IEC 63452 - Toward the first IEC International Standard on Railway Cybersecurity – Progress status

Serge BENOLIEL, PT 63452 Leader

5th ERA / ENISA Conference
2nd December, Tallin, Estonia

IEC 63452

Vertical Railway Cybersecurity standard

Adaptation of IEC 62443 industrial cybersecurity standards to railway sector

Scope: Railway networks (highspeed lines, mainlines, fret lines), metropolitan transport networks (including metros, tramways, trolleybuses and fully automated transport systems) and magnetic levitated transport systems

Cover the entire life cycle, from development to operation, maintenance and decommissioning

Align expectation between railway stakeholders (Asset Owners, System Integrators, Maintenance Service providers, Product suppliers)

Bridge cybersecurity and railway expertise

Note:

Products (equipment/devices) are out of scope, as 62443 4-1/4-2 or equivalent standard apply. CENELEC provided TS 50701 as input

- Taking as input the TS 50701 from CENELEC

IEC TC9 / Project Team 63452

A still growing number of registered NC members, experts from railway and/or cybersecurity field

- **2022-07 65**
- **2022-10 74**
- **2023-05 93**
- **2023-10 109**
- **2024-01 118**
- **2024-05 128**
- **2024-11 141**
- **2025-05 145**
- **2025-11 150**

4 Continents, 23 Countries, liaison with UITP, ERA, UIC, ERJU, UNIFE, exchanges with ENISA

Strong representativity of the railway sector

Organisation

- Alternance of hybrid workshops & Sub-group working sessions conf. call (15 SG)
- Between 50 to 60 people participating to each hybrid workshop (in person or remotely)

NC	Count
AT	4
BE	3
CA	3
CH	6
CN	8
CZ	1
DE	13
DK	1
ES	6
ET	2
FI	4
FR	17
GB	17
IL	4
IT	24
JP	16
LU	1
NG	1
NO	1
PT	2
RO	2
SE	1
UIC	1
UITP	1
US	11

IEC 63452 Timeline

- ✓ **2022-07** Project Kick-Off
- ✓ **2023-08** Committee Draft (CD)
- ✓ **2025-03** Committee Draft for Vote (CDV) proposed to IEC by PT 63452
- ✓ **2025-08** Start of IEC NC Enquiry
- ✓ **2025-10** Closure of NC vote & comments

  ➔ **CDV approved with comments by NC**

Forecast

- **~2026-03** Final Draft International Standard (FDIS)
- **~2026-08** International Standard (IS)

IEC 63452 key points (1/2)

CDV finalized & approved

- ✓ 70 formal, carefully crafted requirements
- ✓ 265 pages total - Core: 80 pages (from clause 3.3 to clause 10), 144 pages of annexes with extensive guidance

Key concepts adapted from multiple sources

- IEC 62443 series: Risk assessment, Security Level, cybersecurity requirements
- IEC 62278: life-cycle, threat log, cybersecurity case, SecRACs
- CSM-RA: Risk acceptance principles

Support to users

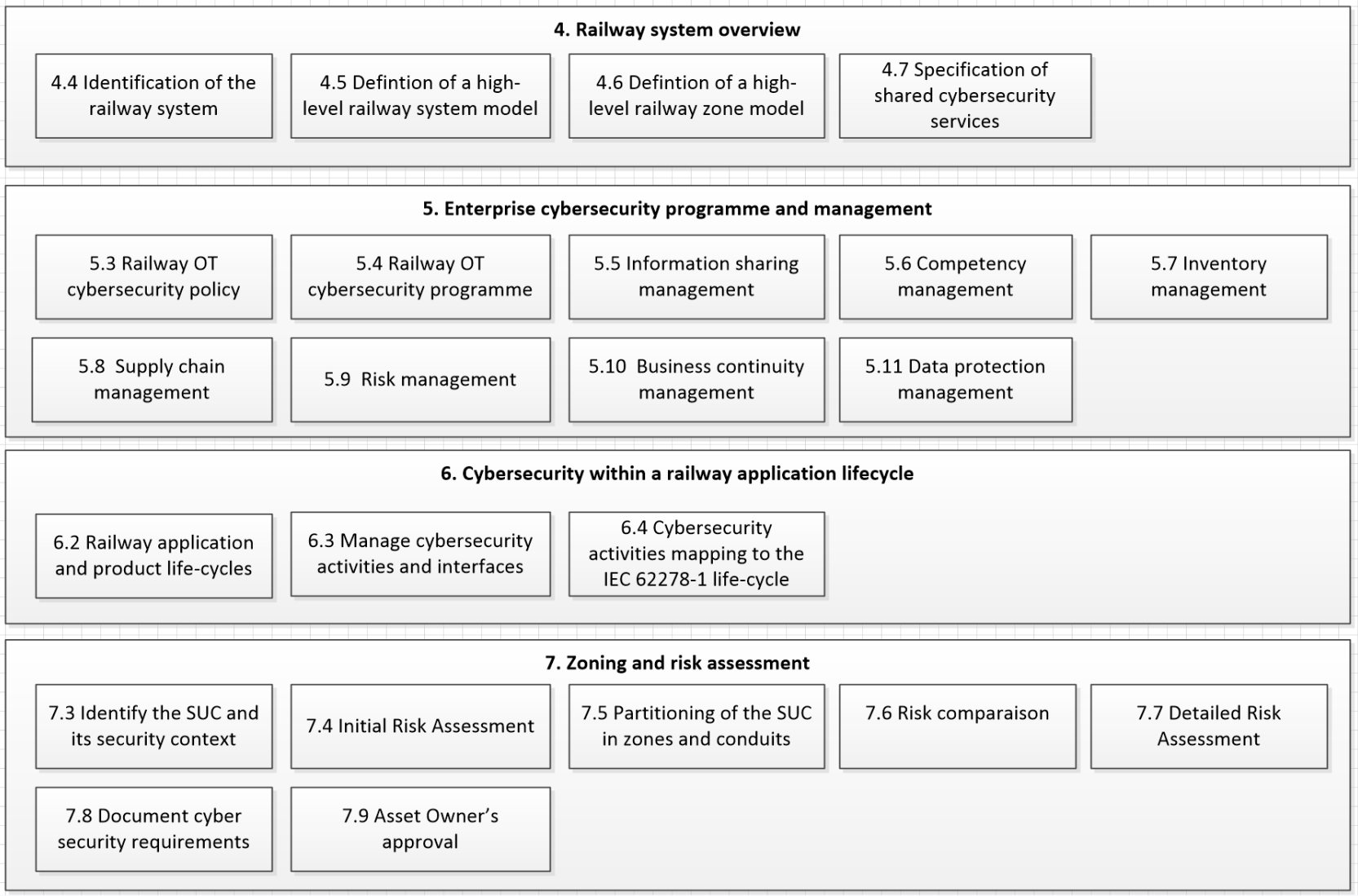
- Requirements with rationale and guidance, Key cybersecurity deliverables content, Cybersecurity competences profiles

IEC 63452 key points (2/2)

Key topics for railway sector:

- Example of railway system modelling & zoning
- Cybersecurity activities mapping with IEC 62278-1 RAMS lifecycle
- Flexibility on allocation of some requirements to handle different contexts (e.g. who shall perform Risk Assessment)
- Railway guidance for 62443-3-3 security requirements
- Operational, maintenance and disposal requirements
- Cybersecurity & safety interface
- Handling legacy system
- Cloud for OT cybersecurity

IEC 63453 CDV – Overall structure (1/2)



IEC 63452 CDV – Overall structure (2/2)

8. Cybersecurity architecture, apportionment of security requirements and integration

- 8.3 SUC cybersecurity functional architecture
- 8.4 Cybersecurity integration
- 8.5 Cybersecurity configuration

9. Cybersecurity assurance for railway solution

- 9.3 Cybersecurity verification and validation
- 9.4 Railway solution acceptance

10. Operational, maintenance and disposal requirements

- 10.3 Cybersecurity maintenance plan
- 10.4 Cybersecurity rules and procedures
- 10.5 Continuous cybersecurity verification
- 10.6 Railway application cybersecurity case
- 10.7 Risk assessment update
- 10.8 Vulnerability advisories
- 10.9 Cybersecurity testing and report
- 10.10 Vulnerability management
- 10.11 Patch management process
- 10.12 Patch management supply chain
- 10.13 End-of-life and end-of-security-support considerations
- 10.14 Incident management
- 10.15 Backup and recovery management
- 10.16 Security monitoring
- 10.17 Decommissioning management

Annexes (informative)

- A – Handling conduits
- B – Handling legacy systems
- C – Cybersecurity design principles and system requirements
- D – Safety and cybersecurity
- E – Risk acceptance methods
- F – Railway system models and zone models
- G – Cybersecurity deliverables content
- H – Cybersecurity competences profiles
- I – Cybersecurity for O&M activities - Operational guidance
- J – Vulnerability management - Operational guidance
- K – Cloud security

European specific topics

- **IEC 63452 is under parallel voting in Europe to become also an EN IEC standard**
- **EN IEC 63452 will replace current EN TS 50701**
- **Work in close relationship with CENELEC WG 26:**
  - **Common coverage analysis of NIS 2 and CRA regulation performed, gaps identified**
  - **Integration in IEC 63452 of gaps meaningful outside Europa**
  - **WG 26 will establish an IEC 63452 European Annex which will, for Railway Applications :**
    - **Explain how IEC 63452 requested activities and deliverable can be used to cover CRA and NIS 2 requirements**
    - **Provide complementary guidance for CRA or NIS 2 application on Railway**

Key benefits of IEC 63452 for Railway Cybersecurity

Global Common Language
First unified cybersecurity standard across EN & IEC, applicable to all railway domains and actors.

Efficient & Consistent Requirements
~70 consistent requirements enabling streamlined assessments and lifecycle coverage (incl. O&M)

Tailored Adaptation of IEC 62443
Integrates railway-specific practices (shared services, secure design, cloud for OT, etc.)

RAM & Safety Integration
Maps cybersecurity to EN 62278 lifecycle and clarifies safety-cybersecurity interactions

Clear Roles & Collaboration
Defines expectations for AO, SI, MSP with flexibility for application on diverse railway contexts.

Guidance & Support
Provides practical guidance on competences, supply chain risk, and system maintenance.

Q & A

Thank you!

BENOLIEL Serge
serge.benoliel@alstomgroup.com
PT 63452 Project Leader

PT 63452
ERA / ENISA conference – Tallinn, 2025 12 02