



SLOVENSKI STANDARD

oSIST prEN IEC 63452:2025

01-september-2025

Železniške naprave - Kibernetika varnost

Railway applications - Cybersecurity

Ta slovenski standard je istoveten z: prEN IEC 63452:2025

ICS:

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

oSIST prEN IEC 63452:2025

en



9/3232A/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

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	
<input checked="" type="checkbox"/> 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.	<input type="checkbox"/> NOT SUBMITTED FOR CENELEC PARALLEL VOTING

oSIST prEN IEC 63452:2025

<https://standards.iteh.ai/> This document is still under study and subject to change. It should not be used for reference purposes. /osist-pren-iec-63452-2025

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 st of August, as reflected on this coverpage.
--

Copyright © 2025 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

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.

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

[oSIST prEN IEC 63452:2025](https://standards.iteh.ai/catalog/standards/sist/8b5bcae0-c1eb-4d59-ba95-aeb6dd577d30/osist-pren-iec-63452-2025)

<https://standards.iteh.ai/catalog/standards/sist/8b5bcae0-c1eb-4d59-ba95-aeb6dd577d30/osist-pren-iec-63452-2025>

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

IEC CDV 63452 ED1 © IEC 2025

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

IEC CDV 63452 ED1 © IEC 2025

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