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.

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

Ref. No. CLC/TS 50701:2023 E

Contents

Page

Figures

Tables

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 it 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.

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.