g. hacker, criminal organization, state sponsored group), including the estimation of the needed efforts of an attacker also known as attack vector. In this approach it is determined which type of attacks by which kind of attacker a zone or conduit of the SuC should withstand, taking into account the identified threats and vulnerabilities (see 7.2.1) and legal constraints, resulting directly in a SL-T, see 7.2.4 for more detail. But also, in this approach, it still has to be checked that the risk is acceptable.

EXAMPLE 1 A railway duty holder decides that a particular zone of the SuC should be protected against hacker groups or criminal organizations that have system knowledge and may apply sophisticated attacks but have only moderate motivation and resources. By the definition of SL-T this is well represented by $SL-T = 3$ (see 7.2.4) and this would be the overall requirement. By EN IEC 62443-3-3 (see Clause 8) the corresponding requirements can be derived for this SL-T. Finally, the risk evaluation would have to confirm the SL-T.

The second approach is based on the difference between unmitigated cybersecurity risk (as derived in Clause 6 as a basis for the zoning) and the acceptable risk (as defined in a risk matrix like Table 4). It is described in this Clause in detail. It has to be mentioned as a precondition, that the zones and conduits to be assessed by a detailed risk assessment should have reached a certain level of maturity of the architecture and possible its (planned) implementation. Generally, the second approach leads to a more appropriate SL-T value but takes more effort.

Generally, the detailed risk assessment described here is proactive e.g. it is not triggered by an incident or vulnerability (see Clause 10).

There may be a need for update of the detailed risk assessment e.g. when compensating countermeasures shall be evaluated (see Clause 8) or if new threats or vulnerabilities become known.

There is a need to emphasize the importance of embedding cybersecurity threat risk assessment as part of the systematic management of risk in rail systems. In particular, cybersecurity risks affecting safety availability and other important business objectives of the railway system have to be addressed.

The detailed risk assessment should be reviewed and updated:

- at each lifecycle phase (if necessary) by the responsible stakeholder for this product or system, and
- at regular intervals or whenever triggered (e.g. when new security threats or vulnerabilities become known), to identify new threats and vulnerabilities of the product or system.

Threat risk assessment may not override mandatory requirements for security protection, e.g. by regulation.

NOTE 2 Clause 7 starts with the requirements for the Railway duty holder. It is well understood that also other stakeholders have their role in detailed risk assessment and that there is a need for exchange of information with respect to security risks.

The dynamic nature of cybersecurity may lead to new identified vulnerabilities being exploitable by an attacker.

EXAMPLE 2

- Increase of attacker capabilities resulting in a higher likelihood of a threat
- Growth of networked systems offering a larger attack surface with new attack vectors
- Digitization of railway assets
- etc.

The risk assessment principles in this Clause shall be applied accordingly during the operation, maintenance and performance monitoring to address the risks and decide on further actions to be taken.

In the case where zones or conduits are similar from a risk perspective, then the detailed risk assessment may be performed only once, but the results need to be applied consistently to all zones and conduits affected.

7.2 Establishment of cybersecurity requirements

7.2.1 General

The general process for the detailed risk assessment by the railway duty holder (or by the system integrator by contractual agreement) is depicted in the flowchart in Figure 8. It adapts ZCR 5 from EN IEC 62443-3-2 to the railway environment.

The zone and conduit cybersecurity requirements are derived in lifecycle phase 3 as a result of the detailed risk assessment. These requirements are detailed and apportioned to components in lifecycle phases 4 and 5.

The basis of the process is the output from the initial risk assessment, the zones and conduits are identified there. In a first step the threat and vulnerability identification is detailed. Then for all identified threats an appropriate risk acceptance principle is chosen and approved by the railway duty holder. Note that for each threat only one principle is applied, but a set of threats can be treated by the same principle. Depending on this choice the cybersecurity requirements are determined. The process is described in more detail in the following clauses.

It is acknowledged that the easiest application of the process is, if only one principle is applied for each zone or conduit, namely that a complete zone or conduit is either covered by a code of practice or by a reference system or by explicit risk evaluation. But for complex systems a mixture of the principles may be necessary.

NOTE 1 The process as described here is used to determine the cybersecurity targets, e.g. target security level SL-T, as part of the security requirements specification. When the architecture is completed a similar assessment is carried out to derive the capability security level SL-C. And finally, after integration of the complete system the achieved security level SL-A can be assessed, see Clause 9 for more information.

NOTE 2 In some cases, e.g. application of codes of practice or reference systems, security targets are not expressed by SL-T. In other cases the SL-T applies only to some threats, as others are controlled by other principles. Finally, in the cybersecurity requirements specification all partial requirements are collected.