

ICS 35.030; 45.020

English Version

Railway applications - Cybersecurity

Applications ferroviaires - Cybersécurité

Bahnanwendungen - IT-Sicherheit

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

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

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



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

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

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

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

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

Figures

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

Tables

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

European foreword

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

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

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

Introduction

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

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

The purpose of this document is that, when a railway system is compliant to this document, it can be demonstrated that this system is at the state of the art in terms of cybersecurity, that it fulfils its targeted Security Level and that its security is maintained during its operation and maintenance.

This document intends to:

- provide requirements and guidance on cybersecurity activities and deliverables
- be adaptable and applicable to various system lifecycles
- be applicable for both safety and non-safety related systems
- identify interfaces between cybersecurity and other disciplines contributing to railway system lifecycles
- be compatible and consistent with EN 50126-1 when it is applied to the system under consideration
- due to lifecycle differences between safety and cybersecurity, separate safety approval and cybersecurity acceptance as much as possible
- identify the key synchronization points related to cybersecurity between system integrator and asset owner
- provide harmonized and standardized way to express technical cybersecurity requirements
- provide cybersecurity design principles promoting simple and modular systems
- allow the usage of market products such as industrial COTS compliant with the 62443 series.

1 Scope

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

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

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

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

2 Normative references

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

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

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

EN IEC 62443-3-3:2019¹, *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*

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

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

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

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

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

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