



SLOVENSKI STANDARD
SIST-TS CLC/TS 50701:2024

01-januar-2024

Železniške naprave - Kibernetska varnost

Railway applications - Cybersecurity

Bahnanwendungen - IT-Sicherheit

Applications ferroviaires - Cybersécurité

Ta slovenski standard je istoveten z: CLC/TS 50701:2023

ICS:

35.030	Informacijska varnost	IT Security
45.020	Železniška tehnika na splošno	Railway engineering in general

SIST-TS CLC/TS 50701:2024

en

TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

CLC/TS 50701

August 2023

ICS 35.030; 45.020

Supersedes CLC/TS 50701:2021

English Version

Railway applications - Cybersecurity

Applications ferroviaires - Cybersécurité

Bahnanwendungen - Cybersecurity

This Technical Specification was approved by CENELEC on 2023-06-19.

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, Türkiye and the United Kingdom.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[SIST-TS CLC/TS 50701:2024](https://standards.iteh.ai/catalog/standards/sist/88dc59d0-2b1f-4c45-80ea-56c55d4ac37b/sist-ts-clc-ts-50701-2024)

<https://standards.iteh.ai/catalog/standards/sist/88dc59d0-2b1f-4c45-80ea-56c55d4ac37b/sist-ts-clc-ts-50701-2024>



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	27
4.1 Introduction	27
4.2 Railway asset model	28
4.3 Railway physical architecture model	29
4.4 High-level railway zone model	30
5 Cybersecurity within a railway application lifecycle	32
5.1 Introduction	32
5.2 Railway application and product lifecycles	32
5.3 Activities, synchronization, and deliverables	32
5.4 Cybersecurity context and cybersecurity management plan	36
5.5 Relationship between cybersecurity and essential functions	36
5.5.1 General.....	36
5.5.2 Defence in depth.....	36
5.5.3 Security-related application conditions.....	37
5.5.4 Interfaces between cybersecurity and design team.....	38
5.5.5 Interfaces between the safety and the cybersecurity processes.....	38
5.6 Cybersecurity assurance process	41
6 System definition and initial risk assessment	42
6.1 Introduction	42
6.2 Identification of the system under consideration	43
6.2.1 Definition of the SuC.....	43
6.2.2 Overall functional description.....	43
6.2.3 Access to the SuC.....	43
6.2.4 Essential functions.....	44
6.2.5 Assets supporting the essential functions.....	44
6.2.6 Threat landscape.....	44
6.3 Initial risk assessment	45
6.3.1 Impact assessment.....	45
6.3.2 Likelihood assessment.....	46
6.3.3 Risk evaluation.....	47
6.4 Partitioning of the SuC	47
6.4.1 Criteria for zones and conduits breakdown.....	47

6.4.2	Process for zones and conduits breakdown.....	48
6.5	Output and documentation	49
6.5.1	Description of the system under consideration.....	49
6.5.2	Documentation of the initial risk assessment	49
6.5.3	Definition of zones and conduits.....	49
7	Detailed risk assessment.....	49
7.1	General aspects	49
7.2	Establishment of cybersecurity requirements	51
7.2.1	General	51
7.2.2	Threat identification and vulnerability identification	52
7.2.3	Vulnerability identification	54
7.2.4	Risk acceptance principles	55
7.2.5	Derivation of SL-T by explicit risk evaluation.....	56
7.2.6	Determine initial SL.....	58
7.2.7	Determine countermeasures from EN IEC 62443-3.....	59
7.2.8	Risk estimation and evaluation	60
7.2.9	Determine security level target	61
7.2.10	Cybersecurity requirements specification for zones and conduits	62
8	Cybersecurity requirements.....	63
8.1	Objectives	63
8.2	System security requirements	63
8.3	Apportionment of cybersecurity requirements	79
8.3.1	Objectives	79
8.3.2	Break down of system requirements to subsystem level	80
8.3.3	System requirement allocation at component level	80
8.3.4	Specific consideration for implementation of cybersecurity requirement on components.	81
8.3.5	Requirement breakdown structure as verification	81
8.3.6	Compensating countermeasures.....	81
9	Cybersecurity assurance and system acceptance for operation.....	83
9.1	Overview	83
9.2	Cybersecurity case	84
9.3	Cybersecurity verification	85
9.3.1	General	85
9.3.2	Cybersecurity integration and verification.....	85
9.3.3	Assessment of results.....	87
9.4	Cybersecurity validation	87
9.5	Cybersecurity system acceptance	88
9.5.1	Independence	88
9.5.2	Objectives	88
9.5.3	Activities	88
9.5.4	Cybersecurity handover.....	88
10	Operational, maintenance and disposal requirements	89
10.1	Introduction	89

CLC/TS 50701:2023 (E)

10.2	Vulnerability management	89
10.3	Security patch management	90
10.3.1	General	90
10.3.2	Patching systems while ensuring operational requirements.....	91
Annex A (informative)	Handling conduits.....	94
Annex B (informative)	Handling legacy systems	97
Annex C (informative)	Cybersecurity design principles	103
Annex D (informative)	Safety and security	132
Annex E (informative)	Risk acceptance methods	136
Annex F (informative)	Railway architecture and zoning	144
Annex G (informative)	Cybersecurity deliverables content.....	161
Bibliography		164

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).....	31
Figure 5	— Defence in depth with example of measures.....	37
Figure 6	— Synchronisation between cybersecurity team and other stakeholders	40
Figure 7	— Relationship Threat Risk Assessment and Security Assurance.....	41
Figure 8	— Initial risk assessment flowchart	42
Figure 9	— Detailed risk assessment flowchart	52
Figure 10	— Explicit risk evaluation flowchart.....	58
Figure 11	— Handling of SL-C	82
Figure 12	— Cybersecurity assurance	83
Figure 13	— Cybersecurity case concept.....	84
Figure 14	— Cybersecurity assurance during integration and validation activities	86
Figure 15	— General vulnerability handling flowchart.....	90
Figure 16	— Vulnerability and outage time during system update (maintenance phase) [example]	92
Figure 17	— Vulnerability and outage time during system update with observation phases [example]	93
Figure A.1	— Zones and conduits example	95
Figure D.1	— Security as an environmental condition for safety	133
Figure F.1	— Adopted generic high-level railway zone model (example).....	151
Figure F.2	— Example of a railway system zone model	152

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 ...	37
Table 3	— Qualitative Impact Assessment example.....	45
Table 4	— Likelihood assessment matrix – Example.....	46
Table 5	— Risk matrix example.....	47
Table 6	— System Security Requirements and Foundational Classes.....	65
Table E.1	— Risk acceptance categories according to EN 50126-1	136
Table E.2	— Mapping severity categories according to EN 50126-1 to cybersecurity severity.....	137
Table E.3	— Likelihood assessment criteria	137
Table E.4	— Mapping Likelihood to accessibility and Probability	138

Table E.5 — Impact assessment matrix – Example 2	139
Table E.6 — Likelihood assessment matrix – Example 2	140
Table E.7 — Risk acceptance matrix – Example 2	140
Table E.8 — Impact assessment matrix – Example 3	141
Table E.9 — Likelihood assessment matrix – Example 3	142
Table E.10 — Likelihood conversion table – Example 3	142
Table E.11 — Risk acceptance matrix – Example 3	142
Table E.12 — Risk severity / Mitigation matrix – Example 3	143
Table F.1 — Railway system glossary	144
Table F.2 — Example – Evaluating groups of criticalities for landside-landside communication	148
Table F.3 — Example – Zone criticality definition for landside-landside communication	148
Table F.4 — Example – Landside-landside communication matrix basic structure	149
Table F.5 — Example – Communication matrix - landside to landside	150
Table F.6 — Example – Rolling stock zone model	153
Table F.7 — Example – Communication matrix - rolling stock to rolling stock	154
Table F.8 — Example – Communication matrix - landside to rolling stock	157
Table F.9 — Example – Communication matrix - rolling stock to landside	158

iTeh Standards
 (<https://standards.iteh.ai>)
 Document Preview

[SIST-TS CLC/TS 50701:2024](https://standards.iteh.ai/catalog/standards/sist/88dc59d0-2b1f-4c45-80ea-56c55d4ac37b/sist-ts-clc-ts-50701-2024)

<https://standards.iteh.ai/catalog/standards/sist/88dc59d0-2b1f-4c45-80ea-56c55d4ac37b/sist-ts-clc-ts-50701-2024>

CLC/TS 50701:2023 (E)**European foreword**

This document (CLC/TS 50701:2023) has been prepared by CLC/TC 9X “Electrical and electronic applications for railways”.

This document supersedes CLC/TS 50701:2021.

CLC/TS 50701:2023 includes the following significant technical changes with respect to CLC/TS 50701:2021:

- 3.1: Addition or update of the definition of the following terms: air-gapped network, attack vector, availability, code of practice, cybersecurity case, data diode, host, host device, intrusion, privilege, railway operator, security device, security event, security objective, SCADA system, validation, virtual routing and forwarding,
- 4.4: Update of legend of Figure 4.
- 5.3: Update of Table 1 content.
- 5.5.4: Recommendation added: to perform common design reviews between cybersecurity team and design team.
- 5.5.5: Addition of Figure 6.
- 6.2.6: MITRE ATT&ACK for ICS added as example of threat library.
- 7.2.3.1: Note added: vulnerabilities are not always within hardware or software, they can also come from configuration, organization and processes.
- 7.2.4.2: Requirement added: demonstration of applicability of code of practice shall be provided.
- 7.2.4.3: Requirement added: demonstration of applicability of reference system shall be provided.
- 8.2: “SR 1.4” railway note updated.
- B.4.6: Recommendation added: passive network monitoring is recommended as active network monitoring may disrupt the availability of OT network.

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 to provide a specification that can be used to demonstrate that the system under consideration is appropriately cyber secured, has set appropriate Target Security Levels and achieved them, and that the cyber security is maintained during its operation and maintenance by demonstrating conformance to this TS.

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 IEC/EN IEC 62443 series.

CLC/TS 50701:2023 (E)

1 Scope

This document provides 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 cyber attacks.

The security models, the concepts and the risk assessment process described in this document are based on or derived from the IEC/EN IEC 62443 series. 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, *Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process*

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

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

IEC 62443-2-1, *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 terminology databases for use in standardization at the following addresses:

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

NOTE The correspondence of the terms IACS, Solution and System used in the IEC/EN IEC 62443 series with the terms in this document might need further clarification in future issues of this document. Particularly, when using EN IEC 62443 definitions and requirements, the term "IACS" is understood and replaced by "railway application" or "railway system" as relevant in the context.

3.1.1**acceptance**

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

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

3.1.2**access**

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

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

3.1.3**access control**

protection of system resources against unauthorized access

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

3.1.4**access control process**

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

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

[SOURCE: EN IEC 62443-4-1:2018, 3.1.3 modified, "process" added]

3.1.5**accident**

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

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

3.1.6**achieved security level**

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

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

3.1.7**air gapped network**

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

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

CLC/TS 50701:2023 (E)**3.1.8****application**

software program executing on the infrastructure that is used to interface with the process of the control system itself

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

Note 2 to entry: This definition does not apply to the term "Railway Application".

3.1.9**approval**

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

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

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

3.1.10**asset**

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

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

3.1.11**asset owner**

individual or organization responsible for one or more IACS

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

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

3.1.12**attack**

attempt to gain access to an information processing system in order to produce damage <https://standards.itih.ai> [7b/sist-ts-clc-ts-50701-2024](https://standards.itih.ai)

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

[SOURCE: IEC 60050-171:2019, 171-08-12, modified, "disruption" added to Note 1 to entry]

3.1.13**attack surface**

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

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

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

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

3.1.14**attack vector**

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

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

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

3.1.15**audit**

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

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

3.1.16**authentication**

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

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

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

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

3.1.17**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]

3.1.18**availability**

<of an item> ability to be in a state to perform as required

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

3.1.19**boundary**

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

3.1.20**boundary device**

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

CLC/TS 50701:2023 (E)**3.1.21****code of practice**

<in cybersecurity> written set of rules, validated by a group of experts, that, when correctly applied, can be used to control one or more specific threats

[SOURCE: CSM Regulation N° 402/2013, modified, “validated by a group of experts” added, and “hazards” replaced by “threats”]

3.1.22**communication channel**

<in cybersecurity> specific logical or physical communication link between assets

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

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

3.1.23**communication path**

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

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

3.1.24**compensating countermeasure**

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

EXAMPLE

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

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

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

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

3.1.25**compromise**

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

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