



PROJECT NUMBER:

**IEC 63452 ED1**

DATE OF CIRCULATION:

**2025-08-08** (2025-07-18)

CLOSING DATE FOR VOTING:

**2025-10-17** (2025-10-10)

SUPERSEDES DOCUMENTS:

**9/3000/CD, 9/3036A/CC**

IEC TC 9 : ELECTRICAL EQUIPMENT AND SYSTEMS FOR RAILWAYS

SECRETARIAT:

France

SECRETARY:

Mr Denis MIGLIANICO

OF INTEREST TO THE FOLLOWING COMMITTEES:

TC 65

HORIZONTAL FUNCTION(S):

ASPECTS CONCERNED:

Information security and data privacy

☒ SUBMITTED FOR CENELEC PARALLEL VOTING☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING**Attention IEC-CENELEC parallel voting**

The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting.

The CENELEC members are invited to vote through the CENELEC online voting system.

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

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

Recipients of this document are invited to submit, with their comments, notification of any relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE:

**Railway applications – Cybersecurity**

PROPOSED STABILITY DATE: 2028

NOTE FROM TC/SC OFFICERS:

This A version shows aligned Word extraction from the OSD in regards of annexes and figures. The closing date for voting has been extended to 2025-10-17. No technical modification has been made.

The Cenelec parallel vote status of this project has been changed on 1<sup>st</sup> of August, as reflected on this coverpage.

## Link to Committee Draft for Vote (CDV) online document:

<https://osd.iec.ch/#/editor/archive/0e847a8f-d663-e6d5-e063-1710000a30d0/en/CCDV/1>

## How to access

This link leads you to the Online Standards Development (OSD) platform for National Mirror Committee's (NMC) comments. The project draft may be found further down this document.

## Resource materials

We recommend NCs to review the available materials to better understand the member commenting on the OSD platform. This includes the:

- OSD NC roles overview: [here](#)
- How to add and submit comments to the IEC: [here](#)

## Contact

Should you require any assistance, please contact the IEC IT Helpdesk at [helpdesk@iec.ch](mailto:helpdesk@iec.ch).

## CONTENTS

CONTENTS .....	1
FOREWORD .....	13
Introduction.....	15
Purpose .....	15
Overview of the structure of this document .....	15
1 Scope .....	17
2 Normative references .....	17
3 Terms and definitions, abbreviated terms and acronyms, taxonomy and terms equivalence .....	17
3.1 Terms and definitions.....	17
3.2 Abbreviated terms and acronyms .....	46
3.3 Railway system taxonomy and terms equivalence .....	50
4 Railway system overview .....	53
4.1 Purpose .....	53
4.2 Overview .....	53
4.3 Inputs / Outputs .....	54
4.4 [SO-01-01] Identification of the railway system .....	54
4.4.1 Requirement.....	54
4.4.2 Rationale and supplemental guidance .....	54
4.5 [SO-02-01] Definition of a high-level railway system model .....	56
4.5.1 Requirement.....	56
4.5.2 Rationale and supplemental guidance .....	56
4.6 [SO-03-01] Definition of a high-level railway zone model.....	58
4.6.1 Requirement.....	58
4.6.2 Rationale and supplemental guidance .....	58
4.7 [SO-04-01] Specification of shared cybersecurity services .....	60
4.7.1 Requirement.....	60
4.7.2 Rationale and supplemental guidance .....	60
5 Enterprise cybersecurity programme and management.....	62
5.1 Overview .....	62
5.2 Inputs / Outputs .....	62
5.3 [CP-01-01] Railway OT cybersecurity policy.....	63
5.3.1 Requirement.....	63
5.3.2 Rationale and supplemental guidance .....	63
5.4 [CP-01-02] Railway OT cybersecurity programme .....	63
5.4.1 Requirement.....	63
5.4.2 Rationale and supplemental guidance .....	64
5.5 [CP-02-01] Information sharing management .....	65
5.5.1 Requirement.....	65
5.5.2 Rationale and supplemental guidance .....	65
5.6 [CP-03-01] Competency management.....	65
5.6.1 Requirement.....	65
5.6.2 Rationale and supplemental guidance .....	66
5.7 [CP-04-01] Inventory management.....	66
5.7.1 Requirement.....	66
5.7.2 Rationale and supplemental guidance .....	67

5.8	[CP-05-01] Supply chain management .....	67
5.8.1	Requirement.....	67
5.8.2	Rationale and supplemental guidance .....	67
5.9	[CP-06-01] Risk management .....	70
5.9.1	Requirement.....	70
5.9.2	Rationale and supplemental guidance .....	71
5.10	[CP-07-01] Business continuity management .....	71
5.10.1	Requirement.....	71
5.10.2	Rationale and supplemental guidance .....	72
5.11	[CP-08-01] Data protection management .....	72
5.11.1	Requirement.....	72
5.11.2	Rationale and supplemental guidance .....	73
6	Cybersecurity within a railway application life cycle .....	74
6.1	Purpose .....	74
6.2	Railway application and product life cycles .....	74
6.3	Manage cybersecurity activities and interfaces .....	74
6.3.1	Inputs / Outputs .....	74
6.3.2	[LC-01-01] Assign Project Cybersecurity Manager .....	74
6.3.3	[LC-02-01] Plan project cybersecurity activities till the handover.....	75
6.3.4	[LC-02-02] Tailoring the cybersecurity management plan.....	76
6.3.5	[LC-02-03] Cybersecurity management plan approval .....	76
6.3.6	[LC-02-04] Management of security issues before handover .....	77
6.3.7	[LC-03-01] Manage product suppliers .....	77
6.3.8	[LC-04-01] Manage interaction with safety and RAM teams .....	77
6.4	Cybersecurity activities mapping to the IEC 62278-1 life cycle .....	78
7	Risk assessment for system design .....	83
7.1	Purpose and outcome .....	83
7.2	Overview .....	83
7.3	Identify the SUC and its security context.....	86
7.3.1	Description .....	86
7.3.2	Inputs / Outputs .....	86
7.3.3	[ZR-01-01] Identify the SUC, its security perimeter and access points .....	86
7.3.4	[ZR-01-02] Identify the cybersecurity context .....	87
7.4	Initial Risk Assessment .....	89
7.4.1	Description .....	89
7.4.2	Inputs / Outputs .....	89
7.4.3	[ZR-02-01] Initial risk assessment.....	89
7.5	Partitioning of the SUC in zones and conduits.....	90
7.5.1	Description .....	90
7.5.2	Inputs / Outputs .....	90
7.5.3	[ZR-03-01] Partitioning of the SUC .....	90
7.6	Risk comparison .....	91
7.6.1	Description .....	91
7.6.2	Inputs / Outputs .....	91
7.6.3	[ZR-04-01] Compare initial risk with tolerable risk .....	91
7.7	Detailed Risk Assessment.....	92
7.7.1	Description .....	92
7.7.2	Inputs / Outputs .....	92
7.7.3	[ZR-05-01] Perform Detailed Risk Assessment .....	92

7.7.4	[ZR-05-02] Identify threats .....	93
7.7.5	[ZR-05-03] Identify vulnerabilities .....	94
7.7.6	[ZR-05-04] Manage identified threats and vulnerabilities .....	95
7.7.7	[ZR-05-05] Apply a code of practice .....	95
7.7.8	[ZR-05-06] Application requirements from a reference system .....	95
7.7.9	Explicit Risk Evaluation [ZR-05-07, ZR-05-08, ZR-05-09] .....	96
7.7.10	[ZR-05-10] Threats coverage and risk acceptance .....	100
7.7.11	[ZR-05-11] Document results of the Detailed Risk Assessment .....	100
7.8	Document cyber security requirements .....	101
7.8.1	Description .....	101
7.8.2	Inputs / Outputs .....	101
7.8.3	[ZR-06-01] Cybersecurity requirements specification .....	101
7.9	Asset owner's approval .....	103
7.9.1	Description .....	103
7.9.2	Inputs / Outputs .....	103
7.9.3	[ZR-07-01] Asset owner's approval .....	103
8	Cybersecurity architecture, integration and configuration .....	103
8.1	Purpose .....	103
8.2	Inputs / Outputs .....	103
8.3	SUC cybersecurity functional architecture .....	104
8.3.1	[AA-01-01] Cybersecurity Architecture .....	104
8.3.2	[AA-01-02] Cybersecurity shall not adversely impact essential functions .....	104
8.3.3	[AA-01-03] Requirements apportionment to subsystems .....	105
8.3.4	[AA-01-04] Inclusion of compensating countermeasures .....	106
8.3.5	[AA-01-05] Cybersecurity requirement traceability .....	106
8.4	Cybersecurity integration .....	106
8.4.1	[AA-02-01] Cybersecurity guidelines for the railway solution .....	106
8.5	Cybersecurity configuration .....	107
8.5.1	[AA-03-01] Cybersecurity parameterization and configuration of the railway solution .....	107
9	Cybersecurity assurance for railway solutions .....	107
9.1	Purpose .....	107
9.2	Overview .....	108
9.3	Cybersecurity verification and validation .....	109
9.3.1	Description .....	109
9.3.2	Inputs / Outputs .....	109
9.3.3	[CA-01-01] Plan cybersecurity evaluation activities .....	110
9.3.4	[CA-01-02] Independence of security testers .....	111
9.3.5	[CA-01-03] Execution of cybersecurity evaluation activities .....	111
9.3.6	[CA-01-04] Verification of cybersecurity deliverables .....	112
9.3.7	[CA-01-05] Cybersecurity validation of the railway solution .....	112
9.3.8	[CA-01-06] Railway solution cybersecurity case .....	113
9.4	Railway solution acceptance .....	114
9.4.1	Description .....	114
9.4.2	Inputs / Outputs .....	114
9.4.3	[CA-02-01] Establish cybersecurity handover plan .....	115
9.4.4	[CA-02-02] Approval of the cybersecurity handover plan .....	115
9.4.5	[CA-02-03] Approval of the cybersecurity case .....	116
9.4.6	[CA-02-04] Perform cybersecurity handover .....	116

10	Operational, maintenance and decommissioning requirements .....	116
10.1	Overview .....	116
10.2	Inputs / Outputs .....	118
10.3	[OM-01-01] Cybersecurity maintenance plan .....	119
10.3.1	Requirement .....	119
10.3.2	Rationale and supplemental guidance .....	119
10.4	[OM-01-02] Cybersecurity rules and procedures .....	120
10.4.1	Requirement .....	120
10.4.2	Rationale and supplemental guidance .....	120
10.5	[OM-01-03] Continuous cybersecurity verification .....	121
10.5.1	Requirement .....	121
10.5.2	Rationale and supplemental guidance .....	121
10.6	[OM-02-01] Railway application cybersecurity case .....	121
10.6.1	Requirement .....	121
10.6.2	Rationale and supplemental guidance .....	121
10.7	[OM-03-01] Risk assessment update .....	122
10.7.1	Requirement .....	122
10.7.2	Rationale and supplemental guidance .....	122
10.8	[OM-04-01] Vulnerability advisories .....	123
10.8.1	Requirement .....	123
10.8.2	Rationale and supplemental guidance .....	123
10.9	[OM-04-02] Cybersecurity testing and report .....	123
10.9.1	Requirement .....	123
10.9.2	Rationale and supplemental guidance .....	123
10.10	[OM-04-03] Vulnerability management .....	124
10.10.1	Requirement .....	124
10.10.2	Rationale and supplemental guidance .....	124
10.11	[OM-05-01] Patch management process .....	124
10.11.1	Requirement .....	124
10.11.2	Rationale and supplemental guidance .....	125
10.12	[OM-05-02] Patch management supply chain .....	125
10.12.1	Requirement .....	125
10.12.2	Rationale and supplemental guidance .....	125
10.13	[OM-05-03] End-of-life and end-of-security-support considerations .....	126
10.13.1	Requirement .....	126
10.13.2	Rationale and supplemental guidance .....	126
10.14	[OM-06-01] Incident management .....	126
10.14.1	Requirement .....	126
10.14.2	Rationale and supplemental guidance .....	126
10.15	[OM-06-02] Backup and recovery management .....	129
10.15.1	Requirement .....	129
10.15.2	Rationale and supplemental guidance .....	129
10.16	[OM-07-01] Security monitoring .....	130
10.16.1	Requirement .....	130
10.16.2	Rationale and supplemental guidance .....	130
10.17	[OM-08-01] Decommissioning management .....	131
10.17.1	Requirement .....	131
10.17.2	Rationale and supplemental guidance .....	131
Annex A	(informative) Handling conduits .....	132

A.1	General.....	132
A.2	Protection profiles for conduits.....	133
Annex B	(informative) Handling legacy systems.....	135
General	.....	136
B.1	Basic security risks.....	136
B.1.1	A denial of service attacks and vulnerability exploits.....	136
B.1.2	Impersonation attack.....	136
B.2	Basic process activities.....	137
B.2.1	General.....	137
B.2.2	Zoning.....	137
B.2.3	Defence in depth.....	137
B.2.4	Basic risk analysis.....	138
B.2.5	(Re-)Commissioning.....	138
B.2.6	Site acceptance test (SAT).....	138
B.2.7	Operation.....	139
B.2.8	Training of personnel.....	139
B.2.9	Asset inventory.....	139
B.3	Basic security countermeasures.....	139
B.3.1	General.....	139
B.3.2	Protect installation.....	139
B.3.3	Regular inspection of installation.....	140
B.3.4	Network / perimeter protection.....	140
B.3.5	Network segmentation / restricted data flow.....	140
B.3.6	Monitoring and network management.....	140
B.3.7	Network management system.....	141
B.3.8	Intrusion detection / SIEM.....	141
B.3.9	Virtual private networks (VPN).....	142
B.3.10	Redundant communication.....	142
B.3.11	Security gateway.....	142
B.3.12	Handling USB connectors.....	142
B.3.13	Encryption.....	143
B.3.14	Authentication.....	143
Annex C	(informative) Cybersecurity design principles and system requirements.....	144
C.1	Cybersecurity design principles.....	144
C.1.1	Introduction.....	144
C.1.2	Secure the weakest link.....	144
C.1.3	Defence in depth.....	145
C.1.4	Fail secure.....	148
C.1.5	Grant least privilege.....	149
C.1.6	Economise mechanism.....	150
C.1.7	Authenticate requests.....	152
C.1.8	Control access.....	154
C.1.9	Assume secrets not safe.....	155
C.1.10	Make security usable.....	156
C.1.11	Promote privacy.....	158
C.1.12	Audit and monitor.....	158
C.1.13	Proportionality principle.....	160
C.1.14	Precautionary principle.....	161
C.1.15	Continuous protection.....	162

C.1.16	Secure metadata .....	163
C.1.17	Secure defaults .....	164
C.1.18	Trusted components .....	165
C.2	Guidelines for implementation in a railway environment .....	166
Annex D (informative)	Safety and cybersecurity .....	202
General	.....	203
D.1	Differences between safety and cybersecurity .....	203
D.2	Security from a safety perspective .....	204
D.3	Co-engineering of safety and security .....	204
D.4	Quantification of security .....	205
D.5	The relationship between safety integrity levels and security levels .....	205
D.6	Responsibility for security .....	206
Annex E (informative)	Risk acceptance methods .....	207
E.1	General .....	207
E.2	Example 1 .....	207
E.2.1	Introduction .....	207
E.2.2	Impact assessment .....	207
E.2.3	Likelihood assessment .....	208
E.2.4	Risk tolerability .....	208
E.2.5	Justification .....	209
E.3	Example 2 .....	209
E.3.1	Introduction .....	209
E.3.2	Impact assessment .....	209
E.3.3	Likelihood assessment .....	210
E.3.4	Risk tolerability .....	211
E.3.5	Justification .....	211
E.4	Example 3 .....	211
E.4.1	Introduction .....	211
E.4.2	Impact assessment .....	211
E.4.3	Likelihood assessment .....	212
E.4.4	Risk tolerability .....	213
E.4.5	Justification .....	213
E.5	Example 4 .....	213
E.5.1	Introduction .....	213
E.5.2	Impact Assessment .....	213
E.5.3	Likelihood assessment .....	214
E.5.4	Risk acceptance .....	216
E.5.5	Justification .....	216
Annex F (informative)	Railway system models and zone models .....	218
F.1	Design guidance and rules .....	218
F.1.1	Design guidance for system models .....	218
F.1.2	Design rules for the area-based model .....	218
F.1.3	Design rules for the topology-based model .....	219
F.2	Magnifications of the high-level railway zone model .....	219
F.2.1	Design Guidance for zone models .....	222
F.3	Train to ground communication .....	234
F.3.1	Introduction .....	234
F.3.2	Communication channel .....	234



F.3.3	Principles .....	235
Annex G (informative)	Cybersecurity deliverables content.....	236
G.1	Purpose .....	236
G.2	Railway OT cybersecurity policy and cybersecurity programme.....	236
G.2.1	Railway OT cybersecurity policy .....	236
G.2.2	Railway OT cybersecurity programme.....	236
G.2.3	Rational and guidance .....	237
G.3	Cybersecurity management plan .....	237
G.4	Risk assessment report.....	239
G.5	Cybersecurity requirement specification .....	239
G.6	Cybersecurity guidelines for the railway solution .....	240
G.7	Cybersecurity evaluation plan .....	241
G.8	Cybersecurity case .....	242
G.9	Cybersecurity maintenance plan .....	243
Annex H (informative)	Cybersecurity competence profiles.....	245
H.1	Purpose .....	245
H.2	Railway cybersecurity competence profiles .....	246
H.2.1	Introduction .....	246
H.2.2	Railway Project Cybersecurity Manager.....	246
H.2.3	Railway Cybersecurity Architect.....	247
H.2.4	Railway Cybersecurity Risk Analyst .....	248
H.2.5	Railway Cybersecurity Implementer .....	249
H.2.6	Railway Cybersecurity Penetration Tester .....	250
H.2.7	Railway Cybersecurity Assessor .....	252
H.2.8	Railway Cybersecurity Verifier .....	253
H.2.9	Railway Cybersecurity Validator .....	254
H.2.10	Railway Cybersecurity Administrator.....	255
H.2.11	Railway Cybersecurity Incident Responder .....	256
H.2.12	Railway Chief Information Security Officer .....	257
Annex I (informative)	Cybersecurity for operation and maintenance activities - Operational guidance .....	260
I.1	Purpose .....	260
I.2	Change to maintenance activities and teams .....	260
I.3	Access Strategy.....	260
I.3.1	Physical Access: .....	260
I.3.2	Role-Based Access: .....	260
I.3.3	Network Access:.....	261
I.3.4	Consistency for Access Protection:.....	261
I.4	Remote Access and Maintenance .....	261
I.4.1	General .....	261
I.4.2	Remote Maintenance OT .....	261
I.4.3	Methods of Remote Maintenance.....	261
I.5	Other aspects to be correctly addressed .....	262
I.5.1	Data Protection:.....	262
I.5.2	Decommissioning: .....	262
I.5.3	Awareness of People: .....	262
I.5.4	Use of Portable Media (such as laptop, USB key):.....	262
I.5.5	Key Exchange and Management:.....	262
Annex J (informative)	Vulnerability Management - Operational guidance .....	263

J.1	Purpose .....	263
J.2	organizational aspects .....	263
J.3	Process scoping .....	263
J.4	Vulnerability identification, analysis and prioritization criteria .....	264
J.5	Vulnerability remediation.....	265
Annex K (informative)	Cloud security .....	268
K.1	General.....	268
K.2	Applicability .....	268
K.3	Cloud Security within the railway application life cycle .....	269
K.3.1	Specification Phase .....	269
K.3.2	Design and Implementation Phase.....	270
K.3.3	Validation Phase .....	274
K.3.4	Operations and Maintenance Phase .....	275
K.3.5	Decommissioning .....	278
K.3.6	Business Continuity and Disaster Recovery .....	278
K.4	Cross-References .....	278
Bibliography	.....	280
Figure 1	– Overview of this document .....	16
Figure 2	– Railway system taxonomy .....	51
Figure 3	– Segregation between IT and OT.....	55
Figure 4	– Example of an area-based railway system model .....	57
Figure 5	– Example of a topology-based railway system model .....	58
Figure 6	– Example of a high-level railway zone model .....	60
Figure 7	– Example of hierarchical structure of shared cybersecurity services (example TIME) .....	61
Figure 8	– OT Cybersecurity Management System.....	62
Figure 9	– IEC 62278-1 V-cycle representation .....	79
Figure 10	– Synchronization between cybersecurity team and other stakeholders .....	82
Figure 11	– Zoning and risk assessment flowchart.....	84
Figure 12	– Detailed Risk assessment flowchart .....	85
Figure 13	– Explicit Risk Evaluation flowchart.....	97
Figure 14	– Overview of assurance activities and applicable requirements. ....	108
Figure 15	– Relationship between risk assessment and cybersecurity assurance.....	109
Figure 16	– Overview of operational activities .....	117
Figure 17	– Cybersecurity incident and response management process.....	128
Figure A.1	– Zones and conduits example .....	133
Figure C.1	– Cyber Security in depth example .....	147
Figure D.1	– Security as an environmental condition for safety .....	204
Figure F.1	– Legend of Figure 6 and Figure F.2 to Figure F.5 .....	220
Figure F.2	– Business-IT and general-IT zones (example) .....	221
Figure F.3	– OT Zones (example) .....	222
Figure F.4	– Example of an adopted generic high-level railway zone model with zone critically levels .....	227
Figure F.5	– Example of a full overview of a high-level railway zone model with all entities.....	228

Figure F.6 – Example of zones criticality in the Rolling Stock environment.....	229
Figure J.1 – Vulnerability remediation .....	266
Table 1 – IEC 63452 to IEC 62443 equivalent terms .....	52
Table 2 – Railway system, application, solution and product examples .....	52
Table 3 – Example of OT/IT classification .....	54
Table 4 – Example of mapping of activities, requirements and life cycle phases .....	79
Table 5 – Security Foundational Requirements .....	105
Table 6 – Required level of independence of testers from developers .....	111
Table C.1 – .....	166
Table E.1 – Risk Tolerability categories according to IEC 62278:2002 [31] .....	207
Table E.2 – Severity categories .....	208
Table E.3 – Likelihood Assessment Criteria .....	208
Table E.4 – Mapping Likelihood to Accessibility and Probability .....	208
Table E.5 – Impact assessment matrix.....	209
Table E.6 – Likelihood assessment matrix .....	210
Table E.7 – Risk matrix.....	211
Table E.8 – Impact assessment matrix.....	211
Table E.9 – Likelihood assessment matrix .....	212
Table E.10 – Likelihood conversion table .....	212
Table E.11 – Risk matrix.....	213
Table E.12 – Risk Severity / Mitigation matrix .....	213
Table E.13 – Impact assessment matrix.....	214
Table E.14 – Expertise of the attacker matrix.....	214
Table E.15 – Equipment means matrix.....	215
Table E.16 – Window of opportunity matrix .....	215
Table E.17 – Knowledge of the target matrix.....	215
Table E.18 – Elapsed Time matrix .....	215
Table E.19 – Contribution of security measures matrix.....	216
Table E.20 – Likelihood matrix.....	216
Table E.21 – Risk acceptance matrix .....	216
Table F.1 – Classification of railway subsystem groups.....	218
Table F.2 – Example - Evaluating groups of criticalities for landside-landside communication.....	224
Table F.3 – Example - Zone criticality definition for landside-landside communication .....	224
Table F.4 – Example - Landside-landside communication matrix basic structure .....	225
Table F.5 – Example - Communication matrix - landside to landside .....	226
Table F.6 – Example - Zone criticality definition for rolling stock .....	229
Table F.7 – Example - Communication matrix - rolling stock to rolling stock.....	230
Table F.8 – Example - Communication matrix - landside to rolling stock .....	232
Table F.9 – Example - Communication matrix - rolling stock to landside .....	233
Table H.1 – Railway Project Cybersecurity Manager Competence Profile .....	246
Table H.2 – Railway Cybersecurity Architect Competence Profile .....	247

Table H.3 – Railway Cybersecurity Risk Analyst Competence Profile .....	248
Table H.4 – Railway Cybersecurity Implementer Competence Profile.....	249
Table H.5 – Railway Cybersecurity Penetration Tester Profile .....	250
Table H.6 – Railway Cybersecurity Assessor Competence Profile.....	252
Table H.7 – Railway Cybersecurity Verifier Competence Profile .....	253
Table H.8 – Railway Cybersecurity Validator Competence Profile .....	254
Table H.9 – Railway Cybersecurity Administrator Competence Profile .....	255
Table H.10 – Railway Cybersecurity Incident Responder Competence Profile .....	256
Table H.11 – Railway Chief Information Security Officer Competence Profile.....	257
Table K.1 – Operational risk considerations .....	270
Table K.2 – Scanning considerations .....	275
Table K.3 – IEC 63452 cross-mapping to standards frameworks .....	278

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

**Railway applications - Cybersecurity**

## FOREWORD

- a) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- b) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- c) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- d) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- e) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- f) All users should ensure that they have the latest edition of this publication.
- g) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- h) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- i) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC [had/had not] received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 63452 has been prepared by IEC technical committee 9: Electrical equipment and systems for railways. It is an International Standard.

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

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

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

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

This document was drafted in accordance with ISO/IEC Directives, Part 2:2021, and developed in accordance with ISO/IEC Directives, Part 1:2023 and ISO/IEC Directives, IEC

Supplement:2023, available at [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs). The main document types developed by IEC are described in greater detail at [www.iec.ch/publications](http://www.iec.ch/publications).

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

- reconfirmed,
- withdrawn, or
- revised.

## Introduction

### Purpose

This document is an international standard (IS) that addresses cybersecurity within the railway sector. It covers all domains within the scope of the IEC TC9, including rolling stock, fixed installations, management systems (including supervision, information, communication, signalling and processing systems) for railway networks (including highspeed lines, mainlines and freight lines), metropolitan transport networks (including metros, tramways, trolleybuses and fully automated transport systems) and magnetic levitated transport systems.

This document is railway-specific adaptation of the IEC 62443 series of standards, offering a set of cybersecurity requirements and guidances for every stage of a railway applications life cycle, from its creation to operation and maintenance.

This standard includes:

- requirements for the system integrator during the development and deployment of a new railway solution, ensuring adequate cybersecurity measures are implemented;
- requirements for the railway duty holder, asset owner, and maintenance service provider to maintain the established level of cybersecurity of railway application during the operation and maintenance phases; and
- requirements related to the management of product suppliers.

### Overview of the structure of this document

An overview of the document structure is given in [Figure 1](#). In this overview, only main clauses or annexes providing requirements or guidance are shown. The elements of [Figure 1](#) do not prescribe an execution sequence of the individual topics.



Figure 1 – Overview of this document



## 1 Scope

This document provides a consistent approach to manage cybersecurity of railway applications in a railway system. It is applicable across all domains within the scope of IEC TC 9, which includes railway networks (including highspeed lines, mainlines, and freight-lines), urban transport networks (including metros, tramways, trolleybuses, and fully automated transport systems), and magnetic levitated transport systems. It includes rolling stock, fixed installations, operational management systems (including supervision, information, communication, signalling, and processing systems) for railway operation.

This document refers and adapts the relevant part of the IEC 62443 series of standards to the railway domain, detailing the cybersecurity management, zoning, risk management, supply chain management, cybersecurity requirements, cybersecurity assurance, as well as operational, maintenance, and decommissioning requirements. It outlines the cybersecurity activities and cybersecurity deliverables needed to identify, monitor, and manage cybersecurity risks within a railway application life cycle and in its operational environment (railway system) to a level tolerable by the railway duty holder. It also provides guidance on how to secure legacy system.

Furthermore, this document provides guidance on coordinating and synchronising the cybersecurity activities with the generic reliability, availability, maintainability, and safety (RAMS) life cycle defined in IEC FDIS 62278-1:2024, and provides criteria for application to other life cycles.

Lastly, while this document does not provide safety requirements or constraints on the safety case for railway applications, it does offer guidance on the relationship between cybersecurity and safety.

## 2 Normative references

There are no normative references in this document.

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

### 3.1 Terms and definitions

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

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

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

#### 3.1.1

##### **acceptance**

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

[SOURCE: IEC FDIS 62278-1:2024, 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 can 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**

<protection> protection of system resources against unauthorised access

[SOURCE: IEC 62443-4-1:2018 [49], 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 of standards.

[SOURCE: IEC 62443-4-1:2018 [49], 3.1.3, modified – "users" replaced by "entities (users, programs, processes, or other systems)"]

### 3.1.5

#### **access point**

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

[SOURCE: IEC 732-01-16]

### 3.1.6

#### **access point name**

APN

name of a gateway between a mobile network (GSM, GPRS, 3G, 4G and 5G) and another computer network, frequently the public Internet.

### 3.1.7

#### **accident**

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

[SOURCE: IEC FDIS 62278-1:2024, 3.2]

### 3.1.8

#### **achieved security level**

SL-A

actual security level provided during the operation of a railway application

Note 1 to entry: SL-A is used to describe the security level of a zone or conduit when all technical, physical and process security measures are in place. SL-A is determined during the operation and maintenance phase of the railway application. They are used to establish that a security system is meeting the goals that were originally set out in the SL-Ts.

[SOURCE: ISA-62443-1-1 (May 2024) 8.6.3, modified – "IACS" replaced by "railway application", zone and conduit added]

### 3.1.9

#### **actively exploited vulnerability**

vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner

### **3.1.10**

#### **air gapped network**

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

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

### **3.1.11**

#### **approval**

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

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

[SOURCE: IEC 902-06-01]

### **3.1.12**

#### **asset owner**

AO

individual or organization responsible for one or more railway applications

Note 1 to entry: An asset owner belongs to a railway duty holder (RDH) organization, and applies the OT cybersecurity policy defined by its RDH organization.

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

### **3.1.13**

#### **attack**

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

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

[SOURCE: IEC 171-08-12, modified – “or operational technology system” added, “disruption” added in the note 1 to entry]

### **3.1.14**

#### **attack surface**

physical and functional interfaces of a system that can be accessed and through which the system can be potentially exploited

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

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

[SOURCE: IEC 62443-2-4:2023 3.1.2]

### **3.1.15**

#### **attack vector**

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

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

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

### **3.1.16**

#### **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 902-03-04, modified - Note 1 to entry has been removed]

### **3.1.17**

#### **authentication**

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

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

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

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

### **3.1.18**

#### **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]

### **3.1.19**

#### **automatic train operation**

ATO

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

Note 1 to entry: Can also be used to name the subsystem implementing automatic train operation

[SOURCE: IEC 821-09-01, modified – Note 1 to entry added]

### **3.1.20**

#### **automatic train protection system**

ATP

system using information of signal aspects, track speed limits, train speed supervision and driver reactions to prevent automatically a train passing a danger point (such as a signal at danger) or exceeding speed restrictions

[SOURCE: IEC 821-08-01]

### **3.1.21**

#### **availability**

ability to be in a state to perform as required under given conditions

[SOURCE: IEC, 192-01-23, modified – The notes to entry have been omitted]

### **3.1.22**

#### **balise**

<signalling> device mounted on the track, which communicates with a train passing over it, transmitting and/or receiving signals over the air

### 3.1.23

#### **base transceiver station**

BTS

<in railway system> piece of equipment that facilitates wireless communication between train or passenger equipment and a network

Note 1 to entry: Train or passenger equipment are devices like mobile phones, computers with wireless Internet connectivity, cab radio, or antennas mounted on train.

### 3.1.24

#### **bridge control system**

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

### 3.1.25

#### **capability security level**

SL-C

security level that components or systems can provide when properly configured

Note 1 to entry: These levels state that a particular component or system is capable of meeting the SL-Ts natively without additional compensating countermeasures when properly configured and integrated.

[SOURCE: SOURCE: 62443 3-2:2020 Annex A]

### 3.1.26

#### **central diagnostic system**

onboard component that centralises all diagnostic messages and signals from other train devices and subsystems

### 3.1.27

#### **closed-circuit television**

CCTV

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

EXAMPLE Surveillance of public places or of places which are dangerous or difficult to access such as tunnels and inside traction sub-stations.

[SOURCE: IEV 723-01-19, example modified - “surgical operation, etc.” replaced by “such as tunnels, inside traction sub-stations”]

### 3.1.28

#### **cloud computing**

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

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

### 3.1.29

#### **code of practice**

CoP

document that recommends practices or procedures for the design, manufacture, installation, maintenance or utilisation of equipment, structures or products

- IEC 62280
- ANSSI protection profiles
- OWASP Top Ten
- CIS benchmarks
- NIST SP 800-160vol1 Secure Design principles;

- MITRE ATT&CK knowledge base

Note 1 to entry: A code of practice may be a standard, a part of a standard or independent of a standard.

Note 2 to entry: In the context of a risk assessment, a CoP means a written set of rules that can be used to address a set of threats.

[SOURCE: ISO/IEC Guide 2:2004, 3.5, modified – Note 2 entry added, Example added]

### 3.1.30

#### **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: IEC 62443-3-3:2019, 3.1.9]

### 3.1.31

#### **communication path**

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

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

### 3.1.32

#### **communication based train control**

CBTC

continuous automatic train control system utilizing high-resolution train location determination, independent of track circuits; continuous, high capacity, bidirectional train-to-wayside data communications; and train-borne and wayside processors capable of implementing vital functions

[SOURCE: IEEE 1474-1:2004, 3.1.13]

### 3.1.33

#### **communication system**

<in railway system> system to communicate with either railway equipment (e.g. GSM-R, 1, Wi-Fi), or personnel (e.g. TETRA, VoIP) or passengers (e.g. Public Announcement)

### 3.1.34

#### **compensating countermeasure**

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

- (component-level): locked cabinet around a controller that does not have sufficient cyber access control countermeasures
- (control system/zone-level): physical access control (guards, gates and guns) to protect a control room to restrict access to a group of known personnel to compensate for the technical requirement for personnel to be uniquely identified by the railway application
- (component-level): a vendor's programmable logic controller (PLC) cannot meet the access control capabilities from an end-user, so the vendor puts a hardware-based firewall in front of the PLC and sells it as a system.

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

### 3.1.35

#### **component**

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

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

### **3.1.36**

#### **compromise**

unauthorized disclosure, modification, substitution, or use of information (including plaintext cryptographic keys and other critical security parameters)

[SOURCE: 62443-1-1:2009 3.1.26]

### **3.1.37**

#### **conduit**

<in cybersecurity> logical grouping of communication channels, 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: IEC 62443-4-2:2019, 3.1.11]

### **3.1.38**

#### **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 a railway application, confidentiality refers to protecting railway application data and information from unauthorised access.

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

### **3.1.39**

#### **control network**

network, often time-critical and/or safety critical, 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.

[SOURCE: IEC 62443-1-1:2009 3.2.21, modified – “often” and “and/or safety critical” added]

### **3.1.40**

#### **control system**

<Railway cybersecurity> integrated set of hardware and software components of a railway application performing control function(s) within a railway solution

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

### **3.1.41**

#### **countermeasure**

action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimising 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: IEC 62443-3-3:2013, 3.1.17]

### **3.1.42**

#### **cybersecurity** security

actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, or damage to systems or informational assets

Note 1 to entry: Cybersecurity includes the concepts of identification, authentication, accountability, authorization, availability, and privacy.

[SOURCE: 62443-1-1 3.1.40 (may 2024)]

### 3.1.43

#### **cybersecurity assurance**

<In railway cybersecurity> grounds for confidence that the set of intended cybersecurity controls/countermeasures in a railway application are effective in their application and that an entity meets its security objectives

[SOURCE: NIST SP 800-39, amended, "information system" replaced by "railway application", "security" by "cybersecurity"]

### 3.1.44

#### **cybersecurity case**

documented demonstration, at a given point in time, that the railway product, railway solution or railway application properly addresses cybersecurity risks and that appropriate design, operation processes and organization have been implemented to achieve tolerable level of cybersecurity risks

Note 1 to entry: The cybersecurity case can exist at different levels:

- "Product cybersecurity case ", as provided by the Product Supplier
- "Railway solution cybersecurity case", as provided by the System Integrator
- "Railway application cybersecurity case", as maintained by the Asset Owner.

### 3.1.45

#### **cyber-critical asset**

##### **CCA**

selected components of the railway solution, considered as either contributing the most to the overall cybersecurity or being part of the attack surface (if compromised, potentially leading to an intolerable risk of cyber-incident) and on which asset owner needs to prioritize treatments of cybersecurity issues

EXAMPLE Firewall and NIDS (contributing to the cybersecurity of railway application), badge reader (providing access control to a physical location)

Note 1 to entry: The cyber resilience of such assets should be maintained in priority: If it's only possible (due to technical, economical or other reasons) to treat only a sub set of vulnerabilities at a given time, a vulnerability treated on a CCA will be more efficient than a vulnerability treated elsewhere. The classification of an asset as CCA depend on the railway application architecture and should be confirmed by the cybersecurity risk assessment. See [Clause J.3](#) for further information.

### 3.1.46

#### **data diode**

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

### 3.1.47

#### **defence in depth**

<in cybersecurity> 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:

- it is based on the idea that any one layer of protection, may and probably will be defeated;
- attackers are faced with breaking through or bypassing each layer without being detected;
- a flaw in one layer can be mitigated by capabilities in other layers;



- system security becomes a set of layers within the overall network security; and
- each layer should be autonomous and not rely on the same functionality nor have the same failure modes as the other layers.

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

### **3.1.48**

#### **demilitarized zone**

DMZ

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

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

[SOURCE: IEC 62443-3-3:2013, 3.1.19]

### **3.1.49**

#### **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]

### **3.1.50**

#### **digital signature**

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

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

### **3.1.51**

#### **driver advisory system**

<in railway system> system providing the driver with real-time guidance on how to drive the train to arrive on time efficiently

### **3.1.52**

#### **driver machine interface**

<in railway system> interface equipments used to manage communications between the train and the driver (e.g. screens, buttons and handles)

### **3.1.53**

#### **encryption**

encipherment

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

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

[SOURCE: IEV, 171-08-09]

### **3.1.54**

#### **entertainment system**

<in railway system> system that provides train passengers with streaming services, internet access and other leisure activities

### **3.1.55**

#### **essential function**

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

Note 1 to entry: Essential functions include, but are not limited to, the safety-related functions, the control functions 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 railway sector, all functions needed to operate the railway system are considered as essential function, such as per example traffic control, speed control, traction/brake control.

[SOURCE: IEC 62443-3-3:2013, 3.1.22 modified – “safety instrumented function (SIF)” replaced by “safety-related function”, and last sentence of Note 1 to entry modified to take into account specifically railway context.]

### **3.1.56**

#### **exploitable vulnerability**

vulnerability that has the potential to be effectively used by an adversary under practical operational conditions

### **3.1.57**

#### **facility management system**

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

### **3.1.58**

#### **fire protection system**

<in railway system> system detecting smoke and fire and activating extinguishing countermeasures

### **3.1.59**

#### **fixed installation**

[railway domain \(3.1.116\)](#) containing all electric supply and earthing systems for public transport equipment and ancillary apparatus

EXAMPLE Power-plants, substations, traction mains, switch/point heating, emergency systems, power backup systems, and power supply greater than 50V AC.

### **3.1.60**

#### **firewall**

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

Note 1 to entry: The protected network is generally a private network, internal to an organization.

Note 2 to entry: A firewall may permit messages or files to be transferred to a high-security workstation within the internal network, without permitting such transfer in the opposite direction.

Note 3 to entry: The firewall may have different types of implementation. Examples are dual-homed-host, screened subnet, screening router, or bastion host.

[SOURCE: IEV 732-06-01, modified - The note 4 to entry have been omitted]

### **3.1.61**

#### **future railway mobile communication system**

##### **FRMCS**

<in railway system> telecommunication system based of 5G technology for European railway system, as the successor of GSM-R

Note 1 to entry: FRMCS is the successor of global systems for mobile communications - railway (GSM-R) and intended to serve train radio, both for voice and data communication.

### **3.1.62**

#### **gateway**

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

Note 1 to entry: The computer networks may be local area networks, wide area networks, or other types of networks.

[SOURCE: IEC 732-01-17]

### 3.1.63

#### **global system for mobile communications railway**

GSM-R

international wireless communications standard for railway communication and applications

### 3.1.64

#### **handover**

<in railway cybersecurity> 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 system integrator to the asset owner and generally occurs after successful completion of system test, often referred to as site acceptance test (SAT).

[SOURCE: IEC 62443-2-4:2023, 3.1.9, modified – “automation solution” replaced by “railway solution”, “integration service provider” replaced by “system integrator”]

### 3.1.65

#### **host**

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

### 3.1.66

#### **host device**

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

Note 1 to entry: Typical attributes include filesystem(s), programmable services, and full HMI (keyboard and mouse)

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

### 3.1.67

#### **industrial automation and control systems**

IACS

collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process

Note 1 to entry: These systems include, but are not limited to:

- Industrial control systems, including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, supervisory control and data acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems. In this context, process control systems include basic process control system and safety-instrumented system (SIS) functions, whether they are physically separate or integrated
- Associated information systems such as advanced or multi-variable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems
- Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

[SOURCE: IEC 62443-1-1:2009 3.2.57]

### 3.1.68

#### **impact**

measure of the ultimate loss or harm associated with a consequence

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

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

or disruption of business (delay of trains), breaches of legal and regulatory requirements, market share loss and recovery costs.

[SOURCE: IEC 62443-3-2:2020, 3.1.10, modified – "lost production" replaced by "degradation or disruption of business (delay of trains), breaches of legal and regulatory requirements"]

### **3.1.69 incident**

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

[SOURCE: IEC 62443-3-3:2013, 3.1.28]

### **3.1.70 infrastructure as a service (IaaS)**

cloud computing services model by means of which computing resources are supplied to a customer

Note 1 to entry: This service enables customer to free themselves from maintaining an on-premises data center. The customer does not manage or control the underlying physical or virtual resources but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources.

Note 2 to entry: The IaaS provider is hosting these resources in either the public cloud (meaning users share the same hardware, storage, and network devices with other users), the private cloud (meaning users do not share these resources), or the hybrid cloud (combination of both). It provides the customer with high-level APIs used to hide various low-level details of underlying network infrastructure like backup, data partitioning, scaling, security, physical computing resources, etc.

### **3.1.71 information security management system ISMS**

policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets

[SOURCE: [ISO/IEC 27000:2018 \[1\]](#), 4.2.1]

### **3.1.72 information technology IT**

technology for gathering, storing, retrieving, processing, analysing and transmitting information

Note 1 to entry: An information technology system (IT system) is generally an information system, a communications system, or, more specifically speaking, a computer system.

[SOURCE: ISO 9241-20:2008, 3.4, Note 1 to entry added]

### **3.1.73 integrity**

<of data> property of data that have not been altered or destroyed in an unauthorised and undetected manner

[SOURCE: IEC 171-08-05]

### **3.1.74 intercom call**

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

### 3.1.75

#### **interlocking**

<in railway signalling> interdependent liaison between the control levers or the electric control circuits of different apparatus such as points and signals, which makes it impossible to place them in positions which are unsafe

Note 1 to entry: In English, the term “interlocking” refers also to the place where interlocking is achieved.

Note 2 to entry: In French, the term “enclenchement” refers also to the individual locking of an apparatus such as points.

[SOURCE: IEV 821-05-02]

### 3.1.76

#### **internet of things**

IoT

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

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

### 3.1.77

#### **internet on board**

<in railway system> internet access for train passengers

### 3.1.78

#### **intrusion**

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

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

### 3.1.79

#### **intrusion detection**

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

### 3.1.80

#### **juridical recording unit**

<in railway system> equipment dedicated to record all actions and exchanges relating to the movement of trains sufficient for off line analysis of all events leading to an incident

Note 1 to entry: A juridical recording unit can also be used for diagnostics purposes

### 3.1.81

#### **least privilege**

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

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

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

### 3.1.82

#### **landside**

[railway domain \(3.1.116\)](#) containing communication and processing systems which are not covered by other railway areas (track-side, rolling stock, fixed installation) of the railway system

EXAMPLE Operation control center (OCC).

### 3.1.83

#### **legacy system**

<in railway cybersecurity> existing system that is already in use and meets the needs it was originally designed for, but which could not have the required native cybersecurity capabilities needed from today's perspective, and needs mitigating countermeasures

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

### 3.1.84

#### **level crossing**

<in railway system> location where railway and other traffic types cross each other at the same level (for example, without overpass or underpass)

Note 1 to entry: Level crossings may be technically secured or non-technically secured. Technically secured level crossings can have gates, barriers, traffic lights or other means of securing.

[SOURCE: ISO/TS 4398:2022(en), 3.28]

### 3.1.85

#### **life time buy**

purchase of a part in quantities enough for the remaining life time of the product or system where the part is used

Note 1 to entry: Life time buy is a risk mitigation approach to the part obsolescence.

### 3.1.86

#### **lighting system**

<in railway system> system including the electronics dedicated to ensure correct illumination of railway cars both internally and externally, as well as track-side or landside location such as station, depots, control rooms and tunnels

Note 1 to entry: A special case of car external lighting are headlights.

### 3.1.87

#### **likelihood**

chance of something happening

Note 1 to entry: In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: A number of factors are considered when estimating likelihood in information system risk management such as the motivation and capability of the threat source, the history of similar threats, known vulnerabilities, the attractiveness of the target, etc.

[SOURCE: 62443 3-2:2020, 3.1.11]

### 3.1.88

#### **maintenance and diagnostic system**

<In railway system>  
system dedicated to collecting data from different sources for monitoring, analysis, and maintenance purposes, assessing maintenance needs, and planning and logging of maintenance activities

### 3.1.89

#### **maintenance service provider**

MSP

<in railway system> service provider that provides support activities for a railway application after handover

Note 1 to entry: Maintenance is often considered to be distinguished from operation (e.g. in common colloquial language it is often assumed that a railway application is either in operation or under maintenance). Maintenance service providers can also perform cybersecurity related support activities during operations, e.g. managing user accounts, security monitoring, and security assessments.

[SOURCE: IEC 62443-2-4:2023, 3.1.13, modified – “Automation Solution” replaced by “railway application”]

### **3.1.90**

#### **malware**

malicious software

software containing features that could potentially cause harm to an information processing system or its user

[SOURCE: IEC 171-08-14]

### **3.1.91**

#### **mobile communication gateway**

<in railway system> subsystem providing on-board to track-side communication services for the on-board end devices

### **3.1.92**

#### **network management centre**

<in railway system> entity in charge of controlling the railway network, analysing traffic, recording calls with drivers and ensuring configuration control, fault detection and diagnosis and maintenance

### **3.1.93**

#### **network management system**

<in railway system> system in charge of monitoring and administrating communication networks

### **3.1.94**

#### **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: IEC 62443-3-3:2013, 3.1.33]

### **3.1.95**

#### **on-board multimedia and telematics**

OMTS

<in railway system> multimedia and telematics subsystems identified as video surveillance/<sup>1</sup>, driver and crew orientated services, passenger orientated services and train operator and maintainer orientated services

### **3.1.96**

#### **operating environment assumption**

description of the physical and logical environment in which the SUC is intended to be established and operated, including all assumptions related to this environment that could influence the cybersecurity of the SUC

### **3.1.97**

#### **operational technology**

OT

<Railway cybersecurity> hardware, software or technology for detecting, managing, or causing changes through direct monitoring or control of physical devices

**EXAMPLE** Transportation systems, interlocking, signalisation systems, physical control access systems, physical environment monitoring systems and physical environment measurement systems.

Note 1 to entry: Operational technology has a direct influence on operational activities, physical processes or is used for the control or monitoring of specific facilities and systems.

Note 2 to entry: Since operational technologies in the railway sector directly or indirectly intervene in railway operational processes to protect people, assets, and information, they may be subject to regulatory decisions, corresponding safety certificates or railway-specific regulations.

Note 3 to entry: Operational technology can include network components, IT components, or management systems to support OT processes or functions.

### **3.1.98**

#### **passenger alarm system**

<in railway system> mechanism that passengers can manually activate in case of immediate danger conditions to alert the railway staff and possibly stop the train

### **3.1.99**

#### **passenger counting system**

<in railway system> on-board system, usually installed over a door, able to count incoming and outgoing passengers and to communicate the balance to a control unit

### **3.1.100**

#### **passenger information system**

<in railway system> system informing passengers about train departure time, platforms, etc.

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

### **3.1.101**

#### **patch management**

set of processes used to monitor patch releases, decide which patches should be installed to which railway solution, if the patch should be tested prior to installation on a railway solution, at which specified time the patch should be installed and of tracking the installation status

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 third party libraries current before releasing a product.

Note 3 to entry: A patch can be a new software version of a product.

[SOURCE: IEC 62443-2-3:2015 modified – "system under consideration" replaced by "railway application", addition of notes to entry]

### **3.1.102**

#### **penetration testing**

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

Note 1 to entry: Many companies specialize in penetration testing for traditional [information technology \(3.1.72\)](#) systems. It could be more difficult to find a group that understands the special requirements of a railway application.

### **3.1.103**

#### **physical security**

security measures that are designed to deny unauthorized access to facilities, equipment, and resources and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks)

Note 1 to entry: Physical security involves the use of multiple layers of interdependent systems that can include CCTV surveillance, security guards, protective barriers, locks, access control, perimeter intrusion detection, deterrent systems, fire protection, and other systems designed to protect persons and property.



**3.1.104**

**platform as a service (PaaS)**

category of cloud computing services that allows to the customer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider

**3.1.105**

**platform screen doors**

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

**3.1.106**

**privilege**

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

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

**3.1.107**

**point heating**

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

**3.1.108**

**point machine**

assembly, within a casing, of the apparatus for operating blades from a source of power, usually electric

Note 1 to entry: A point machine sets points/switches to left or right position according to the route setting for a train.

[SOURCE: IEC 821-04-22, modified – addition of note 1 to entry]

**3.1.109**

**product**

system, subsystem or component that is manufactured, developed or refined for use by other products

[SOURCE: IEC 62443-4-1:2018, 3.1.22, modified - Note 1 to entry removed]

**3.1.110**

**product supplier**

manufacturer of hardware and/or software product

Note 1 to entry: The product supplier includes the entity responsible for developing and maintaining a product which can include more than just the manufacturer (for example, integrator).

[SOURCE: IEC 62443-4-1:2018, 3.1.24]

**3.1.111**

**protection profile**

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

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

**3.1.112****public address**

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

**3.1.113****purdue model**

function based model that was adopted from the Purdue Enterprise Reference Architecture (PERA) model in IEC 62264-1, and used as a concept model for industrial control system (ICS) network segmentation

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

**3.1.114****radio block center**

RBC

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

**3.1.115****railway application**

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

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

Note 2 to entry: The railway application can include components that are not installed at the asset owner's site.

[SOURCE: IEC 62443-2-4:2023 [50] 3.1.11 modified - “IACS” replaced by “railway application”, <industrial process> replaced with <railway service>, Note 1 added]

**3.1.116****railway domain**

<Railway cybersecurity> predefined geographical or logical grouping of railway assets

Note 1 to entry: 4 railway domains are defined in the scope of this standard, covering the whole railway system: [fixed installation](#) (3.1.59), [landside](#) (3.1.82), [rolling stock](#) (3.1.133), and [track-side](#) (3.1.180).

**3.1.117****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 life cycle 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 life cycle.

[SOURCE: IEC FDIS 62278-1:2024, 3.48]

**3.1.118****railway OT cybersecurity programme**

set of processes and procedures defined by an asset owner to address cybersecurity concerns of one or several railway application(s) of the railway system

### **3.1.119**

#### **railway OT cybersecurity policy**

high-level organizational document defined by a railway duty holder that outlines the objectives and principles to be applied to protect the railway system from cyber attacks

Note 1 to entry: The railway cybersecurity policy is intanced by railway cybersecurity programmes which address a sub-set of railway application from the railway system.

### **3.1.120**

#### **railway solution**

collection of control system and any hardware and software components that have been installed and configured to operate in a railway application

Note 1 to entry: Railway solution is used as a proper noun in this document.

Note 2 to entry: The difference between the control system and the railway solution is that the control system is incorporated into the railway solution design (e.g. a specific number of workstations, controllers, and devices in a specific configuration), which is then implemented. The resulting configuration is referred to as the railway solution.

Note 3 to entry: The railway solution can be provided by multiple suppliers, including the product supplier of the control system and the product suppliers of components.

Note 4 to entry: The railway solution does not include the processes and procedures used during integration, maintenance, and operation of the railway application.

Note 5 to entry: A railway solution, once integration into a given environment is complete, is ready for operation.

[SOURCE: IEC 62443-2-4:2023 3.1.3 modified - "automation solution" replaced by "railway solution", "IACS" replaced with "railway application", term complementary was removed.]

### **3.1.121**

#### **railway system**

overall system consisting of multiple related railway applications needed to deliver railway transportation

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

### **3.1.122**

#### **reference system**

documented system demonstrated as compliant with state of the art of cybersecurity standards and frameworks, implementing a combination of countermeasures which can be used to address identified cybersecurity risks of a SUC

### **3.1.123**

#### **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: IEC 62443-3-3:2013, 3.1.35]

### **3.1.124**

#### **residual risk**

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

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

### **3.1.125**

#### **risk**

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

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

### 3.1.126

#### **risk acceptance criteria**

<cybersecurity> terms of reference used to determine whether a risk is acceptable or not

[SOURCE: ISO27005:2022 7.2.5]

### 3.1.127

#### **risk assessment**

<cybersecurity> process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, evaluates loss exposures and consequences based on likelihood 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 evaluate 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.

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

### 3.1.128

#### **risk management**

<cybersecurity> process of identifying and applying risk reduction measures commensurate with the tolerable risk of the asset owner

[SOURCE: 62443-1-1 may 2024, 1.1.99, modified – “authority having jurisdiction” replaced by “asset owner”]

### 3.1.129

#### **risk matrix**

matrix used in risk assessment to qualitatively determine the level of risk by assessing the likelihood of an incident occurring and the impact of the consequence should the incident occur

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

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

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

### 3.1.130

#### **risk mitigation**

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

### 3.1.131

#### **risk register**

repository of risk information including the data understood about risks over time

Note 1 to entry: The risk register is the compilation for all risks identified, analysed and evaluated in the risk assessment process. Typically, a risk register contains a description of the risk, the impact if the risk should occur, the probability of its occurrence, mitigation strategies, risk owners, and a ranking to identify higher priority risks

[SOURCE: [SOURCE: NIST SP 800-221: November 2023]]

### **3.1.132**

#### **role**

<railway cybersecurity> set of connected behaviours, privileges and obligations associated with all users (humans, software processes or devices) of a railway application

EXAMPLE Asset owner, railway duty holder, system integrator, maintenance service provider.

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

[SOURCE: IEC 62443-3-3:2013, 3.1.36, modified – “IACS” replaced by “railway application” and examples added]

### **3.1.133**

#### **rolling stock**

<In railway cybersecurity> [railway domain \(3.1.116\)](#) corresponding to all electrical, electronic and electromechanical material on board rolling stock

Note 1 to entry: It includes components for signalling, control and command, auxiliary, comfort, communication, and internet on board.

### **3.1.134**

#### **safety**

freedom from unacceptable risk of harm

[SOURCE: IEC FDIS 62278:2024 3.63]

### **3.1.135**

#### **safety lighting**

that part of emergency lighting provided to ensure the safety of people involved in a potentially hazardous process

[SOURCE: IEC 845-29-012, modified – Note 1 to entry omitted.]

### **3.1.136**

#### **safety function**

function whose sole purpose is to ensure safety

Note 1 to entry: All safety functions are safety-related functions, but not vice versa.

Note 2 to entry: A safety function can contribute to one or more safety barriers. However, a safety barrier is not necessarily implemented by a safety function.

[SOURCE: IEC FDIS 62228-1:2024 3.67]

### **3.1.137**

#### **safety-related**

carries responsibility for safety

Note 1 to entry: A function, component, product, system or procedure is called safety-related if at least one of its properties is used in the safety argument for the system in which it is applied. These properties can be of functional or non-functional nature.

[SOURCE: IEC FDIS 62278-1, 3.73]

### **3.1.138**

#### **safety-related system**

system used to implement functional safety

Note 1 to entry: See the IEC 61508 series and the IEC 61511 series for more information on functional safety

Note 2 to entry: Not all industry sectors use the "safety instrumented system". This term is not restricted to any specific industry sector, and it is used generically to refer to systems that enforce functional safety. Other equivalent terms include "safety systems" and "safety related systems".

[SOURCE: IEC 62443-2-4:2023, 3.1.19, modified - term "safety instrumented system" replaced by "safety-related system" as term reference]

### **3.1.139**

#### **safety tunnel earthing system**

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

### **3.1.140**

#### **sandbox**

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

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

### **3.1.141**

#### **SCADA system**

supervisory control and data acquisition system

monitoring and control system including computers, networked data communications and graphical user interfaces (GUI) for high-level process supervisory management

Note 1 to entry: SCADA system also includes other peripheral devices like programmable logic controllers (PLC) and ICS to interface with process systems such as rolling stock, interlocking, energy and buildings, or machinery

### **3.1.142**

#### **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]

### **3.1.143**

#### **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]

### **3.1.144**

#### **security compromise**

violation of the security of a system such that an unauthorized (1) disclosure or modification of information or (2) denial of service could possibly have occurred

Note 1 to entry: A security compromise represents a breach of the security of a system or an infraction of its security policies. It is independent of impact or potential impact to the system.

[SOURCE: IEC:62443-2-4 3.1.20]

### **3.1.145**

#### **security context**

security provided to the railway solution by the environment (asset owner deployment) in which the railway solution is or is intended to be used

### **3.1.146**

#### **security device**

<in cybersecurity> device that performs a protective or detective security function

### **3.1.147**

#### **security event**

<in railway cybersecurity> event that can have a cybersecurity impact on the railway application (e.g. a login attempt)

### **3.1.148**

#### **security incident**

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 expression "of some significance" is relative to the environment in which the security compromise is detected. For example, the same compromise can 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: IEC 62443-2-4:2023, 3.1.21]

### **3.1.149**

#### **security information event management**

SIEM

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

### **3.1.150**

#### **security level**

SL

<In cybersecurity> set of security measures that supports a degree of risk reduction

Note 1 to entry: Security levels (SLs) are SL-1 – Low, SL-2 – Medium, SL-3 – High, and SL-4 - Very high.

Note 2 to entry: Security level types are capability security level (SL-C), target security level (SL-T), Achieved security level (SL-A).

[SOURCE: IEC CD 62443-1-1:2025, 3.1.135, modified, note 2 replaced]

### **3.1.151**

#### **security objective**

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

[SOURCE: IEC/TS 63443-1-1:2009 3.2.109]

### **3.1.152**

#### **security operation centre**

SOC

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

### **3.1.153**

#### **security patch**

software update 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 can address known or potential vulnerabilities, or simply improve the security of the software component, including its reliable operation.

[SOURCE: IEC 62443-2-4:2023, 3.1.22]

### **3.1.154**

#### **security perimeter**

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

[SOURCE: IEC/TS 63443-1-1:2009 3.2.110]

### **3.1.155**

#### **security policy**

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

[SOURCE: EC/TS 63443-1-1:2009 3.2.112]

### **3.1.156**

#### **security-related application condition**

SecRAC

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

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

### **3.1.157**

#### **security service**

capability that supports one, or many of the security goals

EXAMPLE Examples of security services include key management, access control, and authentication.

### **3.1.158**

#### **sensitive data**

data that is likely to cause to its owner some adverse impact if either it becomes known to others when not intended or it is modified without consent of the affected stakeholder

Note 1 to entry: Sensitive data thus requires protection from unauthorised disclosure or modification

### **3.1.159**

#### **service provider**

role of an 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.

Note 2 to entry: The service provider can be an organization within the asset owner’s organization.

[SOURCE: IEC 62443-2-4:2023, 3.1.39, modified – Note 2 added]



### 3.1.160

#### **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: IEC 62443-3-3:2013, 3.1.40]

### 3.1.161

#### **shared cybersecurity services**

common security functions provided by a dedicated subsystem to the assets of a railway application

EXAMPLE user identification and authentication, log service, identity and access management, time service, backup and restore service, and intrusion detection.

### 3.1.162

#### **signal**

<in railway signalling> apparatus by means of which a conventional indication is given

Note 1 to entry: This conventional indication, visual or acoustic, generally concerning the movements of railway vehicles, is transmitted to the staff entrusted to observe it.

[SOURCE: IEV 821-02-01]

### 3.1.163

#### **signalling system**

<for railways> system to ensure the safe movement of trains by means of one or more of the following:

- lineside indications,
- wayside/on-board data exchange,
- indications given in the driver's cab

[SOURCE: IEV 821-01-03]

### 3.1.164

#### **significant incident**

incident exceeding the impact acceptable for the organization, requiring additional countermeasures

### 3.1.165

#### **software as a service (SaaS)**

capability provided to the customer to use the provider's applications running on a cloud infrastructure

### 3.1.166

#### **software-defined wide area network**

SD-WAN

wide area network that uses software-defined network technology, such as communicating over the internet using overlay tunnels which are encrypted when destined for internal organization locations

### 3.1.167

#### **spoke network**

<virtual private cloud> virtual network peered with the central service (hub) to enable cross-virtual network communication

### **3.1.168**

#### **subsystem**

part of a system, which is itself, a system

- A control system can be itself a subsystem of an higher level system.
- When relevant, a control system can be also decomposed into several subsystems.

### **3.1.169**

#### **system**

set of interrelated elements considered in a defined context as a whole and separated from their environment

Note 1 to entry: A system is generally defined with the view of achieving a given objective, e.g. by performing a definite function.

Note 2 to entry: Elements of a system can be natural or man-made material objects, as well as modes of thinking and the results thereof (e.g. forms of organization, mathematical methods, programming languages).

Note 3 to entry: The system is considered to be separated from the environment and the other external systems by an imaginary surface, which cuts the links between them and the system.

Note 4 to entry: The term "system" should be qualified when it is not clear from the context to what it refers, e.g. control system, colorimetric system, system of units, transmission system.

[SOURCE: IEC 151-11-27]

### **3.1.170**

#### **system integrator**

SI

<railway cybersecurity> service provider that provides integration activities for a railway solution including, specification, design, installation, configuration, testing, commissioning and handover

[SOURCE: IEC 62443-2-4:2023, 3.1.12 modified – “automation solution” replaced by “railway solution”, "Specification activity added", Note 1 to entry removed]

### **3.1.171**

#### **system under consideration**

SUC

<in railway cybersecurity> defined collection of railway application assets that are needed to provide a complete railway solution including any relevant network infrastructure assets

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

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

### **3.1.172**

#### **target security level**

SL-T

desired level of security for a particular railway application, zone or conduit

Note 1 to entry: The target security level is usually determined by performing a risk assessment on a system and determining that it needs a particular level of security to ensure its correct operation.

[SOURCE: 62443 3-2:2020 Annex A, modified – "IACS" replaced by "railway application"]

### **3.1.173**

#### **TETRA**

terrestrial trunked radio

professional mobile radio and two-way transceiver specification

Note 1 to entry: TETRA was specifically designed for use by government agencies, emergency services, (police forces, fire departments, ambulance) for public safety networks, rail transport staff for train radios, transport services and the military.

### **3.1.174**

#### **threat**

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

[SOURCE: IEC 62443-3-3:2013, 3.1.44]

### **3.1.175**

#### **threat environment**

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

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

### **3.1.176**

#### **threat source**

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

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

### **3.1.177**

#### **ticketing system**

system for ordering, sales and validation of tickets

### **3.1.178**

#### **tolerable risk**

level of risk deemed acceptable to an organization

Note 1 to entry: organizations should include considerations of legal requirements when establishing tolerable risk. Additional guidance on establishing tolerable risk can be found in ISO 31000 [14] and NIST 800-39 [16].

### **3.1.179**

#### **track supervision**

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

### **3.1.180**

#### **track-side**

[railway domain \(3.1.116\)](#) containing all railway communication, signalling and processing systems which are located on ground near the tracks

EXAMPLE signal, balise, point-machine, interlocking, level-crossing

### **3.1.181**

#### **traction mains**

<railway> fixed installation systems for the conversion and supply of traction power

### **3.1.182**

#### **traction substation**

<in electric traction> substation the main function of which is to supply an electric traction power supply system

[SOURCE: IEV, 811-36-02]

### **3.1.183**

#### **traction system**

<railway> system which provides traction torque, converting the input supply energy into mechanical energy in motoring and the mechanical energy into electrical or thermal energy in braking (if applicable), comprising of the entire conversion equipment located between the current collector (excluded) and the motor shaft(s) and including all associated auxiliary equipment needed to operate the system

[SOURCE: IEC 61377:2016 3.1]

### **3.1.184**

#### **traffic management system**

TMS

<railway> system controlling the route setting for trains based on timetables and short-term needs

### **3.1.185**

#### **train communication network**

TCN

data communication network for connecting programmable electronic equipment on-board rail vehicles

[SOURCE: IEC 61375-1:2021, 3.1.63]

### **3.1.186**

#### **train control and monitoring system**

TCMS

train-borne distributed control system, comprising computer devices software, human-machine interfaces, digital and analogue input/output (I/O) capability and the data networks to connect all these together in a secure and fault-resistant manner to operate the train

### **3.1.187**

#### **train detection sensor**

device detecting if a given track section is free or occupied by a train (or coach)

### **3.1.188**

#### **train supervision**

ground system for supervision of trains

### **3.1.189**

#### **tunnel control system**

components installed in railway tunnels to support tunnel specific infrastructure functions (for example ventilation, alarm systems, fire and smoke detectors, and fire extinguishers)

### **3.1.190**

#### **validation**

confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

Note 1 to entry: Validation involves a set of activities for gaining confidence that a system is able to accomplish its intended use, goals and objectives in its operational environment. In short, validation gives the confidence that the correct system was built to fulfill what is required for its intended application.

Note 2 to entry: The use conditions for validation can be real or simulated.

[SOURCE: IEV 192-01-18]

### **3.1.191**

#### **vehicle control unit**

VCU

core component of train control and monitoring system (1) that manages and control individual vehicle

### **3.1.192**

#### **verification**

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

Note 1 to entry: The objective evidence needed for a verification can be the result of an inspection or of other forms of determination such as performing alternative calculations or reviewing documents.

Note 2 to entry: The activities carried out for verification are sometimes called a qualification process. In short, verification gives the confidence that the system was built correctly to meet identified requirements and specifications.

Note 3 to entry: In the case of software specifically, verification is conducted at various stages of development, examining the software and its constituents to determine conformity.

[SOURCE: IEC 192-01-17]

### **3.1.193**

#### **virtual private network**

VPN

computer network using intermediate networks for data communication that are transparent for the users and which do not impose restrictions on protocols, such that the network behaves like a local area network

Note 1 to entry: Data communication over intermediate networks typically uses tunnelling.

[SOURCE: IEC 732-01-10]

### **3.1.194**

#### **virtual routing and forwarding**

VRF

technology that allows in IP-based computer networks multiple instances of a routing table to co-exist within the same router at the same time

Note 1 to entry: One or more logical or physical interfaces can have a 1 and these VRFs do not share routes therefore the packets are only forwarded between interfaces on the same 1.

Note 2 to entry: Technology predominantly used for software defined networks in data centres.

### **3.1.195**

#### **voice for critical operation**

voice communication system for critical operation

Note 1 to entry: Both train-to-ground (through dedicated radio system such as cab-radio) and ground-to-ground systems are used.

### **3.1.196**

#### **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: 62443-3-2:2020, 3.1.24]

### **3.1.197**

#### **web application firewall**

WAF

specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service

Note 1 to entry: By inspecting HTTP traffic, WAF can prevent attacks exploiting a web application's known vulnerabilities, such as SQL injection, cross-site scripting (XSS), file inclusion, and improper system configuration. They also introduce a performance degradation and are easily bypassed by attackers so their deployment is not recommended.

### **3.1.198**

#### **wireless local area network**

WLAN

network that allows devices to connect and communicate wirelessly

### **3.1.199**

#### **zero day**

vulnerability in a computer system that was previously unknown to its developers or anyone capable of mitigating it

Note 1 to entry: Until the vulnerability is remedied, threat actors can exploit it in a zero-day exploit, or zero-day attack.

Note 2 to entry: The term "zero-day" is used when the development teams are unaware of their software vulnerability, and they have had "0" days to work on a security patch or an update to fix the issue.

### **3.1.200**

#### **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 (for example, 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 (such as high financial, health, safety, operational or environmental impact), functionality, logical and physical (including location) relationship.

[SOURCE: IEC 62443-3-2:2020, 3.1.25 modified - Note 1 to entry modified, "operational" added]

## **3.2 Abbreviated terms and acronyms**

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

AA	architecture and apportionment
ANSSI	agence nationale de la sécurité des systèmes d'information
AO	asset owner
API	application programming interface
APN	access point name
ATACS	advanced train administration and communications system
ATO	automatic train operation
ATP	automatic train protection
ATS	automatic train supervision
BTS	base transceiver station
CA	cybersecurity assurance
CBTC	communication based train control
CCA	cyber-critical asset
CCTV	closed-circuit television
CEF	common event format
CERT	computer emergency response team

CIA	confidentiality, integrity, and availability
CISA	cybersecurity and infrastructure security agency
CISO	chief information security officer
CMDB	configuration management database
CMO	cellphone network operator
CoP	code of practice
COTS	commercial off-the-shelf
CP	cybersecurity programme
CPU	central processing unit
CR	component requirement
CRL	certificate revocation list
CRS	cybersecurity requirements specification
CSIRT	computer security incident response team
CSMS	cybersecurity management system
CVE	common vulnerabilities and exposures
CVSS	common vulnerability scoring system
DAS	driver advisory system
DC	data confidentiality
DMI	driver machine interface
DMZ	demilitarized zone
DoS	denial of service
DPI	deep packet inspection
DRA	detailed risk assessment
DTLS	datagram transport layer security
EIM	European rail infrastructure managers
EMS	energy management system
ENISA	European network and information security agency
EPSS	exploit prediction scoring system
ERJU	Europe's rail joint undertaking
ERP	enterprise resource planning
ERTMS	European rail traffic management system
ETCS	European train control system
EU NIS	European Union directive on security of network and information systems
FIRST	forum of incident response and security teams
FR	foundational requirement
FRMCS	future railway mobile communication system
GSM-R	global system for mobile communications - railways
HMAC	hash-based message authentication code
HMI	human machine interface
HVAC	heating, ventilation and air-conditioning
HW	hardware
I/O	input/output
IAC	identification and authentication control

IACS	industrial automation and control system(s)
IAM	identity access management
ICS	industrial control systems
ID	identifier
IDS	intrusion detection system
IEC	international electrotechnical commission
IEV	international electrotechnical vocabulary
IIoT	industrial internet of things
IOB	internet on board
IoT	internet of things
IP	internet protocol
IRA	initial risk assessment
ISAC	information sharing and analysis centre
ISDN	integrated services digital network
ISMS	information security management system
ISO	international organization for standardization
ISP	internet service provider
IT	information technology
IXL	interlocking
JRU	juridical recorder unit
KEV	known exploited vulnerabilities
LAN	local area network
LC	life cycle
MAC	media (or medium) access control
MCG	mobile communication gateway
MMS	maintenance management system
MNO	mobile network operator
MSP	maintenance service provider
MVB	multifunction vehicle bus
NDR	network device requirement
NIDS	network intrusion detection system
NIS	network and information systems
NIST	national institute of standards and technology
NMS	network management system
NVD	national vulnerability database
OCC	operation control centre
OM	operation and maintenance
OM	operation and maintenance
OMTS	on-board multimedia and telematic subsystem
OS	operating system
OSI	open systems interconnect
OT	operational technology
PA	public address

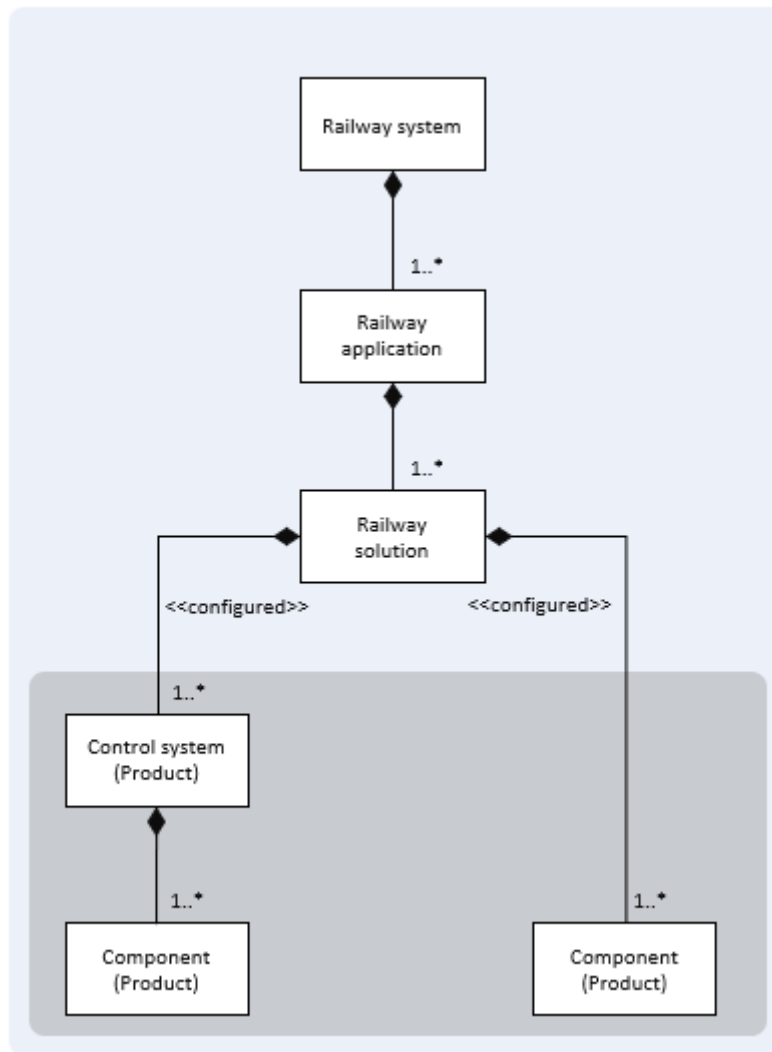


PACIS	public address and customer information system
PAS	passenger alarm system
PERA	purdue enterprise reference architecture
PIN	personal identification number
PIS	passenger information system
PKI	public key infrastructure
PLC	programable logic controller
PS	product supplier
RA	resource availability
RAM	reliability availability maintainability
RAMS	reliability availability maintainability safety
RAS	remote access service
RBC	radio block centre
RDF	restricted data flow
RFC	request for comments
RG	requirements and guidelines
RU	railway undertaker
SAT	site acceptance test
SBOM	software bill of materials
SCADA	supervisory control and data acquisition
SDWAN	software defined wide area network
SecRAC	security-related application condition
SG	security gateway
SI	system integrator
SIEM	security information and event management
SIL	safety integrity level
SL	security level
SL-A	achieved security level
SL-C	capability security level
SL-T	target security level
SMS	short message service
SO	system overview
SOC	security operations centre
SR	system requirement
STES	safety tunnel earthing system
SUC	system under consideration
SW	software
T&C	test & commissioning
TAP	terminal access point / test access point
TCMS	train control and monitoring system
TCN	train communication network
TETRA	terrestrial trunked radio
TLS	transport layer security

TMS	traffic management system
TRA	threat risk assessment
TRE	timely response to events
TS	technical specification
USB	universal serial bus
V&V	verification & validation
VCU	vehicle control unit
VPN	virtual private network
VRF	virtual routing and forwarding
WAF	web application firewall
WIFI	wireless fidelity
WLAN	wireless local area network
ZC-L	zone criticaly - landside
ZC-RS	zone criticaly - rolling stock
ZR	zoning and risk assessment
ZR	zoning and risk assessment

### **3.3 Railway system taxonomy and terms equivalence**

The railway system taxonomy used in this document is shown in [Figure 2](#).



**Figure 2 – Railway system taxonomy**

NOTE 1 [Figure 2](#) is based on the [Figure 3 System Taxonomy](#) from [ISA-62443-1-1 \(D11E1\):2022 \[5\]](#)

The scope of this document covers the [railway system \(3.1.121\)](#), the [railway application \(3.1.115\)](#) and the [railway solution \(3.1.120\)](#). The secure development life cycle of the products (grey background in [Figure 2](#)) is out-of-scope of this document (see [6.2 Railway application and product life cycles](#)).

The interface between the secure development life cycle of the products and the railway application life cycle, is considered in this standard by supply chain management requirements (see [5.8 Supply chain management on railway duty holder](#)).

Product suppliers can use [IEC 62443-4-1:2018 \[49\]](#), [IEC 62443-4-2:2019/COR1:2022 \[11\]](#), and [IEC 62443-3-3:2013/COR1:2014 \[59\]](#) as well as other standards or frameworks, for example [NIST SP 800-218 \[2\]](#), [NIST SP 800-82 \[3\]](#), or [NIST SP 800-160 Vol1 \[4\]](#).

As shown in [Figure 2](#), a railway system usually comprises various railway applications that can interact with each other, and each of these railway applications can integrate railway solutions from one system integrator or many.

A railway application can include one or more railway solutions handed over by the system integrator to the railway duty holder, the main difference between the railway application and

the railway solution is that a railway application is operational and includes the personnel, policies and procedures required for its operation.

The term [system under consideration \(3.1.171\)](#) (SUC) is used with the same meaning as in the IEC 62443 series. It is used to define the scope of the railway solution to be provided and on which the cybersecurity risk assessment is to be performed.

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

**Table 1 – IEC 63452 to IEC 62443 equivalent terms**

IEC 63452 term	IEC 62443 equivalent term
<a href="#">railway system (3.1.121)</a>	<none>
<a href="#">railway application (3.1.115)</a>	industrial automation and control system (IACS)
<a href="#">railway solution (3.1.120)</a>	automation solution
<a href="#">control system (product) (3.1.40)</a>	control system (product)
<a href="#">component (product) (3.1.35)</a>	component (product)
<a href="#">safety-related system (3.1.138)</a>	safety instrumented system (SIS)
<a href="#">legacy system (3.1.83)</a>	<none>
<a href="#">railway duty holder (3.1.117)</a>	<none>
<a href="#">asset owner (3.1.12)</a>	asset owner
<a href="#">system integrator (3.1.170)</a>	integration service provider
<a href="#">maintenance service provider (3.1.89)</a>	maintenance service provider
<a href="#">product supplier (3.1.110)</a>	product supplier

NOTE 2 In the IEC 62443 series, it is described that automation solutions are installed in asset owner sites by the integration service providers whereas in this standard, railway solutions like trains and other rolling stock subsystems are usually integrated and installed by the system integrators at their sites.

NOTE 3 In this standard, there is no equivalent term for System Integrator as defined in [IEC 62443-3-3:2013/COR1:2014 \[59\]](#).

[Table 2](#) provides some examples of the railway system taxonomy.

**Table 2 – Railway system, application, solution and product examples**

IEC 63452 term	Examples
<a href="#">railway system (3.1.121)</a>	<ul style="list-style-type: none"> <li>A single metro or tramway line (with tracks, signalling, trains, stations and OCC) if not connected with any other lines.</li> <li>The whole metro system of a city if its lines are connected.</li> <li>A single railway line (with tracks, signalling, trains, stations and OCC) if not connected with other railway lines.</li> <li>The whole railway system of a country or a region (with tracks, signalling, trains, stations and OCC) when lines are connected.</li> </ul>
<a href="#">railway application (3.1.115)</a>	<ul style="list-style-type: none"> <li>A train fleet in operation, with their associated personnel, policies and procedures.</li> <li>A signalling solution in operation with its associated personnel, policies and procedures.</li> <li>A railway network (and relevant elements including traffic management, tracking and navigation systems) in operation with their associated personnel, policies and procedures.</li> <li>A train fleet video surveillance/CCTV solution and relevant elements in operation with their associated personnel, policies and procedures.</li> </ul>
<a href="#">railway solution (3.1.120)</a>	<ul style="list-style-type: none"> <li>Manufactured train with relevant subsystems, elements, devices and components designed, manufactured, integrated, configured and maintained to operate as a railway application.</li> </ul>

IEC 63452 term	Examples
	<ul style="list-style-type: none"> <li>• Electrification system, (including overhead lines and the track-side electricity consumption measuring and charging system); designed, manufactured, integrated, configured and maintained to operate as a railway application.</li> <li>• On-board or track-side signalling equipment required to ensure safety and to command and control movements of trains as well as other functional operations; designed, manufactured, integrated, configured and maintained to operate as a railway application.</li> <li>• Platform screen doors subsystem with relevant elements, devices and components on both station and train designed, manufactured, installed, and configured to operate as a railway application.</li> </ul>
control system (product) (3.1.40)	<ul style="list-style-type: none"> <li>• On-board braking system;</li> <li>• Axle counting system;</li> <li>• Level crossing system;</li> <li>• Closed-Circuit Television (CCTV) system.</li> </ul>
component (product) (3.1.35)	<ul style="list-style-type: none"> <li>• Safety-related computer;</li> <li>• Programmable Logic Controller (PLC);</li> <li>• IP camera;</li> <li>• Balise;</li> <li>• Ethernet switch, gateway, firewall, or router;</li> <li>• Door controller;</li> <li>• Traffic management software.</li> </ul>

## 4 Railway system overview

### 4.1 Purpose

This [Clause 4](#) provides requirements and guidance to the railway duty holder to create a comprehensive description of a railway system for projects where cybersecurity is relevant.

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

- Maintainable system documentation;
- Capability to align the interpretation of the general / overall high-level security needs;
- Easier integration of final railway application/solution descriptions into the existing railway system.

Cybersecurity experts and railways stakeholders can benefit from one single and common way to describe the railway application/solution (that can be applicable also to the SUC as defined in [Clause 7](#)).

### 4.2 Overview

A railway system description from a cybersecurity point of view can be established in the following three steps:

- a) Creating a description of the railway system from a cybersecurity perspective to identify all systems belonging to the overarching railway system, as detailed in [4.4](#).
- b) Identifying the subsystems that compose the railway system and their topological or physical distribution, as detailed in [4.5](#).
- c) Creating and updating a high-level railway zone model that comprises all the (main) asset groups of the railway system, as detailed in [4.6](#).

Clause [4.7](#) deals with the applicability of shared security services within the railway system.

NOTE In the context of urban rail transport, the IEC 62290-1:2014 [6] standard provides such a description. Another way to describe the railway system is a model based approach aligned with Annex D of IEC FDIS 62278-1:2024 [17] where the functions are described with the degree of detail appropriate to their importance.

### 4.3 Inputs / Outputs

Input:

- Existing system architecture descriptions.

Outputs:

- Railway system and railway applications identified as part of OT usage [SO-01-01].
- High-level system model of the railway system [SO-02-01].
- High-level zone model of the railway system [SO-03-01].
- Shared cybersecurity services identified as part of the railway system [SO-04-01].

### 4.4 [SO-01-01] Identification of the railway system

#### 4.4.1 Requirement

The railway duty holder shall identify and document the scope of its railway system and railway applications, identifying OT systems, and segregating them from IT systems.

The railway duty holder shall, where no clear assignment to IT or OT is apparent, decide if the system is to be considered as IT or OT.

#### 4.4.2 Rationale and supplemental guidance

IT and OT can be distinguished by their utilization and/or their underlying technology. The utilization of a component is more compelling as a basis for deciding which category it falls into rather than the underlying technology.

Furthermore, it is not recommended to use components that were manufactured for OT (e.g. PLC, sensors) as IT.

The Table 3 provides an example of how IT and OT systems and subsystems can be classified:

**Table 3 – Example of OT/IT classification**

	Technology IT (e.g. cloud, laptop, IT services, ...)	Technology OT (e.g. PLC, sensors, ...)
Utilization as IT	Out of scope of 63452 (Business systems)	Out of scope of 63452 (Not recommended)
Utilization as OT	In scope of 63452 (Operational systems)	In scope of 63452 (Operational systems)

As OT fulfils demanding requirements, e.g. for safety reasons or limited resources in hardware, it is more expedient to assume OT in case of doubt.

Determining the possible interface(s) between IT and OT is a necessary step to identify clearly the (sub)system to IT or OT:

- OT part composed by operational systems and subsystems, under the scope of the OT cybersecurity officer and team; in scope of 63452; applying OT requirements and standards.
- IT part composed by business systems and subsystems, under the scope of the IT cybersecurity officer and team; out of scope of 63452; applying IT requirements and standards.

Describing the railway system is the first step in understanding the applicability of this standard (and the associated IEC 62443 series of standards).

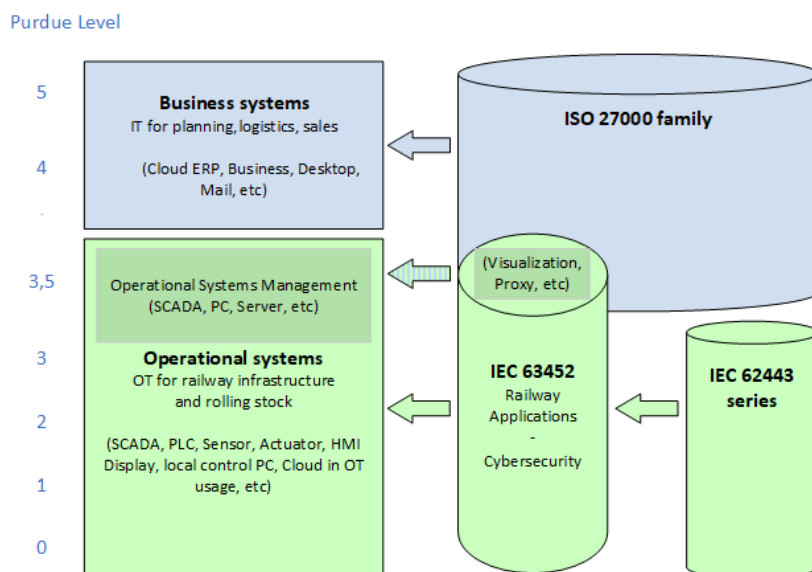
The following subsystems should be included in the scope of this standard:

- rolling stock (3.1.133);
- track-side (3.1.180) including signalling system (3.1.163);
- landside (3.1.82);
- fixed installation (3.1.59).

The railway duty holder can manage its railway systems as a coherent set of railway applications, for example the railway duty holder can specify separate cybersecurity programmes for signalling and rolling stock or combine all or some of them as one single railway application.

Figure 3 shows the segregation of an enterprise's IT systems in an industrial environment. A key element is a tailored segregation between IT systems and OT systems, as well as procedural means which includes different user management policies in the business and operations contexts.

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



**Figure 3 – Segregation between IT and OT**

NOTE For details on purdue levels, see [Clause B.3.2](#).

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

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

## 4.5 [SO-02-01] Definition of a high-level railway system model

### 4.5.1 Requirement

The railway duty holder shall establish and maintain a high-level system model of the railway system that identifies subsystems grouped according to criteria such as location, functionality, or organizational context.

### 4.5.2 Rationale and supplemental guidance

#### 4.5.2.1 General

Based on the OT identification done before, subsystems should be categorized taking the following aspects into account:

- physical areas, such as on-board, de-centralized operational and filed systems, central operational control and maintenance (see [Figure 4](#));
- functional criticality level, such as signalling, command and control, auxiliary, comfort, public and communication (see [Figure 4](#));
- organizational context, such as responsible entities including operators and maintainers.

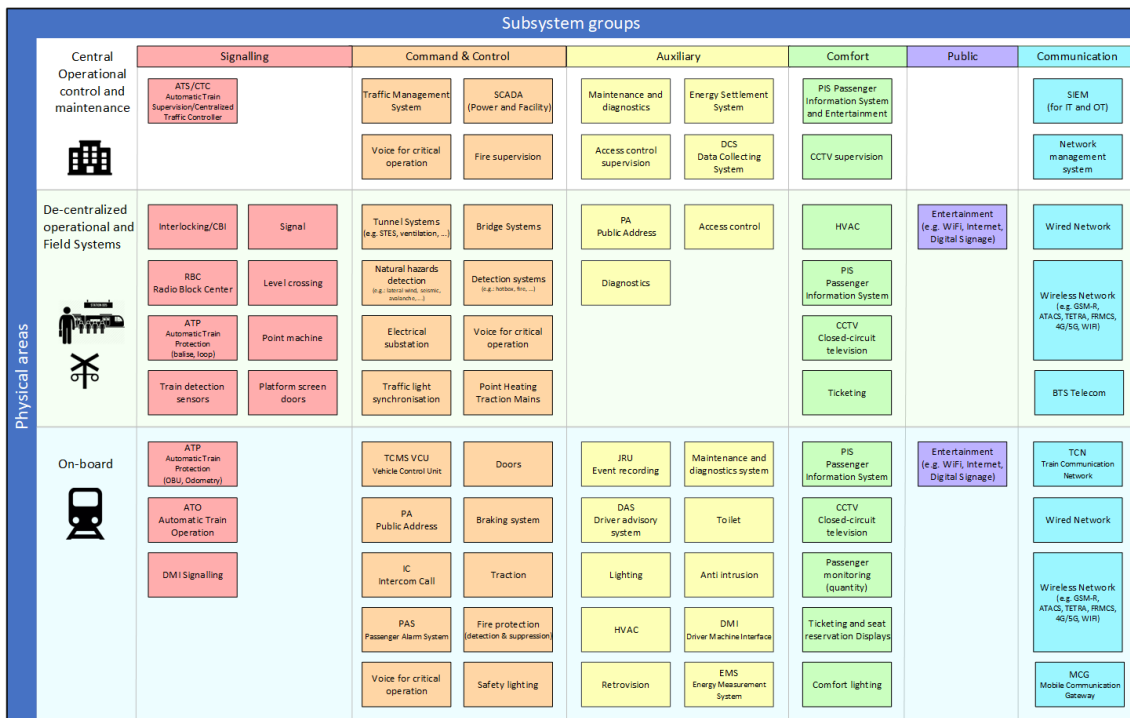
The resulting model can be used as a basis to define the SUC (see [Clause 7](#)) for different railway applications, for example a traffic management system.

[4.5.2.2](#) and [4.5.2.3](#) give examples how to create the high-level railway system model.

#### 4.5.2.2 Area-based approach

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





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

**NOTE** In addition to the subsystems and functionalities shown in [Figure 4](#), there are many network devices, such as switches and routers, spread all over the railway system (including trains) that are also regarded as assets to be protected from cybersecurity attacks. These components can be considered either as part of the security zone or as a part of the subsystem for which they deliver the network service.

[Clause F.1](#) provides guidance on how to build an area-based high-level railway system model.

#### 4.5.2.3 Topology-based approach

One of the main challenges of the railway system is its large geographic coverage across national and/or state boundaries or borders, ranging from a few kilometres up to several thousand kilometers. 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.

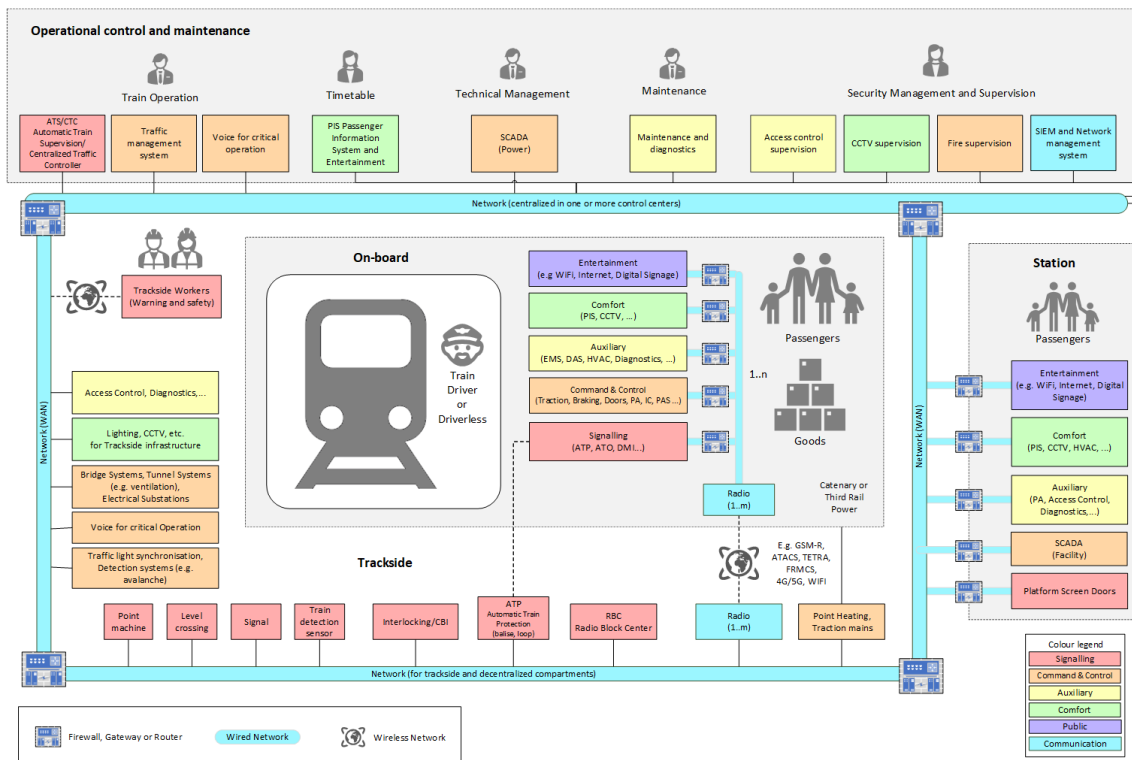
Many subsystems include a variety of products and communication protocols demanding the creation of a comprehensive network architecture of the railway system.

[Figure 5](#) shows an example of a topology-based view of the railway system.

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

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

Railway duty holder, asset owners and integration service providers can identify the network oriented connections between the components in the topology-based model.



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

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

#### 4.6 [SO-03-01] Definition of a high-level railway zone model

##### 4.6.1 Requirement

The railway duty holder shall establish and maintain a high-level zone model of the railway system.

##### 4.6.2 Rationale and supplemental guidance

The principles set out in IEC/TS 62443-1-1:2009 [7] for defining a zone and conduits model have been considered in this subclause, although the term zone is used here in a broader sense, not limiting it to a synonym of security zone or network zone (4.6.2, Note 3). Considering the architecture of its railway system, the railway duty holder creates a high-level railway zone model by grouping the assets of the different railway applications into zones.

The aim of defining zones and conduits is to group systems or components that have the same criticality from the security perspective, due to similar threats and possible impacts in particular for railway operation.

The definition of the zones considers mechanisms to keep particular or essential services running in the case of a security incident in another zone. These mechanisms should have the capability to isolate an incident by closing gateways to an infected zone.

There can also be zones within zones that provide layered security giving defence in depth and addressing multiple levels of security requirements.

In-bound communication via existing IACS systems should be preferred to reduce complexity and communication lines to external entities, which may open backdoors. To run existing decentralized management systems like monitoring and network management, asset management, syslog services, etc., an OT DMZ zone should be foreseen.

This high-level railway zone model is used as an input to the risk assessment for system design, especially in the identification of the SUC (7.3), and the partition of the SUC into zones and conduits (7.5). The outcome of the risk assessment should be fed back and used to maintain the high-level railway zone model up to date.

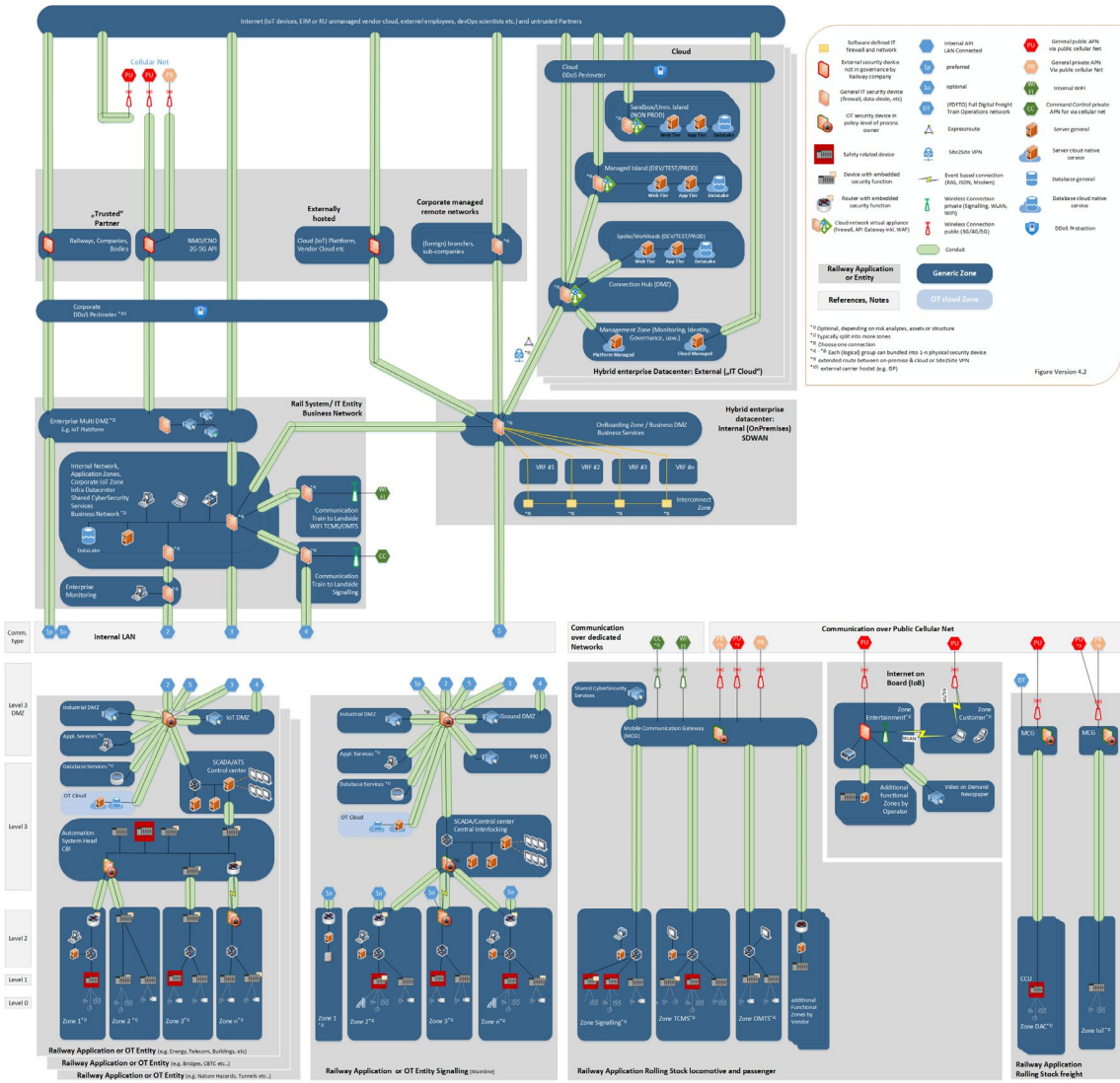
NOTE 1 Zone and conduits models for specific railway domains are available from specialized working groups like ERJU for the signalling domain.

The combination of zones, conduits, subsystems and zone criticality results in a generic zone model including communication rules (for more details, see [Clause F.2.1](#)). [Figure 6](#) shows an example of a high-level railway zone model.

The following principles should be considered to build and update a high-level railway zone model:

- The security events related to communication and human interactions in high criticality zones should be monitored, logged, and stored for forensics at least at the subsystem boundaries (see [IEC 62443-3-2:2020 \[51\]](#), SR 2.8).
- Security devices between zones with different criticality that protect the zone with the higher criticality should be managed by the organization responsible for the higher criticality zone (see [IEC 62443-3-2:2020 \[51\]](#), ZCR 3.1).
- The higher criticality zone should consider inputs from the lower zone as potentially hostile.
- The data flow between rolling stock and land-based subsystems should be reduced to a minimum of conduits (without impacting the availability of the communication) to facilitate the control or the detection of forbidden data flow and malware by security devices.
- The conduits between OT zones hosting essential functions should be Category 1 networks referencing to the [IEC 62280:2014 \[58\]](#) to support seamless and direct diagnostic in case of breakdowns to fulfill the end-to-end responsibility of the asset owner for its zones.
- If available, the zones and conduits can be designed based on defined requirements. The analysis of the protection requirements is based on the possible impact if the system is altered and fails. The impact is usually defined in different classes such as health damage, financial impact, reputation and business continuity. To covers high helves risks and attack surfaces, an initial risk analyses should be done for integration in brownfield and interfaces to other entities at this architecture design phase. The protection requirements analysis only focusses on impact. The integration and application of the zone model is highly dependent on the asset owner's applications, legacy systems or processes.
- In addition to these major principles, some other principles (e.g. safety related devices, temporarily connected devices and externally connected devices) should be considered through the application analysis at project level (see [7.5.3](#) for more details).

The principles are further described in [Clause F.2.1](#), which contains also practical examples how to evaluate the criticality of systems to build security zones.



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

For magnified sections of [Figure 6](#) see [Clause F.2](#).

NOTE 2 The levels on the left side are based on the Purdue Enterprise Reference Architecture (PERA).

NOTE 3 Some technical publications differentiate zones in network zones, security zones, physical zones, virtual zones or other zones.

See also [Annex A](#) (Handling conduits).

#### 4.7 [SO-04-01] Specification of shared cybersecurity services

#### 4.7.1 Requirement

The railway duty holder shall define which shared cybersecurity services are part of the railway system.

#### 4.7.2 Rationale and supplemental guidance

Shared cybersecurity services provide a collection of standardized interfaces of central security functions accessible to all railway solutions and applications.

The railway duty holder should use commonly accepted specifications for shared cybersecurity services and their interfaces.

Since these services require a lot of effort regarding implementation and operation, it is recommended to share them for railway applications.

Based on [IEC 62443-3-3:2013/COR1:2014](#) [59] the following shared cybersecurity services could be used:

- system-wide time synchronization (TIME/STS);
- identity and access management (IAM);
- user authentication service (UAS) - if available;
- asset inventory (INV);
- public key infrastructure (PKI);
- security logging (LOG);
- backup and restore (BKP);
- network intrusion detection system (NIDS);
- security incident and event management (SIEM);
- network access control (NAC);
- remote software and configuration update (SWU);
- domain name system (DNS) - if available.

Shared cybersecurity services typically form unified or hierarchical systems in a railway system. A railway application in the operational systems area is interfacing with a shared cybersecurity service in this same operational area which interfaces with another shared services in the business systems area, crossing the boundary through a DMZ or other security measures.



**Figure 7 – Example of hierarchical structure of shared cybersecurity services (example TIME)**

Examples of typical hierarchies of shared cybersecurity services are:

- TIME: time sync client in railway solution, OT time server, IT/corporate time server, GNSS or national time server;
- PKI: PKI client, (Local) Registration Authority, Issuing Certificate Authority, Root Certificate Authority;
- IAM: IAM client, OT IAM, Corporate Directory;
- LOG: log client, log server, SIEM.

Therefore, the shared cybersecurity services may have multiple instances in the same and different parts of the system architecture.

The hierarchies and federation structure can be adjusted in complexity depending on the scope of the railway system and railway duty holder company structure. Commonly accepted interface specifications support the modularity and adaptation to different architectures.

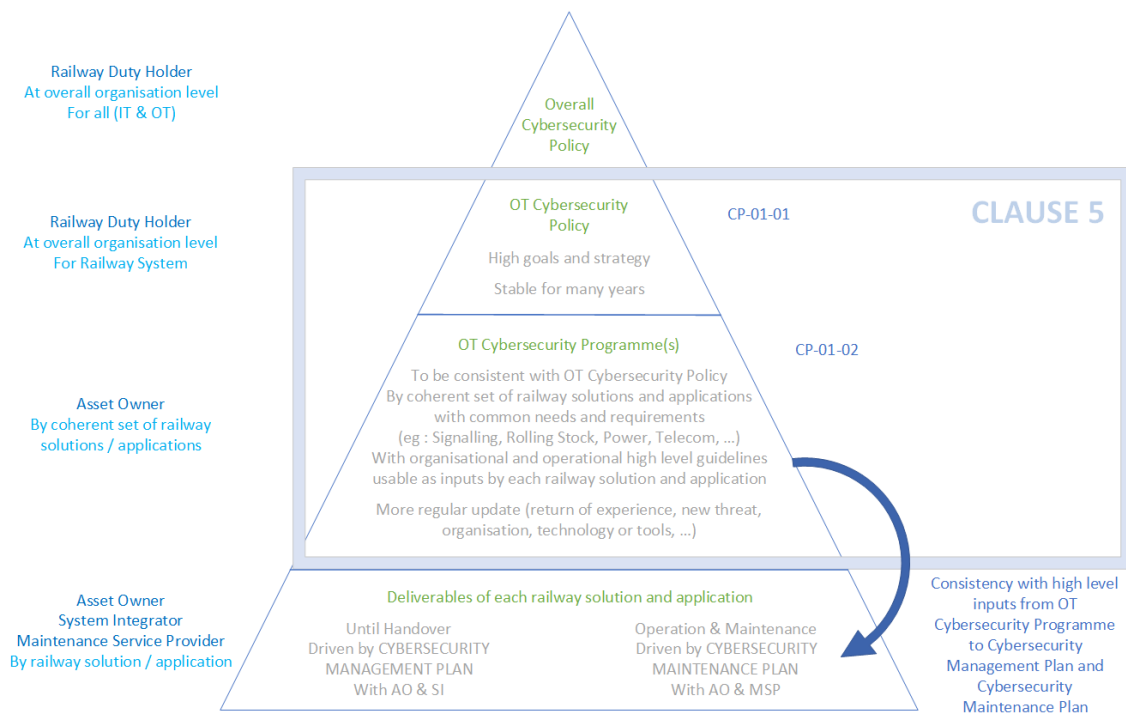
In cases where multiple stakeholders are involved in the operation of shared cybersecurity services, the organizational aspects should be managed (supply chain - see [5.8](#)).

NOTE See also [X2R3-Deliverable D8.2-2:2020 \[8\]](#) [TO BE CHANGED BY FUTURE SPEC ERJU WHEN AVAILABLE] for more information.

## 5 Enterprise cybersecurity programme and management

### 5.1 Overview

The following subclauses deal with requirements on processes and procedures for the OT cybersecurity management system for OT systems. These activities are not related to a specific cybersecurity life cycle for a specific railway application or specific railway project. They are managed at an organizational level and applied before, during and after any railway application life cycle. Also they are required to be in place independent of a given railway application for the railway duty holder and asset owner, system integrator and maintenance service provider.



**Figure 8 – OT Cybersecurity Management System**

### 5.2 Inputs / Outputs

#### Input

- The overall cybersecurity policy of the organization.

#### Outputs

- A railway OT cybersecurity policy [CP-01-01].
- A railway OT cybersecurity programme [CP-01-02].
- A documented process for Information sharing [CP-02-01].
- A documented process for Competency management [CP-03-01].
- A documented process for Inventory management [CP-04-01].
- Up-to-date inventory [CP-04-01].
- A documented process for Supply chain management [CP-05-01].
- A documented process for Risk management [CP-06-01].
- A risk acceptance criteria [CP-06-01].

- A risk register [CP-06-01].
- A threat log [CP-06-01]
- A plan of risk treatment [CP-06-01].
- A documented process for Business continuity management (Business continuity plan) [CP-07-01].
- A documented process for Data protection management [CP-08-01].

### **5.3 [CP-01-01] Railway OT cybersecurity policy**

#### **5.3.1 Requirement**

The railway duty holder shall establish, apply and maintain a railway OT cybersecurity policy that:

- a) includes the high-level objectives and challenges including the management aspect in [5.4.1](#) of the organization for securing the railway system;
- b) is aligned with the overall cybersecurity policy of the organization;
- c) is approved by management.

#### **5.3.2 Rationale and supplemental guidance**

The railway OT cybersecurity policy should be aligned with other cybersecurity policies of the organization to support its strategy and achieve its objectives; policies should be stable for longer periods than processes and procedures.

Challenges could help defining priorities of actions to be cascaded into OT cybersecurity programme, for example maintaining railway applications in a secure state, monitoring, etc.

The railway OT cybersecurity policy can be a dedicated document or part of the overall cybersecurity policy document.

NOTE Refer to [IEC 62443-2-1:2024 \[52\]](#) for further guidance,

- ORG 1.1 (Information security management system)

### **5.4 [CP-01-02] Railway OT cybersecurity programme**

#### **5.4.1 Requirement**

The asset owner shall establish, apply and maintain a railway OT cybersecurity programme for each of its railway applications.

A railway OT cybersecurity programme shall be aligned with the railway OT cybersecurity policy (see [5.3](#)), and shall cover cybersecurity aspects of at least the following topics:

- a) Scope and security objectives
- b) Information sharing management (see [5.5](#))
- c) Competency management (see [5.6](#))
- d) Inventory management (see [5.7](#))
- e) Supply chain management (see [5.8](#))
- f) Risk management (see [5.9](#))
- g) Business continuity management (see [5.10](#))
- h) Data protection management (see [5.11](#))
- i) Operations and maintenance management (see [Clause 10](#))
  - 1) Vulnerability management (see [10.10](#))
  - 2) Patch management (see [10.11](#))



- 3) Incident management (see [10.14](#))
- 4) Cybersecurity monitoring (see [10.16](#))
- 5) Backup and recovery management (see [10.15](#))
- 6) Continuous cybersecurity assurance including cybersecurity case update (see [10.4](#), [10.5](#), [10.6](#) and [10.7](#))
- 7) Decommissioning management (see [10.17](#))

#### 5.4.2 Rationale and supplemental guidance

The railway OT cybersecurity programme describes the cybersecurity management policy (see [5.3.1](#)), set of processes and procedures to protect their scope of railway system or their railway applications from cybersecurity risks and achieve to keep intended availability, integrity and confidentiality. Hence, scope and security objectives should be clearly described in OT cybersecurity programme.

The railway OT cybersecurity programme should be updated to consider the return of experience, the threat evolutions, the organizational changes and the new technologies or tools available.

To facilitate readability, dissemination and updates, the railway OT cybersecurity programme could be divided in multiple OT cybersecurity programmes established for each common group of consistent functions, railway applications (e.g. for signalling, for rolling stock, for power installations, for telecoms) in organization levels.

OT cybersecurity programme should have defined integration and synchronisation points with the safety processes as cybersecurity risks may impact safety related functions.

All the management topics listed in the requirement should be covered by the railway OT cybersecurity programme at organization level.

- Requirements for topic that are mostly or completely independent of specific railway applications or solutions and can be addressed at the organization level are provided in Clause 5.
- For topics that are specifically handled by the individual railway applications, the requirements defined in [Clause 6](#) to [Clause 10](#) help to complete the key aspects of the railway OT cybersecurity programme with the experience of specific railway applications and solutions.

Once the handover of a railway solution has taken place, the operational aspects and refinements should be defined for each railway application.

- For the topics that needs propagation for stakeholders (system integrator, maintenance service provider and product supplier), this is covered by the supply chain requirement (see [5.8](#)).

The OT cybersecurity programme should be maintained and reviewed at least annually and updated when appropriate (e.g. when significant cybersecurity incidents or significant changes to the railway application or risks occur).

NOTE Refer to [IEC 62443-2-1:2024 \[52\]](#) for further guidance,

- ORG 1.3 (Security role and responsibilities)
- ORG 2.2 (Processes for discovery of security anomalies)
- COMP 1.2 (Dedicated portable media)



## 5.5 [CP-02-01] Information sharing management

### 5.5.1 Requirement

The asset owner shall establish, apply and maintain an information sharing management process.

This process shall include:

- a) Confidentiality management for sharing technical information between stakeholders through the supply chain and for each phase of life cycle (from tender to decommissioning);
- b) Confidentiality management for sharing sensitive information directly linked to cybersecurity aspects (e.g. on secrets, vulnerabilities);
- c) Incident process to mitigate leak of data.

The information sharing management process shall comply with applicable relevant legislation (e.g. personal data).

### 5.5.2 Rationale and supplemental guidance

The information sharing policy:

- Should be addressed with an overall approach in the overall cybersecurity policy (e.g. what kind of measures need to be applied for confidential information such as documents and data);
- May need a propagation in the OT cybersecurity programme if relevant or the OT cybersecurity programme should refer to the overall cybersecurity policy if not relevant for this preliminary stage (e.g. what kind of document for what level of confidentiality);
- May be declined at specific railway application level (in tender, agreement or contract) if needed, coming from previous level requirements (company policy or OT cybersecurity programme).

The confidentiality for technical information between stakeholders through the supply chain should be predefined, for example in a document production plan, for each type of document / data, a defined level of confidentiality, the list of people allowed to access it, and the set of measures to be taken for creation, storage, identification, exchange and destruction. Typically, encryption (of data or storage or flows) and strong access measures (like MFA) should be required.

The confidentiality for sharing sensitive information directly linked to cybersecurity should be precisely defined. This typically concerns vulnerability disclosure or incident sharing, under contractual agreement in case of vulnerability surveillance for example, or through sharing organizations like ISAC, CERTs, CSIRTs and PSIRTs. The rules should be compatible with regulations or laws which define mandatory sharing with, for example, agencies.

In case of non-compliance of the process, or an identified real leak of data, an incident should be opened try to solve the issue. Mitigation measures, like changing secrets or deploying a patch quickly, could be needed.

NOTE Refer to [IEC 62443-2-4:2023 \[50\]](#) for further guidance,

- SP 01.03 (Solution staffing)

## 5.6 [CP-03-01] Competency management

### 5.6.1 Requirement

The asset owner shall establish, apply and maintain a cybersecurity competency management process to ensure the cybersecurity competencies of personnel participating in the life cycle of the railway application, including system integrator and maintenance service provider, according to their role and responsibilities.

The process shall include:

- a) identification of cybersecurity roles and responsibilities and their associated skills;
- b) periodic evaluation of people current competencies versus the ones requested by their role (competency gap);
- c) delivering of the training / awareness programs to achieve the required competencies.

### 5.6.2 Rationale and supplemental guidance

Managing competencies, which includes training and awareness, is a crucial element of cybersecurity programme set by asset owner. This is because cybersecurity breaches often occur where personnel lack awareness of key organizational principles and knowledge which includes policies, programmes, rules, processes, procedures, technical knowledge, and lessons learned from past cybersecurity experiences within the organization and from various projects. The process of competency management at an organizational level should mitigate these risks.

The asset owner should first establish a clear process identifying target competencies, current gaps, and set a clear organizational action plan for training and awareness to bridge these gaps. The results should be designed in a way that makes processes and procedures related to specific railway applications easily understandable and implementable.

Cybersecurity specialised training should equip personnel with the skills needed to perform the tasks that are specific to their respective roles. [Annex H](#) provides useful guidance for fundamental competencies. This organizational competency management process should be tailored and cascaded down to railway applications and its operational environments with the competencies of OT cybersecurity programme. Cybersecurity should be a dedicated topic in functional training sessions and should be regularly provided to teams, such as maintenance teams, for example, through companywide awareness campaigns, security-regular messages (e.g. "Your operation is always being recorded and monitored") and team meetings.

It is important that the railway duty holder ensures that suppliers, such as system integrator, maintenance service provider, external service providers, product suppliers and maintenance service suppliers, also comply with cybersecurity competency requirements. The asset owner can either provide the training directly or accept the competency programmes of them (see supply chain management (see [5.8](#))).

Competency management should be continuously reviewed, so that it is kept up to date with upcoming regulations, the organization security objectives, the effectiveness of training and the ever-evolving threat environment.

The delivery of the training can be either internal or external to the organization (e.g. purchased training).

NOTE 1 Refer to [IEC 62443-2-1:2024 \[52\]](#) for further guidance,

- ORG 1.4 and ORG 1.5

NOTE 2 Refer to [IEC 62443-2-4:2023 \[50\]](#) for further guidance,

- SP 01.01 - 07 (Solution staffing)

NOTE 3 The framework of competency management in cybersecurity aspect can be referred to ISO 9001:2015/Amd 1:2024 Quality management systems - Requirements [\[9\]](#) and [ISO 22163:2023 \[10\]](#).

## 5.7 [CP-04-01] Inventory management

### 5.7.1 Requirement

The asset owner shall establish, apply and maintain the process to identify and document the baseline of the railway assets and make sure that it is consistent with what is currently in operation.

### 5.7.2 Rationale and supplemental guidance

The railway assets include all products, hardware and software components and associated application data configured for use in each railway application.

The railway duty holder should define the necessary inventory information to be maintained. This information can encompass various aspects such as the type of asset, its manufacturer, hardware and software versions, configuration settings, applied patch version, asset location, organizational responsibility, and the asset's criticality.

Baseline properties and documentation on the entire cybersecurity life cycle about the railway assets should be collected, correlated and verified with available means including application tools, which includes railway application management systems, network sensors, software agents, spreadsheets (low level designs) and application programming interfaces (APIs).

This inventory information should be documented within a configuration management database (CMDB) to get a company-wide overview of the state of assets, patching updates and system vulnerabilities.

Also, the change management process is essential to keep the correctness of baseline.

The goal is to ensure that the inventory is always up to date regarding the current state of each railway application.

NOTE 1 Refer to [IEC 62443-2-1:2024 \[52\]](#) for further guidance on inventory management

- CM 1.1 (Asset Inventory baseline)
- CM 1.2 (Infrastructure drawings / documentation)
- CM 1.3 (Configuration settings)
- CM 1.4 (Change control)

NOTE 2 Refer to [IEC 62443-2-4:2023 \[50\]](#) for further guidance,

- SP 01.04 (Solution staffing)

NOTE 3 Refer to [ISO 22163:2023 \[10\]](#) for further guidance on change management

## 5.8 [CP-05-01] Supply chain management

### 5.8.1 Requirement

Each organization involved in the cybersecurity life cycle of a railway application shall establish, apply and maintain a management process to manage its supply chain risks.

This process shall ensure:

- a) Clear identification of the delegated cybersecurity tasks including the scope of work and the relationship between acquirer and its suppliers;
- b) Identification of relevant cybersecurity criteria applicable to the supplier selection process and to the supplier evaluation process;
- c) Identification of the cybersecurity requirements for suppliers, from both technical and management process perspectives;
- d) Continuous monitoring of suppliers including the improvement action plan for suppliers.

### 5.8.2 Rationale and supplemental guidance

#### (1) General Guidance

A railway system, along with its railway applications and railway solutions, can be composed of various products, control systems and components. These may include hardware and software

components, as well as shared cybersecurity services. These components and services are often provided by a range of system integrator, maintenance service provider, suppliers (i.e. product suppliers, external service providers, maintenance service suppliers). It is important to note that these organization of acquirer (i.e. asset owner, system integrator and maintenance service provider) may also utilize products or services from other suppliers throughout the entire cybersecurity life cycle.

The complexity of the supply chain can make it difficult to maintain visibility and traceability of cybersecurity risks and practices during life cycle of railway applications or railway solutions and products. This complexity can pose several risks to the acquiring organization. These risks include:

- non-compliance with cybersecurity technical requirements due to inadequate cybersecurity competency management among suppliers;
- non compliance with regulatory requirements from acquirer as well as on supplier themselves;
- unintentional incidents, such as substandard software development processes, which can lead to design flaws and vulnerable products;
- deliberate attacks, such as the introduction of counterfeit items or malware into products,
- accidental deployment of incorrect versions due to a lack of inventory management processes;
- unintentional security gaps that can occur during the integration of multiple products;
- unnecessary disclosure of confidential cybersecurity information to parties who do not need to know, due to poor information sharing management.

To mitigate supply chain risks like as above, the acquirer should:

- define the supplier selection and evaluation process through supply chain risk assessment with supply chain risk criteria (e.g. capability of cybersecurity life cycle activities including vulnerability and incident management, implementation of cybersecurity requirement including regulatory requirements, supply business continuity and so forth).
- based on the extent of risks associated with suppliers, acquirers should define a set of cybersecurity requirements on suppliers. These requirements, which can be technical and/or related to management processes (see 5.4), should be tailored to the specific risk level and degree of each supplier.
- the cybersecurity requirements on suppliers should be explicitly communicated and enforced, not only by the primary supplier but also by any subsequent suppliers involved in the process and life cycle.
- make sure suppliers to initiate improvements and inform the fact in case of known any changes in warranty or cybersecurity vulnerabilities.

In basis of above, the examples of the cybersecurity requirements on suppliers are provided below.

EXAMPLE 1 Acquirer could request to keep defined SLA, RTO and RPO to suppliers.

EXAMPLE 2 Acquirer could request to have access to the software bill of materials in particular for the cybersecurity-critical assets.

EXAMPLE 3 Acquirer can request the product supplier to be compliant with [IEC 62443-4-1:2018 \[49\]](#) and [IEC 62443-4-2:2019/COR1:2022 \[11\]](#) IEC62443-4-2:2019 [6]

EXAMPLE 4 A process to define cybersecurity requirement stating the need to perform and deliver an initial cybersecurity risk assessment.

EXAMPLE 5 A technical cybersecurity requirement stating that all train to land communication should be encrypted. The suppliers should deliver the product or service in accordance with the agreed requirements and support the acquirer with response, disclosure and patch management

NOTE 1 The standards below could be used as reference to capture requirements related to maintenance service provider and system integrators,

- IEC 62443-2-4:2023 [50]
- IEC 62443-2-1:2024 [52],
  - ORG 1.6 (Supply chain security)
  - ORG 2.3 (Secure development and support)

In general, on supply chain stakeholders, the following standards also address several aspects regarding IT/OT cybersecurity.

- ISO/IEC 27001:2022 [12]
- ISO/IEC 27036-2:2022 [13] 7.2
- ISO/IEC 27036-3:2023 [14]
- ISO/IEC 27036-4:2016 [15] for OT Cloud
- NIST SP-800-161: Cybersecurity supply chain risk management practices
- ISO 22163:2023 [10]

### (2) Guidance for Railway OT cybersecurity programme(s) in supply chain

From view of asset owner as acquirer, the needs defined in the railway OT cybersecurity programme should be included in the contractual agreements to be declined at railway applications or railway solutions, to supply chain (system integrator, maintenance service provider, and suppliers).

- Some topics should be cascaded down to system integrator, suppliers inside their cybersecurity management plan applicable for the considered railway application or solution on specific railway project.
- Some topics should be cascaded down within the cybersecurity maintenance plan (applicable for a railway application maintenance) to maintenance service provider and suppliers.

The topics of governance, supply chain management, or awareness could be covered with an overall view, independent of any specific project or railway application. In contrast, the specific topics of vulnerability management, patch management or decommissioning management could be defined at application level.

The acquirer should have clear point of contacts to aggregate the information such as critical vulnerability and cybersecurity incident from suppliers. This makes the correct, efficient communication to mitigate supply chain risks as possible.

NOTE 2 This concept above could also be applicable from viewpoint of system integrators and maintenance service providers to manage their own suppliers.

### (3) Guidance for cybersecurity requirements between acquirer and product supplier

#### **a) For COTS**

- Acquirer should define the selection criteria related to cybersecurity for COTS supplier, if necessary. Here are some examples of selection criteria:
  - compliance with cybersecurity requirement;
  - availability of a product cybersecurity case;
  - availability of product cybersecurity guidelines;
  - availability of SBOM data;
  - evidence of implementation of secure development life cycle (e.g. IEC 62443-4-1);
  - availability for track records of vulnerability management and delivery of security updates;
  - third party conformity assessment such as IEC 62443-4-1, IEC 62443-2 or IEC 15408 (Common Criteria);
  - trust on the provider.

- Acquirer should get the evidences or documentation related to above on specific COTS or external provided product.

NOTE IEC62443-4-1 SM-09 provides more information related to COTS.

#### **b) For custom developed product**

- Acquirer should define the evaluation criteria related to cybersecurity for custom developed product supplier, if necessary. Here are some examples of selection criteria:
  - experience of compliance with cybersecurity requirement;
  - availability of a product cybersecurity case;
  - availability of product cybersecurity guidelines;
  - availability of SBOM data;
  - experience of implementation of a secure development life cycle (e.g. IEC 62443-4-1);
  - availability for track records of vulnerability management and delivery of security updates;
  - availability for third party conformity assessment such as IEC 62443-4-1, IEC 62443-2 or IEC15408 (Common Criteria);
  - trust on the provider.
- Acquirer should provide to the product supplier, if necessary, the following items:
  - threat environment applicable to the product;
  - regulatory requirements (see prerequisites in 6.3.2);
  - list of technical security requirements:
    - IEC 62443-3-3 and 62443-4-2
  - list of security management requirements if necessary:
    - IEC 62443-4-1
    - cybersecurity management area defined in 5.3.1 and 10.5.1 on this document
- Acquirer should get from the product supplier, if necessary, the following items::
  - cybersecurity management plan for the developed product (see 6.3.1);
  - cybersecurity evaluation plan for the developed product (see 9.3.4);
  - conformity evidence to security requirements (as defined by contract):
    - “product cybersecurity case”
    - third party conformity assessment at product level, (e.g. conformity to 4-1/4-2 or common criteria)
  - cybersecurity guideline (as defined by IEC 62443-4-1 – Practice 8);
  - vulnerability / Incident / Patch service guide (see IEC 62443-4-1 – Practice 6);
  - SBOM data

NOTE IEC 62443-4-1 SM-10 provides more information to custom provided products.

## **5.9 [CP-06-01] Risk management**

### **5.9.1 Requirement**

The asset owner shall establish, apply and maintain the risk management process to identify and address the cybersecurity risks related to its railway system.

This shall include:

- a) identification of the threats, vulnerabilities, and risks related to its railway applications;

- b) risk acceptance criteria and risk matrices to decide level of likelihood, impact, risk;
- c) procedure to document and keep track of the identified threat in threat log;
- d) procedure to document and keep track of the identified risks in a risk register
- e) establishment of the plan of risk treatment in line with the risk register;
- f) follow-up of the execution of the risk treatment plan until its closure.

### 5.9.2 Rationale and supplemental guidance

Cybersecurity is a category of risk management to address uncertainties across the organization such as general technical threats and risks in its railway applications as well as the human factor, the organizational environment, the organizational processes and so on.

For example, the following threats and risks should be handled.

- Common technical threats and risks for railway system and/or group of railway applications such as network intrusion, data tampering, unintentional encrypted data, disclosure of confidential data, DoS and so forth (organizational threat log and risk register).
- To gather information on known threats generally applicable to railway applications, the threat landscapes published by security associations (e.g. ENISA, IPA (JP), Verizon, etc.) are useful.

These issues below will be input in risk assessment on specific projects described in Clause 7.

- State-sponsored cybersecurity attacks.
- Multiple cybersecurity attacks in railway system and multiple railway applications.
- Unknown vulnerability attacks including zero-day attacks.

These issues below will be related to Operation and Maintenance Management described in Clause 10 for specific railway application.

- Internal violation of organization policy, process and procedure by internal employees, suppliers and stakeholders.
- Sudden outage of supply chain including shared cybersecurity services.
- Miscommunication among railway duty holder and suppliers.
- Fail to perform defined processes in organization and railway applications.

Each organization should identify any threats and risks in the entire organization and decide how to respond (e.g. mitigation, handover, sharing, acceptance, avoidance) and treat them according to risk level. The decision should be recorded in the plan of risk treatment in line with the risk register. The contents of the risk register and the plan of risk treatment should be cascaded down to specific cybersecurity processes and techniques for specific railway applications.

The organization should also maintain and review a threat log and risk register periodically with the latest cybersecurity context and actual cases in other organization and industries as well as the lists of residual risks in specific railway application and solution.

NOTE [ISO 31000:2018 \[16\]](#) Risk management — Guidelines is also an useful reference for managing the cybersecurity aspect of an organization.

## 5.10 [CP-07-01] Business continuity management

### 5.10.1 Requirement

The railway duty holder shall establish, apply and maintain the business continuity management plan addressing disruptions of train operation due to a cybersecurity incident.

This plan shall include a clear, accessible, step-by-step recovery procedure to restore the proper operation of the railway system within a targeted time-frame.

### 5.10.2 Rationale and supplemental guidance

A business continuity management plan should be established to anticipate an efficient and pragmatic action plan to be executed in case of a critical incident taking into account the greatest possible disruption of railway operation. This plan should be established and approved by top management and cybersecurity stakeholders according to a business impact analysis.

In addition, this plan should be coordinated with organizational management processes related to specific railway applications in advance.

For example, the criteria and procedures to launch the redundant second architecture and migration planning are agreed with organization and this should be also communicated from organization level to specific railway application.

Then, the gradual recovery process should be clearly identified, agreed and communicated in entire organization and specific railway application.

Each asset owner should designate a point of contact (adequate people knowing the railway application and available during its operation) to aggregate information on high-critical vulnerabilities and significant cybersecurity incidents. This approach ensures effective communication, thereby minimizing potential impact of disruptions to train services.

Also, business continuity training process should be in business continuity plan and performed including lessons learnt action to improve this process.

A disaster recovery plan should be part of, or linked, to the business continuity plan.

Usually, business continuity management also addresses other aspects such as environmental and dishonest action, natural disaster, physical threats, cybersecurity attacks including DoS attacks. In each railway application level, the recovery management process in asset owner should be consistent with this plan. (see [10.15](#))

The business continuity plan related to cybersecurity should be maintained as reviewed at least annually, and updated when appropriate (e.g. when significant cybersecurity incidents or significant changes to the railway application or risks occur).

NOTE 1 Refer to [IEC 62443-2-1:2024 \[52\]](#) for further guidance

– AVAIL 1.1 to 2.5

NOTE 2 Refer to [IEC 62443-2-4:2023 \[50\]](#) for further guidance

– SP 12.01 - 09 (Backup / Restore)

NOTE 3 Refer to [ISO 22301:2019 \[53\]](#) for further guidance on business continuity management.

## 5.11 [CP-08-01] Data protection management

### 5.11.1 Requirement

The asset owner shall establish, apply and maintain a data management process to protect the railway applications sensitive data throughout the entire life cycle.

This management process shall include:

- a) identification and classification of data with the level of criticality or confidentiality;
- b) identification of ownership for sensitive data



- c) definition of the minimum retention time for the sensitive data;
- d) definition of account to be able to access for each sensitive data;
- e) method and safeguard of protecting sensitive data including encryption key management;
- f) logging of events of generation, transfer/store, use, update and disposal of sensitive data;
- g) incident response procedure in case of disclosure or compromise of sensitive data.

### 5.11.2 **Rationale and supplemental guidance**

Data protection should be thoroughly managed from creation until disposal of the data.

- a) Asset owner should identify all data utilised in their railway system or railway application and identify which data is sensitive with the criticality level of sensitivity. This sensitive data list should be handled with confidentiality.
- b) Asset owner should clearly identify the role responsible for managing sensitive data identified as critical. At the same time, this role should have be responsible for implementing measures, including safeguards and monitoring, to properly protect sensitive data.
- c) Asset owner should manage account to access sensitive data based on its criticality, ensuring adequate access rights through mechanisms such as DAC (Discretionary Access Control), MAC (Mandatory Access Control), and RBAC (Rule-Based Access Control)) throughout the cybersecurity life cycle of railway system and application.
- d) Asset owner should consider the adequate data security measures such as encryption. Asset owner should apply for non-vulnerable secure encryption method (see NIST SP800-175, NESSIE, CRYPTREC and so forth) to each sensitive data. Also encryption key should be strictly managed as one of sensitive data. The best practices of managing encryption keys can be found in NIST SP800-57 and NIST SP800-130. In data disposal phase, asset owner should execute secure sanitizing method defined in [10.17](#) and NIST SP800-8.
- e) Asset owner should collect logs for a duration that is long enough to monitor the status of sensitive data through cybersecurity life cycle. Log should be included in tracking for generation, transfer, store, access (use), update and dispose with who accesses and acts. In addition, Logging data should also be protected for the threats of tampering to keep reliability and the property of nonrepudiation. NIST SP800-92 is reference for log management aspect.
- f) Asset owner should prepare the incident response procedures to limit the impact of railway system and railway application once sensitive data is under disclosure, unauthorised access, unfair tampering and so forth. See [10.14](#) Incident Management is worth using to prepare above.

This management process should be applied to specific railway application and/or solution level by maintenance service provider. (See [10.4](#))

NOTE 1 Refer to [IEC 62443-2-1:2024 \[52\]](#) for further guidance,

- DATA 1.1 (Data classification)
- DATA 1.2 (Data confidentiality)
- DATA 1.4 (Data retention policy)
- EVENT 1.6 (Log access)

NOTE 2 Refer to [IEC 62443-2-4:2023 \[50\]](#) for further guidance

- SP 03.09 - 10 (Architecture)
- SP 07.04 (Remote Access)
- SP 08.02 - 03 (Event Management)
- SP 09.04 (Account Management)

## 6 Cybersecurity within a railway application life cycle

### 6.1 Purpose

Clause 6 provides requirements and guidance for cybersecurity activities to be carried out during the development of a railway solution and its operation and maintenance. It is given within the framework of the life cycle described in IEC FDIS 62278-1:2024 [17], but different life cycles can be applied depending on the SUC.

### 6.2 Railway application and product life cycles

In the IEC 62443 framework, which is the basis of this document, the life cycle of a railway application can be distinguished from the life cycle of products that are integrated into the SUC during the integration phase.

The possibility of integrating industrial products designed, and possibly certified, in accordance with various cybersecurity standards is an important option to ensure flexibility and cost-effectiveness of the SUC.

Thus, product life cycle (see for instance IEC 62443-4-1:2018 [49]) is not in the scope of this document, and therefore no synchronisation points or deliverables are prescribed for the corresponding life cycle phases (6 and 7) of IEC FDIS 62278-1:2024 [17].

Nevertheless, the interface with product suppliers is addressed in CP-05-01.

### 6.3 Manage cybersecurity activities and interfaces

#### 6.3.1 Inputs / Outputs

Outputs:

- Cybersecurity project management assignment [LC-01-01].
- Cybersecurity management plans [LC-02-01].
- Common design review reports [LC-02-01], [LC-03-01].

#### 6.3.2 [LC-01-01] Assign Project Cybersecurity Manager

##### 6.3.2.1 Requirement

The asset owner, the system integrator and the maintenance service provider shall each respectively assign a project cybersecurity manager to be the single point of contact for their respective organizations and to be responsible for the cybersecurity of the delivered or maintained railway solution/application.

The project cybersecurity managers within their respective organizations shall monitor all cybersecurity activities for which they are responsible throughout the entire life cycle.

##### 6.3.2.2 Rationale and additional guidance

The asset owner / system integrator project cybersecurity managers are responsible for developing and maintaining the cybersecurity management plan, ensuring its effective application by monitoring the implementation of the related cybersecurity activities. The maintenance service provider project cybersecurity manager is responsible for developing and maintaining the cybersecurity maintenance plan (this is addressed in 10.3).

Please refer to [Clause H.2.2](#) for a description of competency profiles applicable for a project cybersecurity manager in a railway OT cybersecurity context.

### **6.3.3 [LC-02-01] Plan project cybersecurity activities till the handover**

#### **6.3.3.1 Requirement**

The asset owner and system integrator(s) shall plan and document their cybersecurity activities in their own cybersecurity management plans, by identifying the applicable requirements from Clause 6 to Clause 9 of this document.

The cybersecurity management plans shall define the activities to be carried out during each phase of the applied life cycle. The following aspects shall be defined for each of these activities:

- a) objective;
- b) dependencies on other activities;
- c) assumptions;
- d) deliverables to be produced;
- e) link with the phases of the life cycle used for the railway solution;
- f) people's responsibilities.

The cybersecurity management plans shall consider all cybersecurity activities and deliverables listed in 6.4, applicable to the asset owner or system integrator respectively, till the handover (see Clauses 6 to 9).

#### **6.3.3.2 Rationale and additional guidance**

The cybersecurity management plans should allocate cybersecurity responsibilities. Please refer to [Annex H](#) for competence profiles.

The cybersecurity management plans should incorporate cross-references to other project plans (e.g. project management plan, development plan, configuration management plan, requirement management plan). The cybersecurity management plans should also be referenced in the project management plan or an equivalent document.

After handover, cybersecurity activities are defined in the AO "cybersecurity maintenance plan" (see clause 10.3).

The cybersecurity management plans should be updated when a change or a refinement of the activities to be performed are identified.

#### **Design reviews:**

The SI cybersecurity management plan should include a plan for design reviews, both within the cybersecurity team and between the cybersecurity team and relevant stakeholders, to ensure that:

- a) architectural, design and implementation choices allow specified cybersecurity requirements to be met;
- b) cybersecurity measures are balanced with regard to life cycle cost, safety, operability, reliability, maintainability and performance of the railway solution.

Relevant stakeholders can include not only people from the SI development team (Design, V&V, RAM, Safety) but also representatives of the MSP or AO for topics related to maintenance activities.

The following documents should be included in the design reviews:

- network plan

- system architecture
- cybersecurity architecture

NOTE Life cycle costs include the effort and cost related to both development phases and operation and maintenance phases.

For additional guidance, refer [IEC 62443-2-4:2023 \[50\]](#) Table 4 which provides requirements on the design of the solution.

In the railway sector, the life cycle given in IEC FDIS 62278-1:2024 [\[17\]](#) is typically used, but different life cycles can be used as long as all the cybersecurity activities presented in Table 4 are performed, associated deliverables are produced and mapping between activities and life cycle phases is provided. Examples of mapping of cybersecurity activities to railway solution life cycle are provided in clause [6.4](#).

Informative [Annex G](#), [Clause G.3](#) provides an example of the typical content of a cybersecurity management plan.

### **6.3.4 [LC-02-02] Tailoring the cybersecurity management plan**

#### **6.3.4.1 Requirement**

The asset owner and the system integrator may tailor the cybersecurity activities described in Clauses 6 to 9, subject to asset owner approval (see LC-02-03).

If there are any deviations and derogations with respect to the requirements of this document, they shall be documented and justified in the corresponding cybersecurity management plan.

#### **6.3.4.2 Rationale and additional guidance**

Depending on the project, it is possible to simplify the activities to be carried out.

These simplifications are useful for minor projects, or modification of a component with the same functionality, interfaces and cybersecurity capabilities, minor enhancements with limited cybersecurity impact to an existing railway application. In these cases, it is advantageous not to require formal approval. Also, if the AO organization also takes on the role of SI or maintenance service provider, there is no need for a handover plan.

The justification can be based on a pre-defined zone model, an acceptance of the initial risk assessment or a reference system. In the most complex cases, it is recommended that a security analysis is developed to support these exceptions.

### **6.3.5 [LC-02-03] Cybersecurity management plan approval**

#### **6.3.5.1 Requirement**

The asset owner shall approve the SI cybersecurity management plan.

To this aim, the asset owner shall verify that:

- a) any shared responsibilities have been accepted, and
- b) all the activities from Clause 6 to Clause 9 have been assigned and related requirements have been taken care of, or
- c) records are kept where requirements in these clauses have been derogated or deviated from.

### **6.3.5.2 Rationale and additional guidance**

The AO's approval of the management plan should verify that the plans are complete with respect to the required activities and that the justification of any tailoring is appropriate. It should also take into account that the organizations involved have the process and capability to carry out the activities assigned to them (risk assessment, system design, cybersecurity evaluation, etc.).

### **6.3.6 [LC-02-04] Management of security issues before handover**

#### **6.3.6.1 Requirement**

The SI shall specify and document in the cybersecurity management plan the process for addressing the following cybersecurity management issues related to events that occur prior to the handover of the railway solution:

- a) vulnerability management
- b) patch management
- c) risk management
- d) incident management

#### **6.3.6.2 Rationale and additional guidance**

Cybersecurity needs continuous monitoring (e.g. log checking, anti-malware alarms, intrusion detection). Cyber vulnerabilities could be exploited and incidents could happen during the development and validation of the system and specific activities need to be performed to manage these unpredictable issues. The cybersecurity management plan should define how these aspects should be addressed in organizational (sharing of information, decision process) and technical (impacts on products or design) dimensions.

### **6.3.7 [LC-03-01] Manage product suppliers**

#### **6.3.7.1 Requirement**

In order to ensure the specified cybersecurity capability of the supplied products integrated in the railway solution, the system integrator shall:

- a) establish and document the cybersecurity requirements applicable to supplied products;
- b) use cybersecurity as one of the criteria used to select supplier;
- c) monitor suppliers implementation of cybersecurity requirements;
- d) assess supplier deliveries from the cybersecurity point of view.

#### **6.3.7.2 Rationale and additional guidance**

This requirement correspond to the application during the railway solution development of the processes defined in [CP-05-01] "Supply chain management".

Note that the activity can be different if the supplied product is a COTS (Component-Off-The-Shelf) or a COS (Component-On-Specification).

### **6.3.8 [LC-04-01] Manage interaction with safety and RAM teams**

#### **6.3.8.1 Requirement**

The project cybersecurity management plans shall document the interaction between safety, RAM and cybersecurity teams throughout the development of the railway solution, identifying the synchronization points and the deliverable to be reviewed in each case.

The cybersecurity case shall be communicated to the safety and RAM teams.

### 6.3.8.2 Rational and additional guidance

For a railway application to operate in a safe and dependable 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 environmental factors, and availability of the system. For railway applications, a loss of protection, loss of control or loss of availability would be considered as a loss of essential functions. Since attacks on the system can lead to losses of any of these properties, security countermeasures need to be implemented to provide appropriate protection without a negative effect on these functions.

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 disorder, 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.

Cybersecurity and safety process should be separated as far as possible, while keeping a relevant minimum level of coordination. To decouple the two processes will ensure the necessary stability and viability of safety-related documentation and approval. Otherwise, each change affecting the security of the system could trigger a new safety approval.

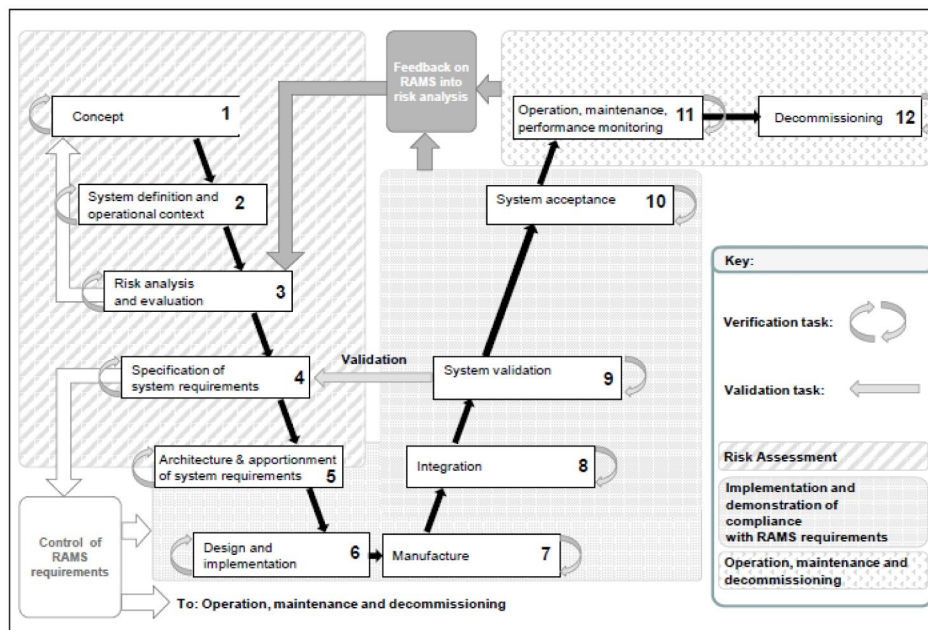
The deliverables to be respectively reviewed and discussed typically include:

- a) From the safety team:
  - 1) safety hazard and associated event
- b) From the cybersecurity team:
  - 1) status of risks impacting safety, from initial risk assessment report and detailed risk assessment report
  - 2) cybersecurity requirement specification
  - 3) cybersecurity case

The cybersecurity case identifies the 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 acceptably achieved.

## 6.4 Cybersecurity activities mapping to the IEC 62278-1 life cycle

Life cycle described in IEC FDIS 62278-1 2024 is reproduced in [Figure 9](#):



**Figure 9 – IEC 62278-1 V-cycle representation**

This subclause describes life cycle phases and provide an overview of:

- Descriptions of the security activities relevant to the life cycle of the SUC.
- Phases required to achieve coordination between the security activities and activities of all the stakeholders, including system engineering, safety, RAM, V&V, Test & Commissioning activities.
- Deliverables (inputs and outputs) to be exchanged, as covered in the relevant detailed clauses.

**Table 4** provides a list of cybersecurity activities to be performed during the railway application life cycle, associated with their main deliverables as described in the Clauses 7, 8, 9, 10.

NOTE 1 A deliverable is defined as a document produced from an activity and communicated to relevant stakeholders, whether internal or external to each organization. This standard addresses other documents not included in this table, such as internal work products or processes.

**Table 4** lists the activities to be performed (column 1) and the corresponding requirements (column 2) defined elsewhere in this document.

Columns 3 and 4 identify the roles involved in each activity. In particular, some cells as marked with an asterisk “\*”. These cells indicate content that is defined based on the agreed-upon responsibility allocation among asset owner, system integrator, maintenance service provider, as documented in their respective cybersecurity management plans (see [LC-02-01]).

For example, there can be cases where the asset owner carries out all initial activities: IRA, DRA and CRS; others where this is done by the SI; or mixed cases where the AO performs only IRA and the system integrator develops DRA and CRS.

Finally, column 5 identifies the corresponding life cycle phases, as defined in IEC FDIS 62278-1:2024 [17].

**Table 4 – Example of mapping of activities, requirements and life cycle phases**

Cybersecurity activities 63452	Requirements	Applicable directly to (AO, SI, MSP)	impact indirectly to (SI, MSP, PS)	LC phase (IEC 62278)
--------------------------------	--------------	--------------------------------------	------------------------------------	----------------------

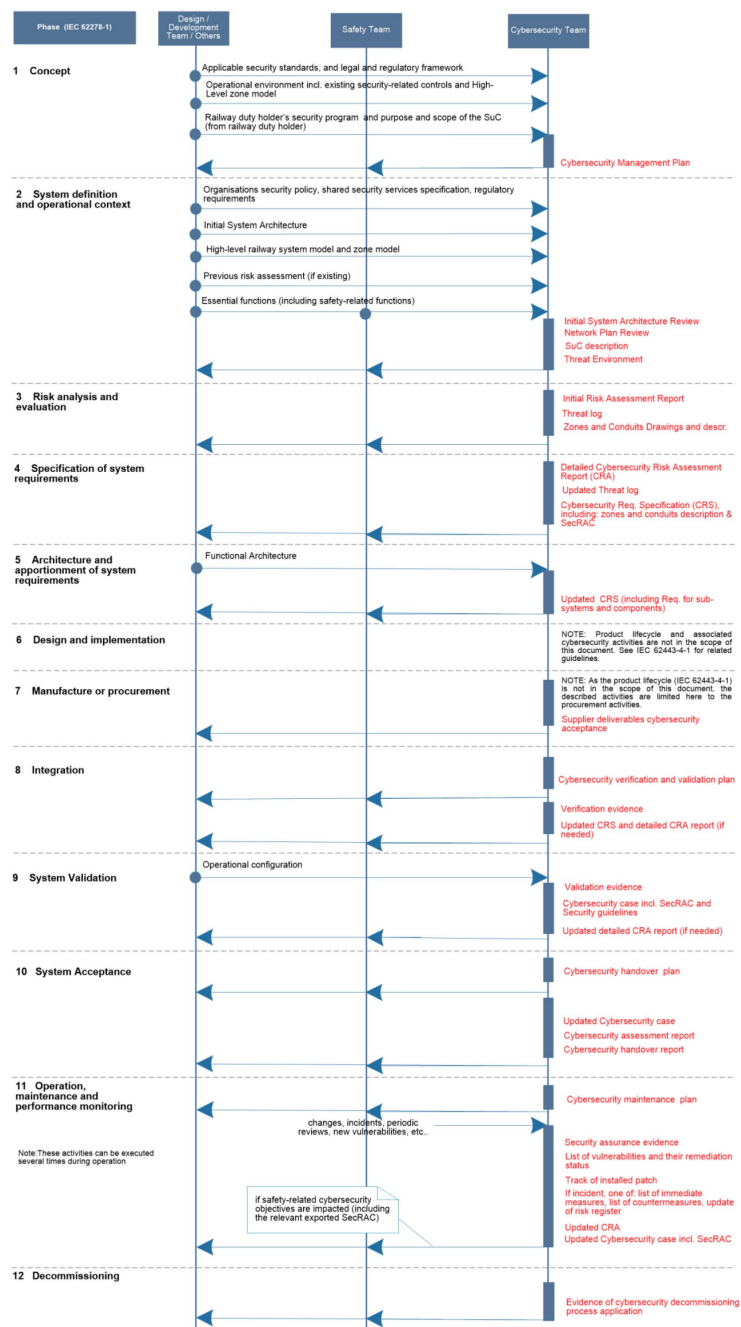
Identify and model the railway system, define shared cybersecurity services	SO-01-01, SO-02-01, SO-03-01, SO-04-01	RDH, AO	-	0
Establish, apply and maintain a railway OT cybersecurity policy	CP-01-01	RDH	-	0
Establish, apply and maintain a railway OT cybersecurity programme	CP-01-02	AO	SI, MSP	0
Establish, apply and maintain management processes related to cybersecurity	CP-02-01 to CP-08-01	AO	SI, MSP	0
Manage cybersecurity activities during railway solution life cycle	LC-01-01 to LC-02-04	AO, SI, MSP	-	1-11
Manage product suppliers	LC-03-01	AO, SI, MSP	SI, MSP, PS	6-11
Manage interaction with safety and RAM teams	LC-04-01	AO, SI, MSP	-	1-11
Identify the SUC, its security context and applicable design constraints	ZR-01-01, ZR-01-02	AO	-	1-5
Perform Initial Risk Assessment (IRA) and define zone and conduits	ZR-02-01, ZR-03-01, ZR-04-01	(*)	-	3, 4
Establish and maintain detailed risk assessment (DRA) and document cyber security requirements (CRS)	ZR-05-01 to ZR-05-11, ZR-06-01	(*)	-	5, 6, 8-11
Approve RA and CRS	ZR-07-01	AO	-	5
Establish cybersecurity architecture and apportion cybersecurity requirements	AA-01-01 to AA-01-04	SI	-	5, 6
Ensure cybersecurity requirement traceability throughout railway solution life cycle	AA-01-05	(*)	-	1-11
Establish and maintain railway solution cybersecurity guidelines	AA-02-01	SI	-	8-11
Define, implement and check rules for establishing cybersecurity configuration	AA-03-01	SI	-	5, 6
Plan cybersecurity evaluation	CA-01-01, CA-01-02	(*)	-	6
Evaluate cybersecurity	CA-01-03, CA-01-04, CA-01-05	(*)	-	6, 8-10
Document cybersecurity case	CA-01-06	(*)	-	10
Plan and perform cybersecurity handover (including approval of cybersecurity case)	CA-02-01, CA-02-02, CA-02-03, CA 02-04	SI, AO	-	10
Plan cybersecurity maintenance and establish cybersecurity rules and procedures	OM-01-01, OM-01-02	AO	-	11
Verify continuously cybersecurity	OM-01-03	AO	-	11
Establish and maintain railway application cybersecurity case	OM-02-01	AO	-	11
Update risk assessment	OM-03-01	AO	-	11



Manage vulnerabilities	OM-04-01, OM-04-02, OM-04-03	AO	SI, MSP, PS	11
Manage patches	OM-05-01, OM-05-02, OM-05-03	AO	SI, MSP, PS	11
Manage incident, backup and recovery	OM-06-01, OM-06-02	AO	SI, MSP, PS	11
Monitor security	OM-07-01	AO	MSP	11
Manage decommissioning of subsystems and components	OM-08-01	AO	MSP	11, 12

Figure 10 provides another informative view of the IEC FDIS 62778-1:2024 [17] phases, with related cybersecurity activities and deliverables as well as their exchange with other stakeholders (e.g. engineering, safety), regardless of whether they belong to asset owner, system integrator or maintenance service provider organization.

NOTE 2 All inputs provided during one phase are assumed to be available for the subsequent phases.



Key:

- Represents the moment when other stakeholders provide input to the cybersecurity team
- Input from other stakeholders to cybersecurity team
- Represents cybersecurity team activities
- Output from cybersecurity team to other stakeholders

**Figure 10 – Synchronization between cybersecurity team and other stakeholders**

## 7 Risk assessment for system design

### 7.1 Purpose and outcome

This clause is an adaptation of the requirements of 62443-3-2 to railways IEC 62443-3-2:2020 [51].

The objective of the clause is to describe the security risk assessment for system design. It is a risk-based approach, where a cybersecurity risk is defined with respect to a threat linked to one or more vulnerabilities that could be exploited by an attacker (see definition for a cybersecurity risk (3.1.125)).

The emphasis in this clause is on essential documents, such as the cybersecurity requirements specification (see ZR-06-01 in 7.8.3) applied to SUC zones and conduits, and those which are required by the overall life cycle (see Clause 6).

### 7.2 Overview

An overview of the structure and content of the clause is provided in Figure 11. This figure describes the risk assessment process to be applied, which is an adaptation of the IEC 62443-3-2:2020 [51]. The references (ZR) relate to the zone and conduit requirements.

Figure 11 illustrates the steps to perform the initial risk assessment and derive a security architecture in zones and conduits. It then describes the detailed risk assessment, which should be performed for each zone and conduit (or cluster of zones and conduits) resulting in the definition of the cybersecurity requirements specification, as the central outcome of this activity.

Several risk assessment methods can be applied to each identified threat:

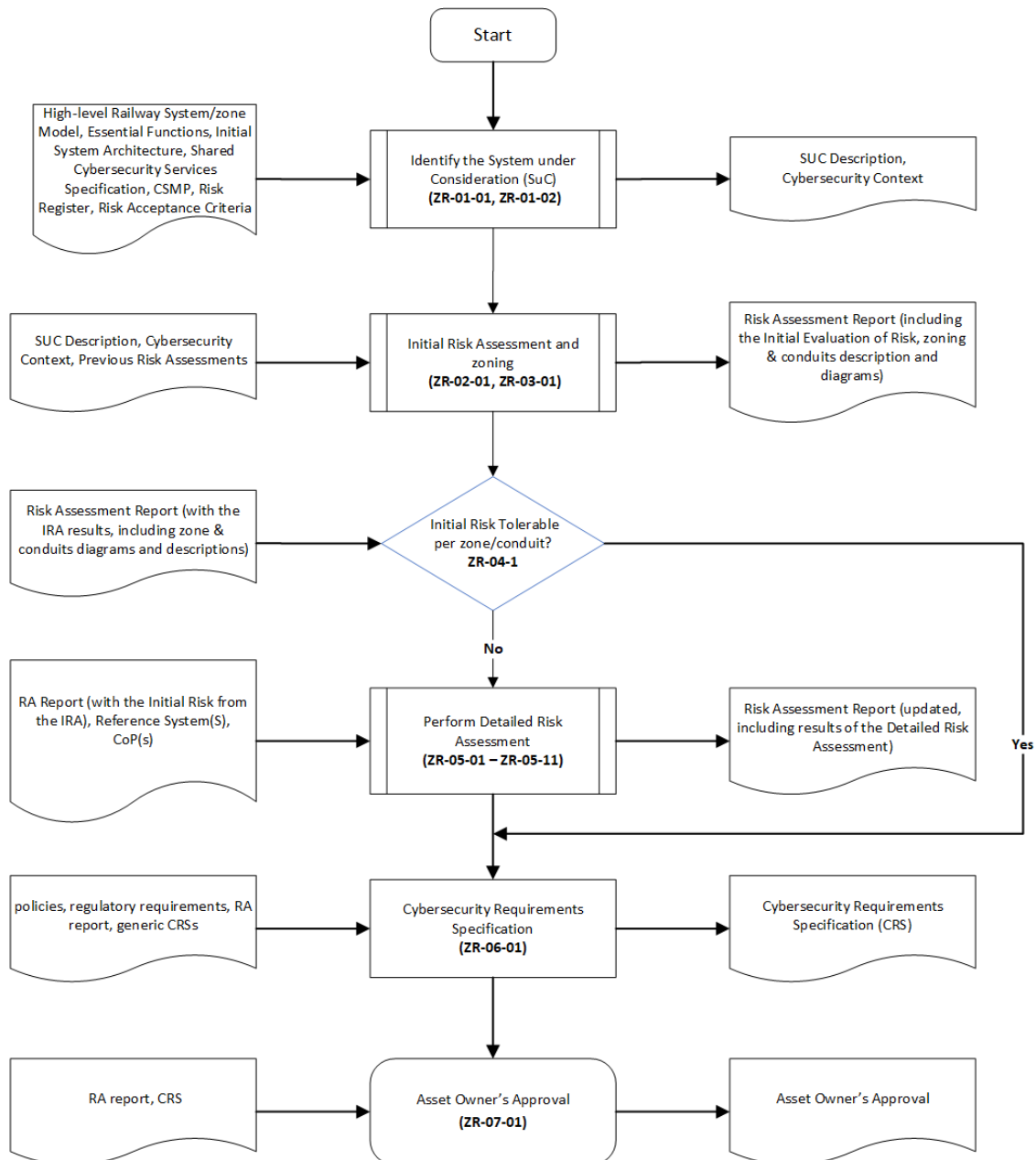
- Either the application of codes of practice (e.g. standard or protection profile), see ZR-05-05 in 7.7.7; or
- The analysis of similarity with reference systems, see ZR-05-06 in 7.7.8; or
- Explicit risk evaluation, see ZR-05-07 to ZR-05-09 in 7.7.9.

It is recommended that the initial risk assessment and the detailed risk assessment are derived from the same framework, standard or source and are using a consistent risk scale to produce consistent and coherent results.

NOTE 1 For each threat, only one risk assessment should be applied, while a set of threats could be treated by the same principle.

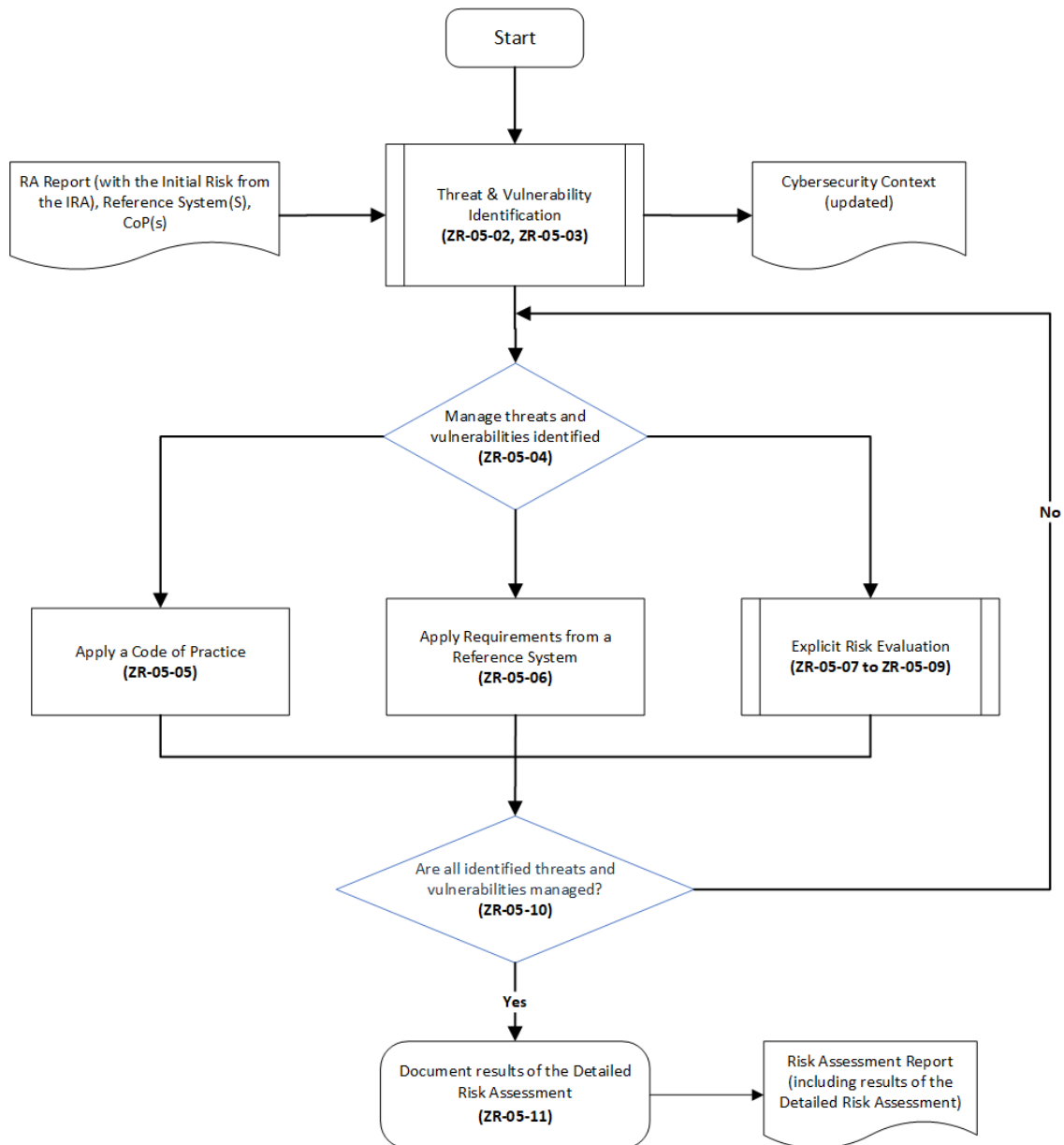
NOTE 2 The whole process as described here is used to determine the cybersecurity requirements, as part of the cybersecurity requirements specification (see Clause 8). These requirements are the outcome of performing a detailed risk assessment. The latter allows us to select either to perform a detailed risk evaluation, to apply a code of practice, or a reference system. This standard does not define any preference or priority regarding the selection of one or more of the three mitigation methods, in order to manage all identified threats and vulnerabilities.

Figure 11 and Figure 12 show an overview of the risk assessment process. Further iterations may be needed, for example in the case where the application of a code of practice does not reduce all risks to an acceptable risk level.



**Figure 11 – Zoning and risk assessment flowchart**

It is acknowledged that the easiest application of the risk assessment process is that 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, a reference system or an explicit risk evaluation; however, for complex systems a mixture of the principles may be necessary.



**Figure 12 – Detailed Risk assessment flowchart**

In case that an explicit risk evaluation is performed, an initial SL-T can be allocated directly as an option, derived from an impact assessment. While preparing the cybersecurity requirements specification, a generic CRS, for example derived from a product line approach, can be re-used.

It is assumed that for railway applications, a detailed risk assessment is almost always necessary. If the outcome from the initial risk assessment is that all risks are sufficiently mitigated without any additional countermeasures, the detailed risk assessment may be skipped.

- For example, in the case where there is very strong physical and organizational protection (see ZCR4.1 of [IEC 62443-3-2:2020 \[51\]](#)).

With respect to physical security, as part of a comprehensive security for railway solutions /applications, the following points are acknowledged:

- Physical security control is considered in the initial risk assessment (but not any technical cybersecurity measures).

- In the detailed risk assessment, a combination of technical solutions, operational policies and procedures, plus physical security solutions are considered to manage identified risks.
- Physical security is also related to SecRACs.

It should be noted that any deviations in the process described are allowed and should be justified by a documented security analysis (see LC-02-01 in 6.3.3).

### 7.3 Identify the SUC and its security context

#### 7.3.1 Description

The 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.

The identification of cybersecurity threats (see ZR-01-02 in 7.3.4 and ZR-05-02 in 7.7.4) requires a description of the SUC, of the functions it provides, and of all its access points.

#### 7.3.2 Inputs / Outputs

Inputs:

- Cybersecurity Management Plan (from LC-01-01 in 6.3.2).
- High-level railway system model (from SO-02-01 in 4.5).
- High-level railway zone model (from SO-03-01 in 4.6).
- Shared cybersecurity services specification (from SO-04-01 in 4.7).
- Initial system architecture (from design/development team).
- Essential functions (from design/development team).
- Relevant information from Risk Register related to the threat environment (from CP-06-01 in 5.9).
- Cybersecurity Risk Acceptance Criteria (from CP-06-01 in 5.9).

Outputs:

- SUC description (ZR-01-01 in 7.3.3).
- Cybersecurity context (including threat environment, cybersecurity risk acceptance criteria, operational environment assumptions) (ZR-01-02 in 7.3.4).

#### 7.3.3 [ZR-01-01] Identify the SUC, its security perimeter and access points

##### 7.3.3.1 Requirement

The asset owner shall identify the SUC, including its essential functions, the demarcation of the security perimeter and the identification of all access points to the SUC.

##### 7.3.3.2 Rationale and supplemental guidance

The security perimeter is understood as the boundary of the SUC. Access points include all points where information can cross the logical boundary of a zone or conduit, such as interfaces. They also include all the places where people can gain physical access to assets of a zone or conduit. Note that protections for physical access points (e.g. enclosures) may already be foreseen and the characteristics of these protections should be documented (e.g. tamper resistance).

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 may be identified by requirements from the system engineering process that are labelled with the appropriate properties, such as those which are safety related.

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 due a successful cybersecurity attack, this usually means a loss of one or more of the main cybersecurity principles:

- Loss of confidentiality;
- Loss of integrity;
- Loss of availability.

NOTE The security functions protect the essential functions.

The functional and architectural description of the SUC should follow the hierarchical approach given in [17] IEC FDIS 62278-1:2024, Railway applications – Specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS process 5.2 considering the SUC perimeter and access points.

The identification of the SUC functions should be detailed by providing information related to:

- The objective (intended purpose) and the mission profile of the SUC comprising the definition of the functions, the SUC perimeter and the access points;
- The operational scenarios, which define how the SUC will be used and which actors are interfering or interfacing with the SUC;
- The context of implementation and use;
- The planned lifetime and therefore possibly necessary system updates in hardware and software;
- Maintenance plans and concepts for the SUC;
- Constraints linked to environment which is integrated the SUC.

Compromising the SUC is possible via access to the SUC (such as through physical or logical access points). Such access points include HMIs and technical interfaces which could enable rogue devices to be added to the system and communication interfaces via a network.

A complete list of the SUC access points should be provided with the definition of the:

- Function for which the access point is used (e.g. maintenance interfaces);
- Protocol for the transmission via networks (if already available);
- Functional data being used;
- Impact (in case of loss of confidentiality, integrity or availability);
- Function of neighbouring systems;
- Organizational interfaces.

The asset owner can be supported by the system integrator to formalize the SUC definition.

This requirement is adapted from IEC 62443-3-2:2020 [51] ZCR1.1.

### **7.3.4 [ZR-01-02] Identify the cybersecurity context**

#### **7.3.4.1 Requirement**

The asset owner shall define the cybersecurity context applicable to the SUC:

- a) Threat environment;
- b) Cybersecurity risk acceptance criteria;
- c) Operational environment assumptions.

#### 7.3.4.2 Rationale and supplemental guidance

Agreement on the threat environment is crucial, as discrepancies in the set of considered threats by different stakeholders may 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 environment. The threat environment should be based on a recognised and accepted threat library, or reports and built with a high-level approach providing an overview of threats applicable to the railway sector.

Asset owners should make use of intelligence reports and other information sources to determine the potential attackers that they might be targeted by.

Threat libraries and reports like the following can be taken as inputs.

- Manufacturer Product CERT advisories.
- MITRE ATT&CK® framework (see [54], [18]).
- CAPEC Common Attack Pattern Enumerations and Classifications (see [19]).
- Open-source intelligence (OSINT)
- National or sector threat report link to OT, IACS or railway applications, such as:
  - ENISA Threat Landscape Yearly report
  - ENISA Transport Threat Landscape
  - BSI Industrial Control System Security: Top 10 threats and countermeasures

Finally, the threat environment should:

- Be defined or at least approved by the railway duty holder; and
- Be updated at least once a year or according to contractual requirements; and
- Provide a mapping to the input threat libraries or reports; and
- Provide rationale for dismissed threats (it should be noted that natural hazards, environmental threats, natural disasters and system failures are out of scope of this threat landscape).

The threat environment, as part of the cybersecurity context, is an important input to the detailed threat identification and is usually documented in a threat log.

For each threat at least the following information should be documented:

- Threat sources;
- Capability or skills or motivation of the threat source;
- Possible threat scenarios and actions;
- Potentially affected assets;
- Vulnerabilities of the SUC (if known).

The threat log, or any document providing the details of the threat environment, should be a live document, maintained and updated during the design phase and whenever needed during the operation phase.

Assumptions often relate to the operational environment or the operational staff. Often the following assumptions can be made in railway applications (which need to be justified by the railway duty holder):



- **Physical access:** System components, such as **Radio Block Center (in trackside)**, **Interlocking**, Embedded devices, safety controllers as well as workstations, are situated within controlled premises, access to which is monitored and denied to unauthorised persons.
- **Installation:** Measures are taken to ensure that the technical system is delivered and installed in a way that does not compromise security.
- **Operators training:** Operators are adequately trained for the tasks assigned to them, to be able to apply the cybersecurity functions used by them correctly and in compliance with the security policy.
- **Operators trusted:** Within the scope of the tasks assigned to them, the operators may be considered to be trustworthy.

## 7.4 Initial Risk Assessment

### 7.4.1 Description

The purpose of the initial risk assessment is to gain an initial understanding of the worst-case unmitigated cybersecurity risk the SUC presents if compromised. This is typically evaluated in terms like impacts to health, safety, environment, business interruption, production loss, product quality, financials, legal or regulatory aspects and reputation. This assessment assists with the prioritization of detailed risk assessments and facilitates the grouping of assets into zones and conduits within the SUC. It adapts ZCR 2 from [IEC 62443-3-2:2020 \[51\]](#) to the railway environment.

### 7.4.2 Inputs / Outputs

Inputs:

- SUC description (from ZR-01-01 in [7.3.3](#)).
- Cybersecurity context (from ZR-01-02 in [7.3.4](#)).
- Previous risk assessments (from ZR-05-11 in [7.7.3](#)), if they exist.

Output:

- Risk assessment report, including the Initial Evaluation of Risk (ZR-02-01 in [7.4.3](#)).

### 7.4.3 [ZR-02-01] Initial risk assessment

#### 7.4.3.1 Requirement

The appointed organization, according to the cybersecurity management plan, shall perform an initial risk assessment on the SUC or confirm that a previous initial risk assessment is still applicable.

The initial risk assessment shall identify the worst-case unmitigated cybersecurity risks that could result from the interference with, breach, disruption of or disablement of the SUC's operation.

#### 7.4.3.2 Rationale and supplemental guidance

The first step of the initial risk assessment is establishing the impact assessment: for each essential function of the SUC, the consequences of losing the integrity, availability or confidentiality should be evaluated considering the worst case scenarios without considering any technical cybersecurity countermeasures in place. The outcome of this process is the initial risk of losing an essential function.

A previous risk assessment, if available, may be used.

[Clause G.4](#) provides an example of the structure of the risk assessment report.

Examples of a qualitative impact assessment are provided in [Annex E](#).

This requirement is adapted from [IEC 62443-3-2:2020 \[51\]](#) ZCR 2.1.

## **7.5 Partitioning of the SUC in zones and conduits**

### **7.5.1 Description**

This section provides a requirement for partitioning the SUC into zones and conduits. Grouping the assets into zones and conduits sharing common security requirements, allows identifying common means of mitigation. It adapts the requirement ZCR 3 from [IEC 62443-3-2:2020 \[51\]](#) to the railway environment.

### **7.5.2 Inputs / Outputs**

Input:

- Risk assessment report(from ZR-02-01 in [7.4.3](#)).

Output:

- Risk assessment report (updated, with zones and conduits descriptions and diagrams, in [7.5.3](#)).

### **7.5.3 [ZR-03-01] Partitioning of the SUC**

#### **7.5.3.1 Requirement**

The appointed organization, according to the cybersecurity management plan, shall establish the zones and conduits of the SUC. The assets shall be grouped to security zones that are connected by conduits, based upon the results of the initial cyber security risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization.

The following rules shall be used for grouping assets to zones:

- a) Business assets are separated from control assets, into different zones;
- b) Safety-related assets are grouped into dedicated zones which are logically or physically separated from zones with non-safety-related assets;
- c) Temporarily connected devices are grouped into separate zones from permanently connected devices;
- d) Wireless connected devices are grouped into separate zones from wired devices;
- e) Devices permitted to make connections to the SUC remotely via external networks are grouped into a separate zone or zones;
- f) Security devices are located at the zone boundary, protecting the zone;
- g) Assets belonging to an OT cloud (e.g. cloud application) are grouped into a separate zone or zones.

Exceptions (e.g. due to architecture constraints) to the above rules shall be justified in the risk assessment report.

#### **7.5.3.2 Rationale and supplemental guidance**

The following criteria should be used to partition the SUC into zones and conduits:

- Risk of the assets, in terms of integrity, availability and confidentiality;
- Type of interface access points or connection to the other parts of the SUC (such as wireless);

- Physical or logical location;
- Access requirements;
- Operational function;
- Organization accountable for each asset;
- Safety aspect;
- Technology life cycle, for example, product life cycle and obsolescence.

In the railway domain, “risk”, “physical location” and “safety aspect” are commonly used criteria to break down the SUC into zones and conduits.

Direct maintenance access from business zones to control zones without control by a security device or similar (such as a proxy server) should not be allowed.

NOTE 1 Examples of operational functions are braking, traction control, doors open/close, train control, diagnostics and maintenance.

External maintenance access, for example, via the internet, should be grouped into a separate zone.

Any exceptions to the rules defined in the requirement should be agreed, for example between the system integrator and the asset owner, at the early stages of the risk assessment.

NOTE 2 Requirements in ZR-03-01 are adapted from [IEC 62443-3-2:2020 \[51\]](#) ZCR 3.1 to ZCR 3.6, and from [IEC 62443-3-3:2013/COR1:2014 \[59\]](#) SR 5.2. Requirements (c), (d), (e) and (f) as well are more restrictive than their [IEC 62443-3-2:2020 \[51\]](#) and [IEC 62443-3-3:2013/COR1:2014 \[59\]](#) counterparts: deviations are possible if justified.

## 7.6 Risk comparison

### 7.6.1 Description

This section provides a requirement for comparing the initial risk on business factors such as on health, safety, environment, business interruption, production loss, product quality, financials, legal or regulatory aspects and reputation, by considering unmitigated worst-case scenarios, when a cybersecurity attack either on confidentiality, integrity or availability of the SUC is successful, with the tolerable risk determined by the Asset Owner. It adapts ZCR 4 from [IEC 62443-3-2:2020 \[51\]](#) to the railway environment.

### 7.6.2 Inputs / Outputs

Inputs:

- Risk assessment report, with the IRA results, including zone & conduits diagrams and descriptions (from ZR-02-01 in [7.4.3](#), and ZR-03-01 in [7.5.3](#)).

Output:

- Risk assessment report (updated) (from ZR-03-01 in [7.6.3](#)).

### 7.6.3 [ZR-04-01] Compare initial risk with tolerable risk

#### 7.6.3.1 Requirement

The appointed organization, according to the cybersecurity management plan, shall compare the initial risk determined in ZR-02-01 (see [7.4.3](#)) to the asset owner's tolerable risk defined for the SUC (see cybersecurity context, including Risk acceptance criteria from ZR-01-02 in [7.3.4](#)). If the initial risk exceeds the tolerable risk, the appointed organization shall perform a detailed risk assessment as defined in ZR-05-01 (see [7.7.3](#)). The results of this comparison shall be documented into the risk assessment report.

### 7.6.3.2 Rationale and supplemental guidance

The purpose of this step is to determine if the initial risk is tolerable. If not, then the mitigations needed should be determined by a detailed risk assessment in the next step of the process.

## 7.7 Detailed Risk Assessment

### 7.7.1 Description

The general procedure for the detailed risk assessment is depicted in [Figure 12](#). It adapts ZCR 5 from [IEC 62443-3-2:2020 \[51\]](#) to the railway environment.

The detailed risk assessment process presented in this clause can be re-used in later life cycle phases.

### 7.7.2 Inputs / Outputs

Inputs:

- Risk assessment report (from (from ZR-04-01 in [7.6.3](#)).
- Reference system(s).
- Code of practice(s).

Output:

- Risk assessment report, updated with the results of the Detailed Risk Assessment (ZR-05-11 in [7.7.11](#)).

### 7.7.3 [ZR-05-01] Perform Detailed Risk Assessment

#### 7.7.3.1 Requirement

The appointed organization, according to the cybersecurity management plan, shall perform a detailed risk assessment on each zone and conduit of the SUC, which are impacted by initial risk exceeding the tolerable risk.

The detailed risk assessment shall implement requirements from ZR-05-02 to ZR-05-11.

#### 7.7.3.2 Rationale and supplemental guidance

Any systematic methodology for the identification, evaluation and management of cyber threats may be implemented if is aligned with the process described in this clause.

In the case where several zones or conduits are similar from a risk perspective, the detailed risk assessment may be performed globally only once on all of them, and the results are to be applied consistently to all considered zones and conduits.

The detailed risk assessment should be reviewed and updated (if necessary):

- At each project life cycle phase by the responsible stakeholder for the SUC;
- When compensating countermeasures need to be evaluated (see [Clause 8](#));
- At regular intervals or whenever triggered (such as when new security threats or vulnerabilities become known), to identify new threats and vulnerabilities of the SUC.

NOTE With respect to threats related to the chosen OT cloud model (IaaS, PaaS, SaaS), the detailed risk assessment should evaluate how to enforce separation at different levels (operating system, network, data storage) to defend against direct attacks and lateral movements. As an example, virtual switches and virtual firewalls should be used to enforce segregation and create virtual conduits and zones within the cloud. See [Annex K](#) for additional guidance.

## 7.7.4 [ZR-05-02] Identify threats

### 7.7.4.1 Requirement

A list of the threats which could affect the assets contained in each zone or conduit shall be established and maintained.

### 7.7.4.2 Rationale and supplemental guidance

It is important to prepare a comprehensive and realistic list of threats to perform a security risk assessment. A threat description should include, but is not limited to, the following:

- Description of the threat source;
- Description of the capability or skill-level of the threat source;
- Description of possible threat vectors;
- Identification of potentially affected asset(s).

NOTE Examples of threat descriptions are:

- Anon-malicious employee physically accesses the signalling zone and plugs a USB memory stick into one of the components.
- Authorized maintenance personnel logically accesses the on-board unit using an infected laptop.
- Anon-malicious employee in a control centre opens a phishing email, compromising their access credentials.
- Commercial software from a product supplier contains an exploitable vulnerability.
- An adversary manages to access a physical cabinet to install rogue equipment to launch a cyber-attack.

The initial threat identification takes place in the form of the identification of the threat environment in phase 2 [Figure 10](#) and is being detailed and checked here, for completeness, considering also threats described in clause 5, CP-06-01 ([5.9.2](#)).

Threat sources can be subdivided in the following categories:

a) Internal actors (staff, contractors, and service providers) including:

Operational staff;

Maintenance staff;

IT and OT engineering staff;

Contractors and service providers;

Suppliers; and

other staff.

b) External actors including:

Cyber terrorists;

Issue-motivated groups;

Former staff and contractors;

Cybercrime groups;

Nation state actors;

Hackers; and

Others, such as passengers with infected devices

Each of the actors have different motivations, be it financial, political or personal, capabilities from using simple tools to development of novel malware and freedom of action. The choice of considered actors depends on the context of the application and is documented by the entity executing the detailed risk assessment.

Due to the high number of possible combinations, the following items may be classified into adequate qualitative classes:

- Cyber capability/skills and resources;
- Interest/motivation of each attacker;
- Knowledge of target;
- Vulnerability of the SUC (if known); and
- Risk.

The requirement is adapted from [IEC 62443-3-2:2020 \[51\]](#) ZCR 5.1.

## **7.7.5 [ZR-05-03] Identify vulnerabilities**

### **7.7.5.1 Requirement**

Analysis shall be performed on each zone or conduit to identify and document known vulnerabilities associated with the assets contained within them, including their associated access points.

### **7.7.5.2 Rationale and supplemental guidance**

In order for a threat to materialise, it is necessary to exploit one or more vulnerabilities in the SUC. Therefore, it is necessary to identify known vulnerabilities associated with the assets to better understand threat vectors. A generally accepted approach to identifying vulnerabilities in an SUC is to perform a vulnerability assessment. This activity needs concise identification of the assets of the zone or conduit as well as their hardware and software elements, such as operating systems.

NOTE 1 There are several types of vulnerabilities, such as exploitable vulnerabilities ([exploitable vulnerability \(3.1.56\)](#)) or actively exploited vulnerabilities ([actively exploited vulnerability \(3.1.9\)](#)).

Vulnerabilities may generally be grouped into several categories that should be covered, such as:

- Device vulnerabilities (hardware, firmware, operating system);
- Software applications vulnerabilities;
- Network vulnerabilities;
- Organizational vulnerabilities, for example, by deviations from organizational security policy;
- System vulnerabilities, for example, across different devices or zones and conduits.

The evolution of IT and OT may lead to new identified vulnerabilities being exploitable by an attacker.

- Growth of networked systems offering a larger attack surface with new attack vectors.
- Digitalisation of railway assets.

This requirement is adapted from [IEC 62443-3-2:2020 \[51\]](#) ZCR 5.2.

NOTE 2 Known device vulnerabilities can be extracted from appropriate vulnerability databases, such as the US National Vulnerability Database (NVD) available on the NIST website, including their criticality classification by the product supplier.

NOTE 3 For new designs, for example hardware or software, specific vulnerabilities may not be known, therefore analysis may be restricted to threats or generic vulnerabilities.

## **7.7.6 [ZR-05-04] Manage identified threats and vulnerabilities**

### **7.7.6.1 Requirement**

All identified threats and vulnerabilities shall be addressed, either by:

- a) Using a code of practice (see 7.7.7), or
- b) Using a reference system (see 7.7.8), or
- c) Performing an explicit risk evaluation (see 7.7.9).

### **7.7.6.2 Rationale and supplemental guidance**

Threats identified in ZR-05-02 and in ZR-05-03 should be managed by defining appropriate countermeasures. The latter could be derived either by applying a valid, acceptable and justified code of practice, or by applying requirements from a reference system similar to the SUC, or as the result of an explicit risk evaluation. There is no priority among these three options.

## **7.7.7 [ZR-05-05] Apply a code of practice**

### **7.7.7.1 Requirement**

In the application of a code of practice to mitigate a set of threats, the following points shall be fulfilled and documented:

- a) The code of practice is widely recognised, technically valid, lists the threats it addresses and provides justification for mitigation;
- b) The code of practice is relevant to the SUC's selected threats;
- c) The application of the code of practice is justified and documented in the risk assessment report.

Any deviations shall be justified and remaining risks shall be covered by either the use of a reference system or by performing an explicit risk evaluation.

### **7.7.7.2 Rationale and supplemental guidance**

The cybersecurity field is a rapidly changing environment, and a cybersecurity code of practice can become technically obsolete. Before its application, it is important to check whether a code of practice is still valid according to the current cybersecurity state-of-the-art.

Laws, regulations or standards can be consulted along with internal codes of practice, such as protection profiles. Requirement specifications are an important source of codes of practice.

- IEC 62280:2014 [58] is used in railways signalling as a code of practice to cope with threats related to safety-related communication.
- ANSSI Protection Profiles [20].

The criteria for the applicability of codes of practice should be re-evaluated at the update of the detailed risk assessment.

NOTE A code of practice can rule out a set of threats, and different codes of practices can be applied to different set of threats.

## **7.7.8 [ZR-05-06] Application requirements from a reference system**

### **7.7.8.1 Requirement**

In the application of a reference system, the following points shall be fulfilled and documented:

- a) It is demonstrated that the reference system addresses the risk associated to a set of identified threats to a tolerable level. This demonstration is valid at the time of application;
- b) The reference system functions and interfaces are similar to the SUC;
- c) The operating environment and environmental conditions are similar;
- d) The reference system has a cybersecurity requirement specification, if not, the security requirements shall be collected from the documentation of the reference system and checked for correctness and completeness;
- e) All selected threats are considered to be effectively treated by the reference system;
- f) The application of requirements from a reference system is justified and documented in the risk assessment report.

Any deviations shall be justified and remaining risks shall be covered by either the use of a code of practice or by performing an explicit risk evaluation.

### 7.7.8.2 Rationale and supplemental guidance

If no relevant code of practice exists for a threat or set of threats, comparison with a reference system can help to determine requirements for which the risk can be tolerable.

On the other hand, requirements from a reference system may be applied directly to mitigate identified threats and vulnerabilities, as there is no priority defined for the three options of a detailed risk assessment.

The documentation of a reference system should include the following elements:

- System description, including the system architecture and the zoning model.
- Security context, including the list of threats and vulnerabilities.
- Operating environment conditions.
- List of countermeasures against identified threats and vulnerabilities, including countermeasures evaluation and threat coverage.
- A cybersecurity requirements specification

**EXAMPLE** Security gateways (see [Clause B.4.11](#)) are used to couple operational control centres and sub-centres. If similar coupling is to be used in a different application, then relevant cybersecurity requirements can be determined and be re-used (with respect similar functions, interfaces as well as to operating and environmental conditions).

The cybersecurity field is a rapidly changing environment, and a reference system can become technically obsolete. Before its application, it is important to check whether the risk implied by use of a reference system is still acceptable.

**NOTE** Security requirements from a reference system can cover more than a single threat and multiple reference systems may be applied to different sets of threats.

## 7.7.9 Explicit Risk Evaluation [ZR-05-07, ZR-05-08, ZR-05-09]

### 7.7.9.1 Description

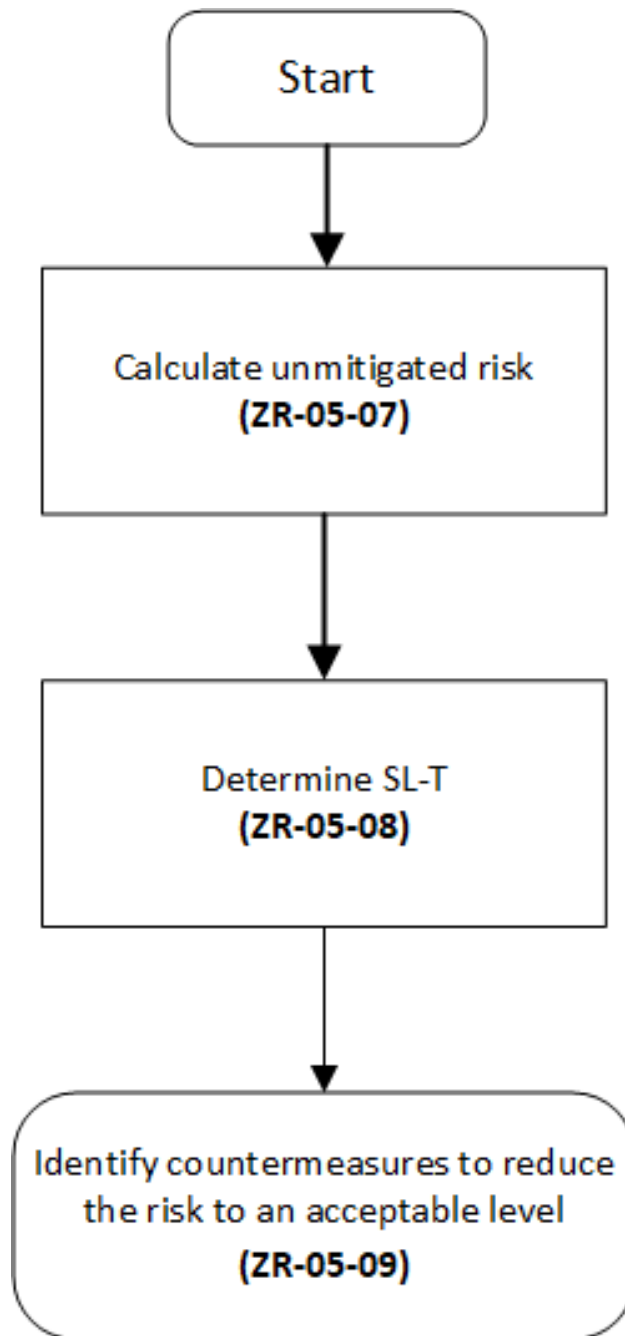
The explicit risk evaluation is one the three mitigation methods of the detailed risk assessment process, to manage identified threats and vulnerabilities.

The basic procedure can use an initial SL-T value as a starting point (see [Figure 13](#)), which may be determined based on experience or on the attacker's profile.

As it is infeasible to quantify cybersecurity risks, all risk acceptance criteria, as part of cybersecurity context, are understood and applied in a qualitative or semi-quantitative manner.



Figure 13 presents the flowchart for an explicit risk evaluation. Initially, the unmitigated risk is calculated and the target security level (SL-T) is determined. Following that, countermeasures are identified to reduce the risk to an acceptable risk level.



**Figure 13 – Explicit Risk Evaluation flowchart**

NOTE The requirement is adapted from IEC 62443-3-2:2020 [51] ZCR 5.1-5.13.

#### **7.7.9.2 [ZR-05-07] Explicit Risk Evaluation - Calculate unmitigated risk**

##### **7.7.9.2.1 Requirement**

The unmitigated cybersecurity risk for each threat shall be determined by combining the unmitigated impact and the unmitigated likelihood.

### 7.7.9.2.2 Rationale and supplemental guidance

The unmitigated cybersecurity risk is usually determined using a risk matrix that combines the worst case impact if the threat, linked to an attack scenario, is realized, with the unmitigated likelihood of this scenario to be successful. In this approach, any technical cybersecurity countermeasures in place should not be considered, while other countermeasures such as physical security or operational cybersecurity policies and procedures should be taken into account. Examples of using a risk matrix can be found in [Annex E](#).

### 7.7.9.3 [ZR-05-08] Explicit Risk Evaluation - Determine SL-T

#### 7.7.9.3.1 Requirement

An SL-T shall be established for each security zone and conduit of the SUC, considering the unmitigated cyber security risk for each threat.

#### 7.7.9.3.2 Rationale and supplemental guidance

In [IEC 62443-3-2:2020 \[51\]](#) ZCR 5.6, different approaches for the derivation of SL-T, according to [IEC 62443-3-3:2013/COR1:2014 \[59\]](#), are described. The first approach is based on a more informal interpretation of a security level definition in Annex A.3.2 which is directly derived on the need of protection against a particular kind of attacker, for example a hacker, criminal organization or 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, considering the identified threats and vulnerabilities (see ZR-05-02 in [7.7.4](#) and ZR-05-03 in [7.7.5](#)) and regulatory constraints, resulting directly in an SL-T.

EXAMPLE 1 An asset owner 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 [IEC 62443-3-2:2020 \[51\]](#)) and this would be the overall requirement.

The second approach, which is directly motivated by the SL definition in [security level \(3.1.150\)](#), is based on the difference between unmitigated cybersecurity risk (as derived in ZR-02-01 (see [7.4.3](#)) as a basis for the zoning) and the tolerable risk (as defined in a risk matrix like in the examples of [Annex E](#)). It is described in this clause in detail. As a precondition, the zones and conduits to be assessed by a detailed risk evaluation should have reached a certain level of maturity of the architecture and its planned implementation understood. The detailed risk evaluation described here is proactive, for example it is not triggered by an incident or vulnerability (see [Clause 10](#)).

NOTE 1 In general SL-T is a vector consisting of the partial security levels for the different foundational requirements (see [IEC 62443-3-2:2020 \[51\]](#) for more detail).

As a starting point, an initial SL vector for a zone or conduit can be chosen. This can be based on the initial risk assessment, directly on the type of threats assumed or on particular approaches considering railway specific parameters like the location from which the attack can be launched or traceability or by considering confidentiality, integrity and availability security objectives.

Although [IEC 62443-3-3:2013/COR1:2014 \[59\]](#) allows a value of '0' for a certain foundational requirement (FR) of a zone/conduit, it is proposed as a starting point to take SL1 = (1,1,1,1,1,1,1), the vector of the individual foundational requirements, which should be fulfilled and can be used as a general starting point if no additional information is available and it may be updated incrementally when new requirements from the IEC 62443-3-3 are chosen.

EXAMPLE 2 Assuming that for all integrity aspects a high protection is needed, while availability and confidentiality need less protection, this might lead to SL= (3,3,3,1,3,3,2).

NOTE 2 The final SL-T does not depend on the starting point. It is recommended to start rather with a low initial SL than an SL which is too high to ensure that adequate requirements are derived by the procedure described here.

The requirement is adapted from ZCR 5.6 in [IEC 62443-3-2:2020 \[51\]](#).

#### **7.7.9.4 [ZR-05-09] Explicit Risk Evaluation - Identify countermeasures to reduce the risk to a tolerable level**

##### **7.7.9.4.1 Requirement**

Cybersecurity countermeasures such as technical, administrative or procedural shall be identified to address all threats and vulnerabilities where the risk exceeds the tolerable risk, unless a documented decision was made by the asset owner to accept, avoid, or transfer the risk.

For each threat identified, the likelihood and impact shall be re-evaluated, considering the countermeasures and their effectiveness to mitigate the threat. The risk shall be determined by combining the re-evaluated likelihood and impact.

##### **7.7.9.4.2 Rationale and supplemental guidance**

Existing countermeasures of the SUC should be evaluated to identify at which level they effectively reduce the likelihood or impact of the considered threats. In case of remaining unacceptable risk, additional countermeasures would need to be selected. [IEC 62443-3-2:2013/COR1:2014 \[59\]](#) can be used as a guide for selecting technical countermeasures, in which case the SL-T should be taken into account. Depending on the approach chosen for determining the SL-T, the latter may also be updated to reflect the countermeasures that have been selected. Alternatively, when applicable, a protection profile, a code of practice, or the [IEC 62443-4-2:2019 \[21\]](#) could also be relevant to identify countermeasures.

Non-technical countermeasures, such as administrative or procedural controls may also be necessary to address all the risks. Such countermeasures are typically captured as SecRACs.

NOTE 1 Addressing the risk does not always require selecting countermeasures. For example it may also be possible to reassign a component to a different zone that is better protected. Similarly, it may be possible to disable interfaces or features that are not strictly necessary.

Examples of risk evaluation methods are provided in [Annex E](#). It is recommended that the same risk acceptance criteria applied to the initial risk assessment will be also applied to the detailed risk assessment, and thus to the explicit risk evaluation.

NOTE 2 An assessment of the likelihood of a threat manifesting is particularly challenging and differs from traditional assessment of environmental hazards as there can be little historical evidence to predict a threat and no current evidence of such a threat developing within a control system. For this reason, some risk assessment methodologies assume all threats are manifest and assess the impacts rather than likelihood.

Residual risks that exceed the tolerable risk should be analysed for the related threats and the reason why they cannot be reduced should be provided.

EXAMPLE A typical risk matrix is known from [ISO/IEC 27005:2022 \[32\]](#). Details of how to construct the risk matrix following this approach are given in [Clause E.5](#). For each threat, the assessment would lead to the assignment of a semi quantitative risk score on a scale of 0 to 8. Often, a colour code is used to group the results into different categories, such as:

- 0-2 risk is tolerable;
- 3-5 risk is only tolerable if no additional countermeasures exist or if additional countermeasures are not proportionate;
- 6-8 risk is not tolerable.

For threats with a score of 0-2 or low risk no additional measures are necessary

For those that have a score between 3 and 5 or a medium risk, additional countermeasures need to be discussed considering the proportionality principle.

If there exist threats with a score of 6 to 8, or the risk is at least significant, then usually additional countermeasures need to be defined.

Examples of risk matrices are provided in [Annex E](#).

The requirement is adapted from [IEC 62443-3-2:2020 \[51\]](#) ZCR 5.8 and ZCR-5.12.

### **7.7.10 [ZR-05-10] Threats coverage and risk acceptance**

#### **7.7.10.1 Requirement**

Coverage of all identified threats shall be checked considering that any risk is either mitigated, accepted, avoided or transferred.

#### **7.7.10.2 Rationale and supplemental guidance**

It should be demonstrated that threats of the SUC threat landscape are covered by either codes of practice, references systems or an explicit risk assessment.

In case that there are still threats or vulnerabilities not managed, one or more mitigation methods (a code of practice, a reference system, or an explicit risk evaluation) should be followed to mitigate risks identified.

NOTE If a risk is less or equal to the tolerable risk level then it should be accepted by default.

If a risk is greater than the tolerable risk level then a decision should be taken by the asset owner whether it would be accepted, avoided (e.g. function removed), transferred (e.g. insurance policy subscription) or mitigated (e.g. addition of additional compensating countermeasure).

### **7.7.11 [ZR-05-11] Document results of the Detailed Risk Assessment**

#### **7.7.11.1 Requirement**

The results of the detailed risk assessment shall be documented and made available to the appropriate stakeholders, in the risk assessment report.

The risk assessment report shall include:

- a) Rationale for selection and applicability of a code of practice (if selected), as well as threat coverage achieved, with respect to the sub-set of the SUC considered;
- b) Rationale for selection and applicability of a reference system (if selected), as well as threat coverage achieved, with respect to the sub-set of the SUC considered;
- c) Explicit risk evaluation results and methodology (if performed);
- d) Any assumptions made (to be exported as SecRACs).

Furthermore, the following elements shall be documented:

- e) Operating environmental assumptions;
- f) Risk acceptance criteria;
- g) Threat environment;
- h) List of vulnerabilities;
- i) Unmitigated risks;
- j) List of countermeasures (including SecRACs);
- k) Residual risk and their status (avoided, accepted or transferred).

#### **7.7.11.2 Rationale and supplemental guidance**

The risk assessment report can be used for multiple purposes including testing, auditing and future risk assessments.

It is important to protect the information in the report, as it often contains sensitive details about the systems, known vulnerabilities and existing countermeasures. The risk assessment documentation typically contains sensitive information which should be protected accordingly (see CP-08-01 in 5.11).

## 7.8 Document cyber security requirements

### 7.8.1 Description

This section adapts ZCR 6 from IEC 62443-3-2:2020 [51] to the railway environment to document cyber security requirements as needed to achieve the security of the SUC.

### 7.8.2 Inputs / Outputs

Inputs:

- Cybersecurity policy (from CP-01-01 in 5.3) and OT cybersecurity programme (CP-02-01 in 5.4).
- Regulatory requirements (from legal team, tender requirements or contract).
- Generic cybersecurity requirement specifications (if existing).
- Risk assessment report (from ZR-05-11 in 7.7.11).

Output:

- Cybersecurity requirements specification (ZR-06-01 in 7.8.3).

### 7.8.3 [ZR-06-01] Cybersecurity requirements specification

#### 7.8.3.1 Requirement

The appointed organization, according to the cybersecurity management plan, shall document all cybersecurity requirements results from the risk assessment in the cybersecurity requirements specification.

The CRS shall include or refer to the following:

- a) The SUC description (see ZR-01-01 in 7.3.3).
- b) Zone and conduit drawings (see ZR-03-01 in 7.5.3).
- c) Zone and conduit characteristics (see ZR-03-01 in 7.5.3), with their associated requirements:
  - 1) Security requirements based on the risk assessment report (see ZR-05-11 in 7.7.11)
  - 2) SL-T, if applicable (see ZR-05-08 in 7.7.9.3)
  - 3) Assumptions (see ZR-05-11 in 7.7.11)
  - 4) Security-related application conditions (SecRACs) (see ZR-05-11 in 7.7.11)
- d) Operating environment assumptions (see ZR-05-11 in 7.7.11).
- e) The threat environment (see ZR-01-02 in 7.3.4).
- f) Tolerable Risk (see ZR-04-01 in 7.6.3).
- g) Regulatory requirements ((from legal team, tender requirements or contract).

Cybersecurity requirements and SecRACs shall be communicated to all the stakeholders of the SUC, which includes engineering, RAM, the safety team and the asset owner.

Appropriate information security classification shall be assigned to protect the confidentiality of the documentation. Documentation that was instrumental in performing the cyber risk assessment shall be recorded and archived along with the cyber risk assessment.

### 7.8.3.2 Rationale and supplemental guidance

The final step of the risk assessment is to collect the cybersecurity requirements for the SUC, including all zones or conduits related to all threats or vulnerabilities from the different sources such as:

- Requirements stated by used codes of practice, for threats covered by this principle.
- Requirements from the CRS of the applicable reference systems, for threats covered by this principle.
- Requirements derived during the explicit risk evaluation.
- System security requirements that have been incorporated in the CRS from diverse sources including [IEC 62443-3-3:2013/COR1:2014 \[59\]](#) should be applied taking into account railway specific context. Refer [Annex C](#) and [Table C.1](#).

The SUC description should include:

- the scope, the interfaces, and the boundary of the SUC;
- the name, high-level description of all functions (including the essential functions) and the intended usage of the SUC;
- the assets supporting the essential functions.

During the detailed risk assessment, the SUC description (ZR-01-01) should be completed to achieve a detailed description of all assets (reference and version).

The operating environment assumptions should document the physical and logical environment of the SUC:

- The physical environment for the SUC should be documented in order to ensure the railway application assets are properly protected. Examples of documentation that can be used to communicate the physical environment would be maps, plans, wiring schematics, connector configurations and site security plans.
- The logical environment for the SUC also should be documented to provide a clear understanding of the networks, information technology, protocols and other systems that interface with the SUC. Examples of relevant documentation would be network architecture diagrams, system architecture diagrams, wiring diagrams (electric schemas), heating, ventilation and air conditioning (HVAC), fire detection and suppression, and other relevant design documents.

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

- Type (zone or conduit), name or unique identifier or both;
- Definition of the logical boundary;
- Definition of the physical boundary, if applicable;
- Safety designation;
- List of all logical access points;
- List of all physical access points, if applicable;
- List of data flows associated with each access point;
- Connected zones or conduits;
- List of assets and their risk classification and business value.

[IEC 62443-3-2:2020 \[51\]](#) contains more detailed information on the contents of the CRS.

## 7.9 Asset owner's approval

### 7.9.1 Description

This section adapts ZCR 7 from IEC 62443-3-2:2020 to the railway environment to attain the asset owner's approval on the risk assessment report.

### 7.9.2 Inputs / Outputs

Inputs:

- Risk assessment report (from ZR-05-11 in [7.7.11](#)).
- Cybersecurity requirements specification (from ZR-06-01 in [7.8.3](#)).

Output:

- Asset owner's approval (ZR-07-01 in [7.9.3](#)).

### 7.9.3 [ZR-07-01] Asset owner's approval

#### 7.9.3.1 Requirement

The asset owner shall review and approve the risk assessment report and the CRS.

#### 7.9.3.2 Rationale and supplemental guidance

While system integrators have the system knowledge required to perform the risk assessment, they typically do not have the authority to make decisions to accept risk. Therefore, the results of the assessment, as well as the resulting CRS, are presented to the asset owner which has the authority to make such decisions.

## 8 Cybersecurity architecture, integration and configuration

### 8.1 Purpose

The objective of this clause is to define the SUC's cybersecurity functional architecture, the apportionment of system cybersecurity requirements to subsystems and components, and to address system integration and configuration requirements.

### 8.2 Inputs / Outputs

Inputs:

- Cybersecurity requirements specification (CRS).

Outputs:

- Defined SUC functional cybersecurity architecture.
- Cybersecurity requirements apportioned to each zone, conduit and subsystems within the SUC.
- SUC cybersecurity integration.
- SUC cybersecurity parameters and configuration management system.
- Cybersecurity guidelines for the railway solution

### 8.3 SUC cybersecurity functional architecture

#### 8.3.1 [AA-01-01] Cybersecurity Architecture

##### 8.3.1.1 Requirement

The organization in charge of the SUC integration (in conformity with cybersecurity management plan) shall devise a cybersecurity architecture that implements the functions necessary to meet the requirements defined in the CRS.

##### 8.3.1.2 Rationale and supplemental guidance

While addressing the CRS requirements allocated to the SUC for which it is responsible, the organization in charge of the SUC integration (in conformity with cybersecurity management plan) should consider the following aspects:

##### Functional architecture

The activity described in [SO-02-01] 4.5 identifies and groups high level railway functions. Within the SUC allocated to a given system integrator, the proposed architectural implementation of the cybersecurity requirements and/or SL-T from the CRS should consider the availability and maturity of cybersecurity functions.

##### Integration with shared security services

When SL-T is defined, implementing the requirements can require shared security services.

These security services could be shared by the railway system, as described in [SO-04-01] 4.7. The cybersecurity architecture proposed should either include (host), make provisions to relay or allow its subsystems to access them (if based outside the SUC).

##### Consideration of total life cost of the solution proposed

The technical solutions may have many implications on cost, time scale and long term viability of the railway solution. The proposed cybersecurity architecture should consider how it could affect the design, manufacturing, acceptance of the railway solution, and operation and maintenance of the railway application. These costs may include, but are not limited to:

- possible re-certifications of safety related subsystems due to cybersecurity updates;
- recurrent licencing of proprietary software;
- establishment of specialised technical teams to operate and maintain the architecture;
- obsolescence.

The cybersecurity architecture should be reviewed and approved by the asset owner.

#### 8.3.2 [AA-01-02] Cybersecurity shall not adversely impact essential functions

##### 8.3.2.1 Requirement

The potential impact of the implementation of cybersecurity requirements on essential functions shall be assessed and documented by the system integrator for acceptance by the asset owner.

##### 8.3.2.2 Rationale and supplemental guidance

The railway sector has a strong tradition and record of regulation and practices for safety that embraces [essential functions](#) (3.1.55). Additional guidance is given in [Clause D.4](#)

NOTE See [IEC 62443-3-3:2013/COR1:2014](#) [59] 4.2 for more information.



### 8.3.3 [AA-01-03] Requirements apportionment to subsystems

#### 8.3.3.1 Requirement

The system integrator, in conformity with the cybersecurity management plan, shall apportion cybersecurity requirements identified during risk assessment as requirements at subsystem and component level.

#### 8.3.3.2 Rationale and supplemental guidance

The high-level cybersecurity requirements detailed in [ZR-06-01] 7.8.3 can have specific applicability according to their characteristic, such as:

- Host requirements (allocation of computer resources, call stack).
- Application requirement (allocated on different device types like mobile/embedded/networks/cloud).
- Interface properties (robustness, parameter range checks, buffer principles).
- Additional security function integrated (to enforce rule and policies).

For each subsystem in the SUC it should be clearly stated which of the security requirements are applicable to that subsystem.

In apportioning subsystem requirements, the security architecture within a zone should be considered. The harmonisation of the dedicated security design within the zone and the functionality itself should also be addressed. As an example, complex functionality between different zones should be avoided as much as possible. This should only be considered if clear segregated sub-functionalities with loose coupling characteristics exist for such a function.

When needed, network related cybersecurity requirements may also be implemented and allocated for zone protection, for example:

- a) for security of the zone: dedicated gateways for the control of the communication load in a bidirectional way, or usage of data diodes for ensuring unidirectional data-flows;
- b) monitoring and logging capabilities to support anomaly detection can be on a centralized server with a system for incident and event detection;
- c) support of a unique system time for logging to make the zone monitoring consistent from a time perspective.

System security requirements that have been incorporated in the CRS from diverse sources, including IEC 62443-3-3:2013/COR1:2014 [59], should be applied taking into account the railway specific context. The normative system security requirements, set out in IEC 62443-3-3:2013/COR1:2014 [59] underpinning the seven foundational requirements classes, are applicable to railway applications according to the requisite security levels (SL-T) apportioned for the zones and conduits in the SUC and depicted in Table C.1.

The seven foundational security requirements are set out in IEC/TS 62443-1-1:2009 [7]. These are applicable and depicted in Table 5.

**Table 5 – Security Foundational Requirements**

<u>Foundational Requirement</u>	<u>Title</u>
<b>FR 1</b>	<b><u>Identification and authentication control (IAC)</u></b>
<b>FR 2</b>	<b><u>Use control (UC)</u></b>
<b>FR 3</b>	<b><u>System integrity (SI)</u></b>
<b>FR 4</b>	<b><u>Data confidentiality (DC)</u></b>

<b>FR 5</b>	<b><u>Restricted data flow (RDF)</u></b>
<b>FR 6</b>	<b><u>Timely response to events (TRE)</u></b>
<b>FR 7</b>	<b><u>Resource availability (RA)</u></b>

### **8.3.4 [AA-01-04] Inclusion of compensating countermeasures**

#### **8.3.4.1 Requirement**

If a subsystem or component of the SUC does not meet the apportioned security requirements, the organization in charge of the SUC integration (in conformity with the cybersecurity management plan) shall define compensating countermeasures and reassess the risk as described in ZR-05-09. Fulfilment of compensating countermeasures and SecRACs shall be demonstrated to meet the same security objective intended by the original requirements and shall be documented in a new version of the CRS. If needed, the requirement apportionment to subsystem and component shall be updated accordingly.

#### **8.3.4.2 Rationale and supplemental guidance**

Compensating countermeasures are required in cases where the security level inherently provided by a specific zone or component does not fulfill the security requirements defined in the CRS. This inherent security level and the SL-C state what security level can be provided intrinsically without compensating countermeasures when properly configured and integrated.

The need for compensating countermeasures may arise due to technical or resource limitations, such as contradictory requirements from system engineering with higher priority. Compensating countermeasures should be related to cybersecurity requirements and are therefore traceable to them.

### **8.3.5 [AA-01-05] Cybersecurity requirement traceability**

#### **8.3.5.1 Requirement**

The system integrator shall ensure that cybersecurity requirements are systematically identified and have complete and correct traceability throughout the railway solution development life cycle up to the handover.

#### **8.3.5.2 Rationale and supplemental guidance**

To facilitate test cases, which are specified at a different level of requirements for verification purposes (see [Clause 9](#)), it is essential that the cybersecurity requirements are verifiable and traceable, especially in the railway domain, where the majority of the functionality relates to distributed components.

Traceability is not just between requirements, implementation and testing: it should start with user needs and continue through the risk assessment phase.

## **8.4 Cybersecurity integration**

### **8.4.1 [AA-02-01] Cybersecurity guidelines for the railway solution**

#### **8.4.1.1 Requirement**

The organization in charge of the SUC integration (in conformity with cybersecurity management plan) shall develop guidelines for the deployment, operation and maintenance of the railway solution.

#### **8.4.1.2 Rationale and supplemental guidance**

The organization responsible for the integration of the SUC is best placed to compile the information about the parameters of the cybersecurity functions as they were designed and

implemented, integrating information from both the architecture and the sub-systems implementation. This activity is complementary to the Practice 8 described in [IEC 62443-4-1:2018 \[49\]](#).

The asset owner and assigned organizations will use the information to properly operate and maintain the SUC, with respect to its cybersecurity.

These characteristics include, but are not limited to:

- SecRACs defined for the SUC, as described in [8.3.4](#)
- Secure operation guidelines
- Account management policies
- Security hardening guidelines.

This information is input to activity [OM-01-02] [10.4](#) and is part of the acceptance and handover activities, as described in [9.4](#).

## **8.5 Cybersecurity configuration**

### **8.5.1 [AA-03-01] Cybersecurity parameterization and configuration of the railway solution**

#### **8.5.1.1 Requirement**

The organization in charge of the integration of the SUC (in conformity with cybersecurity management plan) shall:

- a) devise the rules for security parameterization and configuration, and,
- b) in collaboration with the asset owner, check and document the correct application of these rules (security parameterization and configuration) in the railway solution.

#### **8.5.1.2 Rationale and supplemental guidance**

The collection of rules for parameterization and configuration of the cybersecurity functions as intended in the design of the SUC, under the context of the railway solution, is compiled by the organization in charge of the integration of the SUC.

These rules include, but are not limited to, the following:

- network configuration parameters;
- firewall rules;
- certificates;
- safekeeping of the security parameters;
- configuration management items.

The information is part of the acceptance and handover activities, as described in [9.4](#).

## **9 Cybersecurity assurance for railway solutions**

### **9.1 Purpose**

Cybersecurity assurance includes several activities that are performed throughout the development of the railway solution, which culminate in its acceptance by the asset owner at handover.

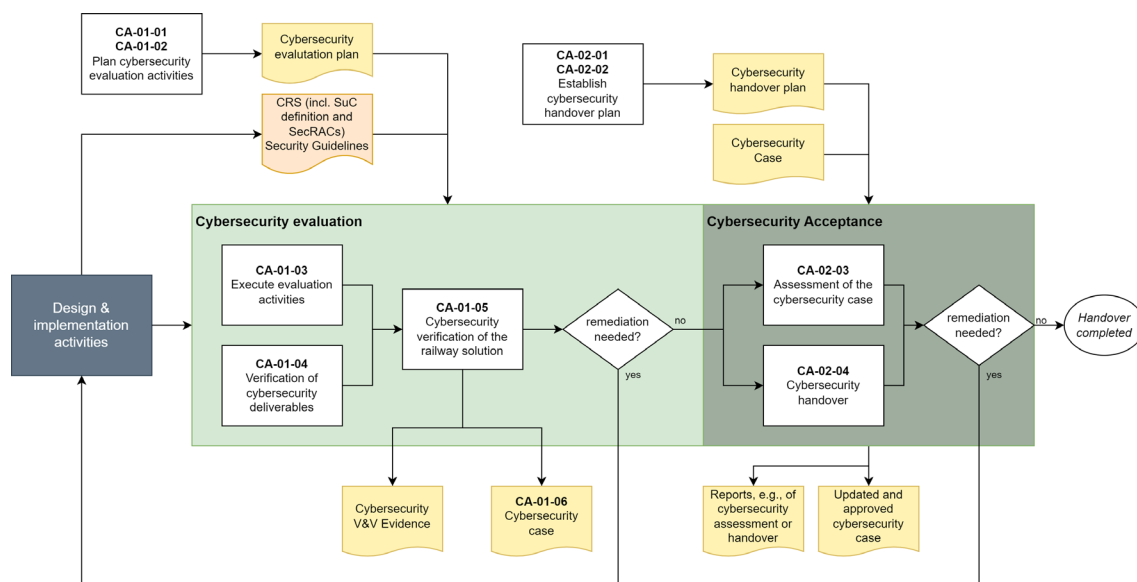
NOTE Assurance activities and related requirements for asset owner and maintenance service providers for ensuring that the railway solution maintains its security during operations, as well as following maintenance activities, are not in the scope of this clause. These aspects are covered in Clause 10.5.

## 9.2 Overview

This clause sets out requirements on cybersecurity assurance activities and deliverables. The following requirements refer to the appointed organization that is responsible for their execution. This is typically the system integrator but can also be the asset owner. It can also be both, either working independently in their respective scope of work or collaboratively on a common deliverable, in which case the corresponding requirement would apply to both organizations. Figure 14 provides a visual overview of the inputs, outputs and activities related to cybersecurity assurance, linked with the requirements of this clause.

The main input to the activities of this clause is the CRS and all identified SecRACs. The results of each assurance activity are collected in the railway solution cybersecurity case, which provides the input for the activities that follow during the operational life cycle of the railway application.

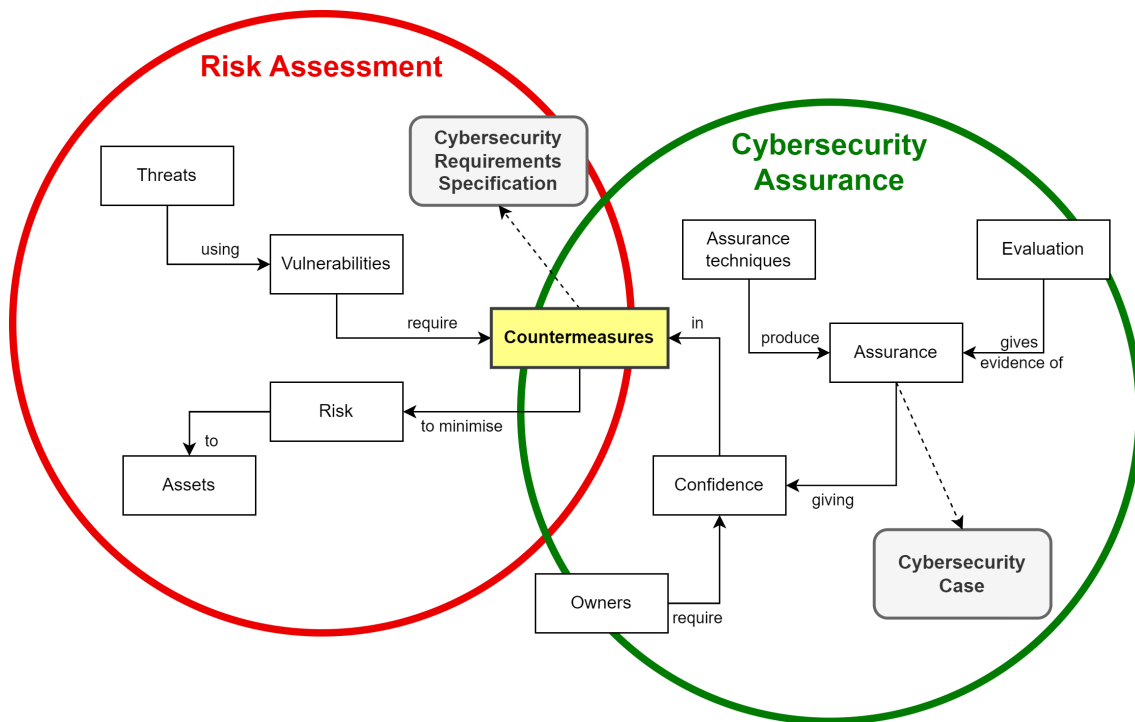
The cybersecurity case contains or refers to all relevant assurance evidence, as well as the SecRACs that are necessary for the secure operation of the railway solution. It is typically delivered by the system integrator to the asset owner for review. Acceptance of the cybersecurity case by the asset owner completes the cybersecurity handover.



**Figure 14 – Overview of assurance activities and applicable requirements.**

An overview of the relationship between risk assessment (covered in Clause 7) and cybersecurity assurance is shown in Figure 15:

- During the risk assessment threats and vulnerabilities are identified that pose a risk to the railway solution.
- The CRS defines security countermeasures for addressing these threats and vulnerabilities for achieving an acceptable level of residual risk.
- Assurance techniques are applied to give confidence that the countermeasures as implemented actually address the risks identified and that the railway solution given its operational environment and configuration achieves the security objectives.
- The results of the cybersecurity evaluation activities are documented in the railway solution cybersecurity case.



**Figure 15 – Relationship between risk assessment and cybersecurity assurance**

### 9.3 Cybersecurity verification and validation

#### 9.3.1 Description

This section provides requirements applying to the cybersecurity verification and validation activities carried out during the development of a railway solution. The railway solution is subject to inspection and test procedures that verify that the requirements of the CRS and compensating countermeasures (if present) have been implemented correctly and effectively. System functions and cybersecurity functions ought to be integrated in an incremental, systematic approach with a dedicated test plan for both.

A key output of these activities is the cybersecurity case which contains or refers to all relevant assurance evidence, as well as the SecRACs that are necessary for the secure operation of the railway solution. It is delivered by the system integrator to the asset owner for review. Acceptance of the cybersecurity case by the asset owner completes the cybersecurity handover, which is the topic of the next section.

NOTE Further guidance can be found in [IEC 62443-2-4:2023 \[50\]](#) “Security program requirements for IACS service providers”, in particular all requirements of the subtopic “Verification”.

#### 9.3.2 Inputs / Outputs

Inputs:

- Risk assessment report [ZR-05-11].
- Cybersecurity requirements specification [ZR-06-01].
- Cybersecurity management plan [LC-02-01].
- Security guidelines, e.g. from implementation or manufacturing activities or from suppliers.

Outputs:

- Cybersecurity evaluation plan [CA-01-01].
- Verification evidence [CA-01-03].

- If needed, updated CRS and associated risk assessment report [CA-01-04].
- Cybersecurity case of the railway solution [CA-01-06].

### 9.3.3 [CA-01-01] Plan cybersecurity evaluation activities

#### 9.3.3.1 Requirement

The appointed organization, according to the cybersecurity management plan, shall develop a cybersecurity evaluation plan for assessing the cybersecurity design, implementation and configuration of the railway solution through the provision and examination of objective evidence.

The cybersecurity evaluation plan shall include:

- a) the types of security tests to be performed; and
- b) the type of reviews, analysis, inspections to be performed; and
- c) their depth and coverage.

#### 9.3.3.2 Rationale and supplemental guidance

The cybersecurity evaluation plan details the cybersecurity verification and validation activities to be carried out throughout the development life cycle of the railway solution. It may expand on the information previously provided in the cybersecurity management plan or be incorporated into it, thereby negating the need for a separate document. Early feedback from the asset owner on the plan is advisable to avoid issues during handover.

The plan should identify a range of review, analysis and inspection activities aimed at identifying potential cybersecurity issues. This may include reviewing work products against best practices, cybersecurity policies and cybersecurity requirements, as well as testing activities. These activities should be scheduled at appropriate milestones throughout the life cycle to ensure that cybersecurity issues can be addressed as early and in an as cost-effective way as possible.

A key aspect that should be addressed is the planning of the testing activities. Testing activities are performed within a determined coverage and depth that is based on the impact and risks associated with a system, zone or component as determined in the risk assessment.

If external suppliers are used for planning, executing or evaluating tests, an assessment is advised to ensure that they can demonstrate both required competences (technical expertise) and domain knowledge, for example via relevant certifications.

There are several types of security testing:

- Security requirements testing: verification of the correct implementation of cybersecurity requirements specified in the CRS [ZR-06-01].
- Threat mitigation testing: verification that the threats identified during risk assessment have been adequately mitigated so that the residual risk is tolerable. This results in testing that does not only verify that a security function was correctly implemented, but that the associated risk has been addressed.
- Vulnerability testing: vulnerability testing ensures that known and unknown vulnerabilities have been treated in the railway solution using methods such as attack surface analysis, vulnerability scanning, vulnerability scenario testing and fuzzing.
- Penetration testing: penetration testing is security testing in which real-world attacks are simulated to identify methods for circumventing the security features of a system or network. Typically, they are performed by trained penetration testers (see [Annex H](#)) who use predetermined rules of engagement, which covers criteria such as which systems may or may not be attacked, the time period of the engagement and what can be modified.

[IEC 62443-4-1:2018 \[49\]](#) gives guidance on inspection and test procedures.

[Clause G.7](#) provides an example of content of a possible cybersecurity evaluation plan.

### 9.3.4 [CA-01-02] Independence of security testers

#### 9.3.4.1 Requirement

The system integrator shall apply a process to ensure that individuals performing testing are independent from the developers who designed and implemented the railway solution according to [Table 6](#).

**Table 6 – Required level of independence of testers from developers**

Test type	Level of independence
Security requirements testing	Independent department
Threat mitigation testing	Independent department
Abuse case testing	Independent person
Static code analysis	None
Attack surface analysis	Independent person
Known vulnerability scanning	Independent person
Software composition analysis	None
Penetration testing	Independent department or organization

The levels of independence are defined as follows:

- **None** – no independence required. Developer can perform the testing.
- **Independent person** – the person who performs the testing cannot be one of the developers of the product.
- **Independent department** – the person who performs the testing cannot report to the same first line manager as any developers of the product. Alternatively, they could be a member of a quality assurance (QA) department.
- **Independent organization** – the person who performs the testing cannot be part of the same organization as any developers of the product. An organization can be a separate legal entity, a division of a company or a department of a company that reports to a different executive such as a vice president or similar level.

NOTE This requirement has been adopted from requirement SVV-5 in [IEC 62443-4-1:2018 \[49\]](#).

#### 9.3.4.2 Rationale and supplemental guidance

In general, testers should have an appropriate level of independence from the people, teams, department or organizations that designed and implemented the railway solution. This is because dedicated, independent testers that possess the required competences (see [Annex H](#)) do not have preconceptions about the system under test that could lead to unwarranted assumptions about its functionality, and they cannot be held responsible for delays or other issues due to them discovering defects. Stricter independence, such as through an independent organization, may be necessary depending on the security level, test type, asset owner requirements, organizational policies, or regulatory requirements.

NOTE In agile development environments, it may be difficult to implement high levels of independence, in which case other measures should be taken to ensure that no undue influence is placed on the testers by the developers.

### 9.3.5 [CA-01-03] Execution of cybersecurity evaluation activities

#### 9.3.5.1 Requirement

The appointed organization, according to the cybersecurity management plan, shall execute all the activities described in the cybersecurity evaluation plan and document the methods, processes and results.

### 9.3.5.2 Rationale and supplemental guidance

Appropriate documentation of the cybersecurity evaluation activities enables evidence-based verification of their execution that can be later leveraged for demonstrating that the railway solution is fit for operation. It may also be helpful in cybersecurity assessments, as well as an input for similar activities during operation and maintenance.

Asset owners should consider whether they need to inspect or approve the results of the activities carried out by the system integrator during the development life cycle and identify such requirements and relevant artifacts in their contracts.

The verification evidence should be traceable back to the CRS [ZR-06-01] to ensure that their coverage is sufficient.

NOTE Verification evidence may be captured in multiple documents or other forms, such as machine-readable reports or security dashboards.

## 9.3.6 [CA-01-04] Verification of cybersecurity deliverables

### 9.3.6.1 Requirement

The appointed organization, according to the cybersecurity management plan, shall ensure that all cybersecurity deliverables defined in the cybersecurity evaluation plan are reviewed for completeness and consistency. Any identified issue shall be logged, communicated and addressed.

### 9.3.6.2 Rationale and supplemental guidance

Cybersecurity verification is applied continuously during all phases of the development life cycle to provide confidence in the correct execution of cybersecurity activities. Key in this respect is also the verification of the outputs of all activities both in terms of completeness as well as consistency.

## 9.3.7 [CA-01-05] Cybersecurity validation of the railway solution

### 9.3.7.1 Requirement

The appointed organization, according to the cybersecurity management plan, shall demonstrate through the provision of objective evidence that the railway solution, in its operational configuration and with application of the documented SecRACs, meets the cybersecurity requirements of the CRS and that the cybersecurity risk level is acceptable according to the agreed risk acceptance criteria.

### 9.3.7.2 Rationale and supplemental guidance

To demonstrate compliance with the cybersecurity requirements, evidence in form of inspection and testing reports that cover the requirements in the CRS can be provided. Demonstrating whether the risk level is acceptable assumes access to the risk assessment results and should be performed by the organization that performed the risk assessment.

Other relevant evidence may include:

- a review of logical and physical network plans;
- lists of installed components;
- documentation that hardening measures have been applied, such as for components that have been securely configured, unnecessary software that has been removed and unused interfaces that have been disabled
- component documentation, for example security configuration options, specifications, manuals, risk assessment reports, (security) test reports and security certifications;



- supplier documentation, such as ISMS or CSMS certification or certification of the product development process;
- documentation on the testing or other methods used.

See also [IEC 62443-4-1:2018 \[49\]](#) (Practice 8 - Security guidelines) for component documentation requirements, as well as [IEC 62443-4-1:2018 \[49\]](#), [IEC 62443-4-2:2019 \[55\]](#) and [ISO/IEC 27036-3:2013 \[22\]](#) for supply chain requirements.

Important aspects that should be verified include that:

- the security guidelines are sufficient and correctly documented; and
- the security-related functionality and configuration is correctly implemented; and
- the organizational requirements and SecRACs identified are sufficient for managing the identified risks.

The asset owner can also provide valuable input on covering the aforementioned aspects, in particular with respect to the validation of the SecRACs. In case of deviations the system integrator should develop possible remediation and, where necessary, verify them by updating the risk assessment, the CRS and the SecRACs. This may require renewed approval by the asset owner [ZR-07-01].

### **9.3.8 [CA-01-06] Railway solution cybersecurity case**

#### **9.3.8.1 Requirement**

The appointed organization, according to the cybersecurity management plan, shall prepare the railway solution cybersecurity case.

The railway solution cybersecurity case shall include or refer to:

- a) the CRS; and
- b) evidence demonstrating that the security objectives have been fulfilled and the solution is fit for operation, such as verification and validation reports; and
- c) information for the secure operation of the railway solution including the SecRACs; and
- d) information on how cybersecurity risks affecting safety-related functions have been evaluated and how protection against the adverse influence has been achieved.

**NOTE** This requirement and the corresponding guidance only address the cybersecurity case of the railway solution provided by the system integrator. The asset owner may maintain a cybersecurity case for their railway system that can refer to several cybersecurity cases from different system integrators (see [OM-02-01]).

#### **9.3.8.2 Rationale and supplemental guidance**

The railway solution cybersecurity case provides the assurance that the railway solution as designed and implemented meets all cybersecurity requirements for entering into service. This is achieved by, among other things, providing evidence that the cybersecurity activities defined in the cybersecurity management plan have been carried out and that the risks have been adequately addressed, or, where not, the SecRACs defined are sufficient to mitigate them. It also provides the necessary conditions for maintaining the railway solution security during the operation, maintenance and decommissioning phases. Documenting how risks affecting safety-related functions have been evaluated and address assumes access to the risk assessment results and should be performed by the organization that performed the risk assessment. The cybersecurity case is a live document and should be continuously updated by the asset owner over the operation life of the railway solution.

The cybersecurity case may build upon lower-level cybersecurity cases, for example for control systems included in the railway solution. If these lower-level cybersecurity cases contain

SecRACs that are not guaranteed to be fulfilled through integration, these SecRACs should be captured in the cybersecurity case of the railway solution.

The cybersecurity case is associated to a collection of documents that is delivered to the asset owner. It may also refer to documents that are confidential and are not shared with the asset owner, e.g. penetration test reports. Such documents could be made available on a need-to-know basis, such as during an audit. Although the cybersecurity case is first needed during handover, it will be typically put together at the early stages of development and expanded as new relevant documents become available.

The information for the secure operation of the railway solution may vary depending on the nature of the solution. In addition to the SecRACs that are mandatory, other aspects may include:

- updates to the risk assessment report based on the results of the assurance activities; and
- security guidelines, including guidance on incident response, for example the recommended emergency technical measures and vulnerability management; and
- recommended mitigations for ongoing management of identified risks; and
- hardening guidelines and documentation on how to verify they have been applied; and
- guidelines for the use of cybersecurity tools, such as possible adverse effects and instructions on use.

An example of the structure of a railway solution cybersecurity case is given in [Clause G.8](#).

The railway solution cybersecurity case can also refer to the documentation of products or components, for example requirement specifications, product cybersecurity cases, application manuals and security certifications. In such cases, a holistic view for the solution should be used that takes into consideration how the product or component is integrated. For example, the attack surface of a product may be smaller when integrated, but at the same time increase the attack surface of the solution.

## **9.4 Railway solution acceptance**

### **9.4.1 Description**

The objective of this section is to specify the prerequisites for accepting the railway solution for entry into service. This includes in particular the requirements on the definition and approval of the cybersecurity handover plan, the approval of the railway solution cybersecurity case and the execution of the cybersecurity handover of the railway solution from the system integrator to the asset owner.

### **9.4.2 Inputs / Outputs**

Inputs:

- Verification evidence [CA-01-03].
- Railway solution cybersecurity case [CA-01-06].
- Cybersecurity management plan [LC-02-01].
- Cybersecurity requirements specification [ZR-06-01].
- Regulatory requirements.

Outputs:

- Cybersecurity handover plan [CA-02-01].
- Cybersecurity case approval [CA-02-03].
- Cybersecurity handover report [CA-02-04].

### **9.4.3 [CA-02-01] Establish cybersecurity handover plan**

#### **9.4.3.1 Requirement**

The appointed organization, according to the cybersecurity management plan, shall document a cybersecurity handover plan that includes all cybersecurity-related deliverables as well as activities to be performed during handover.

#### **9.4.3.2 Rationale and supplemental guidance**

The cybersecurity handover formally transfers the responsibility of the cybersecurity of the railway solution from the system integrator to the asset owner. While the overall responsibility after handover is with the asset owner, joint effort is still necessary during the operation of the solution, e.g. for vulnerability management, patch management, risk management and incident management. See [Clause 10](#).

A common activity during handover involves an operational readiness demonstration. If such an activity is foreseen, the following aspects should be considered in the handover plan:

- The organization responsible for performing it, for example, the asset owner may assign responsibility to the system integrator or contract an external service provider.
- The scope of the demonstration, such as which functions will be included.
- The target environment, which is recommended to be a staging environment, but in some cases such an environment may not be available.
- Risks and constraints when it is possible that certain cybersecurity functions cannot be demonstrated or can only be demonstrated in a limited way, such as when they could influence operational systems or safety functions.
- The configuration baseline to be used to enable repeatability.
- The formalization of the completion of the cybersecurity handover and its agreement by both parties.

Other cybersecurity aspects for the handover plan may include:

- Review and acceptance of the cybersecurity deliverables, as required, by relevant stakeholders, that can include the asset owner.
- The transfer of the responsibility for vulnerability management and incident management.
- The change of trust anchors, such as from the system integrator to the operator or from staging to production.
- The reconfiguration of the interfaces to connect to operator production systems, for example asset management and security monitoring systems.
- The revocation of temporary (remote) access to the railway solution that was used for implementation and testing purposes.
- The specific trainings related to cybersecurity operation of the railway solution that will be delivered to the asset owner.

### **9.4.4 [CA-02-02] Approval of the cybersecurity handover plan**

#### **9.4.4.1 Requirement**

The asset owner shall approve the cybersecurity handover plan.

#### **9.4.4.2 Rationale and supplemental guidance**

The cybersecurity handover plan should be developed together with the asset owner to ensure that all relevant aspects and concerns are addressed. It is further recommended to develop the plan early, so that potential conflicts or complications can be identified and avoided without requiring last-minute changes. The asset owner should verify that the planned activities are

appropriate and sufficient for assuming responsibility for and operating the railway solution in the future.

#### **9.4.5 [CA-02-03] Approval of the cybersecurity case**

##### **9.4.5.1 Requirement**

The asset owner shall approve the railway solution cybersecurity case.

##### **9.4.5.2 Rationale and supplemental guidance**

The asset owner should assess the cybersecurity case to determine whether the railway solution as implemented is fit for operation and the SecRACs are sufficient for secure operations. The asset owner may assign an assessor from their own organization, contract a third party or accept an assessment performed by one belonging to the organization of the service integrator. Independence between the cybersecurity assessor and the project team should be demonstrated, in particular in the latter case. Organizational policies and regulatory requirements may affect the selection of the assessor, e.g. by demanding required competences (see [Annex H](#), “Cybersecurity Assessor”), minimum independence such as through an independent assessment organization or accreditation by a railway regulatory authority.

The assessment results are typically captured in a cybersecurity assessment report which is associated with the cybersecurity case. Findings may need to be addressed by reviewing the design and, if necessary, implementing additional countermeasures. In this case an update of the cybersecurity case will be necessary, followed by a partial or complete reassessment. As such, the cybersecurity assessor should be involved earlier in the process and not only just before handover for approving the cybersecurity case of the railway solution.

NOTE Requirements on the conformity assessment process and on the cybersecurity assessor are not in scope of this standard. See also IEC 62443-2-1 ED2, Clause 5 for additional guidance on conformity assessments.

#### **9.4.6 [CA-02-04] Perform cybersecurity handover**

##### **9.4.6.1 Requirement**

The system integrator and the asset owner shall execute the activities specified in the cybersecurity handover plan, document the results and formally agree on its completion.

##### **9.4.6.2 Rationale and supplemental guidance**

It is recommended that a report is compiled that provides a record of the handover process identifying the version of both software and documentation of the delivered railway solution. The handover typically concludes with a review of the report and the addressing of any remaining concerns before being signed-off by the asset owner.

## **10 Operational, maintenance and decommissioning requirements**

### **10.1 Overview**

Some topics coming from the OT cybersecurity programme(s) defined in [Clause 5](#) [CP-01-02] for operational and maintenance activities are described in this clause: continuous cybersecurity verification; railway application cybersecurity case; vulnerability management; patch management; incident management; security monitoring; decommissioning management.

Cybersecurity maintenance plan gives the rules of tasks to be done for railway application.

Continuous cybersecurity verification and railway application cybersecurity case update give the status and report of task done.

This clause focuses on the requirements of railway operations and the responsibilities of the railway asset owner, with an emphasis on tasks primarily related to the OT (Operational Technology) environment (refer to clause 4.4).

The requirements of this clause concern first the asset owner of the railway application that establish or maintain the way of work. As a consequence, correct application of this way of work impact directly the maintenance service provider in charge, and can also impact (for vulnerabilities and patches) system integrator or product supplier if needed.

This clause only addresses standard IT measures or methods in the surrounding environment if necessary to enhance the OT measures.

An overview is given in Figure 16. The cybersecurity of the railway application needs to be sustained throughout operation, maintenance, and decommissioning activities.

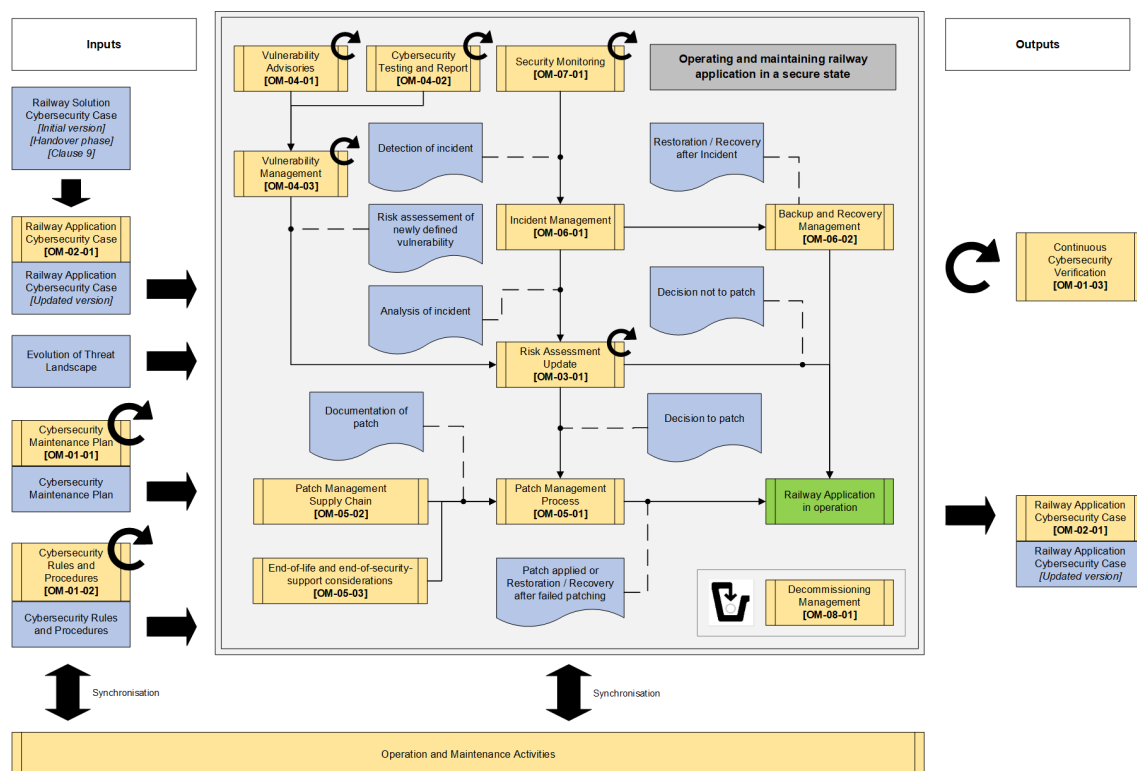


Figure 16 – Overview of operational activities

Changes that are applied to the railway application during operation phase should be covered by application of the same requirements from Clause 6 to Clause 9 (risk assessment, cybersecurity requirement specification, technical implementation of changes, verification and validation) focused on these changes.

If changes have minor impacts on the existing cybersecurity deliverables (DRA, CRS, SecRACs, Cybersecurity Case, etc.) for the railway application, activities could be optimized under accountability of the asset owner. That could result in tasks from Clause 6 to Clause 9 with partially skipped phases, or with no need to step back to Clause 6 and all activities done in operation phase as typical maintenance activity.

Examples of minor changes could be:

- A risk assessment updated and accepted that does not require new measures to be implemented.

- A vulnerability treated with a patch or an updated configuration, without changes regarding operational functionalities and with same or enhanced cybersecurity capabilities.
- Change of component with no or minor changes on functionalities, same interfaces, and without changes regarding operation and cybersecurity threats.
- Small extensions with components or subsystems that have been analyzed already regarding cybersecurity.

## 10.2 Inputs / Outputs

### Inputs

- Applicable for all the OM requirements in this clause:
  - Cybersecurity case of the railway solution [CA-01-06] from the handover, including at least:
    - SecRACs
    - Security guidelines
  - Cybersecurity rules and guidelines from the policies [CP-01-01] and OT cybersecurity programmes [CP-01-02].
- Documented process from [Clause 5](#):
  - Information sharing [CP-02-01] => for [OM-04-01] [OM-04-02] [OM-04-03] [OM-06-01].
  - Competency management [CP-03-01] => for [OM-01-01].
  - Inventory management [CP-04-01] => for [OM-04-03] [OM-05-03] [OM-06-01] [OM-07-01].
  - Supply chain management [CP-05-01] => for [OM-04-01] [OM-04-03] [OM-05-02].
  - Risk management [CP-06-01] => for [OM-03-01].
  - Business continuity management (business continuity plan) [CP-07-01] => for [OM-01-01] [OM-06-01] [OM-07-01].
  - Data protection management [CP-08-01] => for [OM-01-02] [OM-08-01].

### Outputs

- Documentation to be defined, applied for the railway application, and updated when needed:
  - Cybersecurity maintenance plan [OM-01-01].
  - Cybersecurity rules and procedures [OM-01-02].
  - Regular verification reports about implementation of cybersecurity maintenance plan and SecRACs [OM-01-03].
  - Railway application cybersecurity case updated [OM-02-01].
  - Risk assessment updated [OM-03-01].
  - Vulnerability management (including advisories; cybersecurity testing and report) [OM-04-01], [OM-04-02], [OM-04-03].
  - Patch management (including supply chain and end-of-life/end-of-security-support considerations) [OM-05-01], [OM-05-02], [OM-05-03].
  - Incident management [OM-06-01].
  - Security monitoring [OM-07-01].
  - Decommissioning management [OM-08-01].

### 10.3 [OM-01-01] Cybersecurity maintenance plan

#### 10.3.1 Requirement

The asset owner shall identify cybersecurity maintenance activities that are to be applied throughout the railway application life cycle in a cybersecurity maintenance plan.

The cybersecurity maintenance plan shall include at minimum the following topics in the context of the railway application:

- a) continuous cybersecurity verification;
- b) railway application cybersecurity case update;
- c) risk assessment update;
- d) vulnerability management (including advisories; cybersecurity testing and report)
- e) patch management;
- f) incident management (including backup and recovery management);
- g) security monitoring;
- h) decommissioning management.

The cybersecurity maintenance plan shall identify people's responsibilities for planned activities. Where responsibilities are shared with other stakeholders, confirmation shall be provided that these stakeholders have accepted their co-responsibilities.

#### 10.3.2 Rationale and supplemental guidance

Some topics addressed by [Clause 5](#) should be refined in the cybersecurity maintenance plan in the context of the railway application.

Performing regular cybersecurity maintenance activities on operational railway applications, considering their context within the railway system as well as the interfaces with the office-IT systems, provides a sustained level of cybersecurity to the railway system.

Cybersecurity maintenance is usually based on the cybersecurity guidelines which describe the instructions for the secure installation, operation and maintenance of the delivered railway solution and its SecRACs.

Cybersecurity maintenance requirements may include legal or regulatory obligations such as continuous system monitoring and threat management.

Examples of cybersecurity maintenance include the regular review of training and assessment of staff (internal or external), the regular review of the threat landscape (see [7.3.4](#)), the backup strategy (see in rationale of incident management [10.14.2](#)) and the frequency of patching and security testing.

In case of design change, impact on the cybersecurity maintenance plan should be assessed to determine whether it has to be updated.

To keep consistency and enable a highly automated workflow, the relevant parameters (e.g. recovery time objective, delay to deliver a tested patch from notification) should be listed and defined in a contractual agreement SLA between service providers and asset owner. This contractual agreement should be established before commissioning and the content should be kept up to date during the railway application life cycle.

At least one person should report directly to the asset owner management on matters of the railway application security.



Roles, responsibilities and authorities should be reviewed and, where appropriate, updated at planned intervals and when significant incidents or significant changes to railway application or risks occur.

[Clause G.9](#) provides an example of cybersecurity maintenance plan content.

## **10.4 [OM-01-02] Cybersecurity rules and procedures**

### **10.4.1 Requirement**

The asset owner shall accept, adapt, or establish and maintain cybersecurity rules and procedures to be applied during railway operation and maintenance activities addressing cybersecurity.

These rules and procedures shall be based at minimum on:

- a) the provided security guidelines from system integrator and product suppliers (see [8.4.1](#));
- b) the OT cybersecurity programme(s) (see [5.4](#)) and cybersecurity maintenance plan (see [10.3](#));
- c) the asset owner experience;
- d) the applicable regulations.

These rules and procedures shall ensure full coverage of SecRACs of the railway solutions part of the railway application.

These rules and procedures shall include at least:

- e) Consistent access rules for operation and maintenance activities.
- f) Protection of critical data for operation and maintenance activities.

### **10.4.2 Rationale and supplemental guidance**

The rules and procedures should be compatible with the maintenance activities, teams, and capabilities. For this, the following possibilities should be implemented (non exhaustive listing):

- Dedicated tools for cybersecurity during operation and maintenance phase are usable by people, on maintenance laptop, with IT constraints.
- The defined individual account access strategy is compatible with the organization of maintenance teams.
- Certificate update policy periodicity is compatible with the maintenance operations schedule, the available tool capability, and people availability to perform the job.

Regarding the requirement:

- Acceptance refers to the maintenance procedure delivered by system integrator or suppliers and accepted by the asset owner.
- Adaptation refers to asset owner maintenance procedures (with an equal or a larger coverage than the application itself) that need updates.
- Establishment refers to asset owner maintenance procedures to be created if needed,
- Maintenance refers to continuous update due to changes in organization, system, technology, threat landscape.

The asset owner should set out and implement consistent access rules to the railway application for operation and maintenance activities, addressing physical and logical access control including for remote access, and defining role-based access control.

NOTE 1 For further supplemental guidance, see [Clause I.3](#) and [Clause I.4](#) for more operational details.



Railway applications' sensitive data should be protected regarding integrity, availability and confidentiality, such as in the case for particular credentials, keys and secrets, especially if data exchange with portable devices and configuration files are used or when an asset is decommissioned.

NOTE 2 For further supplemental guidance, see:

- [Clause I.5](#) for more operational details.
- [IEC 62443-2-4:2023 \[50\]](#) SP.03.09 BR, SP.03.10 BR, SP.03.10 RE(1), SP.03.10 RE(2), SP.03.10 RE(3), SP.03.10 RE(4). As an application could be maintained by several maintenance service providers under contracts with the asset owner, [IEC 62443-2-4:2023 \[50\]](#) could be used to address the maintenance service provider(s) activities for an application or a part of it.
- [5.11](#) for data protection management.
- [9.3.8](#) for SecRACs at handover, potentially updated during maintenance phase, and verified in [10.5](#).
- [Clause I.5.4](#) for portable media.

## 10.5 [OM-01-03] Continuous cybersecurity verification

### 10.5.1 Requirement

The asset owner shall ensure that the activities defined in the cybersecurity maintenance plan and the SecRACs defined in the railway application cybersecurity case and cybersecurity guidelines are completely and correctly implemented, according the periodicity and criteria defined in the cybersecurity maintenance plan.

### 10.5.2 Rationale and supplemental guidance

During operation, the asset owner should demonstrate that all SecRACs and security guidelines are fulfilled, and should manage any deviation according to the asset owner risk management processes. Implementing mechanisms to identify changes or deviations from the baseline can be very helpful for this continuous cybersecurity verification process.

NOTE 1 Similar approaches as the one described in [Clause 9](#) can be followed to organize cybersecurity assurance activities during operation and maintenance phase.

NOTE 2 See also [IEC 62443-2-1:2024 \[52\]](#) Clause 5.

## 10.6 [OM-02-01] Railway application cybersecurity case

### 10.6.1 Requirement

The asset owner shall establish and maintain a railway application cybersecurity case.

The railway application cybersecurity case shall include or refer the railway solution cybersecurity case(s) and the evidence of the application of SecRACs and of applicable cybersecurity rules and procedures.

The railway application cybersecurity case shall be established before railway application start of service.

The railway application cybersecurity case shall be periodically checked and updated if necessary, according to the criteria defined in the cybersecurity maintenance plan.

### 10.6.2 Rationale and supplemental guidance

The cybersecurity case is associated to a collection of documents (see [Annex G](#)).

The asset owner's cybersecurity case of the railway application is based on cybersecurity case(s) of the railway solution(s) delivered by the system integrator(s). The railway application cybersecurity case of the asset owner can refer to several cybersecurity cases from different system integrators, which serve as an input to the various parts of the railway cybersecurity management (see [Clause 5](#)).

The asset owner and its maintenance service provider(s) use and update the railway application cybersecurity case when carrying out the operational and maintenance activities.

EXAMPLE Any SecRACs of a cybersecurity case are inputs to the cybersecurity maintenance plan.

The events that can impact changes on risks and that can enforce an update of the cybersecurity case include but are not limited to:

- a significant change in the railway application or any of its elements that may result in a significant impact to the assessed risk;
- a significant change of the cybersecurity maintenance plan;
- a significant change of risks (see 10.7 Risk assessment update).

An update of the cybersecurity case may cause the update of the railway application cybersecurity maintenance plan.

Clause G.8 provides an example of cybersecurity case content.

## 10.7 [OM-03-01] Risk assessment update

### 10.7.1 Requirement

The asset owner shall review the risk assessment based on the periodicity and criteria defined in the cybersecurity maintenance plan, update it if necessary, and address any identified cybersecurity risks.

### 10.7.2 Rationale and supplemental guidance

Risk management can be performed in accordance with the following two modalities:

#### a) Limited risk analysis

The following events should trigger a risk analysis limited to the event scope, based on the asset owner's criteria:

- 1) Discovered vulnerabilities (see 10.10); or
- 2) Patches identified as relevant by the asset owner (see 10.11); or
- 3) Incident (see 10.14).

For this, the impact and risk of the cybersecurity related issue are determined and compared to the tolerable risk, to decide on the treatment.

NOTE The impact of compounding from multiple deferred risks could also be considered during the risk analysis process.

#### b) Update of the detailed risk assessment according to Clause 7 when it is no longer valid, for example due to:

- 1) Technical changes of the railway application, such as an asset or essential function being added or changed; or
- 2) Update of railway application design during maintenance; or
- 3) Evolution of threat environment (e.g. threat landscape evolution, evolution of effectiveness of current countermeasure); or
- 4) New critical vulnerabilities; or
- 5) Evolution of SecRAC coverage by organization and maintenance activities.

NOTE Additional trigger for risk assessment update could be:

- 6) new regulations,
- 7) changes in some other system with which this railway application communicates/integrates,
- 8) changes in the organization that is operating.

For railway application considered as critical by the asset owner, it is recommended to review the risk assessment at least once a year.

For legacy systems, a risk assessment with proportioned effort regarding cybersecurity criticality should be done to solve the lack of existing detailed risk assessment. See also [Annex B](#) Handling legacy systems.

NOTE 1 Refer to [IEC 62443-2-1:2024 \[52\]](#) ORG 2.1 for further guidance.

Residual risks applicable to a railway application could be summarized in a risk register. This risk register should be updated in case of risk assessment update (due to vulnerability, threat or incident). This risk register could be escalated in case of residual risk that need validation or correlation at higher level.

NOTE 2 See NIST SP 800-221 for further guidance about risk registers.

See also [5.9](#) for Risk management.

## **10.8 [OM-04-01] Vulnerability advisories**

### **10.8.1 Requirement**

The asset owner shall have a process to request and integrate vulnerability advisories from stakeholders of the supply chain.

### **10.8.2 Rationale and supplemental guidance**

The vulnerability management process (see [10.10](#)) should contain necessary provisions to ensure that the asset owner can receive advisories (see [Clause J.2](#)).

See also [ISO/IEC 29147:2018 \[23\]](#).

## **10.9 [OM-04-02] Cybersecurity testing and report**

### **10.9.1 Requirement**

The asset owner shall establish, apply and maintain a strategy for cybersecurity testing of the railway application during operation and maintenance, and report results.

### **10.9.2 Rationale and supplemental guidance**

The asset owner should specify the scope, coverage target, frequency and type of cybersecurity tests to be performed, and adjust according to the risk assessment update.

Cybersecurity tests should in priority cover the components identified as relevant for secure operation in a risk assessment (e.g. cyber-critical asset; see [Clause J.3](#)) and security configurations if necessary.

Cybersecurity tests should be performed, and security configurations should be reviewed, in particular when significant incidents or significant changes impact the railway application or its risks.

Cybersecurity tests should be performed preferably on test bench. When cybersecurity tests are performed on the operational system, an impact analysis should be done before, and a validation should be done to ensure that the system is back to a well-defined state after the test is completed.

The test report should summarize test results, assessment of criticality of vulnerabilities discovered, and, if possible, proposals for mitigating actions for each finding. This report is an input for the vulnerability management process (see [Clause J.4](#) - [Figure J.1](#)).

## **10.10 [OM-04-03] Vulnerability management**

### **10.10.1 Requirement**

The asset owner shall establish, apply and maintain a vulnerability management process to identify, analyse and resolve vulnerabilities from internal and external sources.

This process shall include:

- a) organizational aspects (roles and responsibilities allocation);
- b) communication aspect (including report and disclosure);
- c) process scoping;
- d) vulnerability identification, analysis and prioritization criteria;
- e) vulnerability handling decision (accept the risk, mitigate, remediate).

### **10.10.2 Rationale and supplemental guidance**

The vulnerability management process should be established before the commissioning of the railway application, considering the interfaces with the risk management process and other elements of the OT cybersecurity programme like asset inventory management and patch management.

The vulnerability management process should also integrate:

- organizational aspects, such as the allocation of roles and responsibilities throughout the activities of the process and the mechanisms to receive and communicate vulnerability information;
- a strategy for scoping the vulnerability handling, a methodology for vulnerability analysis and criteria for prioritization and deciding on the remediation based on risk;
- procedures to monitor and track the identified vulnerabilities until resolution.

NOTE 1 In case of a known date of a component's end-of-life (see [10.13](#)), this date could be tracked in the enterprise life cycle management (e.g. in the inventory database) and crossed with the list of vulnerabilities in order to allow to either apply last version or anticipate hardware and/or software refresh needed to allow continue vulnerability watch.

NOTE 2 The list of vulnerabilities could be an input for the risk assessment update.

NOTE 3 For further supplemental guidance see [IEC 62443-2-1:2024 \[52\]](#) EVENT 1.9.

See [Annex J](#) for more operational details.

## **10.11 [OM-05-01] Patch management process**

### **10.11.1 Requirement**

The asset owner shall establish, apply and maintain a patch management process for the railway application that includes:

- a) identification of the component capabilities related to patching;
- b) identification of all stakeholders with their roles and responsibilities;
- c) monitoring of availability of patches with security fixes for each component;
- d) patch prioritization, selection, testing, and deployment schedule;
- e) patch deployment activities;
- f) verification that patches have been correctly applied.

### 10.11.2 Rationale and supplemental guidance

Railway applications and their components have different capabilities and requirements concerning patching. The specific capabilities may differ based on regulatory requirements like certification requirements or operational requirements like patch windows, availability of test-systems and impact on operation. The requirements may include limitations like unavailable automated patch deployment or manual processes involved.

Requirements may change over time, especially considering the typical long life cycle of the railway application. Specific capabilities may impact the total cost of the system over time, influence operational efficiencies, and impact risk management.

These topics should be considered in the patch management process::

- the definition of how long patches are being provided for the component;
- the requirements regarding the maintenance of testing capabilities for the railway application, dependent on its expected lifetime;
- the requirements regarding the provision of patches in emergency situations or regular patch provisioning;
- the definition of how patches are tested and validated by the manufacturer, and their effectiveness is ensured;
- the requirements on the content of a patch delivery note.

## 10.12 [OM-05-02] Patch management supply chain

### 10.12.1 Requirement

The asset owner shall establish, document and maintain patch management requirements for product supplier, system integrator and maintenance service provider (see 5.8).

### 10.12.2 Rationale and supplemental guidance

The availability of patches with security fixes may vary depending on the manufacturer of a component. For component consisting of COTS hardware or software, the end-of-life may not be known up-front and needs to be assessed in a continuous way. Also, manufacturers might have ceased to exist or stopped supporting the software product with patches.

The patch process created by the asset owner per component should consider at least the following aspects:

- how patch authenticity and integrity are checked and ensured throughout the process;
- how patches are received from the manufacturer;
- how patches are tested and validated, and their effectiveness is ensured;
- how patches are authorized, considering, at least, test results of the manufacturer, test results of the asset owner and the patch delivery notes;
- how to document unauthorized patches and how not applied but required patches are considered in the risk assessment of the railway application;
- how patches are handed over to the asset owner;
- how patches are handled by the asset owner;
- how patches are to be installed on the component;
- how to back-up of the railway application before applying patch in order to be able to rollback if needed;
- how to keep track of installed patches and not installed patches (link to inventory management).

These requirements can either be allocated to product supplier in case of bespoke components or used as supplier selection criteria in case of COTS suppliers.

NOTE 1 See [IEC 62443-2-1:2024 \[52\]](#) (COMP 3.1 - 3.5) and [IEC TR 62443-2-3:2015 \[24\]](#) for further guidance on patch management including patch status.

NOTE 2 Patches could be tested in a test environment reflecting the actual operational environment to avoid negative impact on the railway application. If such a test environment is not available, an alternative may be a progressive deployment or roll-out plan: the patch is first installed in one affected device (or control system) and, only after a watch period where no issues are observed, it is deployed to the rest of affected devices (or control systems).

### **10.13 [OM-05-03] End-of-life and end-of-security-support considerations**

#### **10.13.1 Requirement**

The asset owner shall monitor the end-of-life and end-of-security-support (no more security updates provided) of railway application's asset and anticipate decisions to be able to operate its railway application in a secure state.

#### **10.13.2 Rationale and supplemental guidance**

The obsolescence of software should be surveyed to proactively manage the fact that software will become obsolete in the future (end-of-life management). If software is not updatable as either the software is no longer maintained or hardware is no longer compatible, specific measures to protect the system should be taken. If the intention is to maintain an asset in a secure condition, for example because it is identified as a cyber-critical asset, a technological refresh for hardware and software may be needed and correctly anticipated.

Following resolution measures are recommended:

- last time buy strategy to ensure availability of compatible software patches;
- replacement with a substitute item;
- conducting an emulation and reverse engineer the product;
- conducting a design change or technological refresh.

NOTE See [IEC 62402:2019 \[25\]](#) for further guidance on obsolescence management.

### **10.14 [OM-06-01] Incident management**

#### **10.14.1 Requirement**

The asset owner shall establish, apply and maintain a process for evaluating and responding to cybersecurity incidents affecting the railway application.

The incident management process shall address the following aspects:

- a) communication channels, roles and responsibilities for receiving incident notifications and reacting in a timely manner;
- b) assessing the impact of the incident and defining and applying the countermeasures needed to contain, resolve and recover from the incident;
- c) reporting to authorities or other entities (like ISACs) about ongoing or past incidents;
- d) identifying lessons learnt to eliminate the causes or reduce the likelihood for similar incidents in the long term;
- e) documenting accepted risks associated with incidents.

#### **10.14.2 Rationale and supplemental guidance**

The asset owner's cybersecurity incident process should focus urgently on any cybersecurity incident with safety implications beginning with the cybersecurity incident evaluation.

The [Figure 17](#) provide a possible cybersecurity incident management process.

The incident management process should be communicated to adequate teams in charge of processing, analysing, and deciding in case of incident. All the staff involved in incident management should be properly trained to understand the process and how to perform the incident response activities they are responsible for. The process should be tested to validate its effectiveness and to identify potential gaps and improvements in the documentation. Tests should be performed regularly or when there are significant changes to the railway application or its environment.

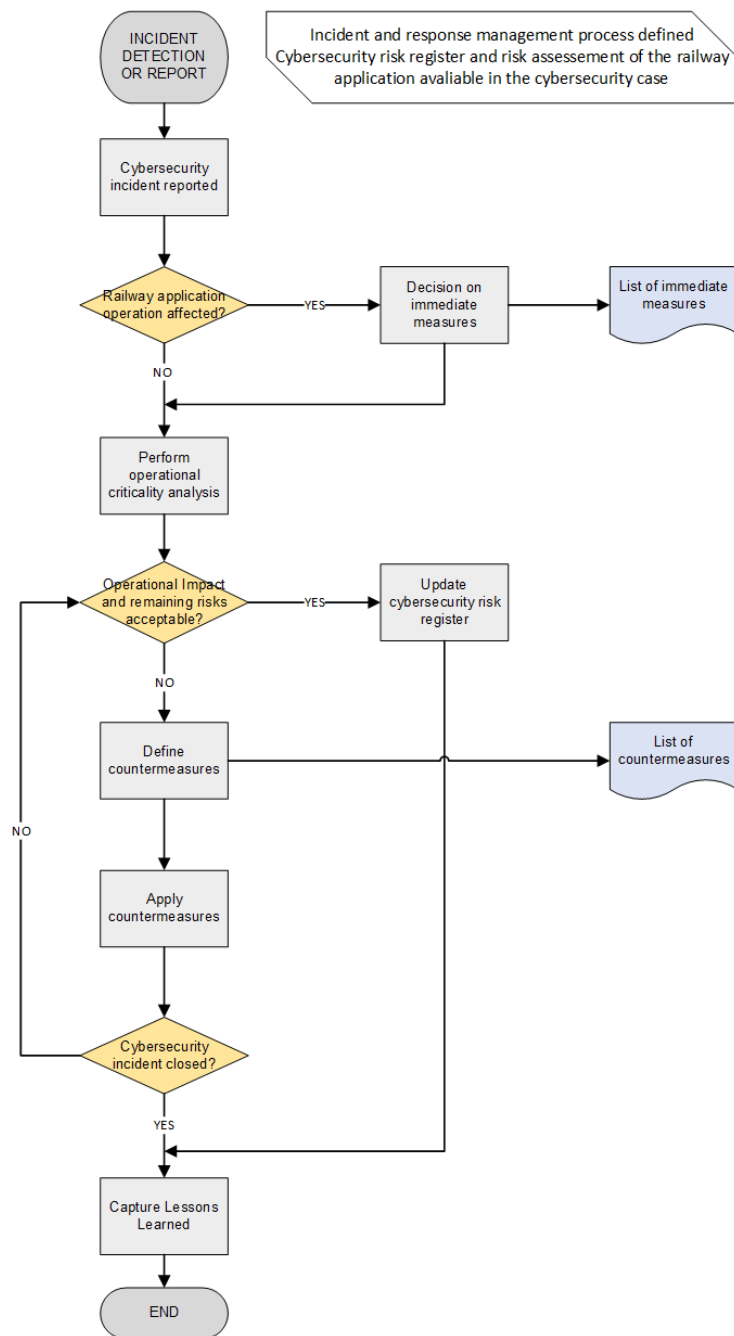
The first step is to assess whether a railway application, which is in operation, is affected (see [Figure 17](#)). In this case, the asset owner decides whether immediate measures should be taken to ensure a sufficient level of security, while the incident is analysed for its operational impact.

Immediate measures may include:

- disconnecting the affected system from the network;
- disabling certain functions of the system;
- issuing instructions not to use certain functions.

These immediate measures should ensure that essential functions of the railway application are not affected. It is therefore important that the asset owner has experts it can contact within or outside its organization, for example from a system integrator, who can provide technical insights on possible measures and their impact.

An incident can need a crisis treatment. The railway duty holder should integrate cybersecurity considerations into their enterprise management processes to ensure that critical cyber incidents are effectively managed and mitigated during a crisis. This integration aims to protect critical railway infrastructure, ensure the continuity of operations, and maintain passenger and staff safety.



**Figure 17 – Cybersecurity incident and response management process**

Decisions relating to cybersecurity incidents should be made quickly as to whether the affected railway application can continue its operation - possibly with the implementation of immediate additional measures.

All incoming messages and activities should be recorded in an incident list or database that is accessible for the incident handling team and serves a single source of truth during the handling activities.

Any disruptive cybersecurity event that possibly has negative implications on the safety of railway operations should be responded to with the utmost urgency.

A risk register could cover the overall railway system for a company, or could cover only one part for a coherent set of applications / solutions. The risk register should list the residual risks and should be referenced in the railway application cybersecurity case.



Depending on legislation, it may be required to notify sector-specific authorities and/or agencies of incidents related to critical infrastructure.

Forensic analysis activities could be required either by law or by the insurance contract clauses. In this case, preserving the chain of custody of the evidence, and supporting the efforts to prosecute the perpetrator or support liability claims should be considered.

In any case, a lesson-learned activity should be performed, to identify, select and implement related improvement opportunities.

NOTE Refer to [IEC 62443-2-1:2024 \[52\]](#) (EVENT 1.1 - 1.8) for further guidance on Incident Management.

Backups should allow restoring / recovering system in operation after an incident. Backups and recovery strategy (frequency, secure storage and retention, access control, testing and logs) for railway applications should be defined, according with business continuity management (see [5.10](#)), capabilities of the system (see Shared Cybersecurity Services [4.7](#)), and Maintenance Plan (see [10.3](#)).

## **10.15 [OM-06-02] Backup and recovery management**

### **10.15.1 Requirement**

The asset owner shall establish, apply and maintain a process for backing up at regular intervals or predefined triggered event, and recovering of the railway application to a stable state in a timely manner.

The backup and recovery management process shall address the following aspects:

- a) conducting backups (frequency or predefined triggered event, content, storage)
- b) testing and recovering backups (frequency, means of validation, conditions of deployment and procedure to restore from a backup)

### **10.15.2 Rationale and supplemental guidance**

Backup and recovery management should be aligned with business continuity management needs (see [5.10](#)).

#### Backup:

The availability of up-to-date backups is essential for recovery from a failure or misconfiguration and should allow restoring / recovering system in operation after an incident.

The asset owner's backup strategy should include, where appropriate, the following:

- frequency (or when backups should be performed e.g. prior to and after changes),
- partial backups, snapshots,
- secure storage (availability, integrity and confidentiality) and access control,
- measurements to prevent malware disruption (e.g. off-line backups to prevent hidden encryption, network disconnection after the job),
- testing,
- logs,
- recovery time objectives
- retention (how much backups are necessary and time span; how and when deleting old backups).

The backup process should not affect the normal operations.

**Recovery:**

The recovery of backups for an application should be applied according to step-by-step procedure defined at higher level (see 5.10), capabilities of the system (see Shared Cybersecurity Services 4.7), and Maintenance Plan (see 10.3).

The recovery strategy should include, where appropriate, the following:

- purpose, scope and audience,
- roles and responsibilities,
- key contacts and (internal and external) communication channels,
- conditions for plan activation and deactivation,
- order of recovery for operations,
- recovery plans for specific operations, including recovery objectives,
- required resources, including backups and redundancies,
- restoring and resuming activities from temporary measures.

The recovery procedure should be tested, reviewed and, where appropriate, updated at planned intervals and following significant incidents or significant changes to railway application or risks.

Components with firmware and parameters only (e.g. network devices, PLC, smart sensors) without operating or hosting system, could be excluded from periodic restore testing.

For safety related applications, the restore process should first proceed on redundant or shadow systems and not on the active running systems.

NOTE For further information, see also:

- [IEC 62443-2-1:2024 \[52\]](#) AVAIL 2.1 to 2.5
- [IEC 62443-2-4:2023 \[50\]](#) SP.09.07; SP.12.01; SP.12.06; SP.12.09
- [IEC 62443-3-3:2013/COR1:2014 \[59\]](#) SR 7.3; SR 7.4

## **10.16 [OM-07-01] Security monitoring**

### **10.16.1 Requirement**

The asset owner shall establish security monitoring capabilities in order to ensure detection, reporting, handling, and timely response to security events in its railway application.

The asset owner shall define the scope of security monitoring (the concerned railway applications or a part of them) according to risk management conclusions and regulatory constraints.

### **10.16.2 Rationale and supplemental guidance**

To establish effective security monitoring, the asset owner should begin by defining their requirements based on risk assessments, threat modelling, and compliance obligations.

Event detection should include security alerts (logs) generated by either end-devices, network-based sensors, host-based sensors or security solutions. The criticality of the railway application, and its physical and logical environment should be considered when selecting effective monitoring strategies.

NOTE 1 Network-based sensors include security solutions that monitor network communications and leverage both anomaly-based and signature-based detection techniques. Use of port mirroring, or non-intrusive devices such as network taps could be preferred.

NOTE 2 Host-based sensors include security logs generated by the device manufacturer or security agents running on the host device, when applicable.

EXAMPLE Using network-based sensors including deep packet inspection (DPI) of protocols used in the railway application.

All detected events should be reported for handling to a security operations centre (SOC), CSIRT or other central entity/team using SIEM or using SCADA to aggregate information (or filter false positives in operation) to be sent to a SIEM, with an optional intermediate step of event handling at an operational control centre for larger, distributed organizations. Security Operations Centre should engage and collaborate with maintenance personnel as necessary.

The architecture and design of management and monitoring systems should support the [IEC 62443-2-1:2024 \[52\]](#) and [IEC 62443-3-3:2013/COR1:2014 \[59\]](#) when this requirement has been selected during the risk assessment or during the security design, see [Clause 7](#) and [Clause 8](#).

Standardized formats should be used for events reporting such as Syslog (RFC 5424).

Reported logs should be stored based on the log retention policy of the railway duty holder and should be protected from tampering. The detection and reporting structure should be consistent with the definition of security zones and conduits and should be structured in a way it will not introduce new security risks.

An holistic approach to security monitoring should be taken by ensuring all the relevant monitoring scope is considered and the appropriate mix of detection techniques is used to identify ongoing threats. For example, correlating system cybersecurity logs, with network intrusion detection alerts and other operational information such as the one coming from predictive maintenance systems can be a very efficient monitoring approach.

The SOC, CSIRT or other central entity/team using SIEM or SCADA should handle the reported events, and conduct further analysis, correlation, and prioritization of events. There should be defined workflows between the SOC to operations and maintenance personnel, to ensure smooth collaboration.

## **10.17 [OM-08-01] Decommissioning management**

### **10.17.1 Requirement**

The asset owner shall establish, apply and maintain a documented process for decommissioning or removal of subsystems and components, referring to cybersecurity guidelines when available, to ensure that no sensitive information can be extracted.

### **10.17.2 Rationale and supplemental guidance**

A decommissioned component which is being scrapped, or an out of service component for repair, may contain sensitive information like binaries and configurations files or even cybersecurity secrets like private keys or certificates.

The asset owner should maintain a decommissioning policy that addresses the erasure or destruction of sensitive data to avoid release of data during, for example, transportation, repair, or disposal. The policy should be enforced with service providers.

In cases where information cannot be erased from a component scheduled for repair, organizational measures should be applied to the supply chain to prevent leak of sensitive data.

NOTE 1 Further information about sanitization techniques could be found in NIST SP 800-88 which describes the different methods for sanitization

NOTE 2 See [5.11](#) for data protection management.

## **Annex A** **(informative)**

### **Handling conduits**

#### **A.1 General**

In IEC 62443-3-2:2020 [51] conduits are the links or channels between zones. Similar concepts have also been discussed in IEC 62443-2-1:2024 [52], but within that standard, communication is only discussed from a safety perspective. Railway specific recommendations for partitioning a SUC is given in 7.5.

In principle three types of implementations for conduits can be used to connect zones, depending on the different security levels of the zones to be connected and the allowed way(s) of communication:

- Transparent conduit such as basic gateway (connecting zones of same security level); or
- Filtering conduit such as firewall appliance, router or proxy (allowing a zone of lower or equal security level to communicate with a zone of a higher security level); or
- Unidirectional conduit such as data diode or network TAP (allowing output from a higher security level zone to other lower-level security zones).

NOTE 1 The gateway protects integrity and potentially confidentiality of data flow between two gateways. A major drawback is that it connects two networks transparently without separation, segmentation, or filtering.

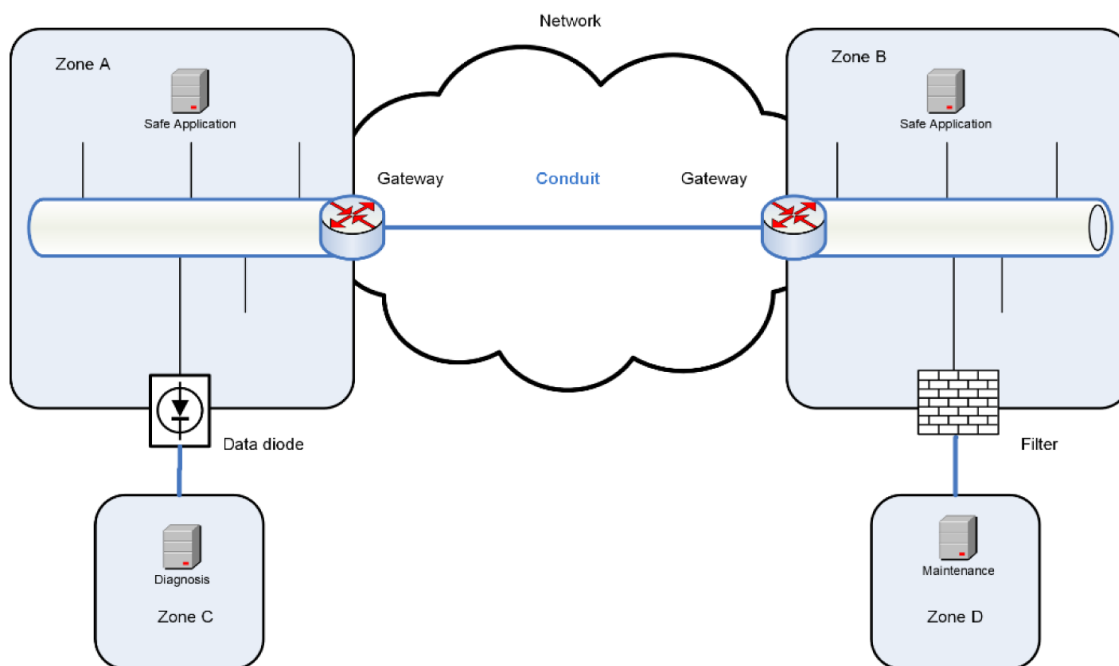
NOTE 2 Firewall devices are also complex and require frequent security patches. In the filtering conduit, filtering rules can get very complex, and are not effective against masquerading attacks.

NOTE 3 When an unidirectional conduit is implemented in hardware (using physical unidirectional flow principles), it is very difficult to remotely compromise. It is therefore more secure than software data diode, which could have other vulnerabilities that can be exploited. In a unidirectional conduit, it should be distinguished how it is implemented such as in hardware or software.

NOTE 4 Network TAPs provide a complete full-duplex copy of network traffic, passing all information including physical level errors.

In IEC 62280:2014 [58] only the case of a transparent gateway is considered and two zones with safety applications are connected with the same security level.

Figure A.1 shows an example of four zones connected by three different types of conduits.



**Figure A.1 – Zones and conduits example**

This [Annex A](#) aims to clarify the requirements for conduits from [IEC 62443-3:2013/COR1:2014 \[59\]](#) and their relation to existing standards such as [IEC 62280:2014 \[58\]](#) and cybersecurity codes of practice, for example, protection profiles for conduits.

## A.2 Protection profiles for conduits

A protection profile is a generic cybersecurity requirement specification (CRS) for a class or type of components or specific configuration setting of different components. Its intent is to enable the re-use and tailoring of cybersecurity requirements. Protection profiles might also act as Codes of Practice.

The general table of contents of a protection profile is:

- a) Description of the component including features, intended use, users and assumptions
- b) Asset protection including environment and essential functions
- c) Threat model
- d) Security objectives (high-level requirements associated to the specified asset protection).

As protection profiles related to components used for the protection of conduits already exist, the question arises how such protection profiles can be used in relationship with railway cybersecurity. One option is to use existing protection profiles as a code of practice. To support standardization, another option may be more useful: security objectives are included in the protection profile, which are traceable to 62443 standard and associated SL-T.

**EXAMPLE** If the security objective for a gateway would need that credentials are stored securely, then this objective can be mapped to CR4.1 (Information confidentiality), CR4.2 (Information persistence) and CR4.3 (Use of Cryptography) from [IEC 62443-4-2:2019/COR1:2022 \[11\]](#).

This way, the objectives can be mapped to the requirements, but also tailored to the SL-T needed in the particular case. Additionally, requirements that are not applicable in the specific context would be excluded as they are not necessary to fulfill any security objective.

Some conduits have been handled successfully by protection profiles e.g. gateways by DIN VDE V 0831-102 (based on Common Criteria). ANSSI has already worked out protection profiles for all three types of conduits (gateway, data diode, filter) for industrial automation [26].

NOTE See also [IEC TS 62443-1-5:2023](#) [27]

**Annex B**  
(informative)

**Handling legacy systems**

## General

In the short- and medium-term future, there will be few components which will implement a set of security requirements compliant with the [IEC 62443-4-2:2019 \[55\]](#) standard. Most current products were designed through processes that did not incorporate comprehensive cybersecurity assurance, but regarded only dedicated aspects like unauthorised access in [IEC 62425:2007 \[28\]](#) or masquerade in [IEC 62280:2014 \[58\]](#). However, a set of security measures can still be defined to ensure a minimum level of security protection for an installation including such products.

This annex provides guidance on defining technical and organizational countermeasures when integrating legacy systems or operating legacy railway applications.

Detection of most cyber-attacks is possible thanks to a mature level of security operation, e.g. an organization managing and operating a security program according to [ISO/IEC 27001:2022 \[12\]](#) or [IEC 62443-2-1:2024 \[52\]](#). Some measures may also support limited activities to recover from a cyber-attack.

**NOTE** In terms of global relevance, [IEC 62280:2014 \[58\]](#) is an international standard that is used worldwide in safety related systems, includes legacy systems and could be adopted as a CoP in this standard. Taking that [IEC 62280:2014 \[58\]](#) as an example, Category 1 transmission systems as defined in [IEC 62280:2014 \[58\]](#) and Category 2 transmission systems, including radio systems, are intended that the system achieves the minimum security level described in this Annex as a legacy system, provided it is properly maintained and operated.

### B.1 Basic security risks

#### B.1.1 A denial of service attacks and vulnerability exploits

A DoS attack and vulnerability exploitation are typically possible if an attacker gets access to the operational network. The attacker sends either malformed data or huge volumes of data that will make the targeted devices unavailable (i.e. unresponsive). When an attacker exploits one or more vulnerabilities of the attacked devices, the attacker can render the device unavailable or compromise the integrity of the device (e.g. change data and code). An attacker can also use a compromised device as a new attack device.

Such attacks can be achieved when the attacker gets physical or logical network access to the operational network to create or attach an attack device. Attaching attack devices to the physical network can be impeded by physical security of the installation as detailed in [Clause B.4.2](#). Detection of such attack devices can be achieved by regular inspections of the installation and by network monitoring.

Compromising an existing device via logical access requires remote access to the operational network. This can be mitigated by air gapped network design and network segmentation. If an air gapped network is not possible, the operational network should be separated from the non-operational network by a data diode (when data are only leaving the operational network) or a Demilitarized Zone (DMZ) when bi-directional communication is required.

#### B.1.2 Impersonation attack

During an impersonation attack, an attacker sends a message with correct syntax to a target. The attacker typically forges all required data (as IP addresses, sequence numbers, identifiers, etc.). Simple attacks just replay a previously sent message, more sophisticated attacks emulate the interface protocol. One variation is the Man-in-the-Middle attack, where arbitrary data from and to the attacked device can be altered.

Since a legacy device might not strongly authenticate the sender of the request, it cannot distinguish between a permitted message and a specifically crafted and forged message.



In order to execute an impersonation attack, the attacker requires either physical access (to place an attack device in the operational network or compromise an existing device) or remote network access. Adding an attack device can be detected by regular physical inspections and by network monitoring. Compromising an existing device via remote network access typically involves several network activities that can be detected by an intrusion detection system. The problem is much more complex if rogue devices are only temporarily attached.

## B.2 Basic process activities

### B.2.1 General

The following process activities enhance a legacy system's protection against cyber-attacks and complement the basic technical measures already present. It is assumed here that no activities in earlier life cycle phases can be carried out, e.g. because of legacy systems or pre-developed components already in place.

### B.2.2 Zoning

Even if no SL is assigned, components of similar functions and security requirements should be integrated in one security zone. The boundaries of security zones should be protected by security gateways, firewalls or data diodes.

As a default, the Purdue model can be used to group components into zones:

Level 0:	All sensors (e.g. axle counters, track circuits, odometers) and actuators (e.g. point machines, signals, brakes) that provide the basic input and output of the control system.
Level 1:	Local Control: All elements that receive input from sensors or provide output to actuators, elements that process data and elements that send or receive data to or from an area control element.
Level 2:	Area Control: All elements that are required for area control or train control functions.
Level 3:	Overall Control: All elements that are needed for central control and business logic (as planning and disposition).
Level 4+5:	The Enterprise/Office network of the railway duty holder.

### B.2.3 Defence in depth

The principle of the defence in depth approach is to ensure that countermeasures are still in place even if a security breach has occurred. Some contributors in Defence in Depth can be derived by example from the following NIST CSF principles to provide a possible solution:

- **Protect** - Prevent attacks against assets to ensure the *Availability, Integrity* and *Data Confidentiality* of systems and information
- **Detect** - Detect abnormal behaviour and trigger alerts for the rapid identification of a security breach, incident or suspect activity
- **Respond** - Respond to a detected security incident by taking appropriate actions for recovery.

Application of the defence in depth principle can be based on the system and component requirements of IIEC 62443-3-3:2013/COR1:2014 [59] and IEC 62443-4-2:2019/COR1:2022 [11]. The requirements of IEC 62443 series can be taken as a guideline to achieve compliance with the NIST principles of security:

- a) **Protect**
  - b) Authentication of users (human users, devices, software)
  - c) Access control & access control process - Control of access to devices
  - d) System integrity (software and hardware)

- e) Segmentation of the network (separation of essential/safety devices from non-essential)
- f) Comprehensive software patching process
- g) **Detect**
- h) System monitoring (situational awareness)
- i) Diversity (safety and security concept essential devices, redundancy)
- j) System and network segmentation

NOTE Awareness is a very helpful measure(see [Clause B.3.8](#))

k) **Respond**

- l) System monitoring (situational awareness)
- m) Diversity (safety and security concept essential devices)
- n) Incident reporting.

As a result, there should be more than one defence that needs to be overcome to breach the system which could be selected and weighted from the variety of the security functions according to feasibility and cost.

#### **B.2.4 Basic risk analysis**

Like newly developed systems, legacy systems should be analysed with respect to security in a structured and comprehensive manner. However, legacy systems are already completely defined while the approaches for risk assessment in [Clause 7](#) are more targeted at systems to be developed. Thus, for legacy systems, potential attack scenarios could be addressed first by identifying and mitigating known design weaknesses or vulnerabilities.

Attack trees are one possible way to systematically identify attack vectors for legacy systems and possible mitigations to underlying vulnerabilities. Attack trees are used to analyse the system in a top-down approach, starting from an abstract “loss of assets” scenario and resulting in possible threats at specific attack vectors.

Dedicated vulnerability databases, e.g. based on Common Vulnerability and Exposures (CVE), are suitable sources for the identification of vulnerabilities in utilised software modules and third-party libraries. Another approach to find vulnerabilities within the system can be penetration testing.

A qualification of attack vectors helps to establish an attack cost model. Based on the outcome of the analysis, additional countermeasures may be prioritised. Measures to reduce the attack surface should be considered.

#### **B.2.5 (Re-)Commissioning**

The following activities are recommended during (re-)commissioning:

- Check of applied basic security mechanisms (e.g. a subset from [Clause B.4](#))
- Create a complete list of all network capable assets
- Create a restoration point / backup of all assets.

#### **B.2.6 Site acceptance test (SAT)**

For a SAT, all security mechanisms related to the essential functions should be tested. This includes the following list:

- If hardening measures have been implemented, the effectiveness should be demonstrated (e.g. disabled services, changed default passwords, etc.)
- Restoration of assets should be demonstrated
- Forged attacks by penetration testers should be visible in a IDS / SIEM if exists.

Additionally, photos of the final installations should be taken and archived for later use.

### **B.2.7 Operation**

The following activities are recommended during operation

- Visual inspection of installed systems (with help of installed-time photos)
- Validation of list of network capable assets
- Check of restoration capabilities (is the backup still accessible and still up-to date?)
- Security operation according to ISO/IEC 27001 or IEC 62443-2-1.

Security operators should monitor the SIEM (or IDS) as a minimum during normal office hours. Alarms should be analysed and investigated.

If an incident is identified, a standard defined procedure of handling the incident should be executed. This typically involves activities as triage (list indicator, type of compromise, amount, criticality and location of affected devices), investigation (evidence collection, analysis of evidence), communication (internally, externally), and remediation (network device shutdowns, clean-up, plan rebuild, plan prevention).

Special care should be taken on maintenance activities, especially on legacy systems where no cyber controls are available. In such cases, maintenance activities, potentially interfacing the unprotected core of the system, can be a threat vector. A dedicated risk analysis considering the maintenance operation could help managing those risks.

### **B.2.8 Training of personnel**

Advanced attacks need escalation of privileges and interaction with legitimate users e.g. phishing attacks. Personnel should be regularly trained. Awareness of cybersecurity risks should be kept at a high level.

### **B.2.9 Asset inventory**

It should be ensured that systems are known in depth and it can be analysed where it is used and which versions are in use.

## **B.3 Basic security countermeasures**

### **B.3.1 General**

This clause describes the suggested cybersecurity measures for legacy devices.

### **B.3.2 Protect installation**

In order to prevent unauthorised access to the operational network, the access should be physically restricted.

Access to installations, especially on the operational network, should be restricted to authorised personnel only.

Any installation should be protected according to the protection classes of IEC TS 22237-6. The standard lists a set of physical and technical access controls according to protection classes

(starting from the outer zone or fence, moving inwards to the building, then the inner building zones and individual room). The technical measures may include security lighting, video surveillance, intruder alarm system, access control and alarm monitoring.

Track-side installation or installations in other open areas (e.g. on-board installations on trains) should be secured by closed cases according to resistance class 3 ([EN 1627:2021 \[29\]](#) as example). If the specific installation allows for access to the operational network, additional elements to detect intrusion in the metal cases should be considered as a means to initiate a visual inspection.

### **B.3.3 Regular inspection of installation**

Installations of equipment in the operational network, especially the locations of installed equipment such as cabinets, racks and cable routes, should be inspected visually for modifications and additions on a regular basis.

Photos of the installed equipment help to identify modifications. It is therefore recommended to have access to the photos of the original installation during the visual inspection (e.g. as printouts or on a mobile device).

Seals can be used to reveal modification and tampering of installations. They can reduce the need for detailed inspection unless the seal is broken.

### **B.3.4 Network / perimeter protection**

Assets of a railway system are least susceptible to cyber-attacks when operated in an air gapped network. Any access to or from the operational network is then prohibited by the network design (strict physical separation).

If data needs to be sent from within the operational network, a data diode (allowing only uni-directional data flow) should be used. Such a device prevents access to the operational network from the outside, but still allows the sending of data outside to the external network. This allows for remote diagnosis, export of data to cloud systems, and external intrusion detection analysis.

For example, if bi-directional data flow is required between the operational network and an external network, a demilitarized zone (DMZ) is required. A [DMZ \(3.1.48\)](#) usually consists of two application level firewalls and at least one bastion host. The bastion host is a hardened server that terminates the data transfer between the two networks. The deny all principle (address ranges, protocols or commands) should be used to restrict transmissions.

**NOTE** Security devices that can provide similar functionality, such as firewalls or gateway, can be used in place of data diodes and DMZs.

### **B.3.5 Network segmentation / restricted data flow**

Operational networks should be segmented to limit the consequences of a successful attack on one part of the network, impeding access to other parts.

Network segmentation requires detailed analysis of the existing network and the data flow of the installed devices. This analysis results in a communication matrix which can be used to restrict the routing of the network resulting in a segmented network.

A network blueprint can be created for standard system configurations. It allows the use of configuration tools that generate the required configuration files for the network elements.

### **B.3.6 Monitoring and network management**

Existing railway systems commonly monitor faults in each subsystem or device and deviations from normal operation in real-time, issuing alerts directly to operators or maintenance personnel

in the event of an incident, prompting a response. These alerts also contain information related to cybersecurity incidents. In contrast, for systems that lack a monitoring or management that do not have a direct interface with an existing monitoring or management, pre- monitoring or management should be installed. This pre- monitoring or management gathers cybersecurity alerts and related information and facilitates their transmission to the SIEM or equivalent organizations.

In respect and to force resilient subsystems, for OT or legacy environments following principles depending on the maturity and security requirement of this entity are highly recommended:

- Use pre-monitoring or management systems (e.g. existing vendor specific engineering system as partial asset management source) like IDS, SIEM, Asset management, real time, network management in every AO responsible entity
- A fault of a corporate wide monitoring or management system on Purdue levels 4 or 5 should not have an impact of the availability or essential functions in the OT environment
- A fault of a pre-monitoring or pre-management system on Purdue level 3 should not have an impact of the availability or essential functions into other OT entity
- Collect all security relevant messages from devices on Purdue level 1 to 3 within the responsible entity
- All necessary information should forward from these pre-systems to the corporate monitoring systems and parallel selected messages to the SCADA system to enable the dispatcher to react on behalf of known maintain operation issues and recognise false/positive in daily business.

### **B.3.7 Network management system**

An [NMS \(3.1.93\)](#)(NMS) can be used to detect new devices on the network when such devices use a different MAC address than the existing ones of the installation. Additionally, configuration changes of network devices, such as managed switches, routers and firewalls, can be detected. The NMS for asset management should itself be protected against cyber-attacks, as the NMS can be used as an entry point for a cyber-attack on the SUC if the confidentiality and integrity properties of the NMS are compromised.

An NMS should be installed in conjunction with managed switches. It should be configured to monitor all network devices and to create alerts when unknown devices appear in the network or when the configuration of network devices changes. If a Security Incident and Event Management System (SIEM) is used, the alerts should be forwarded to the SIEM.

The operator should monitor the alerts generated by the NMS and react to those alarms (e.g. activities to find and inspect the new device, find the reason for configuration change, etc.).

Passive network monitoring is recommended as active network monitoring may disrupt the availability of OT network.

### **B.3.8 Intrusion detection / SIEM**

An IDS requires the analysis of the network data (or at least the meta data of the transferred data) from relevant locations in the network. Depending on the network architecture, this data can be retrieved by means of one or more sources (e.g. network taps, mirror ports, special PLC interface or data diodes) within the operational network.

Alerts from an IDS can be picked up by a [SIEM \(3.1.149\)](#) . The security information event management (3.1.146) provides an overview of security alerts for security operators and can correlate these events with log entries from network devices.

### **B.3.9 Virtual private networks (VPN)**

If site-to-site connectivity is required over an open network (e.g. public networks as Internet), [VPN \(3.1.193\)](#) technology should be used. Typically, access routers or wireless modems provide integrated VPN capabilities. VPN functionality should be enabled to setup a secure channel over a public network.

VPN has a security drawback since they essentially bridge across and combine two distinct networks. It is therefore advisable to include the VPN connections in the overall network analysis and look for network segmentation and filtering opportunities at the VPN end points.

### **B.3.10 Redundant communication**

If redundant communication channels are used in the operational network, this can be used to further enhance the detection rate of a Network Intrusion Detection System (NIDS).

If an attacker influences only one of the two channels, the NIDS can detect this attack instantly.

An alarm will be triggered when one of the channels is not available. If such an alarm is triggered, a physical inspection of the communication path (from device to the communication end point) is recommended, since this can be an indication of an attacker inserting an attack device in the communication path (e.g. for a Man-in-the-Middle attack).

### **B.3.11 Security gateway**

A security gateway (SG) can be added to each communication channel of a system or behind a media converter in a field cabinet. An SG should be placed at each end of the communication path. The SG shields a non-secure legacy device from unauthorised access and protects its communication with other devices. Man-in-the-Middle attacks from the network are successfully prevented. Also, vulnerabilities of the device cannot be exploited from remote locations.

A security gateway can feature filtering capabilities (firewall) to protect inside network from any unexpected access from outside.

Security gateways typically provide confidentiality through encryption (e.g. on transport layer by TLS/DTLS) for all outgoing and incoming network traffic in a many to many relationship. This allows use of the SG not only at the field level, but also at central locations.

The communication path between two security gateways is protected. However, the path between SG and the legacy device is not protected. Therefore, additional protection mechanisms (e.g. door contacts and other physical access restrictions) should be in place.

SG can be equipped by digital I/Os that can be used for door contacts or other tamper protection devices. When the I/O status changes, an alarm is sent via the diagnostic interface.

### **B.3.12 Handling USB connectors**

In legacy systems, some data might be transferred by using mobile devices like USB devices. To protect the system against malware infections, those devices should be checked for malware continuously or limited to only a one-time use.

- a) Prior: whitelist the system, if possible.
- b) Unused ports should be protected by mechanical USB locks.
- c) If a USB device gets connected, the system should detect it and log it.

Automatically logged-messages (for USB detection as for others log-messages) should be sent to the existing supervising platform (as responsible SCADA or dispatcher systems) and process responsible SIEM, NMS, asset management systems to allow the process engineers to decide if messages are false/positive, positive and what are the next steps

concerning possible maintenance work to keep operating disruptions as low as possible. These log-messages should also be forwarded (as-is or after filtering false/positive, depending on the capacity of analysis for OT systems, to the corporate SIEM, NMS, asset management.

If no supervising platform can be used to analyse automatic log-messages, appropriated measures (such as organizational SecRACs and enforced protection) can be taken for USB manipulation.

NOTE Handling USB or mobile devices described in [Clause I.5.4](#).

### **B.3.13 Encryption**

To ensure confidentiality, integrity, and authenticity of data when data are transmitted via wireless communication, encryption algorithms should be used.

IEC 62280:2014 (7.3.9 Cryptographic techniques) can be referred to implement appropriate key management for encryption.

Legacy systems that do not incorporate state-of-the-art technologies may be updated to the latest technology within economically reasonable limits at the next scheduled major release.

### **B.3.14 Authentication**

It is also desirable to implement authentication control as described in [Clause 8](#) even in legacy systems. However, instead of authentication, identification of connecting devices by assigning an ID to each device may be used in legacy systems. In such cases, it is desirable to ensure that the assigned ID is properly managed and cannot be altered by others.

## **Annex C**

### **(informative)**

## **Cybersecurity design principles and system requirements**

### **C.1 Cybersecurity design principles**

#### **C.1.1 Introduction**

##### **C.1.1.1 Cybersecurity design principles**

Cybersecurity design principles provide a roadmap that influences and underpins the process of design and architecture of a system towards meeting its desired security objectives. These design principles also support more detailed requirements that are implemented in a system, enabling improved cybersecurity.

Cybersecurity design principles reflect industry experience and have been derived from best practice and review of existing sources and standards. The selection of the principles is left to the product or system designer at the start of the design process. It is recommended that the principles are selected before the start of design activities to allow for synergies to be identified between principles and so that the security requirements are mapped to the chosen design principles for traceability and consistency.

The implementation of cybersecurity design principles is enabled through collaboration of the relevant stakeholders: the asset owner, the maintainer, the system integrator, and the product supplier. Implementation of cybersecurity design principles is challenging to achieve when a product or system designer is working alone.

##### **C.1.1.1.1 Tailoring and prioritisation**

The principles influence security architecture, design choices and technology adoption throughout the life cycle of products, services, and systems. They are especially useful when security requirements come to conflict with other requirements from other domains, or where limitations due to computer performance or existing (legacy) technologies are present. The cybersecurity design principles are selected and tailored to the railway system and can be used to identify priorities when tailoring the design.

#### **C.1.2 Secure the weakest link**

##### **C.1.2.1 Principle**

Identify and protect all attack vectors in the security architecture.

##### **C.1.2.2 Rationale**

As railway systems normally operate for many years in complex, multi-vendor, international and interconnected environments, it is likely that the robustness of the design will be tested by attackers over time. Cyber-attackers identify and attack first the weakest parts of a system, so security is only as strong as the weakest link in a chain. System designers should therefore consider the weakest links and the least protected aspects in their system at the design stage and ensure that they are secure enough.

Implementation of this principle encourages the designer to consider the security of all the components of the system, looking beyond typical architecture elements such as the protocols used or the interfaces to other systems.



### **C.1.2.3 Guidelines for implementation in a railway environment**

All components, boundaries (internal and external) and data flows need to be explicitly captured and identified and described before the weakest link can be identified in a system or architecture.

A detailed risk analysis (refer to [Clause 7](#)) enables the level of security of a system to be established using methods that define, implement and assess target security levels for a railway system. Even if components are not identified by risk analysis as the most difficult/expensive to protect, implementation of the principle to secure the weakest link principle should be considered.

In many cases, the weakest link of a system is the human one. Implementation of this principle should therefore be considered alongside the “grant the least privilege” design principle when designing every user interaction with the railway applications whereby each user is given the minimum privileges.

A flexible approach to implementation may be required given that legacy systems may contain many weak links. Implementation of the principle also helps to avoid the perception that firewall, encrypted communications, and antivirus software are all that are needed to secure a system.

**NOTE** It is unlikely that a hacker will try to decrypt encrypted communications from train-to-ground if they can simply compromise a maintainer’s laptop, using social engineering, for instance, and installing a malicious software in the train-to-ground communications server.

### **C.1.2.4 System requirements that implement the principle**

Isolation of the system from uncontrolled data, particularly from the non-railway application network:

- SR1.6 Wireless access management
- SR 5.1 (SR 5.1 RE(1)) Network (physical) segmentation
- SR 5.1 RE(2), RE(3) Independence from non-railway application networks, logical and physical isolation of critical networks
- SR 5.2 Zone boundary protection

Identification of the user as the potential weakest link:

- SR 1.6 RE(1) Unique identification and authentication

Prevention of misuse of system functionalities and injection of unwanted code:

- SR 3.2 Malicious code protection
- SR 7.7 Least functionality

## **C.1.3 Defence in depth**

### **C.1.3.1 Principle**

Implement various protections on each attack path to slow down the attacker.

### **C.1.3.2 Rationale**

No single cybersecurity protection is enough to stop an attack.

Implementation of this principle is based on:

- a) Ensuring that no single vulnerability or breach will endanger the system; and

- b) Combining preventative measures that slow down the attacker and detection measures that allow the response team to detect, analyse and respond in order to stop or mitigate the attack.

The basis of defence in depth is the conjunction of several diverse protections each with a different characteristic or security property, and with different behaviours in response to a breach.

The first barrier in following [Figure C.1](#) is physical protection, typically implemented using fences, doors and locks, cameras, and guards. Without trust on who can access the hardware, trust cannot be placed on the data stored on the system.

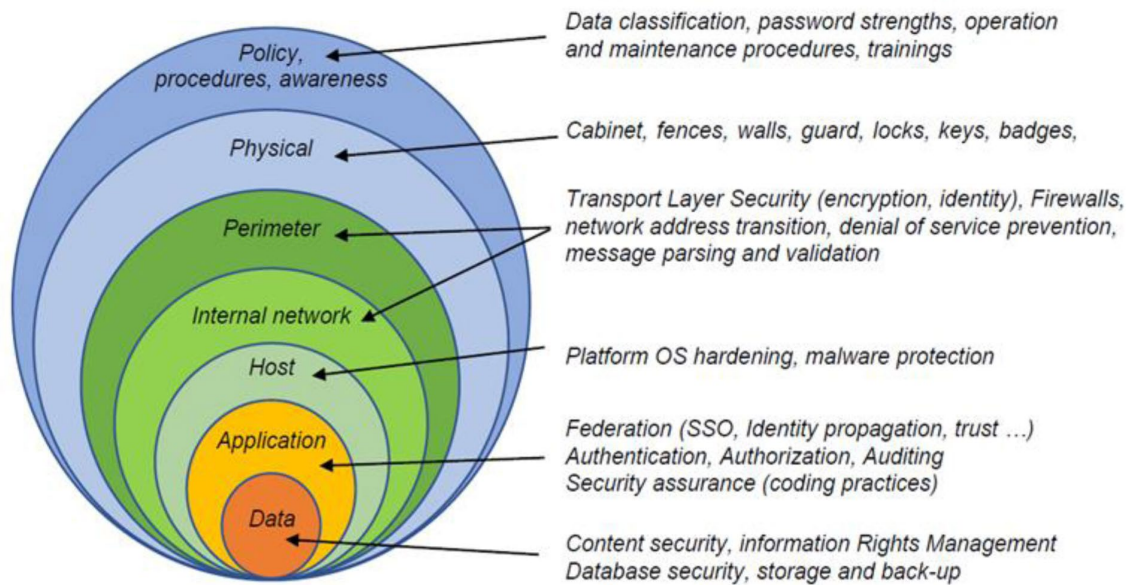
The second barrier is perimeter protection. This is typically implemented through firewall, a proxy inside the DMZ, datadiode, IDS and honeypots. When messages or data enter the network or the system, perimeter protection functions verify the data to ensure that it may cause no harm to the system, either by bringing malicious content, or by providing irrelevant data such as spoofing or forgery.

The third barrier is network access control within a zone. This is typically implemented through asset management, network access control (802.1x, etc.), secure network protocols, IDS, probes, and honeypots. This protection ensures that no unauthorised device is inside the perimeter, bypassing perimeter protection, and able to maliciously interact with legitimate devices.

The fourth barrier is host protection and integrity, implemented as protection at device interfaces and system level. This is typically implemented through host-based firewall, service access control, host IDS, integrity protection and detection systems, hardening and security logging. This protection level should ensure that no interaction with the host is able to undermine the normal behaviour of the host and its guest applications. It is important to protect device interfaces through access control and hardening, but also to detect any anomaly inside the host itself such as an abnormal modification of host integrity.

The fifth barrier is application protection which protects the manipulation of the actual data. This is typically implemented through input validation and authentication, access controls, code hardening and event logging. It ensures that data manipulation is performed by an authorised agent. No application input may modify computing of the data in an uncontrolled manner.

The sixth barrier is data protection. This is typically implemented using hardware data protection through security modules and CPU modes, Operating System protection such as access control, data protection while at rest or on the move through cryptographic means. This level ensures there may be no access to the data in an uncontrolled manner.



**Figure C.1 – Cyber Security in depth example**

#### **C.1.3.3 Guidelines for implementation in a railway environment**

Defence in depth underpins cybersecurity and is used at every level of design, from system level, including physical and operational protection, down to host, application and data level.

An example of the implementation of the defence in depth principle is given by the System Requirements in [Clause 8](#)

Implementation of this principle will balance implementation of cybersecurity measures with meeting the safety critical functions of the operational environment as well as the availability of resources for safety-related functions.

**NOTE** The correct timing requirements for the safe execution of the safety critical functions may be adversely affected by the security mechanisms, requiring an architecture-based implementation. This may lead to incomplete implementation of host protection mechanisms that may also need a delegation on network or perimeter protection level.

#### **C.1.3.4 System requirements that implement the principle**

Limitation of network flow:

- SR 5.1(RE(1)) Network (physical) segmentation
- SR 5.1 RE(2), RE(3) Independence from non-railway application networks, logical and physical isolation of critical networks
- SR 5.2 Zone boundary protection

Usage of secure network protocols:

- SR 4.3 Use of cryptography
- SR 5.3 General purpose person-to-person communication restrictions

Management of device interfaces usages:

- SR 7.1, RE(1), RE(2) Denial of service protection, manage communication loads, limit DoS effects to other systems or networks
- SR 7.2 Resource management
- SR 3.2 Malicious code protection

- SR 3.5 Input validation

#### **C.1.4 Fail secure**

##### **C.1.4.1 Principle**

Ensure that no degraded mode of the system would weaken its security.

##### **C.1.4.2 Rationale**

A fail secure function is designed such that the system remains in a secure state, in case of a failure of the security function or the secure system delivering the function.

For example, in the case of loss of power, the train door remains locked, meaning it remained secure. This is in contrast with a safety-based approach which requires the door to be unlocked following failure of the system.

Strict standards and legislation requirements for product safety mean that the fail secure principle can only be followed in cases where no product safety requirement is undermined or contradicted through its implementation. In all other cases the product safety requirements and architecture should supersede the fail secure principle.

Implementation of this principle is applicable in areas with no safety requirements and architecture, or if implemented elsewhere, as a minimum there should a risk analysis showing no indication of compromise of any safety requirement.

##### **C.1.4.3 Guidelines for implementation in a railway environment**

Fail secure design is linked to the reliability of a railway solution or a security function. The scope of implementation starts with fall-back and restart conditions should computation performance be lost, such as timeouts and power cuts, and may end with complex redundancy concepts.

A reduction of complexity is always considered, as it may be more practicable to have one clear fall-back strategy than a variety of different local approaches. If existing safety requirements are present, this architecture is not modified. The architecture may then be reused as part of a fail secure concept.

Implementation of this principle may be supported by the more in-depth discussion of some system requirements of [IEC 62443-3-3:2013/COR1:2014 \[59\]](#) as system level requirements and component requirements should be carefully defined and allocated in the fail secure case.

Explicitly, interpretation of the principle includes the following:

##### **SR 5.2 RE 3 Fail close**

- The control system provides the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close).
- Given product safety requirements, fail close is a broadly accepted security requirement at system level. It is not only applicable following an attack but also as a fall back condition in case of a failure of the security function itself.

##### **SR 3.6 Deterministic output**

- The control system provides the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack or failure state.
- Given product safety requirements, deterministic output is a system requirement that addresses the outputs of a component. The system level fall-back mechanism will be

affected by this principle. This may then lead to the break down on component level for the predetermined state of outputs. (Refer CR 3.6 Deterministic output)

#### **C.1.4.4 System requirements that implement the principle**

Use Control:

- SR 2.5 Session lock
- SR 2.6 Remote session termination

System Integrity:

- SR 3.6 Deterministic output
- SR 3.7 Error handling

Restricted Data Flow:

- SR 5.2 RE 3 Fail close

Resource Availability:

- SR 7.1 Denial of Service protection
- SR 7.4 Control system recovery and
- SR 7.5 Emergency power supply

#### **C.1.5 Grant least privilege**

##### **C.1.5.1 Principle**

Provide users with only the minimum access rights necessary to perform their mission.

##### **C.1.5.2 Rationale**

Each component should have allocated only those privileges needed to accomplish its specified functions. No additional privileges should be granted.

Typically, during a more sophisticated attack, a hacker looks for a software component that has privileges allowing it to read confidential data, download malicious software, write and run scripts, send commands impersonating authorised user. Once such a component has been discovered, there are many ways to substitute its original code with a malicious one and then use its privileges to do whatever is in the scope of the attack. The fewer privileges the component has, the lesser interest it poses to an attacker.

Interaction between components from different suppliers and even from different owners are necessary and frequent as part of operations. This interaction greatly increases the likelihood for a railway software component to encounter a hacker in search of privileges to exploit with malicious software. Railway components and systems should be designed with this in mind.

##### **C.1.5.3 Guidelines for implementation in a railway environment**

Least privilege is a pervasive principle and is reflected in all aspects of the system.

For instance, different users of the same railway application should be presented with different interfaces, carefully designed to give them all the tools they need to accomplish their tasks and nothing more. The choice of the right interface for a given user is possible only after the user has been identified and authenticated by the system and correct privileges have been retrieved and assigned to the user. The user simply cannot do what the interface does not provide.

Least privileges principle is not limited to giving users the right authorisations, it is also related to the notions of modularity and encapsulation. A good system design is normally characterised

by a high level of modularity. A module is designed to do some specific functions and nothing more. Even if internally it could do something else, because it has full access to low-level components, it exposes to other modules only what it has been designed to do. In this way, the module reduces the privileges of its user to the minimum required. In a railway environment, this is a typical way to design safety-related systems.

When using COTS, least privileges principle should be confronted with the fact that COTS are normally designed to meet the largest possible application needs. Commercial operating systems running in many industrial environments and railway COTS normally have many software components that are not really needed for the specific application but are nevertheless available to the user. The effort to apply the least privileges principle to COTS should be carefully considered or hardened such that unwanted or unused features are not made accessible.

Privileges have to be allocated on a need-to-know basis independent of the access privileges to the system.

#### **C.1.5.4 System requirements that implement the principle**

Identify and authenticate human users, devices, and processes:

- SR 1.1 Human user identification and authentication
- SR 1.2 Software process and device identification and authentication
- SR 2.1 Authorisation enforcement
- SR 2.1 RE(1) Authorisation enforcement for all users
- SR 2.1 RE(2) Permission mapping to roles
- SR 2.1 RE(3) Supervisor override
- SR 2.1 RE(4) Dual approval

Protect confidential information:

- SR 3.9 Protection of audit information
- SR 4.1 Information confidentiality
- SR 4.1 RE(1) Protection of confidentiality at rest or in transit via untrusted networks
- SR 4.1 RE(2) Protection of confidentiality across zone boundaries
- SR 7.7 Least functionality

#### **C.1.6 Economise mechanism**

##### **C.1.6.1 Principle**

Use a simple and clear design to implement system functions.

##### **C.1.6.2 Rationale:**

A defence in depth approach significantly reduces the attack vectors for a potential attacker over a long period of time. The economize mechanism principle supports this approach by avoiding redundancies and overlaps. Counter measures should be implemented in an efficient, clear and demonstrable manner along with a description of the functional behaviour. This supports security analysis, inspection and testing of the railway solution.

##### **C.1.6.3 Guidelines for implementation in a railway environment**

To implement this principle and demonstrate clarity, simplicity, necessity, extensibility of security implementation, the following methods are considered:

- **Abstraction**

Abstraction is a method to reduce complexity. It is based on the identification and extraction of commonality of security services for different functions or components. Abstracted behaviour can be implemented once and reused, or it can be instantiated multiple times such as for avoiding redundant implementation of functions. Specificities are then detailed through configuration means with useful parameters for different instantiations of such services. For example, in the client - server architecture, programmatic interfaces should be defined clearly and combined with a precise definition of the function triggered by events and time.

- **Encapsulation paradigm (also known as information hiding)**

Definition and documentation of external interfaces (or API) for the planned services or function should start directly after abstraction and before the internal functionality design. Use of encapsulation in the design is often an indicator of good design architecture.

- **Transparency and traceability of requirements from system to component design**

The security function implementing a system requirement needs to be clearly identified. Every component requirement needs to be a traceable implementation of a system level requirement and every system requirement should be implemented on components. Implementation of a system requirement across multiple components is often required.

- **Allocation of cybersecurity functions across the architectural layers**

A layered architecture model is established alongside the defence in depth principle. This supports a clear mapping between cybersecurity functionality and the properties of the architecture. For example, during the implementation of a network filter, the allocation of filtering on data from OSI layer 2 (MAC layer) to layer 4 (protocol layer) needs to be done simultaneously even though they may be on different elements.

- **Allocation of cybersecurity functions within system timeline**

Cybersecurity functionality should also be allocated into the railway solution timeline. It could be a state diagram model, which is helpful to provide a time-based context to the specific security functionality.

Both approaches to allocation support clarity of understanding of the overall system.

**NOTE** In safety-related components, the monitoring of computation time (watchdog) is often in place. The execution time provided to additional security functions need to be taken into account, including for worst-case scenarios. Failing to do so may lead to time overrun conditions.

- **Robustness of implementation**

The design of the security function needs to consider the risks of memory overwriting, timeout conditions, missing events. for all task phases. Sufficient memory allocation and memory management to handle such conditions should be in place.

Fall-back solutions, reset and restart status may be defined in order to manage degradation of computation performances, for example for timeouts and power cuts. This prevents data inconsistencies within the system.

The implementation of security measures should not compromise the execution of system functions as security functions are not isolated and support a functional or safety architecture.

#### **C.1.6.4 System requirements that implement this principle**

Simple Account and access management:

- SR 1.3 (RE(1)) (Unified) account management
- SR 2.1 RE(2) Permission mapping to roles
- SR 2.6 Session control
- SR 2.11 RE(1) Time synchronisation

Layered architecture and zone boundary control:

- SR 5.2 Zone boundary protection

Simple asset inventory:

- SR 7.7 Least functionality

### **C.1.7 Authenticate requests**

#### **C.1.7.1 Principle**

Identify and authenticate the requester before each access to resources.

#### **C.1.7.2 Rationale**

The system should validate the identity of the requester before processing any request to avoid threats related to unauthorised requests. Requesters include human users, components or devices and software processes.

Considering each zone, the need and the level of requests authentication should be determined by the security level applied and its effectiveness in mitigating the associated risks.

#### **C.1.7.3 Guidelines for implementation in a railway environment**

Where technically feasible, identification and authentication is needed for all requests to the system by any user such as for humans, software processes/agents and devices.

Identity and authenticators should be assigned at individual level whenever possible, in particular for high privilege or highly critical systems. The use of shared IDs should only be considered when no alternatives are feasible, and the resulting risk should be assessed.

It is important to authenticate every request received from a sender, not only the first one received; however, to avoid repeating the authentication process for interactive sessions, a secure session mechanism should be implemented. This keeps the user authenticated until the session is terminated.

Authentication can take several forms, including:

- ID and password (often used for users)
- physical token containing a non-exportable cryptographic secret, e.g. a cryptographic signature or private key (sometimes for users, e.g. smart card)
- digital cryptographic certificate, e.g. a X.509 certificate (often for portable/mobile devices; for wireless access with e.g. IEEE 802.1X protocol)
- Message Authentication Codes (for communications between control system components, after establishing a secure and authenticated key exchange, e.g. MAC and HMAC)
- Digital cryptographic signatures (for software images or patches)
- Biometrics or location-based authentication can also be used for users.

Strong / multifactor authentication, such as a token and PIN code for VPN access, should be used for remote access.

Requests for access to critical systems should be authenticated from all available interfaces. This includes other linked systems, user access, for example, via a maintenance port, wireless access, etc.

Credentials such as certificates, password and shared keys, should be updatable in line with the appropriate security policy.

Whenever technically feasible, the authentication processes should be centralised to facilitate management, for example using a directory server, LDAP, PKI or Radius.



For onboard networks, it may be harder to implement centralised authentication. Authentication based on usernames and passwords (often shared) is a commonly used mechanism, particularly for legacy fleets. This should be justified on a risk basis and adequate compensating measures should be taken into consideration.

Any interfaces that are not capable of providing authentication should be disabled wherever possible.

#### **C.1.7.4 System requirements that implement the principle**

Identification and authentication control:

- SR 1.1 Human user identification and authentication
- SR 1.1 RE(1) Unique identification and authentication
- SR 1.1 RE(2) Multifactor authentication for untrusted networks
- SR 1.1 RE(3) Multifactor authentication for all networks
- SR 1.2 Identification and authentication of software processes and devices
- SR 1.2 RE(1) Unique identification and authentication of software processes and devices
- SR 1.3 Account management
- SR 1.3 RE(1) Unified account management
- SR 1.4 Identifier management
- SR 1.5 Authenticator management
- SR 1.6 Wireless access management
- SR 1.6 RE(1) Unique identification and authentication
- SR 1.7 Strength of password-based authentication
- SR 1.7 RE(1) Password generation and lifetime restrictions for human users
- SR 1.7 RE(2) Password lifetime restrictions for all users
- SR 1.8 Public key infrastructure (PKI) certificate
- SR 1.9 Strength of public key authentication
- SR 1.9 RE(1) Hardware security for public key authentication
- SR 1.11 Unsuccessful login attempts
- SR 1.12 System use notification
- SR 1.13 Access via untrusted networks
- SR 1.13 RE(1) Explicit access request approval

Use control:

- SR 2.1 Authorisation enforcement
- SR 2.1 RE(1) Authorisation enforcement for all users
- SR 2.1 RE(2) Permission mapping to roles
- SR 2.1 RE(3) Supervisor override
- SR 2.1 RE(4) Dual approval
- SR 2.2 Wireless use control
- SR 2.3 Use control for portable and mobile devices
- SR 2.12 Non-repudiation for human users
- SR 2.12 RE(1) Non-repudiation for all users

System integrity:

- SR 3.1 Communication integrity
- SR 3.1 RE(1) Cryptographic integrity protection
- SR 3.8 Session integrity

Information confidentiality:

- SR 4.1 Information confidentiality
- SR 4.1 RE(1) Protection of confidentiality at rest or in transit via untrusted networks
- SR 4.3 Use of cryptography

### **C.1.8 Control access**

#### **C.1.8.1 Principle**

Verify user permission before granting access to resources.

#### **C.1.8.2 Rationale**

Due to the open nature of the railway environment, limiting physical access is in general insufficient to control and grant access to resources, assets and objects.

Access to all resources, assets and objects in a railway application should be logically controlled in order to grant access only to authorised entities which includes users, programs, processes or other systems. This applies to direct access or remote access through a LAN or WAN.

The implementation of this principle is strongly dependent on the operational concept. It needs to be established in close collaboration with a role-based and origin authenticatable access model. The account management system should be unified and unique.

#### **C.1.8.3 Guidelines for implementation in a railway environment**

Access control consists of two main types:

- a security policy; and
- technical measures to implement this security policy.

The security policy contains a set of rules (access control process) that specify or regulate how a system or organization provides security services to protect its assets. Implementation is based on one or more of the following means:

- Authentication and authorisation (e.g. IAM, passwords, PKI certificates)
- Network access controls (e.g. firewalls, 802.1x network access control)
- Physical countermeasures (e.g. fences, locks).

The responsibilities of train drivers, signallers and maintenance staff in the system under operation are supported by the security policy. The means of authentication and the persistence (validity duration) of an authentication and granted authorisation balance the cybersecurity needs and operability.

#### **C.1.8.4 System requirements that implement the principle**

Identification and Authentication control - Identification, accounts and login:

- SR 1.1 Human user identification and authentication
- SR 1.2 Identification and authentication of software processes and devices
- SR 1.3 Account management

- SR 1.11 Unsuccessful login attempts
- SR 2.5 Session lock
- SR 2.6 Remote session termination
- SR 2.7 Concurrent session control
- SR 3.8 Session integrity

Network access, portable devices and use control:

- SR 1.6 Wireless access management
- SR 2.2 Wireless use control
- SR 2.3 Use control for portable and mobile devices
- SR 3.2 RE(1) Malicious code protection on entry and exit points
- SR 3.5 Input validation
- SR 4.1 RE(2) Protection of confidentiality across zone boundaries
- SR 5.2 RE(1) Deny by default, allow by exception

Authorisation and rights management:

- SR 2.1, RE(1) Authorisation enforcement (for all users)
- SR 2.1 RE(2), RE(3), RE(4) Permissions mapping to role, override and dual approval
- SR 2.4 Mobile Code
- SR 4.1 RE(1) Protection of confidentiality at rest or in transit via untrusted networks
- SR 4.2 Information persistence
- SR 6.1, RE(1) Audit log accessibility

### **C.1.9 Assume secrets not safe**

#### **C.1.9.1 Principle**

Implement the security of the system without relying on the secrecy of its design or its internal data.

#### **C.1.9.2 Rationale**

Cybersecurity design assumes that an attacker has access to all the system details. Public sources, social engineering on internal sources, mapping tools, decompilers and disassemblers are standard and efficient means for an attacker to get any information that was thought to be hidden in the design.

If it is assumed that secrets are not safe, security can rely neither on the secrecy of the inner design nor on encoded values planted into the system such as hidden keys or undocumented accesses. Implementation of this principle is particularly relevant when choosing communication protocols and technologies. It is also appropriate when considering component access control where people may be interested in planting debugging full access on the component, relying on the secrecy of this access or its hardcoded authenticator.

NOTE Hidden key and undocumented access become de-facto backdoors. Those hidden vulnerabilities can be exploited by a knowledgeable attacker.

#### **C.1.9.3 Guidelines for implementation in a railway environment**

Designing using this principle assumes that an attacker knows everything that you know and they have access to all source code and all designs even if this is not true.

The security of the system should rely on algorithms and protocols that minimize or even nullify the need for secret data. One-way functions or asymmetric protocols have been designed with the following goals in mind:

- The use of a password database in which passwords are being stored via cryptographic key derivation function to verify user's identity claims (through password authentication), and uses no direct recoverable knowledge of the passwords
- A public key, signed by a certificate authority, is a practical approach for the establishment of a secure communication channel, which can be distributed all over the system or even released publicly without compromising the secrecy of the secure channel.

Any remaining secret data hold all the security of the system and should be protected as such. Typical protections are:

- The use of key lifetime, where secrets are changed as soon as their secrecy is not guaranteed, or on a regular basis
- Implementation of Forward Secrecy, where the secret is present in the system for a limited time and recoverable afterwards
- Storage of the secret data in a hardware-based secure container (e.g. Trusted Protected Module) where it is used, but never extracted
- Secret sharing among individuals, where n people need to be together for the secret to be usable.

#### **C.1.9.4 System requirements that implement the principle**

Authenticators and secrets:

- SR 1.5, RE(1) Authenticator management
- SR 1.7, RE(1), RE(2) Strength of password-based authentication, generation and lifetime
- SR 1.8, SR 1.9, RE(1) Public key infrastructure (PKI) certificate
- SR 1.10 Authenticator feedback

Data confidentiality and integrity:

- SR 3.4 Software and information integrity
- SR 4.1, RE(1), RE(2) Information confidentiality
- SR 4.3 Use of cryptography
- SR 7.6, RE(1) Network and security configuration settings

Loss of confidentiality in non-functional scenarios:

- SR 4.2, RE(1) Information persistence
- SR 7.3, RE(1), RE(2) Control system backup

#### **C.1.10 Make security usable**

##### **C.1.10.1 Principle**

Make security user-friendly and easy to adopt.

##### **C.1.10.2 Rationale**

Make security user-friendly and easy-to-adopt.

Aim to avoid compromising usability for security by avoiding complex mechanisms or measures which are not easily adopted due to a poor implementation of human factors.

**C.1.10.3 Guidelines for implementation in a railway environment**

If security controls make performing jobs challenging for operators or maintainers), it incentivizes users to bypass them.

Make security transparent for the users when possible and automate security functions wherever possible to reduce the workload for the operational security teams and become more usable for the end user.

When a compromise between usability and security is implemented it should always be supported by a risk analysis.

**C.1.10.4 System requirements that implement the principle**

Identification and authentication control:

- SR 1.3 RE(1) Unified account management
- SR 1.4 Identifier management
- SR 1.5 Authenticator management
- SR 1.7 Strength of password-based authentication
- SR 1.7 RE(1) Password generation and lifetime restrictions for human users
- SR 1.7 RE(2) Password lifetime restrictions for all users
- SR 1.8 Public key infrastructure (PKI) certificate
- SR 1.9 Strength of public key authentication
- SR 1.9 RE(1) Hardware security for public key authentication
- SR 1.11 Unsuccessful login attempts
- SR 1.12 System use notification
- SR 1.13 RE(1) Explicit access request approval

Use control:

- SR 2.1 RE(3) Supervisor override
- SR 2.1 RE(4) Dual approval
- SR 2.5 Session lock

System integrity:

- SR3.2 RE(2) Central management and reporting for malicious code protection
- SR 3.3 RE(1) Automated mechanisms for security functionality verification
- SR 3.3 RE(2) Security functionality verification during normal operation
- SR 3.4 RE(1) Automated notification about integrity violations
- SR 3.7 Error handling

Information confidentiality:

- SR 4.1 Information confidentiality
- SR 4.1 RE(1) Protection of confidentiality at rest or in transit via untrusted networks
- SR 4.3 Use of cryptography

Timely response to events:

- SR6.1 Audit log accessibility
- SR6.1 RE(1) Programmatic access to audit logs

**C.1.11 Promote privacy****C.1.11.1 Principle**

Limit and protect the collection and use of personal identifiable information (PII).

**C.1.11.2 Rationale**

Data or information privacy is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, contextual information norms, and the legal and political issues surrounding them.

This principle requires careful handling of personal identifiable information (PII) as well as all data that is subject to confidentiality.

**C.1.11.3 Guidelines for implementation in a railway environment**

An application of this principle is the entry of a train driver's personal data or the monitoring of passengers on a station by CCTV.

Measures that support this principle include:

- Collect only the minimal personally identifiable data for a given user category in a given application
- Protect and limit access to critical data
- Remove or limit system services status and data display/reports such as IP addresses, version numbers and operating system, system configuration parameters on components
- Deliberate obfuscation or misreporting of system/service configuration data should be considered for SL 3 and 4
- Use a firewall to block access to other services not relevant to the required transaction
- Encrypt all critical/sensitive data stored and maintain the encryption keys on a different, especially secured machine and also ensure encryption and decryption take place on a different machine to where the data are stored
- Enforce requests for additional information before granting access to sensitive data
- After the data request, storage and processing is achieved, the PII should be securely deleted
- Where PII is required for a duration of time beyond a single instance, protect the data and limit access to authorised system operators.

**C.1.11.4 System requirements that implement the principle**

- SR 1.12 System use notification
- SR 4.1 RE(1) Protection of confidentiality at rest or in transit via untrusted networks
- SR 4.1 RE(2) Protection of confidentiality across zone boundaries

**C.1.12 Audit and monitor****C.1.12.1 Principle**

Check the security status of the system and implement the detection of security events.

**C.1.12.2 Rationale**

Auditing and monitoring the railway solution supports detection and response to security incidents as well as monitoring policy violations.

Implementation of this principle is used to establish baselines.

It enables threat hunting and forensic investigations for the railway solution.

NOTE Implementation of this principles supports the fulfilment of regulatory requirements such as the US TSA Directives and EU NIS2 directive.

#### **C.1.12.3 Guidelines for implementation in a railway environment**

The security monitoring strategy should be aligned with the system security requirements, the existing threats and risks and the compliance obligations.

Audit events should include timestamping. This timestamp should be synchronised across all the assets in scope. This enables correlation of the audit events.

Implementation should cover all the defence in depth levels, for example applications and network devices.

Audit events should include at as many sources as possible to ensure the completeness of monitoring. For example, security alerts (logs) should be generated by network-based sensors, host-based sensors and security solutions.

The audit events should include information about the when (timestamp), where (e.g. targeted resources, geolocation, service name/ protocol, IP addresses), who (identifier for the human or process) and what (type of event, severity, description, object)

Using a standard format for the security events is recommended, such as the CEF standard.

Audit logs should be kept long enough to allow for forensic investigation if needed and a minimum of one year is recommended. Some countries might have specific requirements for log retention that will support definition of how long the logs need to be archived for. In any case, it is important to ensure that the storage space is well dimensioned and enough to achieve the target retention.

It is important to ensure that the implementation of the audit and monitoring principle does not impact or degrade the system functions. Critical network passive monitoring solutions might be more appropriate than active approaches.

Monitoring security solutions should leverage both anomaly-based and signature-based detection. Any monitoring solution should be fitted to the rail environment and ideally be able to perform deep packet inspection (DPI), considering railway typical protocols.

Technologies to centralise and automate the review and correlation of logs are recommended.

Investigations of exceptions and anomalies should always be documented.

All detected events should be reported to a centralised security operations centre (SOC) for triage, analysis and remediation. There should be defined workflows between the SOC to operations and maintenance personnel to ensure collaboration.

#### **C.1.12.4 System requirements that implement the principle**

Identification and authentication control:

- SR 1.13 Access via untrusted networks

Use control:

- SR 2.8 Auditable events
- SR 2.8 RE(1) Centrally managed, system-wide audit trail

- SR 2.9 Audit storage capacity
- SR 2.10 Response to audit processing failures
- SR 2.11 Timestamps
- SR 2.11 RE(1) Internal time synchronisation
- SR 2.11 RE(2) Protection of time source integrity
- SR 2.12 Non-repudiation for human users
- SR 2.12 RE(1) Non-repudiation for all users

System integrity:

- SR 3.2 RE(2) Central management and reporting for malicious code protection
- SR 3.3 Security functionality verification
- SR 3.4 Software and information integrity
- SR 3.4 RE(1) Automated notification about integrity violations

Timely response to events:

- SR 6.1 Audit log accessibility
- SR 6.1 RE(1) Programmatic access to audit logs
- SR 6.2 Continuous monitoring

### **C.1.13 Proportionality principle**

#### **C.1.13.1 Principle**

Design system security to achieve an acceptable level of risk.

#### **C.1.13.2 Rationale**

The proportionality principle is based on the understanding that security is a trade-off between operational functionality and security. Security implementation effectiveness should be considered alongside its impact on operational functionality, usability and costs.

#### **C.1.13.3 Guidelines for implementation in a railway environment**

Early identification of system and security design highlights security may conflict with usability and experience. Security implementation costs may be compared with usability, experiences and security costs by evaluating risk linked to sensitivity and criticality of information and control-command assets.

Threat actor definition, especially its objectives, capabilities and resources, is linked to this principle.

To find the most effective security strategy, possible mitigations are evaluated in all of the four following phases:

- avoid
- treat (eliminate, mitigate, control)
- transfer (to other entities)
- tolerate/accept.

Risk treatment is not directed toward achieving a zero risk level but only to ensure that residual risk is at an acceptable level, through considering effectiveness of a defence mechanism in a specific environment and application. Furthermore, only security prevention or risk control mechanisms should be considered for implementation where the cost is lower than the untreated risk.



Prudent assessment of “due care” and the implementation of broadly accepted best practice information on security safeguards may also be an alternative to an economic cost-benefit evaluation approach.

#### **C.1.13.4 System requirements that implement the principle**

User authentication in untrusted environments:

- SR 1.1 RE(2), RE(3) Multifactor authentication
- SR 1.6, RE(1) Wireless access, unique identification and authentication

System integrity control

- SR 3.6 Deterministic output

#### **C.1.14 Precautionary principle**

##### **C.1.14.1 Principle**

Implement security measures to protect health or the environment when the demonstration of risks is scientifically uncertain.

##### **C.1.14.2 Rationale**

When an activity or threats raises risk of harm to humans or the environment, precautionary measures should be taken even if some cause-and-effect relationships are not fully established scientifically/empirically. This principle should be applied when making decisions on cybersecurity design in the face of high uncertainty or lack of adequate scientific knowledge.

This principle is relevant to railway cybersecurity because of the long life cycle of railway system. Therefore, it is recommended to apply at least the precautionary principle instead of the proportionality principle when considering essential devices.

The potential for terror related cyber-attack on railway signalling and control command could justify adopting this principle.

##### **C.1.14.3 Guidelines for implementation in a railway environment**

This principle underpins implementation of preventative and protection mechanisms in the design of railway IT systems and services.

The principle can be applied in strong and weak variants.

The strong precautionary principle justifies security measures and costs in the face of serious concerns over risk to health, safety, or the environment, even if the supporting evidence is speculative.

The weak precautionary principle still applies when certain mechanisms are deemed necessary but as yet unsupported by empirical evidence.

The case for major concerns over known control-command vulnerabilities or major threats should be documented in support of adopting this principle.

The protection and response mechanisms devised under this principle linked to the perceived, yet unproven risks of attack should be stated.

One example of current best practice when implementing this principle is the use of a reference model.

The precautionary principle can be employed to justify implementing cybersecurity design principles in response to perceived threats or known vulnerabilities. This applies even when no historic precedent regarding risk to health, safety, or the environment can be cited or the supporting evidence is speculative.

#### **C.1.14.4 System requirements that implement this principle**

Implementation of this principle is through implementation all the system requirements which enable barriers and continuous verification of system resources and the integrity of software hardware or information by suitable mechanisms.

The system requirements are:

- SR 3.2 Malicious code protection
- SR 3.4 Software and information integrity
- SR 5.1 RE 2 Independence from non-control system networks
- SR 5.1 RE 3 Logical and physical isolation of critical networks
- SR.5.2 RE 1 Deny by default, allow by exception
- SR 5.2 RE 2 Island mode
- SR 5.4 Application partitioning
- SR 7.1 RE 1 Manage communication loads
- SR 7.1 RE 2 Limit DoS effects to other systems or networks
- SR 7.2 Resource management

#### **C.1.15 Continuous protection**

##### **C.1.15.1 Principle**

Maintain security at all times, in all operational modes.

##### **C.1.15.2 Rationale**

Continuous cybersecurity protection should be in place at all times on the railway system.

This principle applies across the entire range of railway information technology. It relates to all security risks in the railway environment on an ongoing basis.

Cybersecurity protection mechanisms may be voluntarily degraded due to operational requirements, including during installation, test and commissioning phases, system downtime, maintenance time, emergency situations and during decommissioning; however the overall system security should not be reduced. To maintain continuous protection the railway duty holder may apply measures such as:

- Design and enforce security controls that take into account the operational requirements and also support maintenance of the overall system security level.
- Add temporary compensatory measures that maintain the overall system security level whilst individual security measures may be in degraded operational mode.
- Continuous monitoring is an integral part of the principle of continuous protection and monitors events that may be linked to a cybersecurity incident through logging, analysis and triggering security alerts for action. It is implemented through continuous event logging, collection and automated analysis at different levels including log collection at system level, centralised log and event management and operational response at an organizational level.

**C.1.15.3 Guidelines for implementation in a railway environment**

All components and data used to enforce the security policy should have continuous protection that is consistent with both the security policy and the security architecture assumptions.

Assurance about the ability to secure operation is based on the data and information to be continuously protected.

Implementation of continuous data protection (cdp) mechanism enables continuous capture and tracking of data modifications, automatically saving every version of the data that is created locally or at a target repository.

Implementation should ensure that there are no time periods during which data and information are left unprotected while under control of the system.

If there are gaps the assurance that the system can provide the specified confidentiality, integrity, availability, and privacy protections for its design capability may not be made.

Data and information should be protected during:

- creation, storage, processing or communication; and
- system initialisation, execution, failure, interruption and shutdown; and
- system and network maintenance and upgrades.

Continuity of protection should be ensured across data, application, server and network stacks as well as through physical infrastructure and policies and procedures.

During system decommissioning and disposal, data and information should be completely erased, and erasure verified.

**C.1.15.4 System requirements that implement this principle**

System integrity:

- SR 3.1 Communication integrity
- SR 3.2 Malicious code protection
- SR 3.5 Input validation

Automated event management:

- SR 3.4 RE(1) Automated notification about integrity violations
- SR 6.1 Audit log accessibility
- SR 6.2 Continuous monitoring
- SR 7.3, RE(1) Control system backup and verification
- SR 7.4 Control system recovery and reconstitution
- SR 7.6 RE(1) Machine-readable reporting of current security settings

Continuous availability:

- SR 7.5 Emergency power
- SR 7.6 Network and security configuration settings

**C.1.16 Secure metadata****C.1.16.1 Principle**

Protect system metadata as data itself.

**C.1.16.2 Rationale**

A system, subsystem, or component should protect the metadata it relies upon for secure execution. In some cases, the metadata itself might be an asset requiring protection. When the security policy requires complete protection of information or it requires the security subsystem to be self-protecting, metadata should be considered by themselves as object to be protected

For example, critical subsystems and components of the railway system may rely on the integrity of the metadata for safe and secure operation.

**C.1.16.3 Guidelines for implementation in a railway environment**

The confidentiality, integrity and availability of the metadata should be considered during the risk assessment process in the same way as the system data.

All data and metadata relating to critical items of infrastructure and rolling stock should be protected.

Access to and modification of metadata should be restricted to the highest level of access control.

NOTE Metadata is generally not interpreted by the system that stores it. It may have semantic value, for example, it comprises information to users and programs that process the data, but not to the system itself. Metadata is defined as information about data, such as a file name or the date when the file was created.

**C.1.16.4 System requirements that implement the principle**

Use control:

- SR 2.11 Timestamps
- SR 2.11 RE(2) Protection of time source integrity

System integrity:

- SR 3.7 Error handling
- SR 3.9 Protection of audit information
- SR 3.9 RE(1) Audit records on write-once media

Data confidentiality:

- SR 4.1 Information confidentiality

Resource availability:

- SR 7.3 Control system backup
- SR 7.3 RE (1) Backup verification
- SR 7.3 RE (2) Backup automation
- SR 7.6 Network and security configuration settings
- SR 7.6 Machine-readable reporting of current security settings

**C.1.17 Secure defaults****C.1.17.1 Principle**

Ensure that the default configuration implements the expected security controls.

**C.1.17.2 Rationale**

The default configuration of a system should reflect the implementation of the security policy.

The principle of secure defaults applies to the initial configuration of a system as well as to the security engineering and design of access control and other security functions. These functions should follow a “deny unless explicitly authorised” strategy.

Implementation of the principle at the initial design stage of the component supports resilience of the system against cyber-attacks.

#### **C.1.17.3 Guidelines for implementation in a railway environment**

The security policy should not be violated by any “as shipped” configuration of a railway system, subsystem, or component.

If the protection provided by the “as-shipped” product is defined as inadequate, for example it is not in line with the security policy, the stakeholder should assess the risk of using it prior to establishing a secure initial state.

Examples of inadequate initial state are:

- built-in accounts with high privileges, for example root, admin or superuser
- availability of account details (address, username, passwords) in the installation procedure documents or in the user manuals
- minimal or absent default security policy, such as a strong password policy disabled by default.

A system designed according to this principle will operate “as shipped” to prevent security breaches before the intended security policy of the system is established.

This principle can be implemented to prevent the system from operating until the security policy is fully configured by the operational user.

Implementation of this principle ensures that a system is brought into operation in a secure state after successfully completing initialisation. In situations where the system fails to complete initialisation, it will either perform a predefined operation based on the secure default principle or it will not perform any operation.

#### **C.1.17.4 System requirements that implement this principle**

This principle is not directly aligned with the system requirements in [IEC 62443-3-3:2013/COR1:2014 \[59\]](#) which form the basis of the secure design principles in this Annex. The following system requirements are linked to the principle of secure defaults.

- SR 7.3 Control system backup
- SR 7.4 Control system recovery and reconstitution
- SR 7.8 Control system component inventories

### **C.1.18 Trusted components**

#### **C.1.18.1 Principle**

Make sure that every component of a system is trustworthy.

#### **C.1.18.2 Rationale**

A component should be trustworthy to at least the level consistent with the security dependencies it supports.

The principle of trusted components underpins the degree of confidence that a component or subsystem is trusted to perform its share of security functions.

### C.1.18.3 Guidelines for implementation in a railway environment

This principle can be applied to all railway applications.

All new railway systems incorporating communications and computing and processing components should ensure that trusted components are incorporated, with consideration of the service, control, and command functions.

The principle is particularly relevant in systems and components in which there are complex supply chains leading to complex chain of trust dependencies.

The principle also applies to a compound component that consists of several subcomponents, for example a subsystem, each of which may have varying levels of trustworthiness.

The overall trustworthiness of a compound component is that of its least trustworthy subcomponent. It may be possible to provide a security engineering rationale that the trustworthiness of a particular compound component is greater than this baseline. Any such rationale should be supported by an analysis demonstrating how the trustworthiness component principle can be met.

### C.1.18.4 System requirements that implement the principle

- SR 3.2 1 Malicious code protection

## C.2 Guidelines for implementation in a railway environment

To assist with performing the potential adaptations in railway applications the following information is embedded in [Table C.1](#) depicting the cybersecurity foundational classes and associated system requirements originally based on [IEC 62443-3-3:2013/COR1:2014 \[59\]](#):

- **Req, SL and Title** lists all the [IEC 62443-3-3:2013/COR1:2014 \[59\]](#) cybersecurity requirements and the requisite security level.
- **Railway guidance** is given about the existence of railway specific considerations and recommendations.
- **Relevant design principles** show the cybersecurity design principles underpinning each requirement (See [Clause C.1](#) for more information on these cybersecurity design principles)
- **Stakeholder** and **Type** offer classification in terms of principal duty holders and type of content.

The [Table C.1](#) proposes adaptation where railway context is too constrained for direct implementation of the IEC 62443-3-3 without compensating measures. Nevertheless, full implementation of the IEC 62443-3-3 system requirements should be targeted, and relevance of proposed compensating measures should be verified against the actual zone and conduit model, risk assessment the achieved security level (SL-A).

For legacy railway systems, some guidance is also provided in [Annex B](#). Further requirements may arise from other sources, operational requirements, legacy systems or the explicit risk evaluation for the SUC.

**Table C.1 –**

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
FR 1		Identification and authentication control (IAC)				

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 1.1	1	Human user identification and authentication	The enforcement of identification and authentication encompasses all interfaces, including physical HMLs and remote access, for all applications, even those that do not convey the authenticated railway application user identity during connection. The identification mechanism involves a standard login interface with a username or identifier, password, certificate (public/private key) challenge, or biometric check. No mechanisms should bypass the full authentication process (e.g. quick login or memorized passwords). If such mechanisms exist, they should be disabled by default. Emergency actions for safety or critical operations without identification may be permitted, but compensating measures (deterrent measures, physical protection and security processes) should be associated to prevent misuse.	Secure the weakest link  defence in depth  Authenticate requests  Control access  Proportionality principle	Op Sys Sup	Tech Proc
SR 1.1 RE(1)	2	Unique identification and authentication	To ensure a clear and unique association between account identifiers and human user identities, it is recommended to implement technologies such as individual certificates, tokens, or a centralized account and permission directory (database). Please refer to <a href="#">Clause I.3</a> for information on compensating measures.	Secure the weakest link  defence in depth  Authenticate requests  Assume secrets not safe	Sys Sup	Tech

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stakeholder	Type
SR 1.1 RE(2)	3	<b>Multifactor authentication for untrusted networks</b>	Multifactor authentication requires two forms of identity proof from the following categories: something the user knows (e.g. PIN, password), something the user owns (e.g. smart card, crypto token, mobile device), or a something inherent to the user (e.g. biometric data, user location or behavior). In railway systems, physical recognition methods, such as badges and smart cards, are typically preferred as the second factor, while passwords or PINs serve as the first factor. When multifactor authentication is necessary, the strength of each factor should be evaluated to ensure overall security. For example, while passwords or PINs provide a basic level of security, their complexity and length are important to consider. Delegated or federated authentication is preferred, as it can enhance security through centralized management and trust frameworks.	<b>defence in depth</b> <b>Authenticate requests</b>	<b>Sys Sup</b>	<b>Tech</b>
SR 1.1 RE(3)	4	<b>Multifactor authentication for all networks</b>	same guidance as RS 1.1 RE(2) for SR 1.1 RE(3).	<b>defence in depth</b> <b>Authenticate requests</b>	<b>Op Sys</b>	<b>Tech</b>
SR 1.2	2	<b>Identification and authentication of software processes and devices</b>	Authentication of devices and software services is achieved either at the link, network, or application layer. This authentication may utilize a pre-shared key (PSK) or a public/private key mechanism, such as certificates. Implementing this requirement in legacy railway applications and systems would necessitate significant redesign of components and systems, as the integration of devices and software services has not been a standard practice in the past.	<b>defence in depth</b> <b>Authenticate requests</b> <b>Control access</b> <b>Assume secrets not safe</b>	<b>Op Sys Sup</b>	<b>Tech Proc</b>
SR 1.2 RE(1)	3	<b>Unique identification and authentication of software processes and devices</b>	The account identifier is unambiguously and uniquely linked to a device or software service identifier, which can be associated with the device's material (such as a serial number) or a specific role or function in the system (e.g. HMI XX in subsystem YY). In cases where asset management is not generic and identifiers correspond to unique assets, the accounts reflect this uniqueness, with their naming aligned to the asset identifier.	<b>defence in depth</b> <b>Authenticate requests</b> <b>Assume secrets not safe</b> <b>Trusted components</b>	<b>Sys Sup</b>	<b>Tech</b>



Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 1.3	1	Account management	Legacy railway systems stored role-based account data with shared passwords on each device within a distributed architecture, alongside multiple commercial contractors, which complicates implementation and compromises overall security. Therefore, a centralized account management system is strongly recommended to facilitate the addition, removal, and modification of account data across the entire system. In the presence of generic passwords, it is essential to define, communicate, and implement SecRAC criteria for password updates. Typically, changing passwords at each turnover is not feasible.	Economise Mechanism	Op Sys Sup	Tech Proc
SR 1.3 RE(1)	3	Unified account management	To support unified account management, it is recommended that all human and non-human accounts are managed using a directory system. The management of human user accounts could be integrated with an external information system, which would require the use of industry-standard protocols for information exchange.	Economize Mechanism Make security usable	Sys Sup	Tech
SR 1.4	1	Identifier management	Identifiers management provides authorized human users with the ability to manage all user roles based on the privileges required to perform specific operations, utilizing a Role-Based Access Control (RBAC) matrix. In the context of a legacy railway system that employs a distributed password-based account management framework, an intermediate key vault and bastion server can serve as a proxy for the identification function.	Make security usable	Sys Sup	Tech

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 1.5	1	Authenticator management	<p>Authenticators, such as passwords, biometrics, physical keys, and smart cards, enable the system to verify each user's identity. Account security is based on the principle that only the account owner should know or hold their credentials. To this end, all accounts should have configurable credentials, including passwords, certificates, public keys, or authentication tokens, with modification rights granted exclusively to agents authenticated as information security officers. The system ensures that all new human or non-human users are provided with default authenticators upon account creation and mandates that human users change these authenticators at their first connection. Additionally, human users should have the ability to change their authenticators at any time, in compliance with minimum and maximum lifetime restrictions. When passwords are utilized, the login mechanism should accommodate unlimited length and accept all valid Unicode characters. Furthermore, the system should ensure the confidentiality of authenticator storage and transmission through robust cryptographic protections. It is important to note that local password management should only be used as a fallback, and unified account and authenticator management should be the primary means of authentication, as it is more secure. In the context of a legacy railway system with a distributed password-based account management system, intermediate key vaults and bastion servers can serve as a proxy for the identification function while managing password renewal on devices.</p>	<p><b>Defence in depth</b></p> <p><b>Make security usable</b></p>	Op Sys Sup	Tech Proc
SR 1.5 RE(1)	3	Hardware security for software process identity credentials	<p>Authenticators for software services and device users are typically X.509 certificates and keys. Certificates and keys should be stored in PKCS#11 compliant cryptographic tokens that protect them while performing cryptographic operations, including encryption, decryption, signing, and verification.</p>	<p><b>Control access</b></p> <p><b>Assume secrets not safe</b></p> <p><b>Trusted components</b></p>	Sys Sup	Tech

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 1.6	1	Wireless access management	Network access to wireless communication systems is granted to human or non-human users only after successful authentication on these wireless connection systems. This security control should be extended to all open communication systems, such as shared wired communication networks and wireless communication systems. A cryptographic link layer protection (VPN, either L2, L3, or L4 to L3) is recommended for implementation and maintaining authentication in open communication systems. This protection can be achieved using VPNs or IPsec for open wired systems, the latest version of WPA for Wi-Fi environments, and cryptographic measures for mobile telecommunication channels.	Secure the weakest link  Defence in depth  Control access	Op Sys Sup	Tech Proc
SR 1.6 RE(1)	2	Unique identification and authentication	In wireless connection systems, dedicated certificates are provided to human and non-human users for authentication to gain network access. This security control should be extended to all open communication system, such as shared wired communication network and wireless communication system. As of the publication date, implementing standards such OAuth based authentication scheme, falling back to or associated with IEEE 802.11x and IEEE 802.15.x link layer authentication ensures the application of best practices in user authentication.	Secure the weakest link  Authenticate requests  Trusted components	Sys Sup	Tech

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 1.7	1	Strength of password-based authentication	Authorized human users are provided with the ability to configure the password policy. Elements such as length, validity period, history, character variety, and the minimum duration between two modifications are modifiable by system administrators or authorized users. Password changes are allowed only if they comply with the established password policy. This policy can be configured by authorized users and may vary based on the account role of the updated passwords. In all cases, the password policy should align with security constraints related to account roles, password usage frequency, and lifetime, as well as operational constraints such as password input interface limitations and acceptable login duration. It is essential that the operational technology (OT) password policy aligns with the company (operator) security policy. In the context of a legacy railway system with a distributed password-based account management system, intermediate key vaults and bastion servers can serve as a proxy for the identification function while managing password renewal on devices.	Assume secrets not safe  Secure defaults	Op Sys Sup	Tech Proc
SR 1.7 RE(1)	3	Password generation and lifetime restrictions for human users	To enhance security, central account management should enforce a password expiration date in accordance with the password policy, aligned with the company (operator) security policy, and notify affected human users before that date. Moreover, the password policy includes provisions to prevent the reuse of passwords (excluding the last ten passwords), and a password history is maintained to avoid the reuse of old passwords when a change is necessary. In the context of a legacy railway system with a distributed password-based account management system, intermediate key vaults and bastion servers can serve as a proxy for the identification function while managing password renewal on devices.	Assume secrets not safe  Secure defaults	Sup	Tech

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 1.7 RE(2)	4	<b>Password lifetime restrictions for all users</b>	Authenticators have a validity period in accordance with the operational technology (OT) security policy, aligned with the company (operator) security policy, and are to be changed once they become outdated. For pre-shared keys (PSK), the update mechanism should include strength policy enforcement, which can be configured by the project or customer. This enforcement includes: – Minimum length – Lifetime restriction – Reuse restriction The PSK auto-generation feature should align with the configured policy proposed by the update mechanism.	<b>Assume secrets not safe  Secure defaults</b>	<b>Op Sup</b>	<b>Proc Tech</b>
SR 1.8	2	<b>Public Key Infrastructure (PKI) Certificate</b>	As of the publication date, the commonly accepted best practices for peer identity authentication are keys and certificates from a latest version X.509-based PKI infrastructure. We recommend the use of PKI-based certificates with IPsec, TLS, 802.1x (EAP-TLS), and other protocols that utilize public key authentication scheme. If certificates are used, authorized human users have the ability to assign certificates to other users within the system's PKI. PKI needs to be integrated with the authentication mechanism. Integration with both the user directory and asset management system would streamline management and enhance security.	<b>Assume secrets not safe  Make security usable</b>	<b>Op Sup</b>	<b>Proc Tech</b>

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 1.9	2	Strength of public key authentication	As of the publication date, the commonly accepted best practices for peer identity authentication are keys and certificates from a latest version X.509-based PKI infrastructure. We recommend the use of PKI-based certificates with IPsec, TLS, 802.1x (EAP-TLS), and other protocols that utilize public key authentication scheme. If certificates are used, a certificate validation process or algorithm is to be provided for human and non-human users. It should also include checking the validity period of the certificate against the current date and time which is the standard usage and a security needed practice. The revocation status of certificates should be verified through the use of a Certificate Revocation List (CRL). This includes ensuring that the CRL validity period aligns with operational constraints and considers the download possibilities for timely access to updated revocation information.	<b>Defence in depth</b>  <b>Assume secrets not safe</b>  <b>Secure defaults</b>	Op Sys Sup	Tech Proc
SR 1.9 RE(1)	3	Hardware security for public key authentication	Dedicated hardware mechanisms are to be used to store and utilize the private keys of certificates. An internal Trusted Platform Module (TPM) or an external hardware security module (HSM) can be employed to fulfill this requirement. On-disk encryption starting from a hardware secure element may also be utilized.	<b>Control access</b>  <b>Assume secrets not safe</b>  <b>Continuous protection</b>	Sup	Tech
SR1.10	1	Authenticator feedback	On user login failure, only a generic authentication failure message is indicated to human or non-human users without providing specific information. To prevent any information disclosure, the element triggering the authentication failure remains confidential. Messages such as "Wrong password" or "Wrong username" should be avoided, and the failure message remains constant regardless of user input or the reason for failure. Input feedback mechanisms should hide credential information, typically displaying ★ characters in place of actual password characters.	<b>Proportionality principle</b>  <b>Secure defaults</b>	Sys	Tech

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 1.11	1	Unsuccessful login attempts	In the context of mission or safety-critical systems that deliver essential railway functions, it is important to recognize that limiting login attempts may lead to system or function unavailability, adversely impacting safety. Implementation of this requirement should fully consider safety and operational availability implications.	Defence in depth Control access Secure defaults	Op Sys Sup	Tech
SR 1.12	1	System use notification	A banner is provided at the external system boundaries (such as the bastion, connection point, and remote connection authentication system) before human user login, informing users about the data they will access, specifics of the system, and any potential legal obligations to which they must adhere to. An example banner could read: "You are accessing a restricted Information System (IS) that is provided for [usage] use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The data present in the system can be intercepted, and the communication can be monitored for purposes including, but not limited to, penetration testing, communication security monitoring, network operations and defence, personal misconduct, or law enforcement. Communications using, or data stored on, this System are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any production or security purpose. (Add constraints if necessary)".		Sys Sup	Tech
SR 1.13	1	Access via untrusted networks	Access via untrusted network may be permitted for non-critical functions, such as passenger information systems; however, in these cases, access should utilize a cryptographically protected communication channel and be authorized, controlled, and monitored. Please refer to <a href="#">Clause 4</a> and <a href="#">Annex F</a> for zone criticality details.	Secure the weakest link Defence in depth Control access Audit and monitor	Op Sys Sup	Proc Tech

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 1.13 RE(1)	2	Explicit access request approval	For remote access from untrusted network (e.g. third-Party network, remote network or cloud) the usage of Secure Access Service Edge or hardware-enforced solutions should be prioritized. When authentication is performed for human or non-human users from an untrusted network, it is essential to ensure that the user belongs to an authorized dedicated group. Please refer to <a href="#">Clause 4</a> and <a href="#">Annex F</a> for zone criticality details.	Defence in depth Authenticate requests Control access Precautionary principle	Op Sys Sup	Proc Tech
FR 2	Use control (UC)					
SR 2.1	1	Authorization enforcement	The least privilege principle involves identifying the permissions strictly needed to accomplish the missions associated with each role. Each account needs to be associated with a defined role or a set of defined rights. Before any action is executed by a human or non-human user, it is essential to verify that the role associated with the user has the right to perform that action to enforce permission control. Operations and Maintenance should be managed according to the designated role for the existing account. Rights management controls should be consistently enforced, preventing any temporary or permanent bypass of these controls for unauthorized commands.	Defence in depth Least privilege Control access Assume secrets not safe	Op Sys Sup	Tech Proc
SR 2.1 RE(1)	2	Authorization enforcement for all users	The least privilege principle and authorization enforcement should be applied to all users, whether they are human users, devices, or software users.	Defence in depth Least privilege Control access Assume secrets not safe	Op Sys Sup	Tech Proc
SR 2.1 RE(2)	2	Permission mapping to roles	Authorized users have the capability to define permissions granted to all users roles associated to its responsibility. No user can modify their own privileges, as this could lead to unauthorized privilege escalation. It is important to refer to the principal cybersecurity roles, ensuring that associated operations and rights effectively manage and separate maintenance, administration, and operational roles. Please refer to <a href="#">Annex H</a> on cybersecurity roles.	Defence in depth Least privilege Economize Mechanism Control access Make security usable	Op Sys Sup	Tech Proc



Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stakeholder	Type
SR 2.1 RE(3)	3	Supervisor override	Operational overrides are necessary in railways for emergency and manual operations, and these operations should be documented in a formal log with automatic log generation and records. Physical security measures, such as managing keys and a golden key control mechanism, should be implemented to control access to the override functions. Human users can be temporarily granted the ability to augment the functions they can access in a controlled manner, for a limited time, or during an event sequence, without causing any operational disturbance. When necessary for operational installation or troubleshooting, a dedicated role should be implemented with high privilege access to automated mechanisms. By default, accounts associated with the troubleshooting role should be disallowed in the system. Additionally, a configurable period of time or sequence of actions should automatically reset these accounts to a deactivated state.	Defence in depth Least privilege Control access Precautionary principle	Op Sys Sup	Tech Proc
SR 2.1 RE(4)	4	Dual approval	The dual approval mechanism requires proof of two distinct credentials allocated to different authorized agents. This approach links to safety requirements, including the four-eyes principle and minimizes the risk of abnormal execution by a single agent, which could lead to dangerous situations. The implementation should not conflict with time-critical activities and functions; in such cases, alternative approaches should be employed to efficiently establish the chain of trust. Efficient implementation approaches may include using two separate orders from different authorized agents or allowing a single agent to enter an authorization code provided by an authorized authority. For instance, changing a set point in the Train Control Management System (TCMS) that affects the computation of the train's speed should require dual approval, as should bypassing the European Train Control System (ETCS) control of the train's speed or issuing an order to stop.	Defence in depth Least privilege Control access	Op Sys Sup	Tech Proc

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 2.2	1	Wireless use control	The system needs to allow an authorized human users to define and manage flows through wireless connection systems. This includes the ability to create and maintain a list of approved equipment and grant access exclusively to this designated list. This security measure should be implemented on all open or shared network. Only legitimate flows should be allowed to transit on open or shared systems. To ensure security, network access to devices is granted only after successful authentication, utilizing certificate-based methods supported by Public Key Infrastructure (PKI). A typical scenario where wireless communications are commonly utilized is in train-to-ground communication, which includes technologies such as GSM-R, Wi-Fi, FRMCS, Radio, and LTE.	Secure the weakest link Defence in depth Authenticate requests Control access Continuous protection	Op Sys Sup	Tech
SR 2.2 RE(1)	3	Identify and report unauthorized wireless devices	Wireless systems are widely used in railway infrastructure for both safety and critical communication, as well as for customer media and entertainment systems. These systems need to be monitored for abnormal devices, including malicious network clients attempting to breach the system and malicious wireless access points trying to intercept legitimate communication flows. Wireless intrusion detection systems should be utilized to implement this requirement effectively.	Defence in depth Authenticate requests Control access Audit and monitor Continuous protection		

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 2.3	1	Use control for portable and mobile devices	Portable and mobile devices may be used in legacy railway infrastructure for diagnostic purposes and tasks in environments without network connections. A mobile media management plan should be implemented, encompassing a sanitization process and outlining authorized uses of mobile media devices. The use of these devices should be strictly limited to scenarios where no network service is available for file transfer. It is necessary that each usage of a mobile device include verification of the user's identification, authentication, and authorization. When a mobile device is necessary for performing activities, no identification or authentication measures should be overlooked, and authorizations for the mobile device should be managed accordingly.	<b>Defence in depth</b> <b>Authenticate requests</b> <b>Control access</b> <b>Secure defaults</b> <b>Trusted components</b>	Op Sys	Tech Proc
SR 2.3 RE(1)	3	Enforcement of security status of portable and mobile devices	Security policy on mobile device may be verified through a cleaning processes that is authenticated using robust cryptographic technology.	<b>Defence in depth</b> <b>Make security usable</b> <b>Secure defaults</b> <b>Trusted components</b>		
SR 2.4	1	Mobile code	Although mobile code is not common in critical rail applications, it may be present in information systems associated with rail applications or maintenance applications. A mobile code policy should be implemented. Mobile code should only be authorized if it has passed the mobile code policy check, which includes, but is not limited to, an anti-malware scan. Execution requests for mobile code is to be logged, as well as any instances of mobile code execution.	<b>Defence in depth</b>	Sys Sup	Tech
SR 2.4 RE(1)	3	Mobile code integrity check	Before executing mobile code, its origin should be authenticated and verified against a list of trusted sources	<b>Defence in depth</b>		

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 2.5	1	Session lock	Authorized users should have the ability to configure the inactivity period that triggers the session lock. To meet security needs, this inactivity period may default to 5 minutes but should be adjustable by authorized users. For operational reasons, operational status may still be provided without a locking mechanism. In any case, session locks should be configured judiciously to avoid negatively impacting availability and access to essential functions. Typically, operational Human-Machine Interfaces (HMI) that manage essential functions in secured environments, such as the driver cab or Operations Control Center (OCC), should never be automatically blocked.	<b>Defence in depth</b> <b>Control access</b> <b>Make security usable</b> <b>Proportionality principle</b> <b>Secure defaults</b>	Op Sys Sup	Tech
SR 2.6	2	Remote session termination	This requirement applies only to remote sessions, defined as sessions that occur outside the immediate operational environment, such as access from business or multimedia locations as opposed with operational technology inter-zone communication. These sessions experience fewer constraints from Human-Machine Interface (HMI) availability issues that could impact essential functions in a timely manner. At any time, both human and non-human users need to have the ability to terminate a remote session. This capability is crucial to ensuring security and preventing data leaks or unauthorized system modifications. Inactivity locks should lead to a mandatory session termination after a configurable period, typically less than 5 minutes. Authorized users should have the ability to configure the inactivity period that triggers session termination. After an inactivity lock, a complete authentication process is required to regain access.	<b>Defence in depth</b> <b>Economise Mechanism</b> <b>Control access</b> <b>Make security usable</b> <b>Secure defaults</b>	Op Sys Sup	Tech
SR 2.7	3	Concurrent session control	This limited number of concurrent sessions should be configurable by authorized users.	<b>Defence in depth</b> <b>Control access</b> <b>Secure defaults</b>	Op Sys Sup	Tech Proc
SR2.8	1	Auditable events	-	<b>Audit and monitor</b> <b>Proportionality principle</b>	Sys Sup	Tech

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 2.8 RE(1)	3	<b>Centrally managed, system-wide audit trail</b>	Components and subsystems that log events locally should also ensure that monitoring and logging information is transmitted to a centrally managed system. There may be a delay between the local logging of data and its transmission to the central system. To enhance investigation efficiency, log management is centralized on a server using industry standard protocols. Additionally, it is important to estimate log bandwidth and manage bandwidth usage effectively to ensure that logging does not overwhelm network resources. Proper bandwidth management strategies should be implemented to prevent potential disruptions due to high log transmission volumes.	<b>Make security usable</b> <b>Audit and monitor</b>	<b>Sys Sup</b>	<b>Tech</b>
SR 2.9	1	<b>Audit storage capacity</b>	Logs are stored in compliance with applicable regulations and standards. The log storage strategy considers the volume of logs generated daily and their retention period to ensure completeness for audit purposes. Event log storage should be resilient to system reboots.	<b>Audit and monitor</b>	<b>Sys Sup</b>	<b>Tech</b>
SR 2.9 RE(1)	3	<b>Warn when audit record storage capacity threshold reached</b>	In systems utilizing a rotating buffer for log storage, it is important to monitor the buffer size and set alarms to trigger as the buffer approaches its capacity. When rotation begins, an alarm should indicate that the buffer is starting to overwrite older logs. Once rotation has commenced, new logs will continuously overwrite preceding ones, and no further alarms will be triggered.	<b>Make security usable</b> <b>Audit and monitor</b>	<b>Sys Sup</b>	<b>Tech</b>
SR 2.10	1	<b>Response to audit processing failures</b>	Log storage and processing should support system functions without hindrance. The design should establish a log recording mechanism that accommodates storage hardware and access requirements, including temporary storage in RAM and periodic flushing to permanent storage. Furthermore, the design should outline a storage strategy for situations when capacity approaches its limits, incorporating measures such as log repetition suppression and log rotation.	<b>Make security usable</b> <b>Audit and monitor</b>	<b>Op Sys Sup</b>	<b>Tech</b>

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 2.11	2	Timestamps	Time management and synchronization is essential for coordinating log management and actions such as backups, timestamping tasks, and access control. A time server is required to facilitate this process and all system components should have the capability to be time-synchronized. At a minimum, if the synchronization source is not available at startup, system components should ensure that the local date and time is not earlier than the last known time, which is the timestamp prior to shutdown. Generated logs should include a timestamp inherited from system time synchronization.	<b>Audit and monitor</b> <b>Proportionality principle</b> <b>Secure metadata management</b>	Sys Sup	Tech
SR 2.11 RE(1)	3	Internal time synchronization	When time inconsistencies that create a security risk—specifically differences of days—are detected, a security event should be generated to notify authorized users for auditing purposes.	<b>Economise Mechanism</b> <b>Audit and monitor</b>	Sys Sup	Tech
SR 2.11 RE(2)	4	Protection of time source integrity	To prevent timestamp alterations in logs and other timed actions, cryptographically protected protocols such as Network Time Security (NTS) should be used to synchronize time servers with components. In the absence of an authenticated time source, multiple time sources utilizing various independent paths should be employed by system components to synchronize time. A local time synchronization strategy should also be established, as multiple sources may have small differences.	<b>Audit and monitor</b> <b>Secure metadata management</b>	Sys Sup	Tech
SR 2.12	3	Non-repudiation for human users	To ensure human action non repudiations, actions should be logged, including their human user identifier and the logs should provide a detailed description of the event.	<b>Audit and monitor</b>	Op Sys Sup	Tech Proc
SR 2.12 RE(1)	4	Non-repudiation for all users	All actions taken by both human and non-human users should be logged, including their user identifier. To ensure the principle of non-repudiation, logs should provide a detailed description of each event.	<b>Audit and monitor</b>	Op Sys Sup	Tech Proc
FR 3	System integrity (SI)					
SR 3.1	1	Communication integrity	Basic communication integrity is already provided in safety related communication protocols.	<b>Defence in depth</b> <b>Authenticate requests</b>	Sys Sup	Tech

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
				<b>Continuous protection</b>  <b>Secure metadata management</b>		
SR 3.1 RE(1)	3	<b>Cryptographic integrity protection</b>	Ensuring data integrity and authenticity in communication should involve the implementation of cryptographic protocols. If communication security cannot be achieved at the application layer, security measures should be applied at the network layer. In railway operations, particularly for rolling stock using outdated or weak protocols, sufficient security boundaries and intrusion detection mechanisms should be established as compensatory measures. When a cryptographically protected protocol is utilized to guarantee data authenticity, the consumer should verify the identity of the producer.	<b>Authenticate requests</b>  <b>Assume secrets not safe</b>  <b>Continuous protection</b>  <b>Secure metadata management</b>	<b>Sys Sup</b>	

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 3.2	1	Malicious code protection	Assets dedicated to human interaction, such as workstations and laptops, should include malware protection. An anti-malware strategy should enable authorized users to manage updates and scan frequencies, with regular automated scans being essential for maintaining security levels. Cryptographic signatures should be used to ensure that software packages come from legitimate sources. All software packages should be cryptographically signed by a trusted authority, with verification and authentication of these signatures required during deployment processes. Once verified, packages should not transit through low-security devices before installation. To secure the verification process, it should be automated and include mechanisms to prevent installing a previous package version. Additionally, preventive measures, such as controlling removable media, should complement detection mechanisms at entry points. USB port usage should be limited, and hardening methods should be employed to prevent code execution from USB devices. A secure boot mechanism should prevent USB booting from unauthorized sources. Furthermore, the control system should provide the capability to update these protection mechanisms to keep pace with evolving threats. The anti-malware strategy and reaction capability should be aligned with operational risks and the company's risk management strategy.	Secure the weakest link  Defence in depth  Continuous protection	Op Sys Sup	Tech Proc
SR 3.2 RE(1)	2	Malicious code protection on entry and exit points	Next-generation firewalls may be used to protect entry and exit points from malicious code or actions. To limit the risk of code injection, communication protocols should implement protocol breaks, and the data syntax at the application interface should be verified.  Some next-generation firewalls can create latency problems, making them difficult to use in safety-critical environments. Hence, their performance should be assessed before implementation.	Defence in depth  Continuous protection	Op Sys Sup	Tech Proc Env



Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 3.2 RE(2)	3	<b>Central management and reporting for malicious code protection</b>	Integrity and security consistency in railway need to use a central management of protection from malware and malicious code. While Security Information and Event Management (SIEM) and incident management systems may offer dynamic anomaly detection, they might be insufficient for comprehensive protection against malicious code. Installed protection solutions should enable authorized users to manage security functions through an integrated environment, facilitating unified configuration and quick adaptation of protection levels when necessary.	<b>Defence in depth</b> <b>Make security usable</b> <b>Audit and monitor</b>	<b>Op Sys</b>	<b>Tech Proc</b>
SR 3.3	1	<b>Security functionality verification</b>	Security verification requires that operational security functions, such as access control, input filtering, integrity verification, and cryptographically protected protocols, are documented in the system design. Each security function should include the capability for testing. To ensure system protection and verify the implementation of security objectives, tests should be conducted for each function. This may involve sending offensive inputs to the system or its components and checking the logs for the correct rejection of those inputs. Authorized users should be provided with the test results for verification.	<b>Make security usable</b>	<b>Sys Sup</b>	<b>Tech</b>
SR 3.3 RE(1)	3	<b>Automated mechanisms for security functionality verification</b>	A tool-based solution should support the on-site execution of security tests for authorized users. Automating these tests is essential to prevent any omissions and ensure consistent application of security measures. As Factory Acceptance Testing (FAT) and Site Acceptance Testing (SAT) are implementation-specific, and the security test procedure should be shared and mutually agreed upon between the system integrator and the asset owner.	<b>Make security usable</b>	<b>Sys Sup</b>	<b>Tech Proc</b>

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 3.3 RE (2)	4	<b>Security functionality verification during normal operation</b>	The system should allow the possibility to perform security tests during operation while maintaining optimal system functional behavior. This verification is typically triggered and periodically conducted by sending offensive inputs to the system or one of its components and checking the system logs for the correct rejection of the input. This requirement should only be considered suitable for safety-related systems with appropriate analysis and safeguards. In areas where it is not suitable, the use of such verification tests on a testbed or virtual twin should be prioritized.	<b>Make security usable</b>	<b>Sys</b>	<b>Tech Proc</b>
SR 3.4	2	<b>Software and information integrity</b>	The system should utilize components that include detection of modifications to data at rest, such as Host-based Intrusion Detection Systems (HIDS), secure boot mechanisms, and application allow-listing. When HIDS or application allow-listing is employed, it should verify the integrity and authenticity of its reference database prior to use. This database should be computed offline before installation on the system and signed by a trusted authority.	<b>Assume secrets not safe</b> <b>Secure metadata management</b>	<b>Sys Sup</b>	<b>Tech</b>
SR 3.4 RE(1)	3	<b>Automated notification about integrity violations</b>	The status of the system integrity check should be logged as a security event, with severity defined depending on the check results. Alarms are to be raised in case of abnormal status detection.	<b>Make security usable</b> <b>Audit and monitor</b>	<b>Sup</b>	<b>Tech</b>
SR 3.5	1	<b>Input validation</b>	Filtering of invalid syntax and content includes out-of-range values, incomplete data, invalid characters, and oversized buffers. Input data should then be validated through positive pattern matching to ensure it aligns with acceptable patterns defined in the system interface specification. This process involves filtering out risky patterns and positively verifying the syntax and grammar of the received content. Once data is filtered, the communication between the data input verification process and the data usage process should be protected against undetected modifications through zone, network, or communication protocol security means.	<b>Secure the weakest link</b> <b>Defence in depth</b> <b>Continuous protection</b>	<b>Sup</b>	<b>Tech</b>

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 3.6	1	<b>Deterministic output</b>	When a system component is unable to ensure relevant functional output, the system should respond by transitioning to a predetermined and safe and secure state. If the system or one of its components becomes compromised, its outputs should not jeopardize any other system or component to prevent potential side effects of an attack.	<b>Defence in depth</b> <b>Fail secure</b> <b>Proportionality principle</b>	<b>Sys Sup</b>	<b>Tech Proc</b>
SR 3.7	2	<b>Error handling</b>	The diagnosis of a degraded operational mode should be facilitated by using error codes and status information. Authorized users should be provided with documentation that includes error and status codes, along with the expected behavior in case of an error. Additionally, information should be provided to help authorized users identify the current state or error state of a system component. Error feedbacks should be designed to avoid revealing detailed information to potential attackers.	<b>Fail secure</b> <b>Make security usable</b> <b>Proportionality principle</b> <b>Secure metadata management</b>	<b>Sys Sup</b>	<b>Tech Proc</b>
SR 3.8	2	<b>Session integrity</b>	When a session mechanism is used to maintain user authorization, the active session should be identified with a session identifier. The system should protect the session against modification, insertion, or hijacking. Any session identifier not linked to an established session is rejected. To prevent man-in-the-middle attacks, the validity of session IDs should be verified.	<b>Defence in depth</b> <b>Authenticate requests</b> <b>Control access</b>	<b>Sup</b>	<b>Tech</b>
SR 3.8 RE(1)	3	<b>Invalidation of session IDs after session termination</b>	The session identifier may be invalidated at any point by the client user or the server.	<b>Defence in depth</b> <b>Authenticate requests</b> <b>Make security usable</b> <b>Secure defaults</b>	<b>Sup</b>	<b>Tech Op</b>
SR 3.8 RE(2)	3	<b>Unique session ID generation</b>	The system should utilize components that generate session identifiers through commonly accepted sources of randomness, ensuring they are long enough to be unguessable and virtually unique for the lifetime of the system.	<b>Defence in depth</b> <b>Authenticate requests</b> <b>Secure defaults</b>	<b>Sup</b>	<b>Tech</b>

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 3.8 RE(3)	4	Randomness of session IDs	Session identifiers should be protected against informed guesses, brute force attacks, hijacking, or modification. Any session identifier not linked to an established session is rejected. To prevent man-in-the-middle attacks, verifying the validity of session IDs is essential. Although this requirement applies at the SL4 system level, it is pushed down to SL2 for components.	Defence in depth  Authenticate requests  Secure defaults	Sup	Tech
SR 3.9	2	Protection of audit information	Audit information, as used in IEC 62443, refers to logs data, while "audit" is generally understood as high-level information created on demand based on logs data. This audit information should not be generated by the operational technology (OT) but by specialized equipment in business or security operations center (SOC) environments. It is important to note that OT still creates log data, which needs to be protected to prevent modification and deletion. Writing to the log storage should be restricted solely to the source device; authorized users should have the ability to access log storage in read-only mode.	Least privilege  Promote privacy  Audit and monitor  Secure metadata management	Sys Sup	Tech
SR 3.9 RE(1)	4	Audit records on write-once media	Identification of causes of a cybersecurity incident as well as legal legitimacy of forensic examination requires that system activities are recorded in a reliable manner. Limiting hacker access to these files is essential, which can be achieved through the use of the system log server. This server is required to store logs on write-once hardware media, prioritizing the use of Write Once Read Many (WORM) technology or a write-only software database. Log retention periods imposed by railway administration and national regulations should be taken into account. Long-term and audit information management should be exported to the IT environment, supplementing the operational technology (OT) system.	Promote privacy  Audit and monitor  Precautionary principle  Secure metadata management	Sup	Tech
FR 4						

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 4.1	1	Information confidentiality	Credentials, passwords (even when hashed), and keys should be protected from exposure in all contexts, including maintenance services and log mechanisms. Administration communication should occur over cryptographically protected protocols that ensure confidentiality, integrity, and authenticity. These sensitive elements should be stored in secure hardware or a secure cryptographic filesystem, with the encryption key protected in secure hardware. For communication that may include these elements over shared or publicly accessible transmission mediums, both application-level and link-level cryptographically protected mechanisms should be implemented, employing diversified technology. Other sensitive data requiring confidentiality protection within the railway environment includes privacy-related data about passengers, cardholder data from automatic fare collection systems, infrastructure details that could be exploited by adversaries, and names and details of crew members. Interfaces to legacy components could be maintained through proxy solutions. When a cryptographically protected protocol is employed to protect confidentiality, the data producer authenticates the consumer.	<b>Defence in depth</b> <b>Least privilege</b> <b>Promote privacy</b> <b>Continuous protection</b> <b>Secure metadata management</b>	Sup Sys	Tech
SR 4.1 RE(1)	2	Protection of confidentiality at rest or in transit via untrusted networks	<p>Implementation of two levels of encryption using different technologies is necessary for communication over open or shared networks, such as radio, shared wired links, or communication systems not under the control of the asset owner. In Wi-Fi environments, cryptographic application protocols or VPNs should be added to the Wi-Fi security layer. For mobile telecommunications, cryptographic application protocols or VPNs should be integrated in addition to mobile telecom encryption.</p> <p>This multi-layered encryption approach ensures that a single vulnerability does not immediately expose sensitive data, as each layer provides an additional barrier against potential breaches.</p>	<b>Defence in depth</b> <b>Least privilege</b> <b>Promote privacy</b> <b>Continuous protection</b> <b>Secure metadata management</b>	Sys Op	Tech Proc

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 4.1 RE(2)	4	Protection of confidentiality across zone boundaries	All data transfers in and out of zone SL4 boundaries should be performed using cryptographically protected protocols.	Defence in depth Least privilege Promote privacy Continuous protection Secure metadata management	Sup Sys	Tech Proc
SR 4.2	2	Information persistence	Authorized users should have the ability to purge any sensitive data from storage and components, including credentials, passwords (even when hashed), keys, privacy-related data about passengers, cardholder data from automatic fare collection systems, infrastructure details that could be exploited by adversaries, and names and details of crew members. This capability is typically used before decommissioning or handing over a component (or part of it) to a third party.  It could involve a dedicated maintenance service that ensures the complete purging of sensitive data before any transfer or decommissioning occurs.	Defence in depth Promote privacy Secure metadata management	Sup Sys Op	Tech Proc
SR 4.2 RE(1)	3	Purging of shared memory resources	The usage of audited and commonly used third-party security software may protect against poorly implemented software mechanisms that could leak sensitive information.  Programming language features in design and coding rules are efficient in limiting the scope and reuse of variables that contain information such as keys and credentials. The design should ensure that an audit of cryptographic code is performed to verify that data derived from those elements does not persist in memory and that the algorithm is robust against side-channel attacks.  The system should utilize components that implement these practices, and this requirement should be communicated to the product provider.	Defence in depth Promote privacy	Op	

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 4.3	1	Use of cryptography	Established and tested encryption and hash algorithms should be utilized. Service configurations should disable the use of any unauthorized cryptographic mechanisms. The railway application product supplier should document practices and procedures related to cryptographic key establishment and management. Cryptographic keys should be generated with a true random generator in a trusted environment. The generation of random elements used in cryptographic protocols should rely on a Cryptographically Secure Pseudorandom Number Generator (CSPRNG), typically gathering entropy from real-world sources. Keys should be used for a single purpose: either encryption or authentication/signature. Key reuse is forbidden, and when a key is generated, its hash should be stored to prevent future use. Service configurations should only accept authorized cryptographic key lengths, even if proposed by another interface peer. Hardware asymmetric cryptographic capabilities should be evaluated to ensure resistance to side-channel attacks. Protocol and communication identifiers should be unpredictable, generated by a random number generator or derived from an unpredictable source. National recommendations can be used for guidance.	<b>Defence in depth</b>  <b>Assume secrets not safe</b>  <b>Secure defaults</b>	Sup Sys	Tech Proc
FR 5						

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 5.1	1	Network segmentation	<p>Critical control and safety-related systems should be designed from the outset to be segmented from other networks. Signalling-related systems should be segmented from other operational networks. Publicly accessible networks, such as passenger Wi-Fi, should be physically separated from control networks and multimedia networks, such as Train Control Management Systems (TCMS), CCTV, and Passenger Information Systems. Physical or logical segmentation can be used to achieve this separation; however, it should be noted that segmentation is efficient only with security devices to control data flow between segments based on least privilege. The system should alert if data that violates established rules attempts to pass from one segment to another. Support for a network authentication mechanism is required for any physically accessible network connection points. Allocation of network services or flows to different network interfaces (physical or logical) should be supported for operational flows and administration services. In response to an incident, it may be necessary to sever connections between different network segments. If this occurs, services essential for supporting operations should be maintained to ensure devices can continue to operate properly and/or shut down in an orderly manner. This may require duplicating certain servers on the control system network to support normal network features, such as Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS), or local Public Key Infrastructure (PKI) artifact distribution points.</p>	<p><b>Secure the weakest link</b></p> <p><b>Defence in depth</b></p> <p><b>Proportionality principle</b></p> <p><b>Continuous protection</b></p> <p><b>Trusted components</b></p>	Sys Op	Tech



Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 5.1 RE(1)	2	Physical network segmentation	Physical segmentation between signalling and control systems, and the business network, is necessary. By utilizing a communication flow matrix and considering the origin and destination of the flow between two zones of different criticality, the bidirectional flow should be allowed, physically restricted, or prohibited. Physical security gateways, such as security proxies or data diodes, should be employed to physically restrict network flow, effectively isolating the higher criticality network.	Secure the weakest link Defence in depth Continuous protection Trusted components	Sys Op	Tech
SR 5.1 RE(2)	3	Independence from non-railway application networks	Signalling and control networks should be independent of the business network. Physical segregation will be implemented between the signalling and other control networks, and the business network. A physical security gateway will isolate the signalling and control networks from the business network in the event of a security breach, preventing any network communication, whether wired or wireless, from the business network to the signalling and control networks.	Secure the weakest link Defence in depth Precautionary principle Continuous protection Trusted components	Sup Sys	Tech
SR 5.1 RE(3)	4	Logical and physical isolation of critical networks	The criticality of railway applications is determined by risk assessment or regulatory requirements, defining the need for logical and physical isolation, with physical isolation being preferred as the default option. Critical systems will be isolated within a dedicated physical network, with each critical system operating on its own dedicated logical network. Control and critical systems will deploy their own network services (such as DNS, NTP, or DHCP) to ensure service continuity in case of a compromise in non-control systems. This setup allows these systems to operate in island mode when necessary. A typical example is the separation of the signalling network from other non-safety-critical and operational networks. Segmentation methods include: – different network cables or fibers; – different carrier frequencies within single fiber-optic cables; – robust cryptographic measures for the foreseeable future.	Secure the weakest link Defence in depth Precautionary principle Continuous protection Trusted components	Sup Sys	Tech

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 5.2	1	Zone boundary protection	Technical solutions should be implemented to safeguard and monitor system network boundaries, as well as, if necessary, system zone boundaries. These devices may include proxies, gateways, routers, firewalls, data diodes, and encrypted tunnels. Any device at the zone boundary should monitor connection and information flow. To enhance overall system security and integrity, these components should be organized within an effective architecture, exemplified by integrating firewalls to protect application gateways located within a demilitarized zone (DMZ). The DMZ should provide a proxy application for both human and non-human users, presenting the necessary system information and accepting relevant commands while preventing unauthorized communication with system elements. It should ensure that remote operators cannot directly access the system, which can be facilitated by providing a dedicated administration console, for example.	Secure the weakest link Defence in depth Economize Mechanism Proportionality principle Continuous protection	Op Sup Sys	Tech
SR 5.2 RE(1)	2	Deny by default, allow by exception	For network devices, a packet drop policy is advisable to reject data that does not conform to the allowed traffic ruleset. Allowed traffic should be clearly defined, documented, and listed to ensure transparency and proper management of network access. Additionally, any ruleset violations should be reported.	Precautionary principle Secure defaults	Sup Sys	Tech

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 5.2 RE(2)	3	Island mode	<p>This capability may be utilized in scenarios such as the detection of a security violation or breach within the control system or during an ongoing attack at the enterprise level. For instance, the system should be designed so that, in the case of a breach or attack, all communication between corporate and operational environments is halted. In case of isolation, the system should still deliver network services to control systems by deploying their own services. These control system service deployment are critical due to the real-time requirements that may impact the availability and stability of essential railway services, such as Automatic Train Protection (ATP), braking systems, and control center operations. Safety Considerations The safety implications of this requirement should be carefully evaluated prior to implementation.</p>	<p><b>Fail secure</b> <b>Precautionary principle</b></p>		Tech
SR 5.2 RE(3)	3	Fail close	<p>This fail-close capability may be utilized in scenarios such as hardware failures or power outages that cause boundary protection devices to function in a degraded mode or fail entirely. In the case of operational failure of the boundary protection, the system should automatically prevent any communication through control system boundaries without impacting ongoing operations. This capability is crucial for maintaining operational integrity during such events. The fail-close function should account for the possibility of degraded modes in system devices, allowing for service continuity without total communication interruption.</p> <p>Railway safety architectures do not generally permit behaviors that could compromise safety on networks. As such, all essential functions should continue to operate, while non-essential functions may be halted in the event of boundary protection violations. High availability solutions where the boundary protection is made redundant and replaceable on-the-fly should be prioritized for critical systems.</p>	<p><b>Fail secure</b></p>		Tech

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 5.3	1	<b>General purpose person-to-person communication restrictions</b>	The system should limit communication means to the strict minimum, preventing all communication from entering the security zone boundary that is not necessary for operation, such as instant messaging protocols. The security gateway between the enterprise or IT environment and the operational network should support application layer filtering. Any attempts to use such protocols should be reported, such as email communications.	<b>Secure the weakest link</b>  <b>Defence in depth</b>	<b>Sys</b>	<b>Tech</b>
SR 5.3 RE(1)	3	<b>Prohibit all general-purpose person-to-person communications</b>	The system should enforce data security by blocking non-legitimate communication at first met zone boundary. This can include, for example, personal webmail systems, social media platforms, or any type of messaging systems.	<b>Secure the weakest link</b>  <b>Defence in depth</b>	<b>Sys</b>	<b>Tech Tools</b>
SR 5.4	1	<b>Application partitioning</b>	-	<b>Defence in depth</b>  <b>Precautionary principle</b>  <b>Continuous protection</b>		<b>Tech</b>
FR 6						
SR 6.1	1	<b>Audit log accessibility</b>	The system should allow authorized human users to access logs in read-only mode to prevent any deletion or falsification of logged events. To ensure the integrity of the logs, the system should guarantee that once written, the logs cannot be modified. This can be achieved through management of system read/write rights, the use of append-only disk partitions, or by utilizing write-once hardware media, for example. The system should also enable authorized human users to retrieve local security log data. In the event of network unavailability or any other incident, the logs should be exportable by authorized users.	<b>Least privilege</b>  <b>Control access</b>  <b>Make security usable</b>  <b>Audit and monitor</b>	<b>Sys Op</b>	<b>Tech Proc</b>

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 6.1 RE(1)	3	Programmatic access to audit logs	The system should enable external services to automatically receive on request logs through a machine interface, with solutions such as Syslog being a common approach to fulfill this requirement. The system should support the management of at least two servers in parallel. For public, open, or shared networks, the system should provide components with the capability to use the Syslog protocol over TLS (version 1.2 or higher) for cryptographically protected transmission of log information to the configured log servers, ensuring at least authenticated data transmission.	Make security usable  Audit and monitor	Sys Op	Tech Proc
SR 6.2	2	Continuous monitoring	As attacks become more sophisticated, the monitoring tools and techniques employed should also evolve, potentially incorporating behavior-based Intrusion Detection Systems (IDS) that support standard and railway protocols, with capabilities such as Deep Packet Inspection (DPI). The system should be connected to a Security Information and Event Management (SIEM) system to enable continuous log monitoring and address response and notification time, which may be constrained by local regulations (see [OM-07-01]). Given that connectivity may not always be available, such as in rolling stock applications, relevant monitoring data should be buffered and transmitted or collected when a connection is reestablished. In such cases, a delay in reporting a breach may be unavoidable.	Audit and monitor  Proportionality principle	Sys Op	Tech Proc Tools
FR 7						

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 7.1	1	Denial of service protection	The usage of functional resources should be anticipated and documented, including the risks associated with resource shortages and the potential impacts from overloaded network interfaces and services. The system zoning architecture and boundary protection should be designed to minimize the risk of powerful Denial of Service (DoS) attacks from reaching the control system. Strategies and limits to mitigate the functional impacts of resource shortages should also be documented. Additionally, Reliability, Availability, Maintainability, and Safety (RAMS) controls for essential services can be leveraged to support the implementation of this requirement.	Fail secure	Sys Sup	Tech Proc
SR 7.1 RE(1)	2	Manage communication loads	The inbound and outbound data flow to the network should be limited to typical functional needs, with dedicated firewall rules employed to achieve this. A host-based firewall should protect control system devices and limit service exposure using a "Deny by Default" strategy. Only service ports necessary for operational tasks should be opened in the host firewall, with explicit documentation of these ports. The ports should be opened dynamically based on application needs and closed once the applications are stopped. The system should ensure that its network components manage communication load through ingress quotas, load balancing, or other network mechanisms. To handle a large amount of data, the system should dynamically route packets through the least congested network.	Precautionary principle	Op Sys Sup	Tech Proc
SR 7.1 RE(2)	3	Limit DoS effects to other systems or networks	It is recommended to provide authorized human users the capability to set dedicated quotas on component resources by user, whether human or non-human. These quotas should align with the specific needs of each component and user.	Precautionary principle	Sys Sup	Tech Proc

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 7.2	1	Resource management	The system should ensure that security and maintenance functions do not impact operations. Modern operating systems offer various tools to control resource usage by each process application. These tools allow for prioritization, preemption, and termination of processes according to predefined rules. Security functions should be treated as background tasks, with scans and analyses performed as frequently as possible outside of operational time. The system should utilize components that implement these practices, and this requirement should be clearly communicated to the product provider.	Least privilege	Op Sys Sup	Tech Proc
SR 7.3	1	Control system backup	<p>To ensure system continuity in the event of a cyberattack or incident, components with modifiable configurations and/or data should be backed up. The system provides authorized human users with backup solutions to back up component data at least as often as required by the security analysis. Backups should include logs generated by the system to facilitate investigations following an attack or incident.</p> <p>Configuration management based on baselines is commonly employed in railway products, and the identity and location of critical files should be known at the application level. Backup operations should include the last modification of configurations and should be clearly defined and formalized through guidance documentation, allowing for the appropriate configuration and full reinstallation processes.</p>	Precautionary principle	Op Sys Sup	Tech Proc
SR 7.3 RE(1)	2	Backup verification	-	Precautionary principle	Op Sys Sup	Tech Proc
SR 7.3 RE(2)	3	Backup Automation	Backups should be conducted without user intervention, and the system should allow authorized human users to activate automated backups at a configurable frequency.	Precautionary principle Make security usable	Op Sys Sup	Tech Proc

Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 7.4	1	<b>Control system recovery and reconstitution.</b>	Authorized human users should have the ability to perform appropriate configuration and reconfiguration, including initial setup, updates, or full reinstallation for all system components that can be logically modified, using processes that are clearly defined and formalized through guidance documentation. This documentation can be included or referenced in the disaster recovery plan. Due to their safety-critical nature, railways have strict policies on recovery and reconstitution to ensure both a safe and secure state.		<b>Op Sys Sup</b>	<b>Tech Proc</b>
SR 7.5	1	<b>Emergency power</b>	The system should manage power supply failures without impacting essential functions. To prevent operational issues, the system should be equipped with a backup power source to maintain essential operations or should switch to a predefined secure mode to prevent any incidents.	<b>Fail secure Continuous protection</b>	<b>Op</b>	<b>Tech</b>
SR 7.6	1	<b>Network and security configuration settings</b>	Cybersecurity guidelines, as well as references from national agencies and industry standards, should be utilized. Recommended practices include limiting available services and modules to those strictly needed for operation.  To verify compliance with standards, the system should set out the current active security configuration. Security settings management services should be accessible only to accounts associated with the OT system administrator role and should provide settings visualization to enable audits of the actual applied state.	<b>Defence in depth Authenticate requests Continuous protection Secure defaults</b>	<b>Op Sys Sup</b>	<b>Tech Proc</b>
SR 7.6 RE(1)	3	<b>Machine- readable reporting of current security settings</b>	To facilitate automatic analysis of the settings state, security settings management services should provide reports in a machine-readable format. It is recommended that security settings management be integrated into the SIEM database.	<b>Audit and monitor Make security usable</b>	<b>Op Sys Sup</b>	<b>Tech Proc</b>



Requirement	SL	Title	Railway guidance (informative)	Relevant design principles	Stake- holder	Type
SR 7.7	1	Least functionality	Interfaces, ports, functions, or services that are not needed for operation in the specific context of installation should be deactivated. This deactivation may be accomplished explicitly in the system configuration or automatically managed through the system's functional configuration or installation. Development, validation, or debugging tools and software should not be present in the delivered system. Furthermore, all components or modules should be justified by a documented operational use case, which typically describes the need for a high-level application (service) that depends on relevant libraries and operating system modules.	Secure the weakest link Least privilege Economize Mechanism Assume secrets not safe Proportionality principle Secure defaults	Op Sys Sup	Tech Proc
SR 7.8	2	Control system component inventory	Upon a change to any component, the system should update the component inventory. This update should occur whenever a component is changed or its properties are modified and can be facilitated using either an active or a passive scanner.	Audit and monitor Make security usable	Op Sys Sup	Tech Proc

**Annex D**  
(informative)

**Safety and cybersecurity**

## General

The discussion on the relationship between cybersecurity and safety has produced many different and contradictory recommendations. In IEC TR 63069:2019 some general guidance for standardization has been worked out, which is used as the basis in this [Annex D](#), which aims at a more specific derivation and justification of basic principles for the railway field.

Concerning terminology, 'security' is used in this annex synonymously for cybersecurity unless physical security or other issues are meant. In the same way, 'safety' is used for functional safety. It is assumed that the reader is familiar with the basic safety and security concepts as stated, e.g. in standards such as IEC FDIS 62278-1:2024 [\[17\]](#) or IEC 62443 series.

### D.1 Differences between safety and cybersecurity

Safety and security have

- complementary goals: safety mainly seeks to protect people or the environment from malfunctions of automation systems, while security aims to protect the technical systems from attacks from the environment;
- different regulatory authorities, e.g. the Federal Railway Authority (EBA) and Federal Office for Information Security (BSI) in Germany, the National Cybersecurity Agency (ANSSI) and the national railways safety agencies in France, the European Union Agency for Railways (ERA) and the European Union Agency for Network and Information Security (ENISA) in Europe, Federal Railway Authority and Department of Homeland Security National Cyber Security Division (NCSD) and Cybersecurity and Infrastructure Security Agency (CISA) in the USA.
- different concepts e.g. hazards are considered in safety and threats are considered in cybersecurity;
- different communities, e.g. journals, conferences and standardization committees are mostly separate;
- different standards, e.g. the IEC 62278 series for RAMS (including safety) and the ISO 27000 or IEC 62443 series for security.

In safety, frequent changes should be avoided because of the cost of updating the safety demonstration. In cybersecurity, updates should be easy to apply in order to be able to patch the system in a timely manner, as frequently as needed. Thus, this is the strong rationale to segregate by design cybersecurity from safety as far as possible.

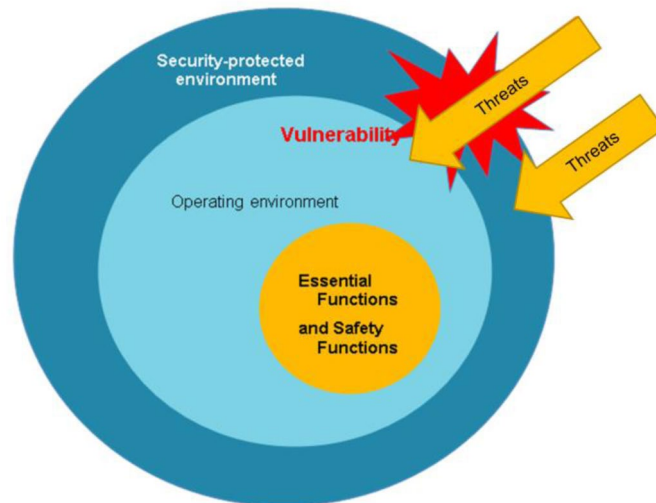
Methods and solutions are also different, as are requirements, which are often conflicting. Let us take as a simple example an emergency message (e.g. to immediately shut down a system or stop a train). From the safety perspective the message should be transmitted as fast as possible, and the reaction should be executed immediately. From a security perspective the message should be authenticated to prevent masquerade which might lead at least to denial of service, if an attacker could simply send emergency messages (like the attack in August 2023 on Polish railways). But the calculation and checking of cryptographic codes consumes time and leads to a delay of the emergency message and the reaction. Alternatively, emergency messages could be pre-calculated at the sender side to save some time, but this could open the door for replay attacks. Another possibility might be the cyclic sending of heartbeat message, which would trigger an emergency reaction if these were not received in time. So, the sender would simply stop sending heartbeats, but the delay would depend on the cycle time. In summary the trade-off in safe and secure design is not easy and it can be sometimes hard to find an optimal solution.

So, we can conclude that safety and security are different and that they cannot easily be merged. Furthermore, security cannot simply be regarded as an add-on to safety or vice versa.

**Principle 1: Safety and cybersecurity are distinct topics and should be managed as such.**

## D.2 Security from a safety perspective

Safety relies on several environmental conditions or influences that need to be controlled in order to guarantee safety. These are listed in 7.2 of IEC FDIS 62278-1 [17] and form a mandatory subclause, “assurance of safety with adverse external influences”, in the technical safety report, see Figure D.1. One of these aspects to be covered is access protection and this is where security has its interface with safety.



**Figure D.1 – Security as an environmental condition for safety**

The view from a security perspective, e.g. IEC 62443- series, is similar. Here safety is viewed as an essential function that needs to be protected. Other essential functions are operational functions or availability. This means that safety functions can only fulfill their intended use in an appropriate security environment. And this also explains why the UK Department of Transport is promoting “If it is not secure, it is probably not safe.” This leads to

**Principle 2: The security environment should protect essential functions, including safety.**

## D.3 Co-engineering of safety and security

Because of the many differences it is not reasonable to integrate safety and security. However, the processes and life cycles need to be coordinated and appropriate interfaces need to be established (see 6.3.8).

In particular, hazards resulting from security threats need to be identified, in the cybersecurity risk assessment. The safety engineer needs to provide support during the Cybersecurity Risk Assessment to assess the safety implications (impact of the risk). The definition of the appropriate security countermeasures states the full responsibility of security engineers in accordance with security standards. This gives

**Principle 3: Cybersecurity Risk Assessment is the main interface with Safety Analysis.**

Finally, conflicts between the identified safety and security measures should be resolved. During the safety risk assessment, the safety assessor assesses the safety implications of the SUC design which includes the implementation of its security requirement (please note that the Safety Assessor does not assess the security of the designed solution). Here it can be helpful if the security management supplies evidence in a manner compatible with safety management, e.g. trusted verification documents with clearly stated assumptions and application rules, so that safety and security assessments can be decoupled. This generally results in

**Principle 4: Separate security and safety as far as possible but coordinate them effectively.**

This also holds for architecture principles or maintenance processes such as SW updates. If safety and security were tightly integrated then any change in security functions might invalidate the safety case. Here an effective strategy could be to rely from a safety case point of view only on those parts of the security functionality that create a secure environment and on the application rules. So, if both the security functionality and the application rules remain unchanged, the safety case might remain valid even if the security SW is updated. Nevertheless, a justification that the changes have no effect on safety should be provided.

This is also recommended by IEC 62425:2025, which recommends referencing security analyses in the safety case only. In order to ease the integration, as well as compatibility, it is recommended to base security considerations on established international standards such as [ISO/IEC 27001:2022 \[12\]](#) or IEC 62443 series. Several analyses, e.g. by CENELEC TC9X or Shift2Rail, have also recommended IEC 62443 series as the baseline security standard for railway application.

**Principle 5: Security should be evaluated on the basis of international cybersecurity standards, e.g. IEC 62443 or this document.**

#### **D.4 Quantification of security**

Safety-related security problems occur because of threats to the integrity of the system. These threats arise from attackers who exploit vulnerabilities in the security environment. Attackers act intentionally, using all the information about the system that they can obtain, according to a certain state of the art in attacking or hacking. The degree might be different, depending on the attacker. So, differently from safety, no probability or rate of an attack exists. The similarity to safety is that the causes of security threats are similar to systematic faults in safety. Vulnerabilities often originate from errors in the security functionality, mainly SW, which is similar to SW faults in safety. It follows the

**Principle 6: It is infeasible to evaluate the Security Risk probabilistically.**

The major difference is that in security an attacker is needed to exploit the vulnerability (and the SL is related to the type of attacker), while in safety certain conditions in the operational environment trigger the SW fault, resulting in a system failure. So, security requirements need to be established in a similar way to safety integrity requirements, i.e., a scheme of target levels similar to safety integrity levels (SIL).

#### **D.5 The relationship between safety integrity levels and security levels**

Security levels (SL) according to IEC 62443 are defined with respect to the type of attacker. SL 1 represents unintentional errors or foreseeable misuse only, while SL 2, SL 3 and SL 4 relate to intentional attacks in which the attacker possesses increasing levels of knowledge, motivation and resources. As safety considers security as an environmental condition it is immediately evident that measures according to any particular SIL do not cover measures against intentional attacks. However, errors and foreseeable misuse also need to be addressed by safety-related systems, so any safety-related system should also cover SL 1, at least for requirements related to integrity. But for other SLs there is no automatic correspondence between SL and SIL as the SL will always depend on the security environment. And it should also be noted that security requirements cannot be fulfilled only by IT measures, but physical security measures are also necessary. In summary the following principle is established

**Principle 7: Safety and Security Target measures should not be coupled.**

However, there is a general relation between safety and security approaches. In safety there is the general rule that the first fault should not be hazardous, see e.g. [EN 50129:2018 \[30\]](#). Depending on the system design only a second similar fault can cause a failure. So many safety designs rely on detection and negation of the first fault.

In security a similar concept exists: defence in depth. This means that no single security measure should be regarded as sufficient. There should always be a second line of defence which protects against an attack. This does not mean that both security measures need to have the same effectiveness, but even for the most effective security measure there should be a fall-back. This implies that security measures should also be monitored for their effectiveness.

## **D.6 Responsibility for security**

As in safety, there is usually no single individual or body fully responsible for all security aspects. It is a joint effort of the operators (often called asset owners in security), the integration service providers (who supply complete systems), and the suppliers (who sell components). But unlike safety, the evaluation processes operate at a higher frequency in security. Even without any incident it is good practice to update threat risk assessments at least once per year and to feed the results forward and backward to the stakeholders at the interfaces. So, the conclusion is

### **Principle 8: Security is a collaborative continuous effort.**

And similar to safety, effective security protection relies heavily on the company culture. Many successful attacks show a similar pattern:

- first, the attacker gains access to the system (network),
- then the attacker explores the system, often trying to gain higher privileges, until
- finally, the attacker carries out the attack.

Access or higher privileges can be obtained by exploiting vulnerabilities (e.g. weak passwords) or by social means such as phishing. Often, the attacker cannot achieve his goals without operators or employees who breach security rules or are complacent. So, it is very important that security awareness is promoted and trained as part of the company culture.

## Annex E (informative)

### Risk acceptance methods

#### E.1 General

This annex contains examples of risk assessment methods that may be used in initial or detailed risk assessment such as risk matrices (see [Clause 7](#)).

For each method the following information should be documented:

- Impact Assessment;
- Likelihood Assessment;
- Risk Tolerability; and
- Justification.

Justification and references may also be documented.

#### E.2 Example 1

##### E.2.1 Introduction

The risk is the combination of the likelihood and the severity. [Table E.1](#) has been taken from [IEC 62278:2002 \[31\]](#). In contrast to [IEC 62278:2002 \[31\]](#), the term “likelihood” in cybersecurity is used in place of “frequency” or “probability”.

**Table E.1 – Risk Tolerability categories according to [IEC 62278:2002 \[31\]](#)**

Frequency of occurrence of an accident (caused by a hazard)	Risk Tolerability Categories			
<b>Frequent</b>	Undesirable	Intolerable	Intolerable	Intolerable
<b>Probable</b>	Tolerable	Undesirable	Intolerable	Intolerable
<b>Occasional</b>	Tolerable	Undesirable	Undesirable	Intolerable
<b>Rare</b>	Negligible	Tolerable	Undesirable	Undesirable
<b>Improbable</b>	Negligible	Negligible	Tolerable	Undesirable
<b>Highly improbable</b>	Negligible	Negligible	Negligible	Tolerable
	Insignificant	Marginal	Critical	Catastrophic
	Severity of an accident (caused by a hazard)			

To use the risk categories in security, a mapping of frequency and severity to the appropriate cybersecurity categories can be performed.

##### E.2.2 Impact assessment

[Table E.2](#) below shows a mapping between severity from [IEC 62278:2002 \[31\]](#) and security consequence, expressed in terms of railway control priority.

**Table E.2 – Severity categories**

Severity category (IEC 62278-1)	Severity description (IEC 62278-1)	Severity description (Cybersecurity)
No impact	No injury	No impact
Insignificant	Single minor injury	Confidentiality
Marginal	Multiple minor injury	Availability, moderate impact on service
Critical	Single fatality and / or single severe injury	System integrity and major impact on service
Catastrophic	Fatalities and / or multiple severe injuries	System integrity and severe service impact

**E.2.3 Likelihood assessment**

In cybersecurity, the term “likelihood” is used instead of frequency or probability. The evaluation of the likelihood or accessibility respectively is done by assessing the following criteria which are detailed in [Table E.3](#):

- Expertise Level (EXP);
- Equipment Needed (EQP);
- Window of Opportunity (WOO); and
- Time Needed (TIM).

**Table E.3 – Likelihood Assessment Criteria**

EXP	EQP	WOO	TIM	Rating / likelihood
Multiple Experts	bespoke equipment	short	long	low
Expert	specialised equipment	moderate	moderate	medium
Proficient	specialised COTS	long	long	high
Laity	standard equipment	unlimited	very short	very high

[Table E.4](#) shows a mapping between Likelihood in terms of Accessibility and Probability according to [IEC 62278:2002 \[31\]](#). The likelihood can only be estimated based upon the accessibility. The rationale is to estimate the likelihood of a successful attack, i.e. the mapping is indicated in [Table E.4](#):

**Table E.4 – Mapping Likelihood to Accessibility and Probability**

Likelihood in terms of Accessibility	Probability according to <a href="#">IEC 62278:2002 [31]</a>
public access	frequent
very easy	probable
easy	occasional
medium	rare
hard	improbable
very hard	highly improbable

The likelihood is derived from frequency levels as indicated in [Table E.3](#), i.e. the likelihood is the result of the different ratings of the 4 parameters EXP, EQP, WOO and TIM according to [Table E.3](#).

**E.2.4 Risk tolerability**

Risk tolerability is based upon risk assessment, definition of mitigations and final risk assessment.

The objectives of risk assessment are:



- To identify threats associated with the system;
- To identify the vulnerabilities regarding the threats to materialize;
- To determine the risk associated with the threats and vulnerabilities; and
- To identify the countermeasures to be implemented in the design to reduce the risk to a tolerable level.

Based upon the initial conceptual system architecture, existing safety and hazard assessments and the functional specification for SUC, a risk identification process is undertaken to provide outputs consisting of target security levels (SL-T) of the SUC and a conceptual zonal model which identifies the risk based system Security levels (SL) and boundary protection.

### E.2.5 Justification

Through this procedure a mapping of the security risk assessment to the [IEC 62278:2002 \[31\]](#) methodology is achieved. Justification of the result of security risk assessment is based upon the following three principles:

- Verification
- Validation
- Consideration of security within the safety case.

These three principles will be supported by the threats log.

## E.3 Example 2

### E.3.1 Introduction

Railway system integrators and turn-key suppliers can use this as a tool in their solution security risk assessment, mainly for large scale projects on both metro and main line networks. The structure is based on [ISO/IEC 27005:2022 \[32\]](#).

### E.3.2 Impact assessment

[Table E.5](#) gives an example of an impact assessment matrix for an system integrator.

**Table E.5 – Impact assessment matrix**

Category	Availability	Integrity (Safety)	Confidentiality	Integrity (Business)
A	Major interruption of operation affecting a network, a fleet or a loss of service for more than 500 000 people for an extended period of time	Catastrophic accident, typically affecting a large number of people and leading to multiple fatalities	Loss of security related information such as credentials, giving direct access to the system and leading to catastrophic safety, availability or business impacts	Catastrophic business impact possibly leading to bankruptcy or loss operator license
B	Major interruption of operation affecting a network, a fleet or a loss of service for more than 500 000 people for a significant time, or of a line, a station or few vehicles for an extended period of time	Critical accident, typically affecting a small number of people and leading to a single fatality	Loss of security related information, no direct access to the system is possible (physical protection), attacker could perform commands leading to at least critical availability, safety and business impacts.	Critical business impact possibly leading to severe impact in revenue or earnings (> 10 % on annual basis)

Category	Availability	Integrity (Safety)	Confidentiality	Integrity (Business)
C	Significant interruption of operation affecting a network, a fleet or more than 500 000 people for a short time, or of a line, station or few vehicles for a significant time	Safety implications, typically leading to injuries requiring hospitalization	Loss of security related information, no direct access to the system is possible (physical protection), attacker cannot perform any critical safety-related commands, for example, read only access to diagnostic data, loss of data under data protection laws or commercially sensitive data	Significant business impact possibly leading to substantial impact on revenue or earnings (on an annual basis)
D	Significant interruption of operation of a line, station or a few vehicles for a significant time	Minor safety implications, typically leading to injuries without hospitalization	Loss of non-security relevant data, data that is not under data protection, the attacker can make commercial use of the data by combining it with other information	Marginal business impact
E	Typically no influence	Typically no safety implications	Loss of non-security relevant data, data this is not under data protection	Negligible business impact

NOTE Down times is application specific, for example, a long time is 1 week for some mainline networks but 1 day for some metro networks, or a significant time is either 1 day or 1 hour, respectively.

### E.3.3 Likelihood assessment

Likelihood is estimated from scales based on the exposure and vulnerability of the asset.

Table E.6 gives an example of a likelihood assessment for an system integrator.

**Table E.6 – Likelihood assessment matrix**

Rating	Exposure	Attacker's competencies and means
1	Highly restricted logical or physical access for the attacker, such as: <ul style="list-style-type: none"> <li>– a highly restricted network and physical access; or</li> <li>– product or components that cannot be acquired by attacker or only with high effort</li> </ul>	<ul style="list-style-type: none"> <li>– A successful attack is only possible for a small group of attackers with high hacking skills (high capabilities needed)</li> <li>– Vulnerabilities are only exploitable with high effort, and if strong technical difficulties can be solved, non-public information about inner workings of a system is required</li> <li>– State of the art security measures to counter the threat</li> <li>– High chance for attacker to be traced and prosecuted</li> </ul>
2	Restricted logical or physical access for attacker, such as: <ul style="list-style-type: none"> <li>– internal network access required; or</li> <li>– restricted physical access; or</li> <li>– product or components can be acquired by attacker with medium effort</li> </ul>	<ul style="list-style-type: none"> <li>– A successful attack is feasible for an attacker with average hacking skills (medium capabilities needed)</li> <li>– Vulnerabilities are exploitable with medium effort, requiring special technology, domain or tool knowledge</li> <li>– Some security measures to counter the threat</li> <li>– Medium chance for attacker to be traced and prosecuted</li> </ul>
3	Easy logical or physical access for attacker, such as: <ul style="list-style-type: none"> <li>– Internet access sufficient; or</li> <li>– public physical access; or</li> <li>– attacker has access as part of daily work, operation, or maintenance activities; or</li> <li>– product or components can be acquired by attacker with low effort</li> </ul>	<ul style="list-style-type: none"> <li>– A successful attack is easy to perform, even for an unskilled attacker (little capabilities needed)</li> <li>– Vulnerabilities can be exploited easily with low effort, since no tools are required, or suitable attack tools freely exist.</li> <li>– No, or only weak, security measures to counter the attack caused by the threat</li> <li>– Low chance for attacker to be traced and prosecuted</li> </ul>

Likelihood index  $L$  is calculated from Exposure and Vulnerability using the formula  $L = (Exposure) + (Attacker's competencies and means) - 1$ .

### E.3.4 Risk tolerability

Table E.7 gives an example of risk matrix assessment for an system integrator. The risk matrix is built on a 5x5 Risk Matrix.

**Table E.7 – Risk matrix**

Impact Likelihood	E	D	C	B	A
1	Low	Low	Low	Low	Low
2	Low	Low	Low	Medium	Medium
3	Low	Low	Medium	Medium	High
4	Low	Medium	Medium	High	Extreme
5	Low	Medium	High	Extreme	Extreme

It is expected that only 'Low' Risks will be tolerable (that is the risk level is below or equal to the Tolerable Risk defined). All other risks should be reduced by applying either technical or other counter measures, and accepted by the railway duty holder.

### E.3.5 Justification

The impact assessment matrix levels the different impacts. For safety consequences it applies the common safety impact criteria.

Likelihood assessments are only based on exposure and vulnerability (exploitability) of the system towards attacks. Subjective judgments are reduced as far as possible. The combination rule reflects a barrier model (both exposure and vulnerability present a barrier).

Both impact and likelihood are measured on ordinal scales. This means that their combination leads to a semi-ordered metric, so per definition, such as. (2,C) and (3,D), they are not directly comparable. Risk evaluation is symmetric and reflects risk isoclines in its diagonals. It starts with observation that (5,E) and (1,A) should be labelled “Low”, as, for example, the highest impact category A should be combined with the most demanding requirement 1. There are exceptions for three combinations such as (4,D), (3,C) and (2,B), which might also have been labelled “Low” but were regarded “Medium” in a risk aversion approach.

## E.4 Example 3

### E.4.1 Introduction

The method is used by a large-scale infrastructure manager.

### E.4.2 Impact assessment

Table E.8 gives an example of impact assessment matrix for an infrastructure manager.

**Table E.8 – Impact assessment matrix**

	Safety	Operational	Financial	Strategy	Reputation	Regulatory
<b>1-Minor</b>	Minor physical /psychological injuries or damage	Impacts on 10 000 people. Perturbation of local economy	Loss < 1 000 000	No market loss.	Impact local and punctuality	No juridical impact or regulatory

	Safety	Operational	Financial	Strategy	Reputation	Regulatory
<b>2-Moderate</b>	Major physical /psychological injuries or damage	Impacts on 100 000 people. Disruption of national economy / temporary loss of major infrastructure	1 000 000< Loss < 10 000 000	Market loss < 5 %	Impact local iterative or regional punctuality	No respect of regulatory or legal obligations with low administrative sanctions
<b>3-Significant</b>	Significant physical /psychological injuries or damage	Impacts on 1 000 000 people. Disruption national economy. Temporary loss of critical infrastructure critique. Definitive loss of a major infrastructure	10 000 000< Loss < 50 000 000	Market loss between 5 % and 10 %	Impact regional iterative or national punctuality.	Conviction and criminal sanction. Financial penalties important
<b>4-Critical</b>	Death or critical injuries on several people	Impacts on 10 000 000 people. Definitive loss of a critical infrastructure	Loss > 50 000 000	Market loss > 10 %	Impact national iterative.	Major infraction resulting in criminal conviction. term of imprisonment

#### E.4.3 Likelihood assessment

Table E.9 gives an example of a likelihood assessment matrix for an infrastructure manager.

The four likelihood factors are evaluated on a scale from 1 to 4, which are then multiplied to provide an overall likelihood score.

**Table E.9 – Likelihood assessment matrix**

Value	IT competency	Motivation	Easy to discover	Exposition
<b>4</b>	Novice	Railway accident / transportation paralysis / critical damages	Known vulnerabilities	Direct access or public access
<b>3</b>	IT knowledge and public information on industrial control system (ICS)	Major blackmail / national or international notoriety	Vulnerabilities identified by superficial analysis	Enterprise network
<b>2</b>	Advanced knowledge on ICS and hacking	Local blackmail / personal revenge	Identification of vulnerabilities with an expertise and need of resources	Internal network with restraint access or access which requires privileged information
<b>1</b>	Expertise in hacking	Curiosity, challenge	Discover extremely improbable during a reasonable time	Local access

Based on the product of the factors the overall likelihood level is determined by Table E.10.

**Table E.10 – Likelihood conversion table**

Conversion limit	
Product	Change of level
16	> 1
24	> 2
64	> 3

#### E.4.4 Risk tolerability

Table E.11 gives an example of a risk tolerability 4x4matrix for an infrastructure manager.

**Table E.11 – Risk matrix**

Likelihood/Impact	1	2	3	4
4	3	3	4	4
3	2	3	3	4
2	2	2	3	3
1	1	2	2	3
Risk Severity Levels				

In this example, the risk severity is used to define the level of mitigation needed according to Table E.12.

**Table E.12 – Risk Severity / Mitigation matrix**

Risk severity	Description	Risk mitigation
4	Very High Risk	Measures required with the highest priority
3	High Risk	Measures required
2	Moderate = medium and significant	Measures recommended
1	Low risk	Measures optional

#### E.4.5 Justification

This methodology identifies the 6 main criteria to be considered for a railway infrastructure manager: Safety, Operational, Financial, Strategy, Reputation and Regulatory.

Likelihood is calculated as a function of 4 parameters, 2 related to the attacker profile (IT competency and Motivation) and 2 related to the SUC itself (Vulnerability easiness to discover and exposition).

A specific addition in this methodology is the link and prioritization made between the severity of a risk and the level of need of a risk mitigation (from optional measure to the highest priority).

### E.5 Example 4

#### E.5.1 Introduction

This method is used by a product supplier as a tool in their solution security risk assessment. Its structure is based on the [ISO/IEC 27005:2022 \[32\]](#) standard and is fully applicable with a cyber Process Hazard Analysis (PHA) methodology.

#### E.5.2 Impact Assessment

Table E.13 gives an example of an impact assessment matrix for a product supplier.

**Table E.13 – Impact assessment matrix**

Category	Safety impact	Financial impact	Availability / Quality of service impact	Customer / Company's image impact	Legal
1- Negligible	No safety involvement	No or little impact	Service is slightly disturbed or interrupted for a very short time	No Customer / Company's image impact Bad internal feedback	Warning
2-Limited	No safety impact	Project issue resolution costs	Service is degraded or interrupted for a short time	Low media coverage Bad feedback from passengers	Fine
3- Important	SIL1 or SIL2 event	Impact on business activities	Service is long term disrupted	Media coverage at national level Specialised press coverage	Moderate legal impact
4-Critical	SIL3 or SIL4 event	Critical losses	Service is interrupted with no putting back to service.	Media coverage at international level Public media coverage	Critical legal impact

**E.5.3 Likelihood assessment****E.5.3.1 General**

Likelihood is calculated from an intrinsic likelihood and contribution of security measures already in place.

**E.5.3.2 Intrinsic likelihood**

The evaluation of the intrinsic likelihood is calculated by formula

$$\text{Intrinsic likelihood} = \frac{\text{EXP} + \text{EQU} + \text{WOO} + \text{KOT} + \text{ETI}}{5} \quad (\text{E.1})$$

where:

EXP	Expertise of the attacker
EQU	Equipment Means
WOO	Window of opportunity
KOT	Knowledge of the target
ETI	Elapse time

Table E.14 gives an example of expertise of attacker matrix.

**Table E.14 – Expertise of the attacker matrix**

Rating	Expertise of the attacker	Description
1	Multiple Expert	Highly skilled in multiple areas (including product operation) necessary to conduct a complex attack.
2	Expert	High and specific knowledge of an attack. The nature of the expertise depends on the type of attack.
3	Proficient	Knowledge of information security or product operation and is familiar with the security behaviour of the target.

Rating	Expertise of the attacker	Description
4	Layman	No particular expertise of information security.

Table E.15 gives an example of equipment means matrix.

**Table E.15 – Equipment means matrix**

Rating	Equipment Means	Description
1	Bespoke equipment	Several specialised equipment needing large resources and time to develop, assemble or build.
2	Specialised equipment	Equipment which cannot be readily bought even in specialised shop. Equipment may be specially produced or developed, assembled, or built for the attack.
3	Specialised COTS	Equipment which can be readily bought, but which is usually not yet in the possession of an average person.
4	None/Standard Equipment	No equipment or equipment (hardware or software), commonly already available and/or easy to buy (e.g. a laptop).

Table E.16 gives an example of window of opportunity matrix.

**Table E.16 – Window of opportunity matrix**

Rating	Window of opportunity	Description
1	Short	The target is rarely accessible or during short period, or both.
2	Moderate	The target is often accessible or during moderate period, or both.
3	Long	The target is frequently accessible or during long period, or both.
4	Unlimited access	The target is always accessible.

Table E.17 gives an example of knowledge of the target matrix.

**Table E.17 – Knowledge of the target matrix**

Rating	Knowledge of the target	Description
1	Critical	Information concerning the target is tightly access controlled to few individuals on a strict need to know basis and individual undertaking.
2	Sensitive	Information concerning the target is access controlled to limited groups of people inside the division or project organization, (e.g. knowledge that is shared between discreet teams within developer organization which is constrained only to members of the specified teams).
3	Restricted	Information concerning the target is access controlled to large group of people inside the division or project organization, (e.g. knowledge that is controlled within the developer organization-disclosure agreement).
4	Public	Information concerning the target is publicly available (e.g. available on the internet).

Table E.18 gives an example of elapsed time matrix.

**Table E.18 – Elapsed Time matrix**

Rating	Elapse time	Description
1	Long	The attack is difficult to prepare - elapse time is greater than a month.
2	Moderate	The attack needs moderate time of preparation - elapse time is less than a month.
3	Short	The attack is easy to prepare - elapse time is less than a week.
4	Very Short	The attack is very easy to prepare - elapse time is less than a day.

### E.5.3.3 Contribution of security measures

Table E.19 gives an example of a contribution of security measures.

**Table E.19 – Contribution of security measures matrix**

Rating	Contribution	Description
1	Low	No major security measures contributing to mitigate the threat scenario are identified.
2	Medium	At least one major security measure contributing to mitigate the threat scenario is identified.
3	High	At least two major security measures contributing to mitigate the threat scenario are identified.
4	Very high	No lack of major security measure identified / More than two major security measures contributing to mitigate the threat scenario are identified.

### E.5.3.4 Likelihood calculation

The likelihood is calculated from the intrinsic likelihood rating and from the contribution of security measures rating.

Table E.20 provides an example of likelihood matrix.

**Table E.20 – Likelihood matrix**

Likelihood		Contribution of security measures			
		1	2	3	4
Intrinsic likelihood	1	Very unlikely	Very unlikely	Very unlikely	Very unlikely
	2	Significant	Very unlikely	Very unlikely	Very unlikely
	3	Likely	Significant	Very unlikely	Very unlikely
	4	Very likely	Likely	Significant	Very unlikely

### E.5.4 Risk acceptance

Table E.21 provides an example of risk acceptance matrix assessment for a product supplier.

**Table E.21 – Risk acceptance matrix**

Likelihood		Likelihood			
		1	2	3	4
Impact	1	Low	Low	Medium	Medium
	2	Low	Medium	Medium	High
	3	Medium	Medium	High	Very High
	4	Medium	High	Very High	Very High

In this matrix, only low and medium risks are acceptable. All other risks should be reduced either by technical or other countermeasures and be accepted by the system integrator.

### E.5.5 Justification

This approach takes in consideration different criteria at product level.

The impact is defined through 5 items: Safety, Financial, Availability / Quality of service, Customer / Company's image and Legal.



The likelihood takes into consideration 5 criteria (Expertise of the attacker, Equipment Means, Window of opportunity, Knowledge of the target, Elapse time) and also takes in consideration the context in which the product is used with the contribution of security measures.

## Annex F (informative)

### Railway system models and zone models

#### F.1 Design guidance and rules

##### F.1.1 Design guidance for system models

A high-level railway system model should be established by defining groups of subsystems and functionalities as in the examples provided in [Table F.1](#). Subsystems and functionalities should be grouped to have the same criticality level for each zone from cybersecurity perspective

The colour scheme for subsystems used in [Figure 4](#) and [Figure 5](#) in [Clause 4](#) is based on a classification by functionality and criticality.

**Table F.1 – Classification of railway subsystem groups**

Subsystem group	Criteria	Examples
Signalling	Safety-related subsystems responsible for safe train routes and movements	Interlocking, Automatic Train Protection, emergency brake
Command & control (for fixed installation and on-board)	Essential subsystems with potential safety related impact when out of order  Fixed installations, energy, natural hazards, building construction.  Automatic route setting for trains, detection, and resolution of potential conflicts.	Doors, braking, fire detection, Traffic Management System, substations, power plants, point heating, lighting, sectioning locations, separation sections, contact line system, return circuit, tunnel systems (oil, water, and pollution detection), UPS systems, emergency systems (ventilation, lighting, evacuation etc), container service systems,
Auxiliary	Subsystems without safety related impact; but with potential availability-related impact regarding continuous operation; with juridical or regulatory needs or other mandatory aspects	Lighting, HVAC, JRU, diagnostic systems
Comfort	Perception and customer relationship; safety for customers, commercial data	Passenger information system, PA, monitoring of seat occupancies, CCTV, billing
Public	Direct interaction between subsystem and customer / device of customer	Internet on board, screen with wireless interaction
Communication	Subsystems for interconnection within other subsystems or between subsystems	Train to ground communication through telecom network, train to train communication through Wi-Fi connection, GSM-R

The Internet, other company networks and public networks, out of compliance of the asset owner, should be considered by default as untrusted.

##### F.1.2 Design rules for the area-based model

For the example in [Figure 4](#) the following design rules have been applied:

- a block represents an (OT) subsystem;
- block name and acronym are chosen from IEC standards, where defined;
- block colour is selected by the railway duty holder according to its railway specific policy or rules;
- physical area as one of the following:

- Central Operational Control and Maintenance: block main function is performed in data centres, railway buildings and offices;
- De-centralized operational and field maintenance: block main function is performed along the rails;
- On-board: block main function is located on trains, locomotives or cars

### **F.1.3 Design rules for the topology-based model**

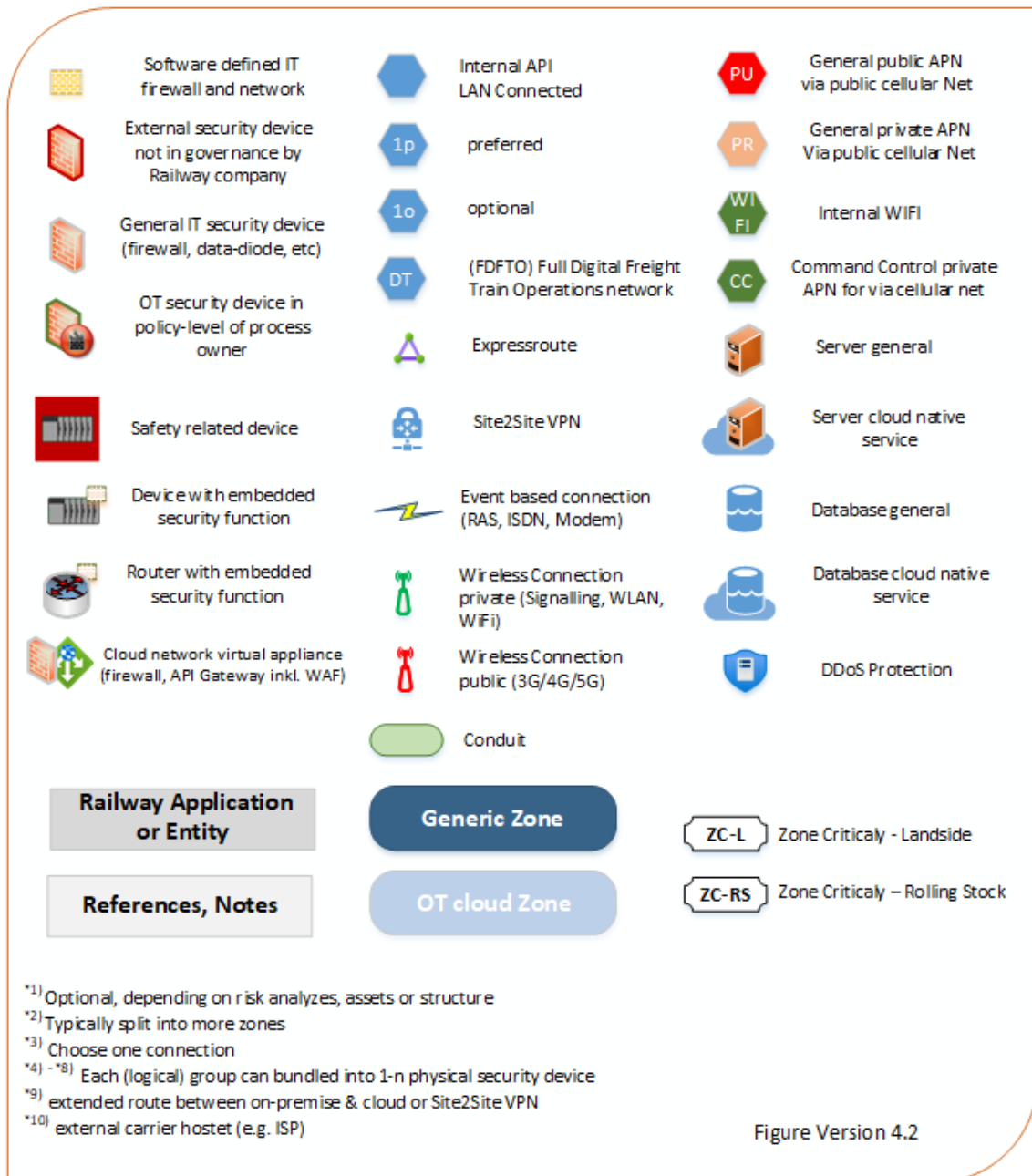
For the example in [Figure 5](#) the following design rules have been applied:

- a block represents an (OT) subsystem.
- block name and acronym are chosen from IEC standards, where defined;
- block colour is selected by the railway duty holder according to its railway specific policy or rules;
- the subsystems are positioned to show their spatial distribution and the coupling to the railway-wide data network

## **F.2 Magnifications of the high-level railway zone model**

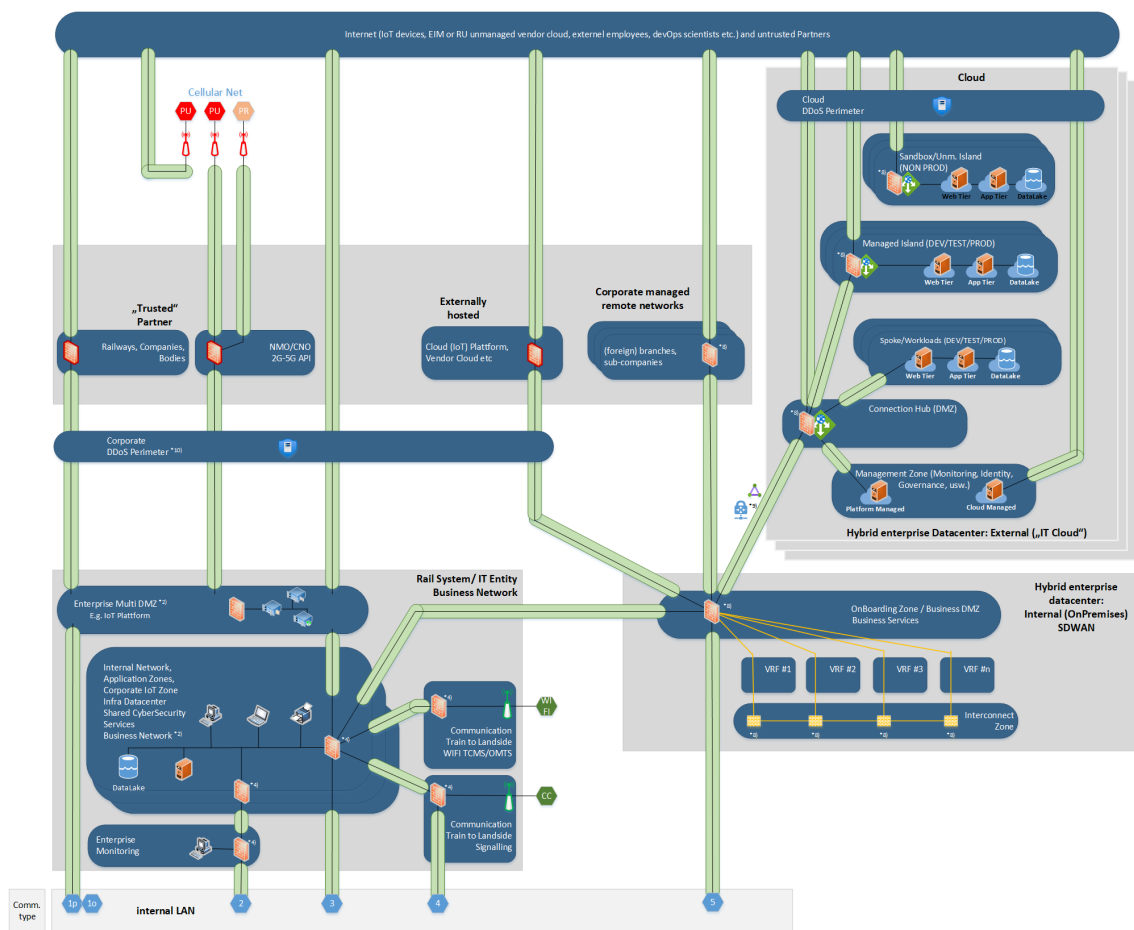
This chapter contains enlarged representations of the high-level railway zone model, as shown in [Figure 6](#).

[Figure F.1](#) shows legend of [Figure 6](#) and [Figure F.2](#) to [Figure F.5](#).



**Figure F.1 – Legend of Figure 6 and Figure F.2 to Figure F.5**

Figure F.2 below shows an example of zones in the corporate office network, business-IT, data centre and cloud environment, that are typical used.



**Figure F.2 – Business-IT and general-IT zones (example)**

Figure F.3 below shows an example of zones in the OT networks of different SUC's or entities, that are typically used.

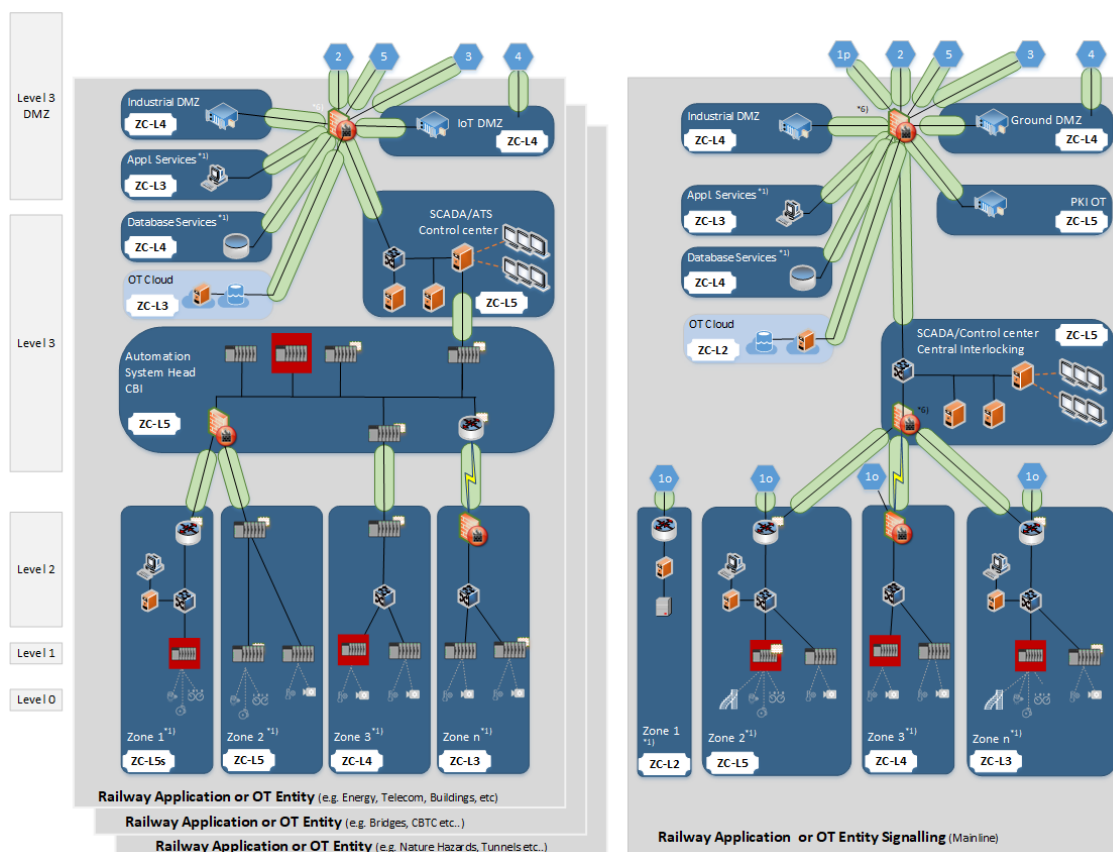


Figure F.3 – OT Zones (example)

## F.2.1 Design Guidance for zone models

### F.2.1.1 Introduction

This annex contains examples for zoning and segmentation of the railway domains: fixed installations, landside, rolling stock and trackside.

NOTE For a better readability in the following tables and figures, the domains fixed installations, landside and trackside are summarized in this Annex as "landside".

Please also note the criteria for zones and conduits breakdown in 7.5.

The following terms are used in this annex:

#### Zone criticality (ZC)

The criticality represents the security demands in a simplified way. The ZC defines the criticality of each zone in comparison to other zones and it is used to determine the communication rules via the communication matrix.

#### Zone criticality landside (ZC-L)

The ZC-L should be defined by the infrastructure manager or railway duty holder ; unique for all entities and branches in trackside, landside and fixed installations.

#### Zone criticality rolling stock (ZC-RS)

The ZC-RS should be defined by the railway undertaking or railway duty holder ; unique for each fleet in the rolling stock environment.

### **Communication matrix**

The communication matrix shows on a high-level the authorized and unauthorized communication. The communication matrix is the base to define rule sets for security devices to control the data flow between zones.

### **Data diode**

Data diodes are security devices that allow data flow only in one direction.

#### **F.2.1.2 General rules**

- Zones that are connected should fulfill a mapping table that identifies allowed data flow between zones
- All data should be checked by a security device in the corresponding subsystem
- The CISO (or a delegated information security officer) approve communication which are not defined in standards or specifications
- Exceptions should be identified in the documentation with associated risk.

#### **F.2.1.3 Landside (fixed installations, landside and trackside)**

##### **F.2.1.3.1 Zone criticality levels**

Every zone identified in the initial or detailed risk assessment should be classified according to the risk's criticality. The criticality represents the security demands in a simplified way to define the allowed communication between zones.

The following steps show an approach for a high-level communication concept.

#### **Step 1: Evaluating “groups of criticalities” with similar security requirements**

Evaluate groups of available criticality levels with well-known security demands of the target network concept based on asset types and their corresponding risks.

Table F.2 below shows an example of a typical result:

**Table F.2 – Example - Evaluating groups of criticalities for landside-landside communication**

<b>Zone Criticality and Communication Matrix</b>			
	<b>Zone Criticality Landside (ZC-L)</b>	<b>Security Maturity</b>	<b>Example</b>
		highly secure / safety	safety: interlocking, high voltage
		highly secure / critical	SCADA, ATS, central ICS, platform screen doors
		secure	data Centre, internal DMZ, ICS/automation
		medium	internal network, office and business network
		low	gateway area, external DMZ
		low	external partner/companies
		untrusted	internet

**Step 2: Define the criticality of ZC-L zones**

The number of zones and criticality levels can be chosen individually by the asset owner; but should be unique for their whole infrastructure. In this example: 6 non-safety plus 1 safety levels are defined in [Table F.3](#):

**Table F.3 – Example - Zone criticality definition for landside-landside communication**

<b>Zone Criticality and Communication Matrix</b>			
	<b>Zone Criticality Landside (ZC-L)</b>	<b>Security Maturity</b>	<b>Example</b>
	<b>ZC-L 5s</b>	highly secure / safety	safety: interlocking, high voltage
	<b>ZC-L 5</b>	highly secure / critical	SCADA, ATS, central ICS, platform screen doors
	<b>ZC-L 4</b>	secure	data Centre, internal DMZ, ICS/automation
	<b>ZC-L 3</b>	medium	internal network, office and business network
	<b>ZC-L 2</b>	low	gateway area, external DMZ
	<b>ZC-L 1</b>	low	external partner/companies
	<b>ZC-L 0</b>	untrusted	internet

**Step 3: Set up a communication matrix**

The matrix can be chosen depending on the number of zone criticality levels but should refer to the communication rules in [Clause F.2.1.3.3](#). The communication matrix is an input for the zones and conduits drawings [ZR-03-01] (see [7.5.3](#)) and shows the communication flows as for example in [Table F.4](#).

The communication matrix is based on the following rules:



- Direct communication between zones with well-known risk (e.g. zones with well-known and fixed mounted OT devices) and unknown risk (e.g. office zones with laptops, printer, internet connectivity) without passing a security device should be refused.
- In general, direct (bidirectional) communication is only allowed between zones with the same or a subsequent zone criticality.
- Communication should sequentially pass all zone critically levels (e.g. ZC-L5 to ZC-L4 to ZC-L3). Bypassing or jump over (e.g. from ZC-L3 direct to ZC-L5) is only allowed if “read only” from higher to lower zone critically or an approved risk acceptance by the asset owner and the CISO.
- A cloud environment fully managed by the infrastructure manager (or responsible) is handled in the same way as an internal on-premise network. A Tenant is like an internal on-premises network, and spokes are similar as zones.

**Table F.4 – Example - Landside-landside communication matrix basic structure**

<b>Zone Criticality and Communication Matrix Landside - Landside</b>				safety: interlocking, high voltage	SCADA, ATS, central ICS, platform screen doors	data Centre, internal DMZ, ICS/automation	internal network, office and business network	gateway area, external DMZ	external partner/companies	internet
				highly secure / safety	highly secure / critical	secure	medium	low	low	untrusted
	<b>Zone Criticality Landside (ZC-L)</b>	<b>Security Maturity</b>	<b>Example</b>	<b>ZC-L5s</b>	<b>ZC-L5</b>	<b>ZC-L4</b>	<b>ZC-L3</b>	<b>ZC-L2</b>	<b>ZC-L1</b>	<b>ZC-L0</b>
	<b>Source / From</b>			<b>Destination / to</b>						
	<b>ZC-L 5s</b>	highly secure / safety	safety: interlocking, high voltage							
	<b>ZC-L 5</b>	highly secure / critical	SCADA, ATS, central ICS, platform screen doors							
	<b>ZC-L 4</b>	secure	data Centre, internal DMZ, ICS/automation							
	<b>ZC-L 3</b>	medium	internal network, office and business network							
	<b>ZC-L 2</b>	low	gateway area, external DMZ							
	<b>ZC-L 1</b>	low	external partner/companies							
	<b>ZC-L 0</b>	untrusted	internet							

**Step 4: Filling the communication matrix with principle rule-set**

The fine tuning of data flow is controlled by rules and access lists (e.g. of the security devices).

The data flow should be controlled depending on the safety and security demands of the zones:

- “+” data flow is allowed in both directions
- “R”: data flow is restricted to read-only only by data diodes or similar measures which maintain unidirectional flow
- “-”: data flow is prohibited

Table F.5 below shows an example of a typical communication matrix for landside:

**Table F.5 – Example - Communication matrix - landside to landside**

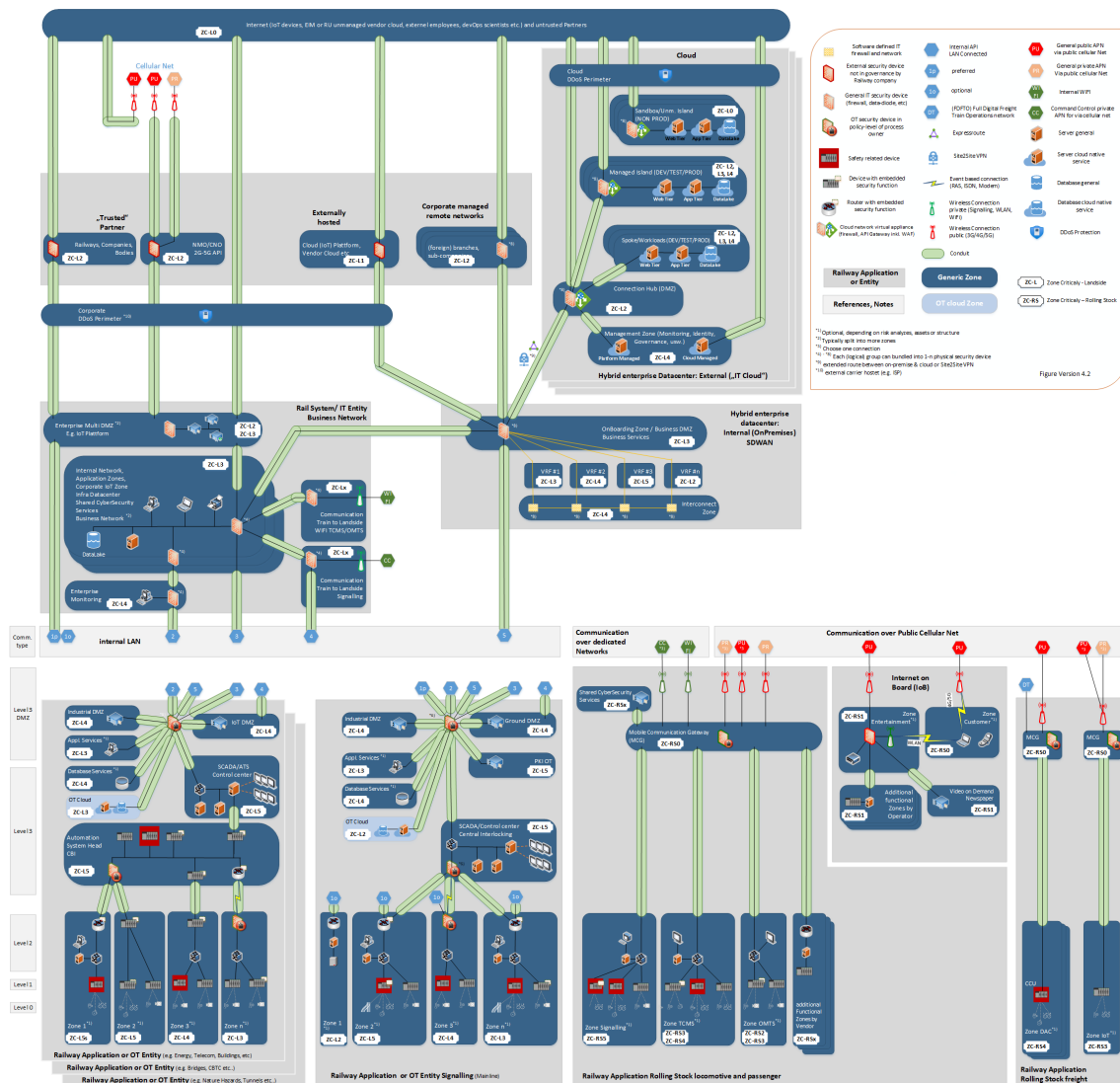
<b>Zone Criticality and Communication Matrix</b> <b>Landside - Landside</b>										
			highly secure / safety		highly secure / critical		secure		medium	
			ZC-L5s	ZC-L5	ZC-L4	ZC-L3	ZC-L2	ZC-L1	ZC-L0	
Zone-Criticality Landside (ZC-L)	Security Maturity	Example								
Source / From			Destination / to							
ZC-L 5s	highly secure / safety	safety: interlocking, high voltage	+	+	R	R	R	R	R	-
ZC-L 5	highly secure / critical	SCADA, ATS, central ICS, platform screen doors	+	+	+	R	R	R	R	-
ZC-L 4	secure	data Centre, internal DMZ, ICS/automation	-	+	+	+	R	R	R	-
ZC-L 3	medium	internal network, office and business network	-	-	+	+	+	R	R	-
ZC-L 2	low	gateway area, external DMZ	-	-	-	+	+	+	+	+
ZC-L 1	low	external partner/companies	-	-	-	-	+	+	+	+
ZC-L 0	untrusted	internet	-	-	-	-	-	+	+	+

This matrix covers data flow for standard operation usage. Temporary connections for remote maintenance are part of standard operations. The conditions to open a maintenance connection may be supported by multi factor authentication (e.g. SMS, email or pressing a button on the local network equipment). Additional physical measures (press a button, plug in or switch on the power supply of a modem e.g. are not part of the rule-set of the corresponding security device and out of scope of the communication matrix.

#### **F.2.1.3.2 Zoning and segmentation**

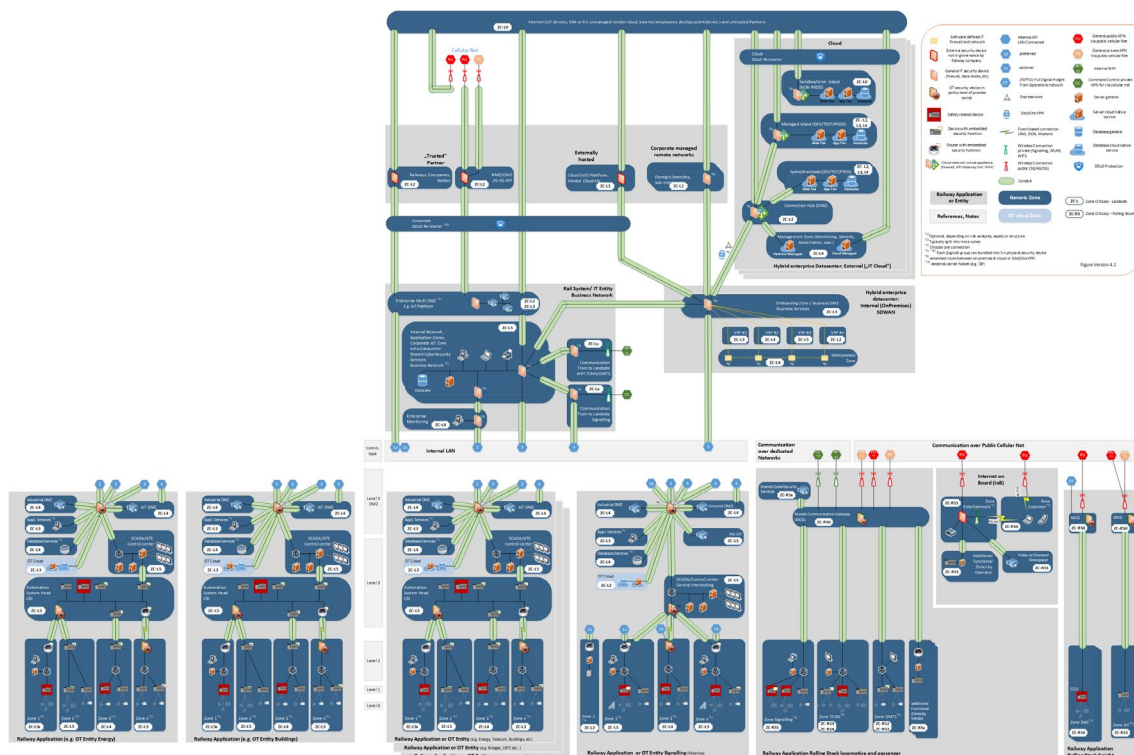
The communication matrix used to define data flows allowed in a generic high-level railway zone model should be compatible with the security needs at the border of these zones.

Figure F.4 below shows an example of high-level railway zone model with zone critically levels:



**Figure F.4 – Example of an adopted generic high-level railway zone model with zone critically levels**

Considering the result of the initial risk assessment (see 7.4) and functional asset groups, the generic high-level railway zone model can be subdivided in subsystems and zones. Figure F.5 shows an example:



**Figure F.5 – Example of a full overview of a high-level railway zone model with all entities**

NOTE The communication between rolling stock and landside is described in [Clause F.2.1.5](#).

### F.2.1.3.3 Communication rules

- The communication should be kept in the subsystem in order not to pass zones with other system responsibilities or different criticality.
- If communication cross-entities is necessary, data should flow via both entities DMZ.
- Communication into and out of zones should be well defined and supervised for detecting unauthorized communication (e.g. by an intrusion detection system).
- Communication between different subsystem groups or entities should be controlled by a security device (e.g. by a firewall).
- Communication between zones with different criticality within subsystem groups should be controlled by a security device.
- All communication into and out of subsystem groups should pass the same security device (or device group if redundant). Backdoors or parallel communication paths (like ISDN modem for direct remote maintenance), bypassing the corresponding security device should be disabled.

### F.2.1.4 Rolling stock

#### F.2.1.4.1 Zone criticality, zoning and segmentation

It is useful to define a high-level railway zone model based on zone criticality. The number of zones criticality levels should be defined by the asset owner and may be adapted depending type or generation of fleet.

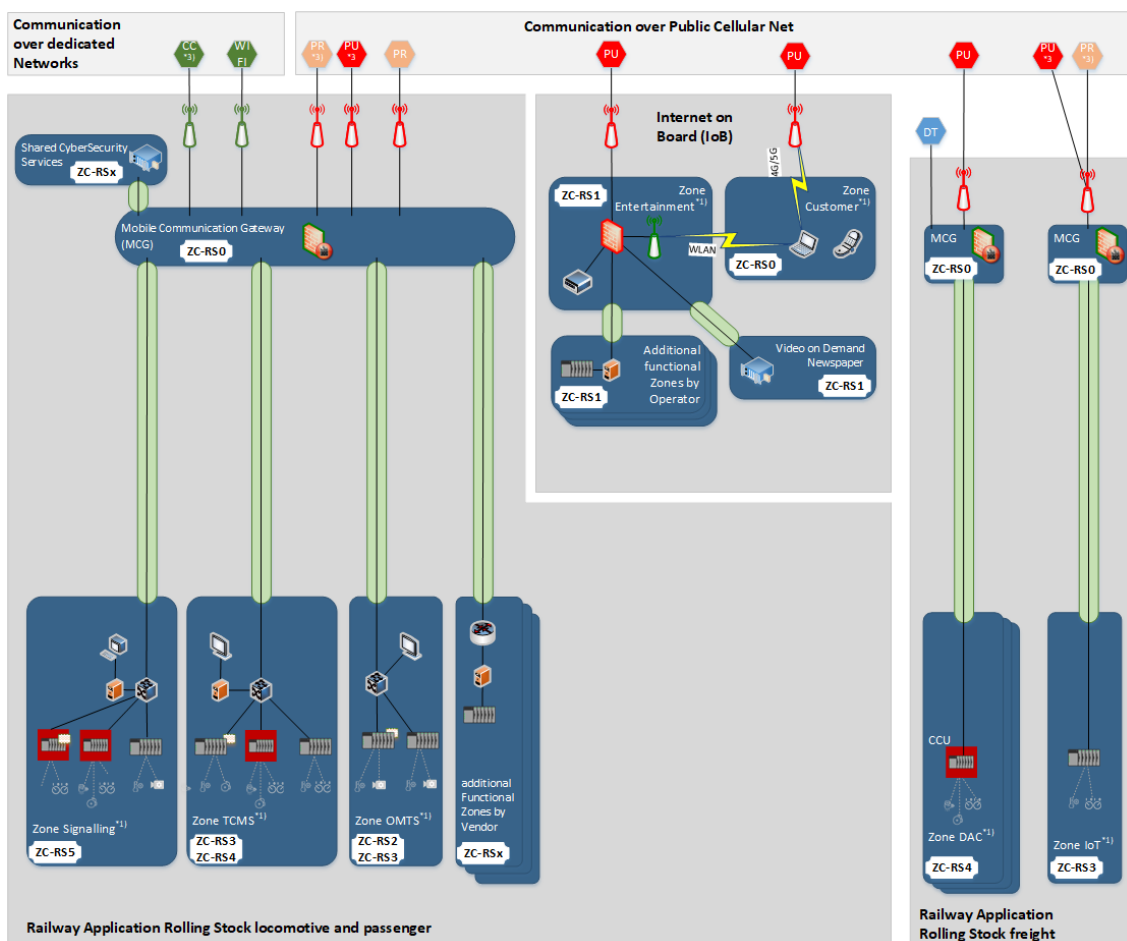
[Table F.6](#) below shows an example for a rolling stock:

**Table F.6 – Example - Zone criticality definition for rolling stock**

Zone criticality rolling stock (ZC-RS)	Security maturity / network layer		Example
<b>ZC-RS 5 / ZC-RS 5s</b>	Highly Secure / Safety	signalling	ATP systems
<b>ZC-RS 4</b>	Secure	command and control	TCMS, doors, traction and braking
<b>ZC-RS 3</b>	Medium	auxiliary	TCMS, CCTV, diagnostic
<b>ZC-RS 2</b>	Medium	comfort	Passenger information system
<b>ZC-RS 1</b>	Low	public interface	Entertainment Wi-Fi
<b>ZC-RS 0</b>	Untrusted	external communication channel	Train-to-ground Train-to-train

In this example, zone criticality levels are aligned with the six-colour scheme by subsystem groups (signalling, command and control, auxiliary, comfort, public, communication) described in [Clause 4](#). As stated before, zone criticality levels can be adapted by the asset owner. Thus, e.g. comfort (ZC-RS 2) and auxiliary (ZC-RS 3) may be gathered in a same level.

Figure F.6 shows an example of zones criticality in a Rolling Stock environment.

**Figure F.6 – Example of zones criticality in the Rolling Stock environment**

#### F.2.1.4.2 Zone criticality and communication matrix in the rolling stock domain

Table F.7 below shows an example of a typical communication matrix for zone criticality and communication rules in the rolling stock domain.

**Table F.7 – Example - Communication matrix - rolling stock to rolling stock**

Zone Criticality and Communication Matrix Rolling Stock - Rolling Stock				Signalling	Command and control	Auxiliary	Comfort	Public interface	External communication channel
				Highly Secure / safety	Secure	Medium	Medium	Low	Untrusted
	Zone-Criticality Rolling Stock (ZC-RS)	Security Maturity	Example	ZC-RS 5	ZC-RS 4	ZC-RS 3	ZC-RS 2	ZC-RS 1	ZC-RS 0
	Source / From			Destination / to					
	ZC-RS 5	Highly Secure / safety	Signalling	+	+	-	-	-	+
	ZC-RS 4	Secure	Command and control	+	+	+	+	R	+
	ZC-RS 3	Medium	Auxiliary	-	+	+	+	+/R	+
	ZC-RS 2	Medium	Comfort	-	+	+	+	+/R	+
	ZC-RS 1	Low	Public interface	-	-	-	-	+	+
	ZC-RS 0	Untrusted	External communication channel	+	+	+	+	+	+
				(a)	(a)	(a)	(a)		
<ul style="list-style-type: none"> <li>– “+” data flow allowed through appropriated security device</li> <li>– “R” data flow restricted to read-only by data diodes or similar measures</li> <li>– “-“ data flow prohibited</li> <li>– (a) data flow generally initiated from on-board device to outside</li> </ul>									

#### F.2.1.4.3 Communication rules

The high-level railway zone model allows defining a communication rules model.

The risk analysis allows correctly adapting communication rules (especially for “should” rules) and sets of measures within the specific context of a project.

Below an example of communication rules model is shown:

- signalling (ZC-RS5) and command and control (ZC-RS4) can be connected
- connection between command and control (ZC-RS4) and signalling (ZC-RS5) should require security device/solution (1)
- signalling (ZC-RS5) and others (different than ZC-RS4) cannot be directly connected
- comfort (ZC-RS2) and command and control (ZC-RS4) can be connected
- auxiliary (ZC-RS3) and command and control (ZC-RS4) can be connected
- connection between comfort (ZC-RS2)/auxiliary (ZC-RS3) and command and control (ZC-RS4) should require security device/solution (1)
- comfort (ZC-RS2) and auxiliary (ZC-RS3) can be connected
- comfort (ZC-RS2) and auxiliary (ZC-RS3) may be gathered in a same level

- connection between comfort (ZC-RS2) and auxiliary (ZC-RS3) may require security device/solution (1)
- comfort (ZC-RS2) and public (ZC-RS1) can be connected (in that case, it is highly recommended to segregate physically these two zones (ZC-RS1 and ZC-RS2) from the rest (ZC-RS3 and higher))
- auxiliary (ZC-RS3) and public (ZC-RS1) can be connected (in that case, it is highly recommended to segregate physically these two zones (ZC-RS1 and ZC-RS3) from the rest (ZC-RS4 and higher))
- connection between comfort (ZC-RS2)/auxiliary (ZC-RS3) and public (ZC-RS1) should require security device/solution (1) and a DMZ; except if using a data-diode to ensure unidirectional communication from (ZC-RS2)/(ZC-RS3) to (ZC-RS1)
- public (ZC-RS1) and command and control (ZC-RS4) cannot be directly connected; except if using a data-diode to ensure unidirectional communication from (ZC-RS4) to (ZC-RS1)
- public (ZC-RS1) and signalling (ZC-RS5) should not be directly connected
- each ZC-RS1/5 on-board network can be connected to ground through train-to-ground component(s) (ZC-RS0)
- connection between ZC-RS1/5 and ZC-RS0 should require security device/solution (1)
- signalling (ZC-RS5) could use dedicated train-to-ground component (ZC-RS0) as transparent communication channel.
- train-to-ground component (ZC-RS0) could be shared for comfort (ZC-RS2), auxiliary (ZC-RS3) and command and control (ZC-RS4) networks; using security device/solution (1) to ensure no possibilities of bouncing between ZC-RSx networks
- train-to-ground component (ZC-RS0) for public (ZC-RS1) cannot be shared with for command and control (ZC-RS4) networks or signalling (ZC-RS5) without a physical segregation of the channels that ensure no possibilities of bouncing between ZC-RSx networks, neither in case of vulnerability issue.
- for ZC-RS0, the set of security measures (using private APN, secured protocols within a public telecom networks, dedicated networks as Wi-Fi or [TETRA \(3.1.173\)](#), authenticate mechanisms, hardening of exposed components) depends on the components used and the capability of the telecom networks; and should fulfill the security needs of the supported applications
- connection between ZC-RS0 and landside network should require a DMZ at the boundary to landside (through Enterprise DMZ and NMO/CNO access)

NOTE See [Clause F.2.1.5.2](#), [Clause F.2.1.5.3](#) and [Clause F.3](#) for more details about train-to-ground,

(1) security device/solution may be e.g. a security gateway with firewalling function, router with appropriate settings function

## **F.2.1.5 Communication rules between rolling stock and landside**

### **F.2.1.5.1 Rolling stock and landside mapping table**

[Table F.5](#) and [Table F.7](#) present examples for zone criticality matrix for landside and for rolling stock.

These examples could be adapted by the asset owner for their responsible perimeter.

In order to define a readable communication matrix, it is strongly recommended to use a mapping-table for each direction of data flow as in the example [Table F.8](#) (landside to rolling stock) and example [Table F.9](#) (rolling stock to landside); according to each zone criticality matrix applied.



**Table F.8 – Example - Communication matrix - landside to rolling stock**

<b>Zone Criticality and Communication Matrix</b> Direction Landside => Rolling Stock				Signalling	Command and control	Auxiliary	Comfort	Public interface	External communication channel
				Highly Secure / safety	Secure	Medium	Medium	Low	Untrusted
	Zone-Criticality Landside (ZC-L)	Security Maturity	Example	ZC-RS 5	ZC-RS 4	ZC-RS 3	ZC-RS 2	ZC-RS 1	ZC-RS 0
	Source / From			Destination / to					
	ZC-L 5s	highly secure / safety	safety: interlocking, high voltage	+	-	-	-	-	-
	ZC-L 5	highly secure / critical	SCADA, ATS, central ICS, platform screen doors	-	-	-	-	-	-
	ZC-L 4	secure	data Centre, internal DMZ, ICS/automation	-	-	-	-	-	-
	ZC-L 3	medium	internal network, office and business network	-	+	+	+	-	-
			enterprise DMZ and NMO/CNO access	-	-	-	-	-	+
	ZC-L 2	low	gateway area, external DMZ	-	-	-	-	-	-
	ZC-L 1	low	external partner/companies	-	-	-	-	+	-
	ZC-L 0	untrusted	internet	-	-	-	-	+	+
<ul style="list-style-type: none"> <li>– “+” data flow allowed through appropriated security device</li> <li>– “-“ data flow prohibited</li> <li>– (a) see <a href="#">Clause F.2.1.5.2</a></li> <li>– (b) see <a href="#">Clause F.2.1.5.3</a></li> </ul>									



**Table F.9 – Example - Communication matrix - rolling stock to landside**

<b>Zone Criticality and Communication Matrix</b> Direction Rolling Stock => Landside				Signalling	Command and control	Auxiliary	Comfort	Public interface	External communication channel
				Highly Secure / Safety	Secure	Medium	Medium	Low	Untrusted
	<b>Zone-Criticality Landside (ZC-L)</b>	<b>Security Maturity</b>	<b>Example</b>	<b>ZC-RS 5</b>	<b>ZC-RS 4</b>	<b>ZC-RS 3</b>	<b>ZC-RS 2</b>	<b>ZC-RS 1</b>	<b>ZC-RS 0</b>
	<b>Destination / to</b>			<b>Source / From</b>					
	<b>ZC-L 5s</b>	highly secure / safety	safety: interlocking, high voltage	+	-	-	-	-	-
	<b>ZC-L 5</b>	highly secure / critical	SCADA, ATS, central ICS, platform screen doors	-	-	-	-	-	-
	<b>ZC-L 4</b>	secure	data Centre, internal DMZ, ICS/automation	-	-	-	-	-	-
	<b>ZC-L 3</b>	medium	internal network, office and business network	-	+	+	+	-	-
			entreprise DMZ and NMO/CNO access	-	-	-	-	-	+
	<b>ZC-L 2</b>	low	gateway area, external DMZ	-	-	-	-	-	-
	<b>ZC-L 1</b>	low	external partner/companies	-	-	-	-	+	-
	<b>ZC-L 0</b>	untrusted	internet	-	-	-	-	+	+

– “+” data flow allowed through appropriated security device  
 – “-“ data flow prohibited  
 – (a) see [Clause F.2.1.5.2](#)  
 – (b) see [Clause F.2.1.5.3](#)

NOTE 1 In an optimized system, landside (fixed installations, trackside and landside) and rolling stock have same groups and same zone criticality.

NOTE 2 The number of ZC levels in this example is freely chosen and can be adopted by the asset owner of the railway undertakings and infrastructure managers.

#### **F.2.1.5.2 Rules for business IT**

For connection between on-board network and IT business/office network landside (examples: diagnostic, CCTV):

- Zone criticality level may be different between on-board and landside.
- Train-to-ground communication should be secured by the application according to security needs. The set of security measures depends on the components used and the capability of the telecom networks.

NOTE Often, public telecom networks are used for communication.

Examples of measures:

- Using private APN (allow reducing the exposure of on-board communication devices)
  - Using secured protocols (to ensure integrity, confidentiality and authenticity of train to ground communication over public telecom networks)
  - Using authenticate mechanisms (to ensure identities)

- Hardening of exposed components (to reduce the attack surface)
- Communication preferentially initiated by on-board software/component
- A DMZ should be required at the boundary to the landside network for each communication channel through the train to ground network.
- Data flow should be checked by a security device in each subsystem (on-board and landside).
- The responsible CISO or delegated information security officer should approve that architecture and measures in place fulfill the security needs.

#### **F.2.1.5.3 Rules for operational technology (OT)**

Connection between on-board network and OT network landside (e.g. ERTMS, etc.):

- If zone criticality level is not the same between on-board and landside, the zone criticality with the same maturity should correspond and shown in the communication matrix mapping table (see [Clause F.2.1.5.1](#)).
- Sometimes, dedicated telecom networks are used for communication.
- Communication components and train-to-ground communication should be secured according to security needs. The set of security measures depends on the components used and the capability of the telecom networks.
- Data flow should be checked by a security device in each subsystem (on-board and landside).
- When a system should respect a normative specification (e.g. ERTMS), components and communications should fulfill the specification requirements, and the CISO (or delegated information security officer) approval may be optional in this case.
- For the other cases, the responsible CISO(s) or delegated information security officer should approve that architecture and measures in place fulfill the security needs.

### **F.3 Train to ground communication**

#### **F.3.1 Introduction**

According to

- the architecture on-board and landside (physical and logical segregation in place),
- the security needs of data flows (availability, integrity, confidentiality),
- the telecom channel and its capabilities,

implementation of train to ground communications can differ much from one project to another. Dedicated or shared equipment and channels (MCG and ground) could be used. The number of MCG on-board could vary. The number of access points could vary.

Choices and measures should fulfill security needs (see risk assessment) for data flows depending on exposure and capabilities; at start-up but also during operation/maintenance (this kind of product / functionalities may require to be included into the strategy for maintain in secure condition - see [Clause 10](#)).

#### **F.3.2 Communication channel**

Various technologies can be used for communication channel. The main ones are:

- dedicated cellular network (e.g. GSM-R, FRMCS, ATACS, TETRA) hosted by infrastructure manager
- public cellular network (public APN or private APN)
- wi-fi infrastructure

NOTE Hybrid channel (e.g. dedicated and public cellular network for FRMCS) could be used. In that case adapted security measures could be put in place to fulfill security needs.

### **F.3.3 Principles**

Some principles should be applied:

- authentication mechanisms should be used (an on-board component trying to connect to a ground device should first authenticate itself before access to ground services)
- secured channel (like VPN, SDWAN) could be used to globally protect application data flow
- communication flow should be secured, from-application-to-application directly routed through modem/MCG, or with flows relayed by communications services for example hosted in a MCG
- services should not be directly exposed to outside by an MCG; if necessary (for example for remote maintenance), other measures should be applied to enforce protection of these potentially exposed services (for example with services exposed only into a pre-established secure channel, with exposure temporarily activated by criteria like port knocking)
- filtering functionalities should be used to isolate communication device and to limit data flow allowed at border of the device
- the communication telecom channel could be used to manage the telecom equipment using secured protocols, such as SNMPv3, and NetCONF over SSH.

## **Annex G** (informative)

### **Cybersecurity deliverables content**

#### **G.1 Purpose**

This annex provides examples of table of content of main cybersecurity deliverables, compliant to the normative part of this standard.

These contents are provided as example and can be tailored according to organisation and project context.

- Railway OT cybersecurity policy;
- Railway OT cybersecurity programme;
- Cybersecurity management plan;
- Risk assessment report;
- Cybersecurity requirement specification;
- Cybersecurity guidelines for the railway solution;
- Cybersecurity evaluation plan;
- Cybersecurity case (for railway solution and railway application);
- Cybersecurity maintenance plan.

#### **G.2 Railway OT cybersecurity policy and cybersecurity programme**

##### **G.2.1 Railway OT cybersecurity policy**

Hereafter is an example of table of content of a railway OT cybersecurity policy, which is applicable to the whole railway duty holder organization:

- Reference documents
- Strategic considerations:
  - Scope of application
  - Challenges and strategic orientations
  - Legal and regulatory aspects
  - Applicable threat landscape and periodicity of update
  - Governance, roles and responsibilities
- Security rules:
  - Organizational security rules and measures
  - People security rules and measures
  - Physical security rules and measures
  - Data security rules and measures
  - Technological security rules and measures.

##### **G.2.2 Railway OT cybersecurity programme**

Hereafter is an example of table of content of a railway OT cybersecurity programme, which is applicable to a sub-set of the railway applications of the railway system:

- Reference documents (including the reference of the applicable OT cybersecurity policy)

- Strategic considerations
  - Scope of application  
(e.g. rolling stock, traction substation, signalling post, etc.)
  - Challenges and strategic orientations  
(e.g. maintaining secure state, security monitoring, continuity management)
  - Legal and regulatory aspects
  - Applicable security needs and groups of threats from threat landscape
  - Governance, roles and responsibilities
- Security rules
  - Organizational security rules and measures
  - People security rules and measures
  - Physical security rules and measures
  - Data security rules and measures
  - Technological security rules and measures

### **G.2.3 Rational and guidance**

Proposed chapter for "security rules" are aligned on the ISO 27002:2022 scheme and corresponding measures inside should be defined in the context of OT.

IEC62443-2-1, 2-4 and 3-2; or Annex C of this standard can be used to complete these chapters.

For better traceability, the same split of chapters in OT cybersecurity policies and OT cybersecurity programmes should be used.

Level of detail will depend on if it is an overall OT cybersecurity policy or an OT cybersecurity programme.

The flexibility given at lower level around a rule will depend on each rule itself.

Rules at programme level should be compatible with the rules at policy level:

- A rule defined in a railway OT security programme should be compatible with the rule defined at overall policy level.
- A rule applied at application level described in cybersecurity maintenance plans should be compatible with the rule defined in the applicable railway OT security programme.
- A rule can be directly applied at lower level without need of change or precision.

If a rule at lower level is not compatible with the rule at higher level, a derogation should be formalized and approved at the higher level (programme or policy). Chapter "Governance, role and responsibilities" should define the applicable derogation process.

## **G.3 Cybersecurity management plan**

The cybersecurity management plan should include the following topics:

Introduction

Cybersecurity activities management

- Project organization chart

- Role and responsibilities related to cybersecurity activities
- Interface with other stakeholders (Engineering, Safety, RAM, V&V, Test & Commissioning)
- Key milestones
- Communication and reporting
- Information protection: data classification, access and transfer
- Project team security skills and training needs.

Cybersecurity context (could be a set of references to other documents)

- High-level description of the system under consideration
- Security objectives
- Applicable cybersecurity regulations and standards
- Operation environment security assumptions, including assumption of cybersecurity shared services that will be provided by the environment to the SUC
- Maintenance environment security assumptions
- Threat environment

Cybersecurity risk management (could be a set of references to other documents)

- Risk assessment methodology description or reference
- Risk impact table
- Likelihood parameters definition
- Risk level definition and acceptance criteria
- Management of security risks and associated treatment plan
- Cybersecurity risk assessment updates: periodicity and triggers event

Cybersecurity design (could be a set of references to other documents)

- SUC partitioning method
- Allocation of cybersecurity requirements
- Organization of cybersecurity design reviews

Secure development life cycle definition (could be a set of references to other documents)

Cybersecurity assurance and acceptance (could be a set of references to other documents)

- Specification of verification and tests activities to be performed
- Review of, integration, V&V, Test & Commissioning, and penetration tests results
- Verification of application of cybersecurity process (application of SecRAC)
- Cybersecurity case production

Vulnerabilities and cybersecurity issues management (could be a set of references to other documents)

- Tools and organization
- Scoring criteria
- Cybersecurity event reporting

Third parties risk management (could be a set of references to other documents)

- Applicable process for supplier cybersecurity assessment, selection and monitoring.

According to context, the cybersecurity management plan can be split in or refer several documents.

#### **G.4 Risk assessment report**

Hereafter are example of topics to be included or referred into the risk assessments reports:

Risk assessment report:

- Operating environmental assumptions
- Risk acceptance criteria
- Threat environment evaluation)
- Zone and conduits Exceptions justification
- For each zone and conduits (aggregation is possible)
  - Results of the comparison of the initial risk with tolerable risk
  - Rationale for selection and applicability of a code of practice (if selected), as well as threat coverage achieved, with respect to the sub-set of the SUC considered
  - rationale for selection and applicability of a reference system (if selected), as well as threat coverage achieved, with respect to the sub-set of the SUC considered.
  - Explicit risk evaluation results and methodology (if performed)
  - any assumptions made
  - List of vulnerabilities
  - Unmitigated risks
  - List of countermeasures (including SecRACs)
  - Residual risk and their status (avoided, accepted or transferred)

#### **G.5 Cybersecurity requirement specification**

Below an example of a cybersecurity requirement specification which include or refer the following information:

##### a) SUC description

Scope and boundary of the SUC

the intended usage of the SUC

the name and high-level description of all functions

the interfaces of the SUC

the assets supporting the essential functions

the operating environment description

physical environment (e.g. maps, plans, wiring schematics, connector configurations and site security plans)

logical environment (e.g. network architecture diagrams, system architecture diagrams, interfaces)

##### b) Cybersecurity Architecture

Zones & conduits drawings

Shared security services

For each zone and conduit:

the name and/or unique identifier indicating also the type (zone or conduit)

the accountable organization(s)

the definition of the logical boundary

the definition of the physical boundary, if applicable

the safety designation

a list of all logical access points

a list of all physical access points, if applicable

a list of data flows associated with each access point

the connected zones or conduits

a list of assets and their risk classification and business value.

Assumptions

Zone Critically Level

SL-T (if applicable, depending if explicit risk evaluation has been performed)

security requirements

security-related application conditions (SecRAC)

The threat environment

Organizational security policy

Tolerable Risks

Regulatory requirements

## **G.6 Cybersecurity guidelines for the railway solution**

The purpose of the cybersecurity guidelines for the railway solution is to provide instructions for the secure installation, operation and maintenance of the railway solution.

The cybersecurity guidelines address organizational and technical measures. They can be a single document or a set of documents.

Example of topics that cybersecurity guidelines could address are provided below:

- Scope (functional and technical)
- Physical security
- Instructions and procedures for installing and maintaining the delivered solution
  - Security privileges required to install or maintain the delivered solution
  - Security options, including removal of default passwords, used to install, configure the delivered solution
  - Security checks to ensure correct installation / update
  - Security considerations/actions associated with removing the delivered solution from use (for example, removing sensitive data).



- Instructions and procedures to administrate the security of the delivered solution
  - Access right management
  - Certificate and Certificate Revocation List (CRL) management
- Instructions and procedures to operate the delivered solution in security
- SecRACs associated with operations and maintenance
- Information on cybersecurity incident, issue and alert management
- Trainings

## **G.7 Cybersecurity evaluation plan**

Cybersecurity evaluation plan could include the following topics:

- Cybersecurity evaluation strategy
  - Organization and responsibilities
  - Activities and phasing
  - Asset Owner specific requirements & constraints
  - Resources (means of validation, involved stakeholders)
  - How to report the results
- Detailed description of activities (description, deliverables, responsibility)
  - Cybersecurity assurance evaluation
- Evaluation of application of the cybersecurity process
- Evaluation of skills, and in case of need, of performed awareness and training related to roles & responsibilities for Cybersecurity.
  - Evaluation of cybersecurity during specification & design phase
- Evaluation of architecture and design & external interfaces (Cybersecurity design review)
- Evaluation of coverage of CRS by cybersecurity-related requirements in specification & architecture
  - Evaluation of cybersecurity during development activities
- Evaluation of the security of development environment (e.g. protection from malware, integrity of deliveries, physical security, etc.)
- Definition and application of software secure coding rules
  - Evaluation of cybersecurity of Supply Chain
- Evaluation of cybersecurity capabilities of supplier products / components
- Evaluation of cybersecurity supplier trustworthiness (from National recommendation)
  - Evaluation of cybersecurity during the installation/integration, validation and acceptance phases
- Expected input from integration and V&V teams
- Evaluation of V&V deliverables, coverage of cybersecurity-related requirements by requirement testing
- Evaluation of validity of security assumption of the cybersecurity context
- Evaluation of site working environment
- Evaluation of testing environment

- Evaluation of application of cybersecurity configuration specification & policies
- Evaluation of application of security-related application conditions (SecRAC)
- Evaluation of security tests results (e.g. pen test)
- Vulnerability assessment until security handover
- Evaluation of cybersecurity guidelines included in project documentation and training (for operation and maintenance activities)
- Evaluation of compliance to cybersecurity standard (if required)

## **G.8 Cybersecurity case**

The cybersecurity case is mainly a collection of reference documents with main conclusions. No sensitive detail should be provided in the cybersecurity case.

The "railway solution cybersecurity case" provided by the System integrator should include the following topics:

Introduction (could be a set of references to other documents)

- System under consideration (SUC) definition (incl. zones and conduits)
- Risks assessment report
  - Assumptions
  - List of threat intelligences sources
  - List of threat Scenarios
  - List of sufficiently mitigated risks (with explanation).
  - Demonstration of applicability of code of practice and/or reference system

Cybersecurity requirement specification (CRS) (could be a set of references to other documents)

- Assumptions
- Cybersecurity needs (including safety-related high-level objectives)
- Cybersecurity requirements
- List of open risks (with explanation).

Cybersecurity management (could be a set of references to other documents)

- Cybersecurity policy
- Cybersecurity plan
- Cybersecurity process
- Vulnerability assessment and management.

Cybersecurity fulfilment (could be a set of references to other documents)

- Implementation of cybersecurity measures - evidences of fulfilment of CRS
- Evidence of application of cybersecurity process
- Verification and validation results
  - Testing of security measures (e.g. V&V, Penetration testing)
  - Traceability to cybersecurity requirements
- Related cybersecurity cases (from included components or subsystems, if any).

Security-related application conditions (could be a set of references to other documents)

- Installation
- Maintenance
- Operation.

Conclusion

- Cybersecurity claim
- Residual risks status.

The "railway application cybersecurity case" established and maintained by the asset owner should include the following topics (could be a set of references to other documents):

- Reference to the railway solution cybersecurity case provided by the System integrator during cybersecurity handover.
- Updated clauses of the railway solution cybersecurity case in case of evolution of threat environment or change of design of the railway solution.
- Evidence of application of the railway application cybersecurity maintenance plan
- Evidence of application of SecRAC during operation and maintenance activities

## **G.9 Cybersecurity maintenance plan**

A cybersecurity maintenance plan may include, or be supported by, the following information:

- Inputs, constraints, and context
  - Documentation as inputs (cybersecurity case, guidelines, ...)
  - Regulatory constraints (laws, external rules, internal rules, ...)
  - Context (Railway application in the overall system, link with IT, assumptions, ...)
  - Environmental conditions required for appropriate cybersecurity maintenance
- Criteria for review of this cybersecurity maintenance plan
- Organization, role and responsibilities
- Schedule of cybersecurity maintenance activities for the railway application
  - Preventative and corrective types of cybersecurity maintenance activities
  - Periodicities for maintenance tasks or when updates to the railway application are applied
- Activities to be performed (description, and periodicity or trigger event)
  - Cybersecurity rules and procedure definition (including access control)
  - Continuous cybersecurity verification
  - Cybersecurity case update (criteria for review, update process, ...)
  - Risk assessment update
  - Security testing
  - Vulnerability management
  - Patch management, including end of life and end of support consideration
  - Back-up and restore management
  - Operations and maintenance management
  - Security monitoring
  - Incident management

- Decommissioning management
- Trainings
- Supporting tool and other information
  - Database of internal and external users with physical access and remote access to railway application
  - Allowed maintenance access solutions through direct and remote access and specific exclusions
  - Railway application authentication measures; access, fault and general logs
  - Information on how to securely deactivate or reactivate the railway application, if necessary
  - Approved configurations of the railway application, including hardware, firmware and software version types permitted

## **Annex H** (informative)

### **Cybersecurity competence profiles**

#### **H.1 Purpose**

The purpose of this annex is to provide the description of for railway cybersecurity competence profiles needed to perform cybersecurity related activities during Railway Application life cycle.

The quality and integrity of the work products generated by human agents performing cybersecurity related activities at various stages life cycle is largely influenced by their requisite knowledge, experience and skills of application, motivational factors, efficiency and innovation capabilities. The totality of these attributes constitute competence in performing a given task, to the satisfaction of the key stakeholders in a given context. A single person may acquire and demonstrate multiple competences in various domains. Competence is a composite attribute and can manifest in varying degrees hence the concept of a competence profile for a given role.

Acknowledging the importance of competence in the cybersecurity domain, the European Agency for Cybersecurity, ENISA have developed the European Cybersecurity Skills Framework (ECSF) that is made available for reuse under a Creative Commons Attribution 4.0 International (CC BY 4.0). The CC BY 4.0 permits sharing and adaptation with relevant credit given to the source.

The cybersecurity competence profile for railways cybersecurity domain described in this annex have been adapted and tailored from the ECSF.

The described profiles intend to cover the principal cybersecurity roles in railway applications life cycle and comprises of:

- Railway Project Cybersecurity Manager (see [Table H.1](#))
- Railway Cybersecurity Architect (see [Table H.2](#))
- Railway Cybersecurity Risk Analyst (see [Table H.3](#))
- Railway Cybersecurity Implementer (see [Table H.4](#))
- Railway Cybersecurity Penetration Tester (see [Table H.5](#))
- Railway Cybersecurity Assessor (see [Table H.6](#))
- Railway Cybersecurity Verifier (see [Table H.7](#))
- Railway Cybersecurity Validator (see [Table H.8](#))
- Railway Cybersecurity Administrator (see [Table H.9](#))
- Railway Cyber Incident Responder (see [Table H.10](#))
- Railway Chief Information Security Officer (see [Table H.11](#))

The role profiles represent a best case that may be combined and delivered by one person taking into account the workload as a constraint. So, one person can hold and fulfill many roles so long as they demonstrate the requisite knowledge and skills and one role can be held by many individuals with varying levels of competence. In this context, role profiles do not impose project team sizes and are intended to ensure requisite competencies are employed in fulfilling cybersecurity tasks and activities thus underpinning the trustworthiness of the targeted, designed and attained cybersecurity.

## H.2 Railway cybersecurity competence profiles

### H.2.1 Introduction

This annex outlines railway cybersecurity roles, competencies and responsibilities. When applying this annex, consider the specific context of and relationship between stakeholders (railway duty holder, asset owner, system integrator, maintenance service provider, product supplier).

### H.2.2 Railway Project Cybersecurity Manager

**Table H.1 – Railway Project Cybersecurity Manager Competence Profile**

Profile Title	Railway Project Cybersecurity Manager
Alternative Title(s)	<ul style="list-style-type: none"> <li>– OT Security Manager</li> <li>– Cyber Risk Manager</li> </ul>
Summary statement	<ul style="list-style-type: none"> <li>– Manage the cybersecurity aspects of organization's projects and associated risks aligned to the organization's strategy.</li> <li>– Develop, maintain and communicate the objectives, challenges, findings, decisions and risk management actions and reports.</li> </ul>
Mission	<ul style="list-style-type: none"> <li>– Continuously manages (identifies, analyses, assesses, estimates, and ensures mitigation of) the cybersecurity-related aspects of a project's Railway infrastructure, systems and services by planning, applying, reporting and communicating objectives, plans, analysis, assessment and treatment.</li> <li>– Establishes a risk management strategy for the project derived from the organization's policies and ensures that risks remain at an acceptable level for the project by selecting mitigation actions and controls.</li> </ul>
Typical Deliverable(s)	<ul style="list-style-type: none"> <li>– Cybersecurity management plan</li> <li>– Cybersecurity risk assessment</li> <li>– Project cybersecurity risk remediation action plan</li> <li>– Cybersecurity risk management outcomes and communications with stakeholders</li> <li>– Vulnerability management plan</li> <li>– Cybersecurity case</li> </ul>
Main task(s)	<ul style="list-style-type: none"> <li>– Analyse project security needs (including laws and local regulations), determine security objectives and develop a project cybersecurity risk management strategy</li> <li>– Plan security activities during project life cycle</li> <li>– Ensure cybersecurity awareness and cybersecurity training is provided as needed to the project team</li> <li>– Manage an inventory of project's assets that are vulnerable to cybersecurity threats</li> <li>– Establish the project cybersecurity context (cybersecurity assumptions, threat environment in the context of the project)</li> <li>– Ensure cybersecurity risks are assessed and the most appropriate risk treatment options, including security countermeasures and risk mitigation and avoidance that best address the project's strategy</li> <li>– Monitor effectiveness of cybersecurity countermeasures and risk levels</li> <li>– Ensure that all cybersecurity risks remain at an acceptable level for the project's assets</li> <li>– Develop, maintain, report and communicate complete risk management cycle</li> <li>– Ensure vulnerability management is implemented</li> <li>– Establish and/or maintain cybersecurity case</li> <li>– Organize and ensure the cybersecurity handover</li> <li>– In case of external cybersecurity audit, manage the relationship with auditors</li> <li>– Liaise with all cybersecurity stakeholders as a single point of contact</li> </ul>
Key skill(s)	<ul style="list-style-type: none"> <li>– Ensure cybersecurity risk management frameworks, methodologies and guidelines are implemented and relevant regulations and standards are complied with</li> <li>– Analyse and consolidate Project's quality and risk management practices</li> <li>– Enable stakeholders to make informed decisions to manage and mitigate risks</li> </ul>

	<ul style="list-style-type: none"> <li>– Build a cybersecurity risk aware environment</li> <li>– Communicate, present and report to relevant stakeholders</li> <li>– Propose and manage risk sharing options</li> </ul>
Key knowledge	<ul style="list-style-type: none"> <li>– Understanding of cyber security regulatory requirements, legislation, standards and best practices</li> <li>– Understanding of railway environment, architecture, operational constraints and safety priorities</li> <li>– Risk management standards, methodologies and frameworks</li> <li>– Risk management approaches</li> <li>– Risk management recommendations and best practices</li> <li>– Cyber threats and sources for cybersecurity intelligence</li> <li>– Computer systems and operational technologies vulnerabilities</li> <li>– Cybersecurity countermeasures and solutions</li> <li>– Cybersecurity risks</li> <li>– Monitoring, testing and evaluating cybersecurity countermeasures' effectiveness</li> <li>– Cybersecurity related certifications</li> <li>– Cybersecurity related technologies</li> </ul>

### H.2.3 Railway Cybersecurity Architect

**Table H.2 – Railway Cybersecurity Architect Competence Profile**

Profile Title	Railway Cybersecurity Architect
Alternative Title(s)	<ul style="list-style-type: none"> <li>– Cybersecurity Solutions Architect</li> <li>– Cybersecurity Designer</li> </ul>
Summary statement	<ul style="list-style-type: none"> <li>– Plans and designs security-by-design solutions (infrastructures, systems, assets, software, hardware and services) and cybersecurity countermeasures.</li> </ul>
Mission	<ul style="list-style-type: none"> <li>– Designs solutions based on security-by-design and privacy-by-design principles.</li> <li>– Creates and continuously improves architectural models and develops appropriate architectural documentation and specifications.</li> <li>– Coordinate secure development, integration and maintenance of cybersecurity components in line with standards and other related requirements.</li> </ul>
Typical Deliverable(s)	<ul style="list-style-type: none"> <li>– Cybersecurity requirements specification (CRS)</li> </ul>
Main task(s)	<ul style="list-style-type: none"> <li>– Design and propose a secure architecture to implement the railway organization's strategy</li> <li>– Develop railway solution cybersecurity architecture to address security and privacy requirements</li> <li>– Produce railway cybersecurity architectural documentation and specifications</li> <li>– Present high level security architecture design to stakeholders</li> <li>– Establish a secure environment during the development life cycle of railways systems, services and products</li> <li>– Coordinate the development, integration and maintenance of cybersecurity components for railway applications ensuring the cybersecurity specifications are implemented</li> <li>– Analyse and evaluate the cybersecurity of the organization's railway solutions' architecture</li> <li>– Ensure the security of the railway solution architectures through security reviews and certification</li> <li>– Collaborate with other teams and colleagues</li> <li>– Evaluate the impact of cybersecurity solutions on the design and performance of the organization's railway projects' architecture</li> <li>– Adapt the organization's railway projects' architecture to emerging threats</li> <li>– Assess the implemented architecture to maintain an appropriate level of security</li> </ul>
Key skill(s)	<ul style="list-style-type: none"> <li>– Conduct user and business security requirements analysis</li> <li>– Draw cybersecurity architectural and functional specifications</li> </ul>

Profile Title	Railway Cybersecurity Architect
	<ul style="list-style-type: none"> <li>– Decompose and analyse systems to develop security and privacy requirements and identify effective solutions</li> <li>– Design systems and architectures based on security and privacy- by-design and by defaults cybersecurity principles</li> <li>– Guide and communicate with implementers and IT/OT personnel</li> <li>– Communicate, present and report to relevant stakeholders</li> <li>– Propose cybersecurity architectures based on stakeholder's needs and budget</li> <li>– Select appropriate specifications, procedures and controls</li> <li>– Build resilience against points of failure across the architecture</li> <li>– Coordinate the integration of security solutions</li> </ul>
Key knowledge	<ul style="list-style-type: none"> <li>– Understanding of railway environment, architecture, operational constraints and safety priorities</li> <li>– Cybersecurity-related certifications</li> <li>– Cybersecurity recommendations and best practices</li> <li>– Cybersecurity applicable standards, methodologies and frameworks</li> <li>– Cybersecurity-related requirements analysis</li> <li>– Secure development life cycle</li> <li>– Security architecture reference models</li> <li>– Cybersecurity-related technologies</li> <li>– Cybersecurity countermeasures and solutions</li> <li>– Cybersecurity risks</li> <li>– Cyber threats</li> <li>– Cybersecurity trends</li> <li>– Legal, regulatory, legislative compliance requirements, recommendations and best practices</li> <li>– Legacy cybersecurity procedures</li> <li>– Privacy-Enhancing Technologies (PET)</li> </ul>

## H.2.4 Railway Cybersecurity Risk Analyst

**Table H.3 – Railway Cybersecurity Risk Analyst Competence Profile**

Profile Title	Railway Cybersecurity Risk Analyst
Alternative Title(s)	<ul style="list-style-type: none"> <li>– Cyber Intelligence Analyst</li> <li>– Cyber Threat Modeller</li> </ul>
Summary statement	– Collect, process, analyse data and information to produce a cybersecurity risk profile in a given project and risk reduction solutions and disseminate them to target stakeholders.
Mission	<ul style="list-style-type: none"> <li>– Conducts threat risk identification and analysis throughout the life cycle including cyber threat information collection, security analysis of the architecture and solutions and production of actionable intelligence and dissemination to security stakeholders and the cyber threat intelligence community, at a tactical, operational and strategic level.</li> <li>– Identifies and monitors the tactics, techniques and procedures used by cyber threat actors and their trends, track threat actors' activities and observe how non-cyber events can influence cyber-related actions.</li> </ul>
Typical Deliverable(s)	<ul style="list-style-type: none"> <li>– Cyber Risk identification and Analysis</li> <li>– Cyber Threat risk mitigation Report</li> <li>– Cybersecurity acceptance reports</li> </ul>
Main task(s)	<ul style="list-style-type: none"> <li>– Develop, implement and manage the organization's cyber threat risk assessment and mitigation strategy</li> <li>– Develop plans and procedures to manage threat risk</li> <li>– Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders</li> <li>– Identify and assess potential cyber threat actors targeting the system under consideration</li> </ul>



	<ul style="list-style-type: none"> <li>– Identify, monitor and assess the tactics, techniques and procedures used by cyber threat actors by analysing open-source and proprietary data, information and intelligence</li> <li>– Produce actionable reports based on threat intelligence and risk data</li> <li>– Elaborate and advise on mitigation plans at the tactical, operational and strategic level</li> <li>– Coordinate with stakeholders to share and consume intelligence on relevant cyber threats</li> <li>– Leverage intelligence and risk data to support and assist with threat modelling, recommendations for risk mitigation and cyber threat hunting</li> <li>– Communicate cybersecurity risks with key stakeholders</li> <li>– Convey the proper security severity by explaining the risk exposure and its consequences to non-technical stakeholders</li> </ul>
Key skill(s)	<ul style="list-style-type: none"> <li>– Cyber threat risk assessment</li> <li>– Collect, analyse and correlate cyber threat information originating from multiple sources</li> <li>– Identify threat actors tactics, techniques and procedures and campaigns</li> <li>– Conduct technical analysis and reporting</li> <li>– Identify non-cyber events with implications on cyber-related activities</li> <li>– Model threats, actors and tactics, techniques and procedures</li> <li>– Communicate, coordinate and cooperate with internal and external stakeholders</li> <li>– Communicate, present and report to relevant stakeholders</li> <li>– Use and apply cyber threat intelligence platforms and tools</li> <li>– Collaborate with other team members and colleagues</li> </ul>
Key knowledge	<ul style="list-style-type: none"> <li>– Understanding of railway environment, architecture, operational constraints and safety priorities</li> <li>– Operating systems security</li> <li>– Computer networks security</li> <li>– Cybersecurity standards</li> <li>– Understanding risk, risk evaluation and management</li> <li>– Understanding risk tolerability and appetite</li> <li>– Cybersecurity threat identification and assessment</li> <li>– Cybersecurity countermeasures and solutions</li> <li>– Cyber threat intelligence sharing standards, methodologies and frameworks</li> <li>– Responsible information disclosure procedures</li> <li>– Cross-domain and border-domain knowledge related to cybersecurity</li> <li>– Cyber threats</li> <li>– Cyber threat actors</li> <li>– Cybersecurity attack procedures</li> <li>– Advanced and persistent cyber threats</li> <li>– Threat actors tactics, techniques and procedures</li> <li>– Cybersecurity related certifications</li> </ul>

## H.2.5 Railway Cybersecurity Implementer

**Table H.4 – Railway Cybersecurity Implementer Competence Profile**

Profile Title	Railway Cybersecurity Implementer
Alternative Titles(s)	<ul style="list-style-type: none"> <li>– Cybersecurity Solutions Expert</li> <li>– Cybersecurity Developer</li> <li>– Cybersecurity Engineer</li> <li>– Development, Security &amp; Operations (DevSecOps) Engineer</li> </ul>
Summary Statement	– Develop, deploy and operate cybersecurity solutions (systems, assets, components, software, controls and services) on infrastructures and products.
Mission	– Provides cybersecurity related technical development, integration, implementation, operation, maintenance and support for cybersecurity solutions.

Profile Title	Railway Cybersecurity Implementer
	<ul style="list-style-type: none"> <li>– Ensures adherence to specifications and conformance requirements, assures sound performance and resolves technical issues required in the organization or projects cybersecurity-related solutions (systems, assets, components, software, controls and services), infrastructures and products</li> </ul>
Typical Deliverable(s)	<ul style="list-style-type: none"> <li>– Cybersecurity solutions</li> <li>– Cybersecurity design and service specifications</li> <li>– Cybersecurity operation and maintenance manuals</li> <li>– Cybersecurity test specifications on design and implementation level</li> </ul>
Main Tasks	<ul style="list-style-type: none"> <li>– Develop, design, implement, maintain, upgrade, cybersecurity products.</li> <li>– Provide cybersecurity related support to users and customers.</li> <li>– Integrate cybersecurity solutions and ensure their sound operation in accordance with cyber security architecture and requirements</li> <li>– Maintain and upgrade the security of systems, services and products</li> <li>– Implement cybersecurity procedures and controls</li> <li>– Document and report on the security of systems, services and products</li> <li>– Work close with the IT/OT personnel on cybersecurity related actions</li> <li>– Implement, apply and manage patches to products to address technical vulnerabilities in cooperation with Cybersecurity Incident Responder</li> </ul>
Key skill(s)	<ul style="list-style-type: none"> <li>– Communicate, present and report to relevant internal and external stakeholders</li> <li>– Integrate cybersecurity solutions to the project's infrastructure in line with cybersecurity architecture and requirements</li> <li>– Assess the security and performance of solutions</li> <li>– Develop network design, software design, code, scripts and programmes</li> <li>– Identify and solve cybersecurity related issues</li> <li>– Collaborate with other team members and colleagues</li> </ul>
Key knowledge	<ul style="list-style-type: none"> <li>– Understanding of railway environment, architecture, operational constraints and safety priorities</li> <li>– Secure development life cycle</li> <li>– Secure design principles</li> <li>– Computer programming</li> <li>– Operating systems security</li> <li>– Computer networks security</li> <li>– Cybersecurity countermeasures and solutions</li> <li>– Offensive and defensive security practices</li> <li>– Secure coding recommendations and best practices</li> <li>– Cybersecurity recommendations and best practices</li> <li>– Cybersecurity design, operation and maintenance standards, methodologies, frameworks and good practices</li> <li>– Cybersecurity related technologies</li> </ul>

## H.2.6 Railway Cybersecurity Penetration Tester

**Table H.5 – Railway Cybersecurity Penetration Tester Profile**

Profile Title	Railway Cybersecurity Penetration Tester
Alternative Titles(s)	<ul style="list-style-type: none"> <li>– Penetration tester</li> <li>– Ethical Hacker</li> <li>– Vulnerability Analyst</li> <li>– Offensive Cybersecurity Expert</li> <li>– Defensive Cybersecurity Expert</li> <li>– Red Team Expert</li> <li>– Red Teamer</li> </ul>

Profile Title	Railway Cybersecurity Penetration Tester
Summary Statement	<ul style="list-style-type: none"> <li>Provides a threat based approach to assess the effectiveness of security countermeasures, identifies and utilises cybersecurity vulnerabilities, assesses their criticality and determines if and how they can be exploited by threat actors.</li> </ul>
Mission	<ul style="list-style-type: none"> <li>Plans, designs, implements and executes penetration testing activities and attack scenarios to evaluate the effectiveness of deployed or planned security measures with reference to the risk assessment report.</li> <li>Identifies vulnerabilities or failures on technical and organizational controls that affect the confidentiality, integrity, availability and safety of railway products (e.g. systems, assets components, hardware, software and services).</li> <li>Report test results and advise what the additional measures are required to protect railway products in line with penetration test results if applicable</li> </ul>
Typical Deliverable(s)	<ul style="list-style-type: none"> <li>Threats and Vulnerability Assessment Results Report</li> <li>Penetration Testing Report</li> </ul>
Main Tasks	<ul style="list-style-type: none"> <li>Identify the results of risk assessment, analyse and assess technical, organizational and project cybersecurity threats and vulnerabilities</li> <li>Identify attack vectors, uncover and demonstrate exploitation of technical cybersecurity threats and vulnerabilities</li> <li>Test systems and operations compliance with regulatory and/or agreed standards</li> <li>Select and develop appropriate penetration testing techniques</li> <li>Organize test plans, procedures and environments for penetration testing</li> <li>Establish procedures and environments for penetration testing result analysis and reporting</li> <li>Deploy penetration testing tools and test programs</li> <li>Document and report penetration testing results to the stakeholders</li> <li>Advise what the additional measure is necessary to implement in line with test results</li> </ul>
Key skill(s)	<ul style="list-style-type: none"> <li>Develop codes, scripts and programs</li> <li>Perform social engineering</li> <li>Identify threats, penetration scenario and exploit vulnerabilities, attacks</li> <li>Conduct ethical hacking</li> <li>Think creatively and outside the box</li> <li>Identify what the status of products under exploiting vulnerabilities and attacks</li> <li>Identify and solve cybersecurity related issues</li> <li>Communicate, present and report to relevant stakeholders</li> <li>Use penetration testing tools effectively</li> <li>Conduct technical analysis and reporting</li> <li>Decompose and analyse systems to identify weaknesses and ineffective controls</li> <li>Review design and codes assess their security</li> </ul>
Key knowledge	<ul style="list-style-type: none"> <li>Cybersecurity attack procedures</li> <li>Risk assessment procedures</li> <li>Information technology (IT) and operational technology (OT) appliances</li> <li>Offensive and defensive security procedures</li> <li>Operating systems security</li> <li>Computer networks security</li> <li>Penetration testing procedures</li> <li>Penetration testing standards, methodologies, frameworks and environments</li> <li>Penetration testing tools</li> <li>Computer programming</li> <li>Computer systems vulnerabilities</li> <li>Cybersecurity recommendations and good practices</li> <li>Cybersecurity related certifications</li> </ul>

**H.2.7 Railway Cybersecurity Assessor****Table H.6 – Railway Cybersecurity Assessor Competence Profile**

<b>Profile Title</b>	<b>Railway Cybersecurity Assessor</b>
Alternative Titles(s)	– Railway Cybersecurity Auditor
Summary Statement	– Perform cybersecurity assessment on the Railway Application, ensure compliance with statutory, regulatory, policy, agreed cybersecurity requirements, industry standards and good practices.
Mission	<ul style="list-style-type: none"> <li>– Conducts independent reviews to assess the effectiveness of processes and controls the overall compliance of the Railway Application with legal, statutory and regulatory frameworks policies.</li> <li>– Evaluates, tests, verifies and validates cybersecurity related products (systems, assets, components, hardware, software and services), functions and policies ensuring, compliance with railway applicable cybersecurity guidelines, standards, regulations and agreed cybersecurity requirements.</li> <li>– Report and communicate the result, corrective actions and recommendation to internal and external stakeholders</li> <li>– Monitor the status of corrective actions</li> </ul>
Typical Deliverable(s)	<ul style="list-style-type: none"> <li>– Cybersecurity assessment plan</li> <li>– Cybersecurity assessment report</li> </ul>
Main Tasks Key skill(s)	<ul style="list-style-type: none"> <li>– Develop the organization's and project's assessment policy, procedures, standards and guidelines</li> <li>– Establish the methodologies and practices used for cybersecurity-related products (systems, assets, components, hardware, software and services) assessment</li> <li>– Establish the target environment and manage assessment activities</li> <li>– Define assessment scope, objectives and criteria to assess against</li> <li>– Develop an assessment plan describing frameworks, standards, methodologies, procedures and tests</li> <li>– Review target of evaluation, security objectives and agreed cybersecurity requirements based on the risk management profile</li> <li>– Assess compliance with cybersecurity-related applicable laws, statutory and regulations. Assess conformity with railway applicable cybersecurity related standards</li> <li>– Execute the assessment plan, collect evidence and measurements and survey actual products on site.</li> <li>– Maintain and protect the integrity of assessment records including evidences.</li> <li>– Develop and communicate assessment, assurance, audit, certification and maintenance reports including corrective actions and recommendations</li> <li>– Monitor activities of risk remediation and corrective actions</li> </ul>
Key skill(s)	<ul style="list-style-type: none"> <li>– Organize and work in a systematic and deterministic way based on evidence and objectives</li> <li>– Follow and practice assessing frameworks, standards and methodologies</li> <li>– Apply a portfolio of assessment tools and techniques</li> <li>– Analyse cybersecurity life cycle processes, assess and review components, software or hardware security, as well as technical and organizational controls</li> <li>– Decompose and analyse systems to identify weaknesses and ineffective controls</li> <li>– Communicate, explain and adapt legal, statutory regulatory requirements, railway cybersecurity related standards, guidelines and cybersecurity requirements</li> <li>– Collect, evaluate, maintain and protect assessment information and evidences</li> <li>– Assess with integrity, being impartial and independent</li> </ul>
Key knowledge	<ul style="list-style-type: none"> <li>– Cybersecurity controls and solutions</li> <li>– Legal, statutory, regulatory and legislative compliance requirements, recommendations and good practices</li> <li>– Monitoring, testing and evaluating cybersecurity controls' effectiveness</li> <li>– Conformity assessment standards, methodologies and frameworks</li> <li>– Assessment standards, methodologies and frameworks</li> <li>– Cybersecurity standards, methodologies and frameworks applicable to railway context</li> </ul>

	<ul style="list-style-type: none"> <li>– Assessment related certification</li> <li>– Industrial and railway cybersecurity related certifications</li> </ul>
--	---

## H.2.8 Railway Cybersecurity Verifier

**Table H.7 – Railway Cybersecurity Verifier Competence Profile**

Profile Title	Railway Cybersecurity Verifier
Alternative Titles(s)	<ul style="list-style-type: none"> <li>– Cybersecurity Tester</li> <li>– Vulnerability Analyst</li> <li>– Offensive Cybersecurity Expert</li> <li>– Defensive Cybersecurity Expert</li> <li>– Red Team Expert</li> <li>– Red Teamer</li> </ul>
Summary Statement	– Evaluates the effectiveness of security countermeasures, reveals and utilize cybersecurity threats and vulnerabilities, assessing their conformity with the cybersecurity requirements.
Mission	<ul style="list-style-type: none"> <li>– Plans, designs, implements and executes analysis, testing and verification activities to evaluate the effectiveness of deployed or planned security architecture and measures with reference to the cybersecurity requirements.</li> <li>– Identifies vulnerabilities or failures on technical and organizational controls that affect the confidentiality, integrity, availability and potentially safety of Railway products (e.g. systems, assets components, hardware, software and services).</li> <li>– Report test and verification results and advise what the additional measures are required to protect railway products in line with cyber security requirements as applicable</li> </ul>
Typical Deliverable(s)	– Cybersecurity Test and Verification Report
Main Tasks	<ul style="list-style-type: none"> <li>– Test systems and operations compliance with regulatory and/or agreed standards</li> <li>– Select and develop appropriate cybersecurity testing techniques and procedures</li> <li>– Establish procedures and environments for cybersecurity testing result analysis and reporting</li> <li>– Organize analysis and test plans and select procedures and environments for cybersecurity testing</li> <li>– Deploy cybersecurity analysis and testing tools and test programs</li> <li>– Document and report specific cybersecurity analysis and testing results to the stakeholders</li> <li>– Advise what additional measures are required to implement, in line with test and requirements verification results</li> </ul>
Key skill(s)	<ul style="list-style-type: none"> <li>– Think creatively and outside the box</li> <li>– Effective use of threat models and relevant analysis techniques</li> <li>– Identify and solve cybersecurity related issues</li> <li>– Communicate, present and report cybersecurity test outcomes to relevant stakeholders</li> <li>– Cybersecurity analysis and verification</li> <li>– Use cybersecurity testing tools effectively</li> <li>– Conduct testing technical analysis and reporting</li> </ul>
Key knowledge	<ul style="list-style-type: none"> <li>– Cybersecurity attack procedures</li> <li>– Risk assessment procedures</li> <li>– Information technology (IT) and operational technology (OT) appliances</li> <li>– Offensive and defensive security procedures</li> <li>– Operating systems security testing and verification</li> <li>– Computer networks security testing and verification</li> <li>– Cybersecurity testing standards, methodologies, frameworks and environments</li> <li>– Cybersecurity testing tools</li> <li>– Computer programming</li> <li>– Computer digital systems vulnerabilities</li> </ul>

Profile Title	Railway Cybersecurity Verifier
	<ul style="list-style-type: none"> <li>– Cybersecurity recommendations and good practices</li> <li>– Cybersecurity related certifications</li> </ul>

## H.2.9 Railway Cybersecurity Validator

**Table H.8 – Railway Cybersecurity Validator Competence Profile**

Profile Title	Railway Cybersecurity Validator
Alternative Titles(s)	<ul style="list-style-type: none"> <li>– Railway Cybersecurity Evaluator</li> </ul>
Summary Statement	<ul style="list-style-type: none"> <li>– Perform cybersecurity validation of the Railway Application, ensure compliance with statutory, regulatory, policy, agreed cybersecurity requirements, industry standards and good practices.</li> </ul>
Mission	<ul style="list-style-type: none"> <li>– Conducts independent reviews to assess the fitness for purpose of processes and controls and the overall compliance of the Railway Application with the legal, statutory and regulatory frameworks policies.</li> <li>– Evaluates, tests, verifies and validates cybersecurity related products (systems, assets, components, hardware, software and services), functions and policies ensuring, compliance with railway applicable cybersecurity guidelines, standards, regulations and agreed cybersecurity requirements.</li> <li>– Report and communicate the result, corrective actions and recommendation to internal and external stakeholders</li> <li>– Monitor the status of corrective actions</li> </ul>
Typical Deliverable(s)	<ul style="list-style-type: none"> <li>– Cybersecurity validation plan</li> <li>– Cybersecurity validation report</li> </ul>
Main Tasks Key skill(s)	<ul style="list-style-type: none"> <li>– Develop the organization's and project's validation policy, procedures, standards and guidelines</li> <li>– Establish the methodologies and practices used for cybersecurity-related products (systems, assets, components, hardware, software and services) validation</li> <li>– Establish the target environment and manage validation activities</li> <li>– Define validation scope, objectives and criteria to assess against</li> <li>– Develop a validation plan describing the frameworks, standards, methodology, procedures and tests</li> <li>– Review target of evaluation, security objectives and agreed cybersecurity requirements based on the risk management profile</li> <li>– Assess compliance with cybersecurity related applicable laws, statutory and regulations</li> <li>– Assess conformity with railway applicable cybersecurity related standards</li> <li>– Execute the validation plan, collect evidence and measurements and survey the actual products on site.</li> <li>– Maintain and protect the integrity of assessment records including evidences.</li> <li>– Develop and communicate conformity validation, assurance, audit, certification and maintenance reports including corrective actions and recommendations</li> <li>– Monitor activities of risk remediation and corrective actions</li> </ul>
Key skill(s)	<ul style="list-style-type: none"> <li>– Organize and work in a systematic and deterministic way based on evidence and objects</li> <li>– Follow and practice assessing frameworks, standards and methodologies</li> <li>– Apply a portfolio of validation tools and techniques</li> <li>– Analyse cybersecurity life cycle processes, assess and review components, software or hardware security, as well as technical and organizational controls</li> <li>– Decompose and analyse systems to identify weaknesses and ineffective controls</li> <li>– Communicate, explain and adapt legal, statutory regulatory requirements, railway cybersecurity-related standards, guidelines and cybersecurity requirements</li> <li>– Collect, evaluate, maintain and protect validation information and evidences</li> <li>– Validate the railway solution with integrity, being impartial and independent</li> </ul>
Key knowledge	<ul style="list-style-type: none"> <li>– Cybersecurity controls and solutions</li> <li>– Legal, statutory, regulatory and legislative compliance requirements, recommendations and good practices</li> </ul>

	<ul style="list-style-type: none"> <li>– Monitoring, testing and evaluating cybersecurity controls' effectiveness</li> <li>– Conformity assessment standards, methodologies and frameworks</li> <li>– Assessment and validation standards, methodologies and frameworks</li> <li>– Cybersecurity standards, methodologies and frameworks applicable to railway context</li> <li>– Validation related certification</li> <li>– Industrial and Railway Cybersecurity related certifications</li> </ul>
--	--

## H.2.10 Railway Cybersecurity Administrator

**Table H.9 – Railway Cybersecurity Administrator Competence Profile**

Profile Title	Railway Cybersecurity Administrator
Alternative Titles(s)	<ul style="list-style-type: none"> <li>– Cybersecurity Administrator</li> <li>– Cybersecurity Account Manager</li> <li>– Cybersecurity Inventory Manager</li> </ul>
Summary Statement	<ul style="list-style-type: none"> <li>– Manage the administration, configuration of data, parameters and rules to keep systems secure.</li> <li>– Manage inventory in assets including the result of configuration and administration</li> </ul>
Mission	<ul style="list-style-type: none"> <li>– Securely administrate and configure systems, services and products on entire security development life cycle like development, test, T&amp;C and operation phases</li> <li>– Administrate and configure solutions including data, parameters or rules like network equipment, identification and account, use of cryptography (e.g. used TLS suites and/or cryptographic certificates), white / black list rules according to the organization's or system's security policy and/or cybersecurity design principle, specification or configuration specification in assets</li> <li>– Ensure setting of data or parameters in asset correctly</li> <li>– Ensure testing to verify cybersecurity function in result of administration / configuration</li> <li>– Ensure correct configured inventory of assets and record</li> <li>– Ensure the application of SecRAC if applicable</li> </ul>
Deliverable(s)	<ul style="list-style-type: none"> <li>– Cybersecurity configuration / administration plan</li> <li>– Cybersecurity inventory management plan</li> <li>– Cybersecurity configuration sheet</li> <li>– Cybersecurity account setting sheet</li> <li>– Cybersecurity configuration / administration test report</li> <li>– Cybersecurity inventory list</li> <li>– Evidence of SecRAC application for cybersecurity Case</li> </ul>
Key skill(s)	<ul style="list-style-type: none"> <li>– Communicate with internal or external stakeholders</li> <li>– Cybersecurity design principle</li> <li>– Configure solutions according to organization's security policy and specified systems</li> <li>– Understand setting procedure of data and parameters in each asset</li> <li>– Understand SecRAC in former phase and specify the additional SecRAC as a result of configuration and administration</li> <li>– Verify or Test the setting in result of configuration and administration</li> <li>– Record the result of configuration and administration into inventory list correctly</li> </ul>
Key knowledge	<ul style="list-style-type: none"> <li>– Secure development life cycle</li> <li>– Computer Programming</li> <li>– Operating systems security</li> <li>– Computer networks security</li> <li>– Cybersecurity controls and solutions</li> <li>– Offensive and defensive security practices</li> <li>– Cybersecurity recommendations and best practices</li> <li>– Testing standards, methodologies and frameworks</li> <li>– Testing procedures</li> </ul>

Profile Title	Railway Cybersecurity Administrator
	<ul style="list-style-type: none"> <li>– Cybersecurity related technologies</li> <li>– Identification and account management</li> <li>– Use of cryptography technology (e.g. encryption)</li> <li>– Inventory or configuration management</li> </ul>

## H.2.11 Railway Cybersecurity Incident Responder

**Table H.10 – Railway Cybersecurity Incident Responder Competence Profile**

Profile Title	Railway Cybersecurity Incident Responder
Alternative Titles(s)	<ul style="list-style-type: none"> <li>– Cyber Incident Handler</li> <li>– Cyber Crisis Expert Incident Response Engineer</li> <li>– Security Operations Centre (SOC) Analyst</li> <li>– Cyber Fighter /Defender</li> <li>– Security Operation Analyst (SOC Analyst)</li> <li>– Computer Security Incident Response Team (CSIRT) Engineer</li> <li>– Project Security Incident Response Team (PSIRT) Engineer</li> <li>– Cybersecurity Security Incident Event Management (SIEM) Manager</li> <li>– Cybersecurity Educator</li> </ul>
Summary Statement	<ul style="list-style-type: none"> <li>– Collect and monitor vulnerability information related to industries on a regular basis</li> <li>– Monitor the cybersecurity state in assets, handle incidents during cyber attacks and ensure the continued operations of systems</li> <li>– Feedback root cause into organization's knowledge repository</li> </ul>
Mission	<ul style="list-style-type: none"> <li>– Collect and monitor vulnerability information and incident information related to industries or similar assets on a regular basis</li> <li>– Monitors and assesses systems' cybersecurity state. Analyses, evaluates and mitigates the impact of cybersecurity incidents</li> <li>– Identifies temporary counter measures of cyber incidents</li> <li>– Identifies cyber incidents root causes and malicious actors.</li> <li>– According to the organization's Incident Response Plan, restores systems' and processes' functionalities to an operational state, collecting evidences and documenting actions taken</li> <li>– Educate the action and handling process of cybersecurity incident on a regular basis</li> <li>– Feedback root causes of incident into organization's knowledge repository.</li> </ul>
Typical Deliverable(s)	<ul style="list-style-type: none"> <li>– Incident Response Plan</li> <li>– Cyber Incident Report</li> <li>– Lessons Learned from Incident response</li> </ul>
Main Task(s)	<ul style="list-style-type: none"> <li>– Collect vulnerability information broadly according to vulnerability management plan</li> <li>– Contribute to the development, maintenance and assessment of the Incident Response Plan</li> <li>– Develop, implement and assess procedures related to incident handling</li> <li>– Respond to cybersecurity attack incidents to stop further damage, repair damage and/or get system running again</li> <li>– Identify, analyse, mitigate and communicate cybersecurity incidents</li> <li>– Assess and manage technical vulnerabilities related to industries and assets</li> <li>– Triage the emergency level from vulnerability or incident information</li> <li>– Measure cybersecurity incidents detection and response effectiveness</li> <li>– Evaluate the resilience of the cybersecurity countermeasures and mitigation actions taken after a cybersecurity incident</li> <li>– Adopt and develop incident handling testing techniques</li> <li>– Establish procedures for incident results analysis and incident handling reporting</li> <li>– Document incident results analysis and incident handling actions</li> </ul>



Profile Title	Railway Cybersecurity Incident Responder
	<ul style="list-style-type: none"> <li>– Cooperate with Secure Operation Centres (SOCs), Computer Security Incident Response Teams (CSIRTs) and Product Incident Response Teams (PSIRTs)</li> <li>– Cooperate with key personnel for reporting of security incidents according to applicable legal framework</li> <li>– Train personnel so that Incident procedure is performed smoothly on a regular basis</li> <li>– Feedback the root cause of incident, some point to improve or strengthen on incident procedure into organization's knowledge repository.</li> </ul>
Key skill(s)	<ul style="list-style-type: none"> <li>– Entire aspect of cybersecurity</li> <li>– Implement all technical, functional and operational aspects of cybersecurity incident handling and response</li> <li>– Collect, analyse and correlate cyber threat information, vulnerability information and incident information originating from multiple sources</li> <li>– Work on operating systems, servers, clouds and relevant infrastructures or assets</li> <li>– Work under pressure</li> <li>– Communicate, present and report to relevant stakeholders</li> <li>– Leadership to manage stakeholder as one team</li> <li>– Manage and analyse log files and identify root causes</li> <li>– Decide rapidly actions with limited information and data</li> <li>– Safety and availability design of systems</li> <li>– Improve the procedure of products from experience of incident response</li> </ul>
Key knowledge	<ul style="list-style-type: none"> <li>– Entire knowledge of cybersecurity</li> <li>– Collect vulnerability or incident information related to industries from adequate sources</li> <li>– Incident handling standards, methodologies and frameworks</li> <li>– Incident handling recommendations and best practices</li> <li>– Incident handling tools</li> <li>– Incident handling communication procedures</li> <li>– Operating systems security</li> <li>– Computer networks security</li> <li>– Cyber threats</li> <li>– Cybersecurity attack procedures</li> <li>– Computer systems vulnerabilities</li> <li>– Cybersecurity related certifications</li> <li>– Cybersecurity related laws, regulations and legislations</li> <li>– Secure Operation Centres (SOCs) operation</li> <li>– Computer Security Incident Response Teams (CSIRTs) operation</li> <li>– Product Security Incident Response Teams (PSIRTs) operation</li> <li>– Leadership management</li> </ul>

## H.2.12 Railway Chief Information Security Officer

**Table H.11 – Railway Chief Information Security Officer Competence Profile**

Profile Title	Railway Chief Information Security Officer (CISO)
Alternative Title(s)	<ul style="list-style-type: none"> <li>– Cybersecurity Programme Director</li> <li>– Information Security Officer (ISO)</li> <li>– Information Security Manager</li> <li>– Head of Information Security</li> <li>– IT/ICT Security Officer</li> </ul>
Summary statement	– Manages as direct report to the C-level board the organization's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.
Mission	– The CISO is provided with the appropriate disciplinary and functional empowerment, to define, maintain and communicate the organization's cybersecurity vision, strategy,

	<p>policies and procedures. Manages the implementation of the cybersecurity policy across the organization. Assures information exchange with external authorities and professional bodies.</p>
Typical Deliverable(s)	<ul style="list-style-type: none"> <li>– Cybersecurity Strategy</li> <li>– Cybersecurity Policy</li> </ul>
Main task(s)	<ul style="list-style-type: none"> <li>– Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organizational objectives</li> <li>– Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organization and ensure their execution</li> <li>– Supervise the application and improvement of the Information Security Management System (ISMS)</li> <li>– Educate senior management about cybersecurity risks, threats and their impact to the organization</li> <li>– Ensure the senior management approves the cybersecurity risks of the organization</li> <li>– Develop cybersecurity plans</li> <li>– Develop relationships with cybersecurity-related authorities and communities</li> <li>– Report cybersecurity incidents, risks, findings to the senior management</li> <li>– Monitor advancement in cybersecurity</li> <li>– Secure resources to implement the cybersecurity strategy</li> <li>– Negotiate the cybersecurity budget with the senior management</li> <li>– Ensure the organization's resiliency to cyber incidents</li> <li>– Manage continuous capacity building within the organization</li> <li>– Review, plan and allocate appropriate cybersecurity resources</li> </ul>
Key skill(s)	<ul style="list-style-type: none"> <li>– Assess and enhance an organization's cybersecurity posture</li> <li>– Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks</li> <li>– Analyse and comply with cybersecurity related laws, regulations and legislations</li> <li>– Implement cybersecurity recommendations and best practices</li> <li>– Manage cybersecurity resources</li> <li>– Develop, champion and lead the execution of a cybersecurity strategy</li> <li>– Influence an organization's cybersecurity culture</li> <li>– Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing</li> <li>– Review and enhance security documents, reports, SLAs and ensure the security objectives</li> <li>– Identify and solve cybersecurity-related issues</li> <li>– Establish a cybersecurity plan</li> <li>– Communicate, coordinate and cooperate with internal and external stakeholders</li> <li>– Anticipate required changes to the organization's information security strategy and formulate new plans</li> <li>– Define and apply maturity models for cybersecurity management</li> <li>– Anticipate cybersecurity threats, needs and upcoming challenges</li> <li>– Motivate and encourage people</li> </ul>
Key knowledge	<ul style="list-style-type: none"> <li>– Cybersecurity policies</li> <li>– Cybersecurity standards, methodologies and frameworks</li> <li>– Cybersecurity recommendations and best practices</li> <li>– Cybersecurity related laws, regulations and legislations</li> <li>– Cybersecurity related certifications</li> <li>– Ethical cybersecurity organization requirements</li> <li>– Cybersecurity maturity models</li> <li>– Cybersecurity procedures</li> <li>– Resource management</li> <li>– Management practices</li> </ul>

	– Risk management standards, methodologies and frameworks
--	---

## **Annex I**

### **(informative)**

## **Cybersecurity for operation and maintenance activities - Operational guidance**

### **I.1 Purpose**

This [Annex I](#) gives some operational guidance for consistent access rules and protection of critical data for operation and maintenance activities (see [10.4](#)).

### **I.2 Change to maintenance activities and teams**

During conception phase, cybersecurity teams should engage early in the project life cycle with the maintenance teams for the operational definition of technical and organizational measures.

It is easier to adapt measures during the design phase to be compatible with maintenance teams capabilities rather than wait for the handover or commissioning phase. This will result in reducing any changes, relax an initial measure or imposing constraints on maintenance teams.

### **I.3 Access Strategy**

#### **I.3.1 Physical Access:**

Several approaches can be used for physical protection, such as protection by personal badge, digital programmable key, security key (e.g. mechanical key with special permissions / copy not allowed) or basic key (e.g. square or triangle key). To make the best choice, the level of protection needed for a zone coming from risk analysis should provide the initial data to correctly split the physical zones first and to put on each, an adequate measure. For the measures, potential complexity exported to organization for distribution, revocation, updating and management of loss should also be analysed with a pragmatic and operational view.

**EXAMPLE** When designing physical enclosures, critical assets could be segregated from other assets for which access is needed by multiple people, such as a cleaning company.

Considering a security key which appears as the best approach for one physical area (e.g. cabinet), if it becomes mandatory to share this key with multiple employees or contractors who do not have adequate security clearances, it may be relevant to use a protection badge or a digital key to ensure that the loss of security key does not quickly become a major vulnerability with a mechanical lock. If a sufficient physical protection is not in place for critical systems, an effective additional countermeasure could be an electronic door contact or a video surveillance system linked to an alarm. This will monitor the door status.

#### **I.3.2 Role-Based Access:**

Individual accounts with associated profiles (based on the least privilege principle) applied should be compatible with maintenance constraints.

The access to sensitive data or essential systems by maintenance staff should be protected by the asset owner for defined person(s) and limited group of assets. The objective is to prevent malicious or accidental access. The access rules should consider need for synchronisation, supervision, and the possibility (with compliant countermeasures) to bypass availability needs without causing significant issues for the person performing the maintenance activity.

**EXAMPLE** If an individual access is deployed on to a fleet of trains, a change of individual password needs to be quickly synchronised and deployed to be used on each train of the fleet without delay or manual actions, such as copying and pasting a database.

### **I.3.3 Network Access:**

When access control to an OT network is deployed, choices for measures should easily allow legitimate access to maintenance service providers and restrict illegitimate access to malicious persons. This should consider the risk, such as exposure of a connector and the tools available, for example, technology, management and process for an update.

**EXAMPLE** If an 802.1x control is in place, the authentication of a laptop on the network could be as transparent as possible for a legitimate user and the certificate used could be managed through a centralised console without the need for manual action by the maintenance service provider. The revocation process could also be efficient.

### **I.3.4 Consistency for Access Protection:**

Access protection should be consistent between physical, role-based and network access. A high-level of protection for one aspect can compensate for another that is less efficient. Consistent protection should be a combination of each aspect determined through capabilities of the railway solution and constraints transferred to maintenance activities.

**EXAMPLE** If an individual account is too complex for logical protection then it is acceptable to have a cabinet with an individual badge at the physical level with generic account at the logical level.

## **I.4 Remote Access and Maintenance**

### **I.4.1 General**

It is essential that remote access and maintenance from external sites pass through the company security gateways, such as a firewall, data diode, bastion or proxy, as the first perimeter of security. Depending on the roles given by enterprise/corporate identity management system and authorized by the internal identity provider, user should be redirected to the perimeter security device located in destination SUC.

To prevent backdoors, security loops and to reduce interfaces and complexity, additional communications (for maintenance) such as Integrated Services Digital Network (ISDN), V92 modem, serial, cell phone and IP in and out landside OT railway application on Purdue Level 0 to 3 are not allowed in general. Bundling communications through the railway application internal perimeter security device and the use of an in-band maintenance method (see definition hereafter) is highly recommended.

### **I.4.2 Remote Maintenance OT**

The perimeter security device located in the destination (entity) railway application should act as second line of defence and restrict access to the necessary zones, assets and applications within.

### **I.4.3 Methods of Remote Maintenance**

Depending on capabilities of the devices and existing environment, two possible methods of remote maintenance are available and should be considered in the design phase, using as input the high-level railway zone model ([Clause 4](#)):

- In-band (common)
- Out-of-band (exceptions)

In-band means that network for administration is the same as operational data.

Out-of-band means that the network for administration is a dedicated one, and does not mix with the network used for data.

Out-of-band communication causes a second external communication channel that is not monitored by the railway duty holder. If out-of-band maintenance is needed, confirmation from

the CISO should be obtained and these communications links are to be added to the high-level railway zone model.

For more information on in-band and out-of-band concepts, see also [\[56\]](#), [\[57\]](#).

## **I.5 Other aspects to be correctly addressed**

### **I.5.1 Data Protection:**

The confidentiality of credentials, for example key pass of security files, such as certificates, sensitive data manipulated around system including binaries, informatics files and personal data, should be managed without complex manipulation for the maintenance service provider. This includes documentation containing sensitive data or security information.

**EXAMPLE** It could be relevant to synchronise between a centralised secured database and laptop for data limited to the activity concerned, local secure storage or an automatically erased system.

Access to documentation with sensitive data should be correctly managed to allow easy access to the maintainer during their activities and avoid need to print, or copy and paste, sensitive data such as on to paper or digital media.

### **I.5.2 Decommissioning:**

See decommissioning management in [10.17](#).

### **I.5.3 Awareness of People:**

See competency management in [5.6](#).

### **I.5.4 Use of Portable Media (such as laptop, USB key):**

Maintenance activities often require use of portable media like laptops or USB keys. Mobility and higher risk of loss or accidental/inappropriate usage should be considered.

Dedicated and professional USB keys should be used and all other devices should be strictly forbidden.

Procedures should allow maintenance service provider to minimise manual operations and portable components should be regularly controlled, for example to check for integrity and for absence of malware.

**NOTE** These procedures correspond typically to an applicable SecRAC of the railway application. These SecRAC can come either from the railway solution cybersecurity case delivered by the system integrator or have been added by the asset owner during the operation and maintenance activities as needed.

### **I.5.5 Key Exchange and Management:**

The manipulation of secrets such as security keys and certificates should be correctly anticipated during the conception phase. A system should be designed to avoid unsecured manipulation, storage or transmission. If secrets are updated or refreshed, automatic processes should be preferred over manual operations, which should be limited.

**NOTE** See to [IEC 62443-2-1:2024 \[52\]](#) (ORG 3.1, CM 1.4, COMP 1.1 - 1.2 and 2.1 - 2.3, DATA 1.1 - 1.7, USER 1.1 - 1.18, AVAIL 2.1 - 2.5) for further guidance on operations/maintenance management.

## **Annex J** (informative)

### **Vulnerability Management - Operational guidance**

#### **J.1 Purpose**

This [Annex J](#) gives some operational guidance for [10.10](#) [OM-05-02] Vulnerability management.

#### **J.2 organizational aspects**

The vulnerability management process of the asset owner should include policies and procedures regarding vulnerability information that address:

- a vulnerability disclosure policy to enable the reporting of vulnerabilities by internal and external sources
- mechanisms to receive vulnerability advisories from product suppliers and service providers
- mechanisms to report vulnerabilities to third parties like product suppliers and service providers.

NOTE 1 Vulnerability information and disclosure could be public (e.g. open source), but it could also be confidential (e.g. for zero-day on specific software)

NOTE 2 See supply chain management in [5.8](#) for interfaces between system level and component level.

Cooperation between different railway stakeholders, for example railway duty holders and system integrators, with respect to vulnerability disclosure can be beneficial when dealing with new vulnerabilities. Cooperation could be organized by information sharing organizations (e.g. CSIRT, CERT and ISAC)..

Depending on the legal framework, it may also be necessary to report to government agencies or other bodies. Best practices of responsible disclosure should be applied (see [ISO/IEC 29147:2018](#) [23] for guidance).

Decision for remediation, and in particular a decision to deploy a patch, is made by the asset owner who is accountable for the railway application.

#### **J.3 Process scoping**

To optimize investment and to prioritize activities on the most important topics regarding maintaining a railway application in a secure condition, the asset owner can choose to prioritize assets to manage the resources force the most critical asset as first, and for that adapt, focus or limit the number of assets for its vulnerability analysis or its remediation activities.

Typical optimization could be based on a cyber-critical asset approach. In such cases, based on the risk assessment and the logical and physical architecture of the railway application, the asset owner defines a list of cyber-critical assets (components or systems) that are relevant for vulnerability management to maintain secure conditions.

The cyber-critical asset approach by choosing focussed components, should allow to maintain an acceptable level of security throughout the system by concentrating processing on these, to optimize or reduce the constraints for treatment on other components and the list of components under monitoring.

Criteria to define this list may include, among others:

- Logical or physical exposure, for example wireless equipment such as MCG or Wi-Fi access points, and components with connectors easily accessible from passenger/public zone.
- Hosted functionality, for example a secure gateway with cybersecurity functionalities such as filtering, unidirectional data-flow or shared-security-services and badge readers which allow high physical security with high benefit for cybersecurity risk assessment.

Other systems or components (not exposed or not dedicated to host security functions) may be also regarded in the vulnerability analysis. Risk assessment should help to consolidate the preliminary list based on exposure or security hosted functionality.

#### **J.4 Vulnerability identification, analysis and prioritization criteria**

The vulnerability management process should define a risk-based vulnerability analysis methodology and the criteria to prioritize its handling.

The asset owner deals mostly with vulnerabilities in third-party components and systems of the railway application. The vulnerability management process should define the mechanisms for secure exchange of vulnerability information with the product supplier or with the system integrator and the mechanisms to receive and use the security advisories as input for the analysis and remediation activities.

Security advisories informing about vulnerabilities in products or systems usually provide a description of the potential impact of the vulnerability, its severity rating without considering the operational environment and a description of the score system.

NOTE 1 Vulnerability disclosure could come from public databases such as Mitre and NVD, industrial/supplier information, information sharing through community, for example the European railway information sharing and analysis centre (ER-ISAC), information for computer security incident response team (CSIRT), test reports, incident reports and internal disclosure.

The asset owner should define the scoring system to be used. The scoring methodology should be correctly defined in order to allow analysis and comparison, in particular when multiple organizations are involved in the process.

In a second step, the asset owner can reassess the severity of the vulnerability considering:

- the railway application risk assessment (including functional impact); and
- the security context of the component/system integrated in the railway application; and
- the configuration of the component/system for its intended use in its operational environment.

For example, the severity of a remote desktop protocol vulnerability with an initial vulnerability score assessed for the generic product can be lower after the contextualised assessment, taking into account a railway application architecture that reduces the exposure of the component interfaces, or it can be even eliminated after hardening after which the vulnerable interface is not exposed.

After the analysis, the asset owner can prioritize the subsequent activities using one or a combination of the criteria given as an example below.

The asset owner can establish prioritization criteria based on the severity score of the vulnerability. For example:

- a high priority for scores higher than 90% of higher score;
- a medium priority for scores between 70% and 90% of higher score;
- a low priority for scores below 70% of higher score.



NOTE 2 The number of common vulnerabilities scoring which could concern several assets of a system could be quite important. Using an automatic system could solve some steps of the analysis, considering the criteria defined in the strategy.

NOTE 3 NIST national vulnerability database (NVD) and information from various CERTs could be a useful source of information.

NOTE 4 The CVSS approach, according to its version, could include temporal aspects, such as exploitability, and environmental aspects, such as impact on the system regarding confidentiality, integrity, availability. If CVSS is used, the version could be identified.

NOTE 5 The impact of compounding from multiple deferred risks could also be considered during the risk analysis process.

Another prioritization criterion is the evidence of actively exploited vulnerability or the likelihood that the vulnerability will be exploited in the short term.

When there is no evidence of an actual exploit for a publicly known exploitable vulnerability, the likelihood that it is exploited can be estimated and rated as low level (unlikely), medium level (possible), or high level (imminent). This likelihood could be high for a vulnerability with low severity score, and to the contrary, the likelihood that a vulnerability with high severity score is exploited could be very low.

A typical choice would be to prioritize the vulnerabilities for which an active exploit is known or estimated as imminent.

NOTE 6 The forum of incident response and security teams (FIRST) exploit prediction scoring system (EPSS) or cybersecurity infrastructure and security agency (CISA) known exploited vulnerability (KEV) could be a useful source of information.

Finally, the threat landscape can assist in analysing the threat posed by the vulnerability to the railway application and prioritizing how it is managed.

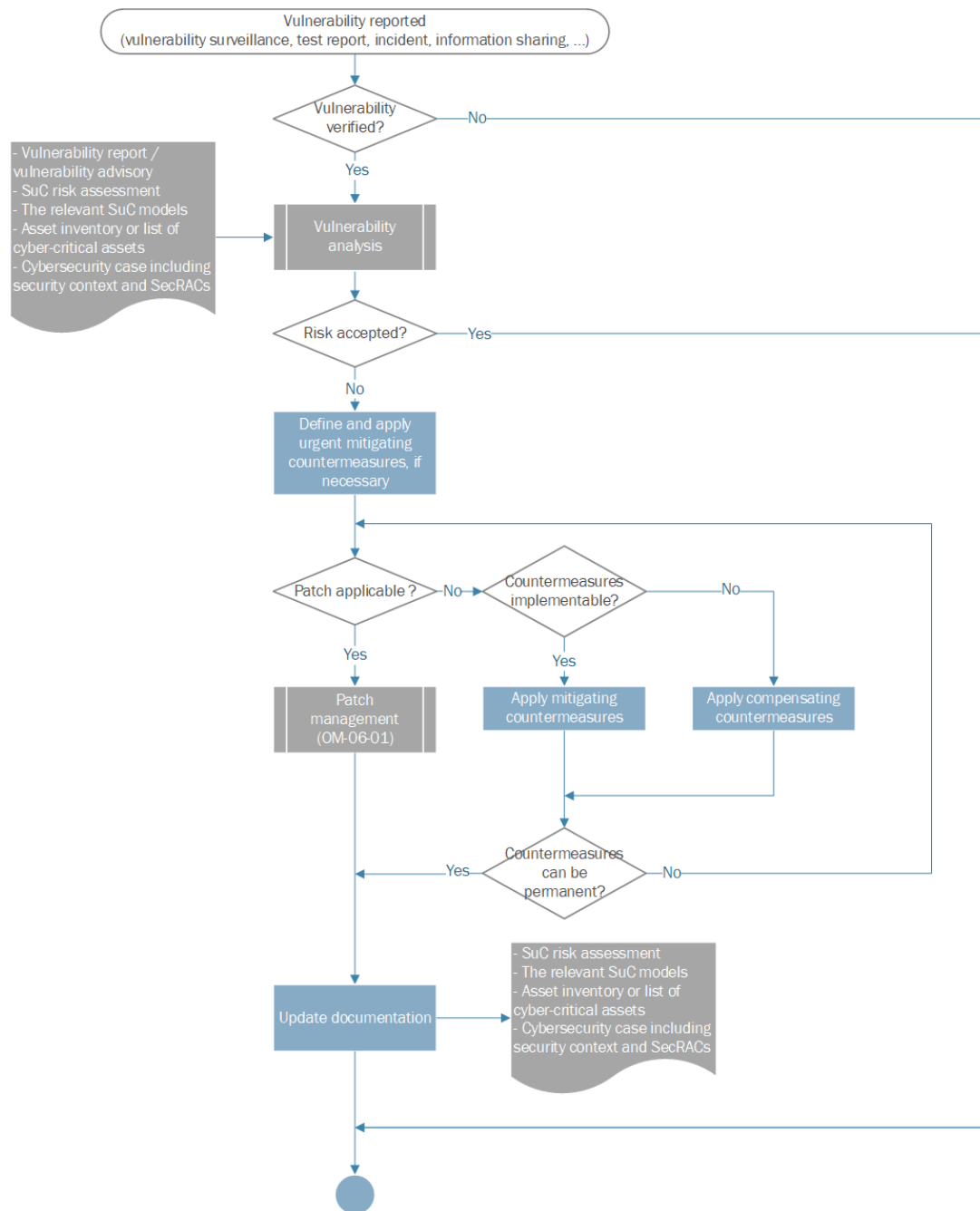
NOTE 7 Regional, sectorial, or company threat landscape analysis could be a useful source of information.

NOTE 8 The scoring method Stakeholder-Specific Vulnerability Categorization (SSVC) from cybersecurity infrastructure and security agency (CISA) propose a decision tree model which include state of exploitation, automatisisation, technical impact, essentiality of mission/function and impact on humans.

## J.5 Vulnerability remediation

Figure J.1 gives an example of a flowchart to illustrate the different possibilities of remediation for a vulnerability which is defined as relevant after analysis and application of the prioritization criteria.

This figure does not allocate responsibility of tasks but identifies the tasks to be done and it is agnostic to the people who do the tasks. The asset owner is accountable for the railway application and the responsibility for ownership of these tasks depend on the project organization, for example, asset owner, system integrator and maintenance service providers. This aspect should be defined into a responsibility assignment matrix according to the organization of project and contractual requirements.



**Figure J.1 – Vulnerability remediation**

The trigger of the process is the disclosure of a vulnerability in an asset to be maintained in secure conditions.

An initial verification should discard reports that do not constitute a vulnerability and other circumstances that may lead to exit the process like:

- The vulnerability is not affecting any asset in the scope of the vulnerability analysis and remediation.
- The vulnerability was reported before and it is already being addressed or it has been remedied.
- The vulnerability is in a system for which the asset owner is not responsible.

The vulnerability analysis, as described above, will lead to a characterization of the vulnerability that provides the necessary information to support the subsequent decisions during remediation.

Relevant inputs for the analysis are, among others, the vulnerability report or advisory, the railway application risk assessment, railway application models and the asset inventory or list of cyber-critical assets, the cybersecurity case including security context and SecRACs and the functionalities potentially affected.

In case the analysis of the vulnerability and the application of the prioritization criteria concludes that the severity has a very high score, and it needs to be handled with high priority, the immediate application of mitigating countermeasures may be needed.

The next question to address is the availability of a patch, and the expected time for its deployment. If all is compatible with the strategy defined or with the decision plan of the asset owner, the deployment of a patch is the best way to solve the vulnerability.

Mitigating measures that reduce or remove the risk (like filtering and port deactivation) should be defined if a patch is available but the time to deploy it is not acceptable, or if a patch is not available, not compatible or not relevant (e.g. technically or economically).

Compensating measures that control the risk, like monitoring or control activities, could be defined to balance the situation temporarily or definitively.

If an acceptable level of security is achieved, and measures can be permanent, the issue can be resolved without patching.

In an extreme case where a vulnerability cannot be solved, the security team can no longer apply the strategy validated by the asset owner. A decision regarding this vulnerability should be raised to higher organization level for acceptance (temporarily or not) or other decision, for example, the shutdown of a service.

## **Annex K** (informative)

### **Cloud security**

#### **K.1 General**

The scope of the cloud security objectives and recommendations apply solely to cloud implementations of the railway solution, devices, applications, data, technology resources and digital assets directly involved in the control, monitoring, and operation of rail infrastructure and rolling stock for both passenger rail and freight.

Cloud services may be connected to the OT system and used for operational support, such as passenger and emergency evacuation information, and in some cases directly control OT systems, e.g. the signalling system. However, it should also be emphasized (4.4, SO-01-01) that in such cases, the railway duty holder will have the authority to decide whether to treat it as an IT system or an OT system.

The information set out in this annex does not apply to individual circumstances where Artificial Intelligence (AI), Internet-of-Things (IoT), Industrial IoT (IIoT) and similar systems are used, as these systems typically have additional security measures in place in their own domains which should be applied alongside the objectives and requirements in this annex as part of the entire SUC. Additionally, the security measures in place for systems such as AI, IoT and IIoT may be more onerous than those set out in this annex due to the complexity of their operational environment, and therefore applying the objectives and requirements in this annex alone may not be enough to meet the necessary target security level.

For the purposes of this annex it is necessary to distinguish between IIoT and cloud-connected OT. IIoT, by definition, is technology with the ubiquitous presence of connectivity that is integrated into the traditional railway application and solution. It gathers data from machines for analysis, improving efficiency. Cloud-connected OT extends traditional OT systems' functionalities by allowing data in the cloud and provisioning, monitoring and business enablement and control from the cloud. While IIoT focuses on the data itself, cloud-connected OT is about using the cloud to improve existing OT systems.

See ISA-TR62443-1-6 Security for industrial automation and control systems Application of the 62443 standards to the Industrial Internet of Things [33] for additional guidance.

#### **K.2 Applicability**

This annex applies to cloud suppliers, vendors, integrators, and entities. The collective may be referred to as third-party entities alternatively. This guidance addresses security technical countermeasures in the context of cloud service models. In general, the following cloud service models are described:

- Infrastructure as a Service (IaaS) – The CSP provisions and secures the physical resources for the customer and maintains isolation between customers. The customer configures network security policies and maintains the security of the operating system and applications hosted on the provided infrastructure.
- Platform as a Service (PaaS) – The customer is responsible for confirming the services are configured properly, developing application code security, and configuring security policies to restrict network access between applications. The CSP secures and maintains the hardware, operating system, networking, and platform software configurations.
- Software as a Service (SaaS) – In this model, the CSP secures and maintains the hardware, operating system, networking, and application software.

However, the focus is on technical aspects of the security countermeasures and acknowledges the influence of cloud deployment models on its applicability:

- Public Cloud: Computing resources are shared among multiple customers using a multi-tenant infrastructure where the railway duty holder and third-party entities are responsible for securing their specific environment within the shared infrastructure.
- Private Cloud: Computing resources are dedicated for the exclusive use of the railway duty holder. In this model, the railway duty holder can assess the cloud environment to identify any gaps and ensure alignment with the recommended security countermeasures.
- Hybrid Cloud: A combination of public and private cloud resources, with orchestration for data and application portability. The railway duty holder and third-party entities should ensure consistent security countermeasures across both public and private cloud deployments.

When considering security countermeasures for OT systems with cloud service capabilities, the railway duty holder should consider the more stringent security countermeasures of this annex. See [4.4.2](#) for additional guidance on applicability.

A risk-based approach should be applied to determine the appropriate level of security measures, considering the whole system, including the cloud-connected OT systems.

### **K.3 Cloud Security within the railway application life cycle**

Consider cloud security countermeasures throughout its entire life cycle in alignment to the overall framework the system is designed. See [Clause 6](#) for additional guidance on cybersecurity activities to be carried out during the life cycle of a railway application.

In general, the life cycle can be grouped into distinct phases which are further defined in the sub-clauses:

- specification;
- design and implementation;
- validation;
- operations and maintenance;
- decommissioning;
- business continuity and disaster recovery.

#### **K.3.1 Specification Phase**

Establishing a cloud security framework is an important component of the overall railway application. These can be formalized by establishing the statement of work, necessary contractual agreements, and addressing risk management. Contracts should encompass legal aspects of cloud security initiatives, including vendor selection, service level agreements (SLAs), data privacy and security provisions, incident response responsibilities, and intellectual property rights. Statements of work should outline the specific deliverables, timelines and resources required for the cloud services project. It serves as a blueprint for collaboration between internal and external stakeholders, ensuring alignment on project objectives and expectations.

##### **K.3.1.1 Risk Management**

Risk management involves identifying, assessing, and prioritizing potential security threats and vulnerabilities within the cloud environment. While mentioned as part of specification in the first phase, risk management should be applied throughout all phases. Implementing appropriate risk mitigation strategies, such as security countermeasures, incident response plans, and continuous monitoring, is essential to protect sensitive data and systems. Refer to [5.9](#) for risk management principles.

Table K.1 presents some operational risk considerations by cloud zone that should be factored into the overall risk assessment. In general, there are three types of cloud zones (region, availability zone, and edge) that will have varying degrees of impact with regard to unavailability, degradation, and misuse. At the region level, it may consist of a large geographical area containing one or more availability zones, providing services across a broad region, and offering disaster recovery options through multiple availability zones. The availability zone (AZ) level is a distinct location within a region, physically isolated from other AZs. It provides high availability through redundancy and fault isolation and offers low latency within the region. At the edge location level, it can be a geographical location that houses computing, storage, database, and content delivery network services. It provides low latency and high performance for applications closer to end-users. It is often used for content delivery and real-time applications.

**Table K.1 – Operational risk considerations**

	Region level concerns	Availability zone (AZ) level concerns	Edge location level concerns
<b>Unavailability</b>	Natural disasters, power outages, infrastructure failures	Isolated failures within the AZ	Localized outages due to distributed nature
<b>Degradation</b>	Network congestion, increased latency, reduced performance	Localized performance issues	Performance issues due to proximity to end-users
<b>Misuse</b>	Increased attack surface due to the number of resources	Targeted attacks on specific resources	Potential attacks from end-users

See 5.9 for additional guidance on risk management.

### K.3.2 Design and Implementation Phase

Prioritizing cybersecurity from the outset for cloud-connected assets, the asset owner can mitigate risks, protect critical infrastructure and maintain operational continuity. A robust design encompasses considerations such as network segmentation, data protection, and access controls.

#### K.3.2.1 Access Control

Access control refers to the set of enforcement mechanisms and policies that dictate how users and systems can interact with cloud resources. It is a framework that uses authentication and authorization techniques to ensure only authorized entities have access to specific resources and can only perform permitted actions. See IEC 62443-3-3:2013/COR1:2014 [59], FR1 – Identification and authentication control and FR2 - Use control for additional guidance.

OT systems are geographically dispersed and involve numerous people. Connecting them to cloud services introduces new access points that require strict control to prevent unauthorized access. Because of these complexities, a dedicated access control policy is necessary to manage how these actors interact with the cloud-connected OT systems. See IEC 63452, clause 8, table 6, FR 1 for additional guidance. Consider the principles in the following subclauses.

##### K.3.2.1.1 Identity and Access Management

Utilize the IAM service managed by the organization. If it does not exist or it cannot interoperate with the organization's cloud service, then use the IAM service provided by the cloud service provider as appropriate within the risk assessment.

- Implement the principle of least privilege, granting users only the minimum permissions required to perform their jobs.
- Apply access control methods. Role-based access control (RBAC) assigns permissions based on user roles and job functions aligned to Annex H – Cybersecurity roles and competence profiles. Attribute-based access control (ABAC) is a method used to control

access to data by assigning attributes to resources and to users, providing more fine-grained policy protection to resources than using RBAC policies alone.

- The asset owner should conduct user access reviews at least quarterly, with consideration for applying least privilege, and more frequently upon events such as:
  - user separation from the company (termination, retirement, etc.);
  - cybersecurity incident;
  - user transfer to a different department with differing access needs;
  - change in user responsibilities that no longer require current access levels.
- Multi-Factor Authentication (MFA):
  - Consider MFA for all user accounts accessing the cloud environment based on risk assessment. This adds an extra layer of security beyond just a username and password.
  - Supported MFA methods may include:
    - hardware tokens (e.g. security keys);
    - authenticator apps on mobile devices;
    - biometric authentication (fingerprint, facial recognition) in conjunction with another authentication factor.

Establish a process for user provisioning and de-provisioning. Disable or delete user accounts promptly when employees leave the company or change roles. Implement strong password policies, including minimum password length, complexity requirements, and regular password rotation. Consider passwordless authentication methods where appropriate (e.g. single sign-on (SSO) with MFA).

#### **K.3.2.1.2 Managing Credentials**

The complete life cycle of credentials (generation, revocation, expiration, etc.) should be managed by the asset owner.

Cloud credentials should never be stored in plain text. If needed, users can leverage secrets management tools (preferably ones that use hardware security features. (e.g. a hardware security module (HSM) or trusted platform module (TPM) to have capabilities to protect secret keys) to manage cloud credentials (e.g. password managers for human secrets or secret stores for workload credentials). To further mitigate risk, users should disable features that allow web sites or programs to remember passwords. MFA, such as one-time PIN tokens, PKI tokens, or smartcards, for users and non-person PKI-based authentication (for workloads) should be implemented where possible.

In situations where PKI-based authentication is not technically feasible, secret keys can be generated to allow applications to manage cloud resources programmatically.

Avoid creating keys with root or administrative privileges. These keys should be generated for short-term use only, and accounts should be granted the least required privileges needed to accomplish operational tasks. These credentials should never be included in plain text in application source code or embedded into binaries. Instead, they should be handled securely by a secrets manager and stored encrypted.

If using secure shell (SSH) key pairs to connect to cloud hosted virtual machines, the private key should be stored in a secrets manager and should not be shared.

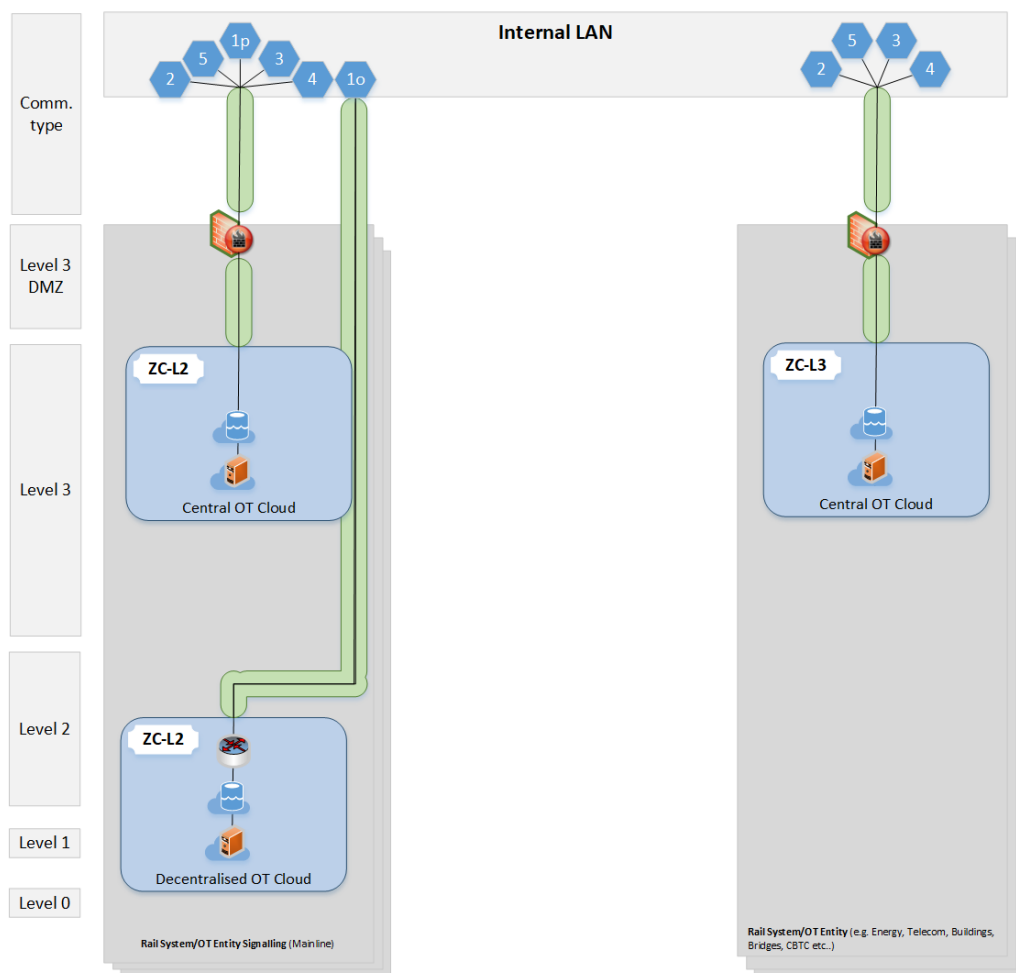
#### **K.3.2.2 Communication and Network**

Cloud-connected OT devices impose unique security considerations within a network security architecture. A zones and conduits model should be applied to the connectivity using the principles of least privilege for any communication between zones. Consider the following principles:

- External cloud systems should not share a zone with any other systems.
- Integration with external cloud environments should require logical access controls such as firewall segmentation between zones (e.g. corporate network, operations networks, and the external cloud environment).
- Hardware-based segmentation solutions (e.g. data diodes) may be implemented in addition or as an alternative technology to define zones as appropriate for risk management.
- Configure cloud network security groups and firewall rules to restrict communication only to authorized host, ports and protocols between zones.
- Consider implementing micro-segmentation within zones to further limit lateral movement of attackers within the cloud environment.
- Consider redundancy of cloud services to ensure a more resilient cloud infrastructure. This also includes using diverse cloud providers to avoid relying solely on one vendor. See [Clause K.3.6](#) for availability considerations.

Cloud connectivity can be initiated from various zones within the OT environment. Below are some reference architectures that depict the connectivity to certain services outside the OT environment. Please reference 4.6.2, figure 6 for full diagram.

**To be read in conjunction with Figure 6 only – DRAFT VERSION, FOR DISCUSSION BY SG-02 – 11/06/2024**



See [IEC 62443-3-3:2013/COR1:2014 \[59\]](#), FR 5 – Restricted Data Flow for additional guidance.

### K.3.2.3 Software Design

Continuous integration/continuous delivery (CI/CD) is a development process for quickly building and testing code changes that helps organizations maintain a consistent code base for their applications while dynamically integrating code changes. CI/CD is a key part of the



development, security, and operations (DevSecOps) approach that integrates security and automation throughout the development life cycle. CI/CD pipelines, which automate the integration and delivery of applications, are attractive targets for cyberattacks as it provides a vector for introducing malicious code into CI/CD applications, gaining access to sensitive data, or causing a denial of service.

Where applicable, it is important to consider how CI/CD pipelines are secured due to their role in delivering and updating software. See [Clause K.3.4.2](#) for cloud security countermeasures guidance.

### **K.3.2.4 Use of Cryptography**

Cryptography Management encompasses the implementation and control of cryptographic mechanisms to protect sensitive data.

#### **K.3.2.4.1 Encryption and Key Management**

All communications between nodes in different zones should employ current state-of-the-art cryptographic security measures, considering the expected lifespan of the solution. Digital certificates from a trusted Public Key Infrastructure (PKI) should be used for authentication of communication parties and for establishing a secure and trusted connection. Cryptographically secured key exchanges should be used for the initiation of encrypted communication channels. Authenticated encryption algorithms and secure integrity protection mechanisms should be used for authentication and integrity protection of the established communication connection.

Encryption Algorithms:

- Utilize current, industry-standard authenticated encryption algorithms used after initiation of a cryptographically secured connection with cryptographic integrity protection algorithms for data in transit between zones. Refer to your country standards body for cryptographic standards. Below is a non-exhaustive list:
  - United States - National Institute of Standards and Technology (NIST);
  - European Union - European Telecommunications Standards Institute (ETSI);
  - Japan - Cryptography Research and Evaluation Committees (CRYPTREC).
- Implement forward secrecy mechanisms within the chosen encryption protocol (e.g. Perfect Forward Secrecy (PFS) with TLS). This ensures that even if an attacker compromises a session key, they cannot decrypt past communications.

Key Management:

Both Cloud Service Customer (CSC) and the Cloud Service Provider (CSP) are accountable for securing cloud environments, but the scope of responsibilities for key management will vary depending on the cloud service model employed.

- Implement a robust key management strategy to protect cryptographic keys used for securing communication. This includes:
  - Leverage cloud provider-managed key services (KMS) whenever possible. These services offer secure key generation, storage, rotation, and access control.
  - Secure key generation and storage using hardware-based mechanisms, e.g. TPMs (Trusted Platform Modules), Hardware Security Modules (HSMs) or other approved methods.
  - Key rotation at regular intervals based on best practices and the chosen algorithm's life cycle recommendations.
  - Secure access controls for key management systems to prevent unauthorized access or key compromise.

Algorithm Selection and life cycle:

- Select encryption algorithms based on a risk assessment considering data sensitivity, processing requirements, and expected solution lifespan.
- Regularly review and update encryption algorithms that are deprecated to stay ahead of evolving threats and cryptographic vulnerabilities.

Transport Layer Security (TLS):

- Enforce the use of TLS (Transport Layer Security) for all communication channels
- Ensure strong cipher suites are used within TLS configurations, following industry best practices.
- Certificates should be renewed within a manageable timeframe before expiration of the certificate. The previous certificate can be revoked by the issuing certificate authority.
- Compromised certificates should be revoked and re-issued.

See [IEC 62443-3-3:2013/COR1:2014 \[59\]](#), FR 4 – Data Confidentiality for additional guidance.

#### **K.3.2.4.2 Manage PKI Certificates**

PKI certificates are commonly used in cloud environments and can be either client certificates or server-side transport layer security (TLS) certificates. Client certificates can be used for authenticating users to a cloud service (either solely or as part of an MFA solution) or to authenticate non-person entities (i.e. “workload identities” or “service identities”) to other systems.

- Ensure proper management through secure key storage and periodic key rotation, and key revocation.
- Organizations using PKI certificates for user authentication should maintain a list of trusted certificate authorities, only allow trusted certificates, document revoked certificates, and remove users and block access associated with revoked certificates.
- Manage the server certificates used for securing web communications and any client certificates used for inter-workload authentication.
- Organizations using customer-managed application servers should refrain from storing private keys in plain text on the virtual instance hosting the server. Certificates should instead be managed with a key management system (KMS), which functions to store the encrypted keys, and control and monitor access to the keys.

#### **K.3.2.5 Secure Cloud Provider Integration**

- Leverage native cloud provider security features like IAM roles and access controls.
- If using SaaS applications, consider utilizing a cloud access security broker (CASB) to manage and monitor access across multiple cloud services.
- Limit login attempts to prevent brute-force attacks.
- Implement CAPTCHAs to detect unusual login attempts and deter automated attacks.
- Use SIEM to analyse events and identify potential security threats.

#### **K.3.2.6 Secure cloud instance metadata service (IMDS)**

Restrict access to IMDS for instances or accounts that do not require it.

### **K.3.3 Validation Phase**

This phase focuses on assessing the effectiveness of implemented security countermeasures and identifying vulnerabilities that may still exist.

#### **K.3.3.1 Vulnerability/Penetration Testing**

The OT security of the railway application needs to be maintained throughout operation, maintenance, decommissioning or divestiture activities. Railway applications using cloud

services will also need continuous monitoring to identify and address security threats in near real-time. Reference clause 10 for operational, maintenance and disposal requirements.

The railway duty holder should implement a vulnerability management process for cloud services consistent with 10.10 to identify, analyse and resolve vulnerabilities from internal and external sources.

The intent is to allow for early threat detection to identify and address security incidents before they cause damage, enable quicker mitigation of security threats, and maintain constant vigilance of the cloud security posture. The Table K.2 provides general guidelines for scanning following the assurance level criteria by the EUCS – CLOUD SERVICES SCHEME EUCS [34].

**Table K.2 – Scanning considerations**

Scanning Considerations	Level 1 (Basic)	Level 2 (Substantial)	Level 3 (High)
Types of scans	Scan operating systems, web applications, and databases monthly The entire inventory (or sampling percentage) within the boundary should be scanned at the operating system level at least one a month. All web interfaces and services (or sampling percentage) should be scanned. All databases (or sampling percentage) should be scanned, including those required to support the infrastructure. Enable all non-destructive detections within the scanner.		
Scanner Resiliency	Patch and security harden through configuration the scanner to resist unauthorized use or modification.		
Authenticated Scanning		Ensure authenticated scans are performed.	
Scanning with full authorization		Ensure scans are being performed with full system authorization.	
Machine-readable findings	Display all scan findings in a structured, machine-readable format (such as XML, CSV, or JSON)Where possible, include the authentication and authorization status of the scans to demonstrate the degree to which an authenticated scan was performed on each host. Include the common vulnerabilities and exposures (CVE) reference number associated with the vulnerability. Use latest CVSS scoring methodology and where one is not included, use the native scanner base risk score.		
Signature Updates	Use a vulnerability scanner that checks for automatic signature updates of the scanner's vulnerability database at least monthly.		
Adequate Asset Identification	The scanner contains an automated mechanism to identify and catalogue all assets, within the authorization boundary, every month. For web scans, a dynamically updated catalogue of web services should be maintained to include the ports where web services reside.		
Image scanning	Scan source virtual images.		

### K.3.4 Operations and Maintenance Phase

This phase focuses on activities to be considered for cloud security monitoring, patching, incident response, and back up management.

#### K.3.4.1 Cloud Security Monitoring

The railway duty holder should establish cloud security monitoring of the railway system where cloud services are used. Monitoring should be in alignment with clause to establish a continuous process of detecting, reporting, handling, and responding to security-related events generated by cloud resources, applications, and user activities. The following principles should be applied:

- Access Logging and Monitoring: Enable access logging for all cloud resources to track user activity, access requests and policy changes.
- Regularly monitor logs for suspicious activity, such as failed login attempts or access from unusual locations or times.
- Monitor identity federation servers for anomalies or abnormal changes. Implement security orchestration, automation, and response (SOAR) to automate alerts that will notify a security operations centre (SOC) of potential security incidents.

- Ensure log files are secured from alteration and readily available for research and consumption both manually and by automated interoperability with security tools such as SIEM.

#### **K.3.4.2 Cloud Security Countermeasures**

The railway duty holder should select the most appropriate framework(s) based on organizational needs, regulatory requirements, and cloud service provider offerings. As the threat to cloud evolves, it is important to have a continuous improvement approach that instills regular assessments and vulnerability management.

- Information System Security Management and Assessment Program (ISMAP) [35] is a framework for registering cloud services through an assessment process to evaluate whether a cloud service properly implements each criterion which is based on international standards.
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) [36] This framework offers a specific set of security controls tailored for cloud environments. The CSA CCM can be used to assess and manage the security risks associated with cloud adoption and ensure compliance with relevant regulations.
- EUCS – CLOUD SERVICES SCHEME EUCS, a candidate cybersecurity certification scheme for cloud services [37]: A: 'basic', 'substantial' and 'high'. The security requirements on cloud services and on their assessment increase with levels in several dimensions: scope, rigour and depth. The requirements at level 'high' are demanding and close to the state-of-the-art, whereas the requirements at level 'basic' define a minimum acceptable baseline for cloud cybersecurity. That baseline is nevertheless comprehensive, as it covers all major aspects of cloud security. Cloud service providers of any size can use it to demonstrate that they have set up a framework for guaranteeing some security of their customers. The 'substantial' level, in between, will serve to protect business, and may be the level of choice for many applicants and their users.
- The Federal Risk and Authorization Management Program (FedRAMP) [38] is a US government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP uses the NIST Special Publication 800 series and requires cloud service providers to complete an independent security assessment conducted by a third-party assessment organization (3PAO) to ensure that authorizations are compliant with the Federal Information Security Modernization Act (FISMA) [39].
- Use secure cloud identity and access management practices, [40]: This information sheet explains the common threats to cloud identity management and recommends best practices organizations should use to mitigate these threats when operating in the cloud.
- EN ISO/IEC 27017:2021 [41] Information technology - security techniques - code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015).
- ISA-TR62443-1-6:2024 [42], Security for industrial automation and control systems, application of the 62443 standards to the Industrial Internet of Things, Draft Technical Report, February 2024

#### **K.3.4.3 Shared Cybersecurity Services**

OT systems with cloud service capability providing shared cybersecurity services should consider the security countermeasures within this annex. Clause 4.7 specifies typical shared cybersecurity services of which some may have cloud service capabilities or be completely hosted in the cloud.

Directionality and type of data will drive risk and appropriate cybersecurity countermeasures. For example, control signals received from a cloud instance to an OT system should be filtered, authenticated, and monitored for cybersecurity anomalies. Non-control signal data such as cybersecurity monitoring and telemetry data from an OT system to a cloud instance should be implemented in a uni-directional fashion.

In multi-tenant hosted cloud environment where VPN is used for remote access, ensure physical isolation of VPN server. There should not be other tenants sharing the same VPN server.

#### **K.3.4.4 Remote Access**

Remote access, in this context, refers to the ability for authorized users to access and manage cloud resources from a remote location. This access typically happens over the internet using various protocols and technologies. The following methods should be considered for remote access using a risk-based approach (see [7.7](#)):

##### **Web-based Access Consoles:**

- Apply secure authentication and authorization where web interface consoles are accessible through a web browser.
- Conduct regular vulnerability assessments to ensure appropriate security measures are implemented.

##### **Secure remote desktop protocol (RDP) (if applicable):**

- Use RDP only when more secure methods to connect remotely are not feasible. If using RDP for remote access, disable unused ports and enforce strong passwords for RDP connections.
- Consider implementing Network Level Authentication (NLA) for additional security.
- Conduct regular vulnerability assessments to ensure appropriate security measures are implemented.

##### **Secure Remote Access Methods:**

- If utilizing a VPN, choose strong cryptographic secured protocols (e.g. authentication, encryption, etc.) using the recommended and state of the art cryptographic primitives, algorithms, parameters (e.g. size of cryptographic keys)" and regularly update VPN software to address vulnerabilities.
- Consider Zero Trust Network Access (ZTNA) for access control with greater resolution and specificity. ZTNA grants access only to authorized users and devices based on real-time security checks, eliminating the need for traditional VPNs.

##### **Secure Remote Access Endpoints:**

- Implement endpoint security solutions (antivirus, anti-malware) on all devices used for remote access to protect them from malware, phishing attacks, and other threats.
- Regularly patch operating systems and applications on remote access devices to address security vulnerabilities.
- Implement mobile device management for devices used to remotely access cloud services.

See [IEC 62443-3-3:2013/COR1:2014 \[59\]](#), SR 3.2 - Malicious Code Protection and SR 4.1 - Information Confidentiality for additional guidance.

#### **K.3.4.5 Privileged Access Workstations**

Consider requiring administrators to connect to cloud resources using privileged access workstations (PAWs), which should be hardened according to established good practices, require MFA, and perform thorough logging. Hardening refers to the specific set of security configurations that significantly reduce the attack surface and minimize the potential for compromise. PAWs are easier for organizations to control, properly harden, and monitor. PAWs can enforce MFA for all administrator actions, even when the protocol does not support it, and simplify auditing of administrator actions.

### K.3.5 Decommissioning

Decommissioning OT systems that involve cloud components presents unique challenges due to the critical nature of OT environments and the complexities of cloud infrastructure.

- Accurately identify and terminate all cloud resources associated with the OT system.
- Maintain audit logs of decommissioning activities for compliance and forensic purposes.
- Collaborate with the CSP to ensure proper decommissioning procedures are followed.
- Consider data residency requirements and data transfer limitations during decommissioning.

Please refer to [10.17](#) on decommissioning management for additional guidance.

### K.3.6 Business Continuity and Disaster Recovery

The dependencies in railway application and solution on cloud services can have an impact on business continuity and availability planning. The railway duty holder should consider methods to achieve availability commensurate with their risk tolerance.

Changes in cloud deployments such as software updates, reconfigurations, changes in cloud service providers, adding or removing resources, changes in availability zones, etc., should be tested prior to being placed into operation to ensure no negative impacts to the performance of the railway application and solution. See [5.10](#) for additional guidance on business continuity management.

## K.4 Cross-References

The [Table K.3](#) proposes adaptation of the IEC 62443 requirements to meet the needs of railway applications that leverage the cloud. See [Clause C.2, Table C.1](#) for additional security requirements.

**Table K.3 – IEC 63452 cross-mapping to standards frameworks**

IEC 63452 REQUIREMENT	TITLE	CROSS-REFERENCES
FR 1, SR 1.1	Multifactor authentication for untrusted networks	See <a href="#">IEC 62443-2-1:2024 [52]</a> : Using MFA for workstations that can be accessed by non- users of the railway application and solution makes it more difficult for these users to defeat a single-factor authentication mechanism, such as a password-only scheme.
FR 2, SR 2.8	Cloud security monitoring	See ISA-TR62443-3-1 Security for industrial automation and control systems Security Technologies for Industrial Automation and Control Systems <a href="#">[43]</a> : Security-logging management is a reporting software technology that establishes a set of procedures as a means of forensic evidence to establish audit and accountability within an organization's operational network. The software harnesses all process and security events from local computer network systems. The logging host is typically a central repository that extracts and stores critical events logs.
FR 6, SR 6.2	Continuous monitoring	See ISA-TR62443-3-1 Security for industrial automation and control systems Security Technologies for Industrial Automation and Control Systems <a href="#">[44]</a> : Vulnerability scanners are used to identify and discover vulnerable parts of a computer network system as a starting point to gain unauthorised access. It is often a tool used by defenders and attackers. For defenders, it is frequently used to assess the state of the cyberinfrastructure within an enterprise network.
FR 7, SR 7.6	Cloud security countermeasures	<a href="#">EN ISO/IEC 27017:2021 [41]</a> , Information technology - security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015)

		<p>Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)<a href="#">[36]</a></p> <p>EUCS – CLOUD SERVICES SCHEME EUCS<a href="#">[45]</a></p> <p>Federal Risk and Authorization Management Program (FedRAMP) <a href="#">[46]</a></p> <p>Information System Security Management and Assessment Program (ISMAP) <a href="#">[35]</a></p>
FR 5, SR 5.1 RE(1,2,3), SR 5.2	Zones & conduits	<p>Cloud service providers should provide a level of isolation between customer tenants. Implement macro segmentation where all resources should be logically separated into distinct segments based on their function, sensitivity, or ownership. Implement micro segmentation to achieve granular control over communication between resources within a segment. In addition, zones and conduits (see <a href="#">IEC TS 62443-1-1:2009 [47]</a> and <a href="#">IEC 62443-3-2:2020 [51]</a>) are used to represent logical partitions of the system and communications channels between them whose implementation can be supported by network segmentation and network devices. Separate devices connected via external networks. 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.</p>
FR 3, SR 3.1 RE(1)FR 4, SR 4.1 RE(1,2), SR 4.3	Data-in-transit	<p>Client connections to the cloud environment should be securely encrypted. Connections to cloud resources should always pass over a secure channel. See <a href="#">IEC TR 62443-3-1:2009 [48]</a>: Some communications between components in industrial control systems are encrypted. When properly implemented, encryption makes it computationally intractable for third parties to understand or spoof communications between encrypted endpoints, protecting control systems from "man in the middle" attacks.</p>
	Supply chain management	<p><a href="#">ISO/IEC 27036-4:2016 [15]</a></p>



## Bibliography

- [1] ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*
- [2] NIST SP 800-218: 2022 Version 1.1 Secure Software Development Framework
- [3] NIST SP 800-82 Rev.3 Guide to Operational Technology (OT) Security
- [4] NIST SP 800-160 Vol. 1 Rev. 1 Engineering Trustworthy Secure Systems
- [5] ISA-62443-1-1 (D11E1):2022, *Security for industrial automation and control systems - Terminology, concepts, and models*
- [6] IEC 62290-1:2014, *Railway applications - Urban guided transport management and command/control systems - Part 1: System principles and fundamental concepts*
- [7] IEC/TS 62443-1-1:2009, *Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*
- [8] X2R3-Deliverable D8.2-2:2020, *Generic cybersecurity architecture and shared security services - final.pdf* -- <https://projects.shift2rail.org/download.aspx?id=0a20cac9-e20f-4cdf-bc63-e0cb28950cfd>
- [9] ISO 9001:2015/Amd 1:2024 Quality management systems — Requirements
- [10] ISO 22163:2023, *Railway applications — Railway quality management system — ISO 9001:2015 and specific requirements for application in the railway sector*
- [11] IEC 62443-4-2:2019/COR1:2022, *Corrigendum 1 - Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*
- [12] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*
- [13] ISO/IEC 27036-2:2022, *Cybersecurity - Supplier relationships - Part 2: Requirements*
- [14] ISO/IEC 27036-3:2023, *Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security*
- [15] ISO/IEC 27036-4:2016, *Information technology - Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of cloud services*
- [16] ISO 31000:2018, *Risk management — Guidelines*
- [17] IEC FDIS 62278-1:2024, *Railway applications – specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: Generic RAMS process*
- [18] MITRE ATT&CK® framework - <https://attack.mitre.org/>
- [19] CAPEC VIEW: Industrial Control System (ICS) Patterns  
<https://capec.mitre.org/data/definitions/703.html>



- [20] [https://cyber.gouv.fr/sites/default/files/2022-08/ANSSI-CC-CPP-P-01-Certification-de-Profiles-de-Protection\\_v35B1D.pdf](https://cyber.gouv.fr/sites/default/files/2022-08/ANSSI-CC-CPP-P-01-Certification-de-Profiles-de-Protection_v35B1D.pdf)
- [21] IEC 62443-4-2:2019, *Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*
- [22] ISO/IEC 27036-3:2013, *Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security*
- [23] ISO/IEC 29147:2018, *Information technology - Security techniques - Vulnerability disclosure*
- [24] IEC TR 62443-2-3:2015, *Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment*
- [25] IEC 62402:2019, *Obsolescence management*
- [26] <https://www.ssi.gouv.fr/guide/profils-de-protection-pour-les-systemes-industriels/>.
- [27] IEC TS 62443-1-5:2023, *Security for industrial automation and control systems - Part 1-5: Scheme for IEC 62443 security profiles*
- [28] IEC 62425:2007, *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*
- [29] EN 1627:2021, *Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Requirements and classification*
- [30] EN 50129:2018, *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*
- [31] IEC 62278:2002, *Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*
- [32] ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*
- [33] ISA-TR62443-1-6 Security for industrial automation and control systems Application of the 62443 standards to the Industrial Internet of Things
- [34] EUCS – CLOUD SERVICES SCHEME EUCS, a candidate cybersecurity certification scheme for cloud services
- [35] Information System Security Management and Assessment Program (ISMAP)
- [36] Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
- [37] EUCS – CLOUD SERVICES SCHEME EUCS, a candidate cybersecurity certification scheme for cloud services
- [38] Federal Risk and Authorization Management Program (FedRAMP)
- [39] Federal Information Security Modernization Act (FISMA)

- [40] Use Secure Cloud Identity and Access Management Practices, National Security Agency and Cybersecurity & Infrastructure Security Agency
- [41] EN ISO/IEC 27017:2021, *Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015)*
- [42] ISA-TR62443-1-6:2024, *ISA-TR62443-1-6, Security for industrial automation and control systems, Application of the 62443 standards to the Industrial Internet of Things*
- [43] ISA-TR62443-3-1 Security for industrial automation and control systems Security Technologies for Industrial Automation and Control Systems
- [44] ISA-TR62443-3-1 Security for industrial automation and control systems Security Technologies for Industrial Automation and Control Systems
- [45] EUCS – CLOUD SERVICES SCHEME EUCS, a candidate cybersecurity certification scheme for cloud services
- [46] Federal Risk and Authorization Management Program (FedRAMP)
- [47] IEC TS 62443-1-1:2009, *Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*
- [48] IEC TR 62443-3-1:2009, *Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems*
- [49] IEC 62443-4-1:2018, *Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements*
- [50] IEC 62443-2-4:2023, *Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers*
- [51] IEC 62443-3-2:2020, *Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design*
- [52] IEC 62443-2-1:2024, *Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners*
- [53] ISO 22301:2019, *Security and resilience — Business continuity management systems — Requirements*
- [54] MITRE ATT&CK® Matrix for ICS - <https://attack.mitre.org/matrices/ics/>
- [55] IEC 62443-4-2:2019, *Technical security requirements for IACS components*
- [56] <https://networkinterview.com/in-band-and-out-of-band-network-management-detailed-comparison/>
- [57] [https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7853/Content/Chp\\_AbtCX/in-ban-out-of-ban-man.htm](https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7853/Content/Chp_AbtCX/in-ban-out-of-ban-man.htm)
- [58] IEC 62280:2014, *Railway applications - Communication, signalling and processing systems - Safety related communication in transmission systems*

- [59] IEC 62443-3-3:2013/COR1:2014, *Corrigendum 1 - Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*
-