SLOVENSKI STANDARD
SIST-TS CLC/TS 50701:2021

01-september-2021

Železniške naprave - Kibernetska varnost

Railway applications - Cybersecurity

Bahnanwendungen - Cybersecurity

Applications ferroviaires - Cybersécurité

Ta slovenski standard je istoveten z: CLC/TS 50701:2021

ICS:

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

SIST-TS CLC/TS 50701:2021 en

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CLC/TS 50701

July 2021

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.

CENELEC

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

Figures

Tables

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 62443-3-3:2019[1], *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*

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

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

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

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

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

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

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

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

3.1.1
acceptance
<for a product, system or process>
status achieved by a product, system or process once it has been agreed that it is suitable for its intended purpose

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

3.1.2
access
<in cybersecurity>
ability and means to communicate with or otherwise interact with a system in order to use system resources

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

3.1.3
access control
<control>
protection of system resources against unauthorized access

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

3.1.4
access control
<process>
process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy

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

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

3.1.5
accident
unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage

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

3.1.6
achieved security level
measure of the security level achieved in the deployed security architecture, elsewhere, sometimes referred to as the “as-built” security level

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

3.1.7
application
software programs executing on the infrastructure that are used to interface with the process of the control system itself

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

Note 2 to entry: This definition doesn't apply to the term “Railway Application”

3.1.8
approval
permission for a product or process to be marketed or used for stated purposes or under stated conditions

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

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

3.1.9
asset
physical or logical object owned by or under the custodial duties of an organization and having either a perceived or actual value to the organization

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

3.1.10
asset owner
individual or organization responsible for one or more IACS

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

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

3.1.11
attack
attempt to gain access to an information processing system in order to produce damage

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

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

3.1.12
attack surface
physical and functional interfaces of a system that can be accessed and, therefore, potentially exploited

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

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

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

3.1.13
attack vector
method or means by which an attacker can gain access to the system under consideration in order to deliver a payload or malicious outcome

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

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

3.1.14
audit
systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled

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

3.1.15
authentication
provision of assurance that a claimed characteristic of an identity is correct

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

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

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

3.1.16
authorization
<in cybersecurity>
right or a permission that is granted to a system entity to access a system resource

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

3.1.17
boundary
software, hardware, or other physical barrier that limits access to a system or part of a system

3.1.18
boundary device
communication security asset, within a zone or conduit, that provides a protected interface between a zone and a conduit

3.1.19
communication channel
<in cybersecurity>
specific logical or physical communication link between assets

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

[SOURCE: EN IEC 62443-3-3:2019[1], 3.1.9]

3.1.20
communication path
logical connection between a source and one or more destinations, which could be devices, physical processes, data items, commands, or programmatic interfaces

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

3.1.21
compensating countermeasure
countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements

EXAMPLE

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

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

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

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

3.1.22
compromise
violation of the security of a system such that an unauthorized disclosure or modification on sensitive information may have occurred, or unauthorized behaviour of the controlled physical process may have occurred

3.1.23
conduit
<in cybersecurity>
logical grouping of communication channels, between connecting two or more zones, that share common security requirements

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

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

3.1.24
confidentiality
<in cybersecurity>
assurance that information is not disclosed to unauthorized individuals, processes, or devices

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

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

3.1.25
connection
<in cybersecurity>
association established between two or more endpoints which supports the establishment of a session

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

3.1.26
control network
time-critical network that is typically connected to equipment that controls physical processes

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

3.1.27
control system
<in industrial automation and control system>
hardware and software components of an IACS

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

[SOURCE: EN IEC 62443-3-3:2019[1], 3.1.16, modified – Note 1 to entry has been added]

3.1.28
countermeasure
action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken

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

[SOURCE: EN IEC 62443-3-3:2019[1], 3.1.17]

3.1.29
cybersecurity
<in railway application>
set of activities and measures taken with the objective to prevent, detect, react to unauthorized access or cyberattack which could lead to an accident, an unsafe situation, or railway application performance degradation

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

3.1.30
data diode
boundary device which ensures that data between two separate networks is only transmitted in one direction

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