



IEC PT 63452 progress status


Serge BENOLIEL,

PT 63452 Leader

3rd ERA / ENISA Conference
2 October, Lille , France

IEC TC9 / PT 63452

Task

- **Establish an International Standard (IS) for handling Cyber Security for the railway sector**, covering all IEC/TC9 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
- Adaptation of the Industrial Cybersecurity security standards IEC 62443 to railway context
- Taking as input the TS 50701 from 

IEC TC9 / PT 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
- **2024-10 138**

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)

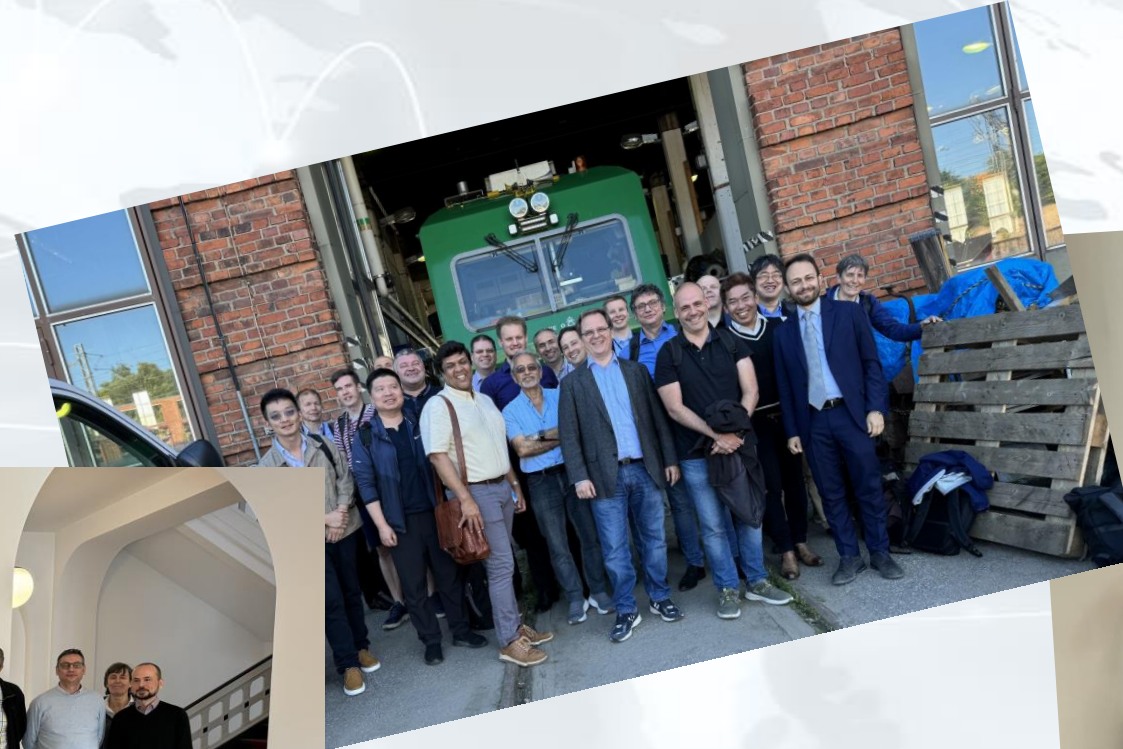
4 Continents, 20 Countries, Liaison with UITP & ERA, Liaison under discussion with ERJU & UNIFE, exchanges with ENISA → **Strong representativity of the railway sector**

Time line

- ✓ 2022-07 Project Kick-Off
- ✓ 2023-08 Committee Draft (**CD**)
- 2024-07 Committee Draft for Vote (**CDV**) → End Q4 2024
- 2025-02 Final Draft International Standard (**FDIS**) → Q3 2024
- 2025-07 International Standard (**IS**) → End Q4 2025

NC	Nb
AT	4
BE	4
CA	2
CH	4
CN	7
CZ	1
DE	12
DK	1
ES	5
ET	2
FI	4
FR	12
GB	17
IL	4
IT	22
JP	12
LU	1
NO	1
PT	2
RO	2
SE	1
UITP	1
US	15

Some hybrid workshops memories ...



Progress Status

IEC 63452 CD Ed1 issued and submitted to National committee comments

- ✓ Improvement and extension of the TS 50701
- ✓ 228 pages, half normative part and half informative annexes
- ✓ 66 formal requirements

NC comments received, CDV preparation

- ✓ Analysis and alignment on answers to received NC comments
- ✓ SG update of their clauses according agreed decision, 1st integration of new draft
- ✓ July/August 2024: consolidation of delivery of each SG and global consistency check
- ✓ September: review of all formal requirements, discussion on last structural points → 62 requirements

Forecast

- October: PT internal review on updated consolidated draft
- November last arbitration within PT
-  December – delivery of CDV

How can the future IEC 63452 support NIS 2 compliance?

Note:

- As this standard do not consider state level related obligations, we will focus on NIS 2 article 21 applicable to essential and important entities
- Reminder: NIS 2 need to be implemented in each country regulation.

63452 & NIS 2 directive article 21

Tentative mapping for Railway Duty Holder, for their railway OT systems



NIS article 21 – requirement impacting essential and important entities	Related clauses in IEC 63452
a) policies on risk analysis and information system security	<ul style="list-style-type: none">- 5.2 Railway OT Cybersecurity Policy- 5.3 Railway OT Cybersecurity Programme
b) incident handling	<ul style="list-style-type: none">- 10.4 Incident management- 10.15 Security monitoring
c) business continuity, such as backup management and disaster recovery, and crisis management;	<ul style="list-style-type: none">- 5. 9 Business continuity management
d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	<ul style="list-style-type: none">- 5.7 Supply chain management
e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	<ul style="list-style-type: none">- Clause 8 – Cybersecurity requirements- Clause 6 – Cybersecurity within railway application life cycle- Annex C – Cybersecurity design principles and system req.- 10.9 Vulnerability management; 10.10 Vulnerability advisories; 10.11 Patch management; 10.13 End of life and security update capabilities

63452 & NIS 2 directive article 21

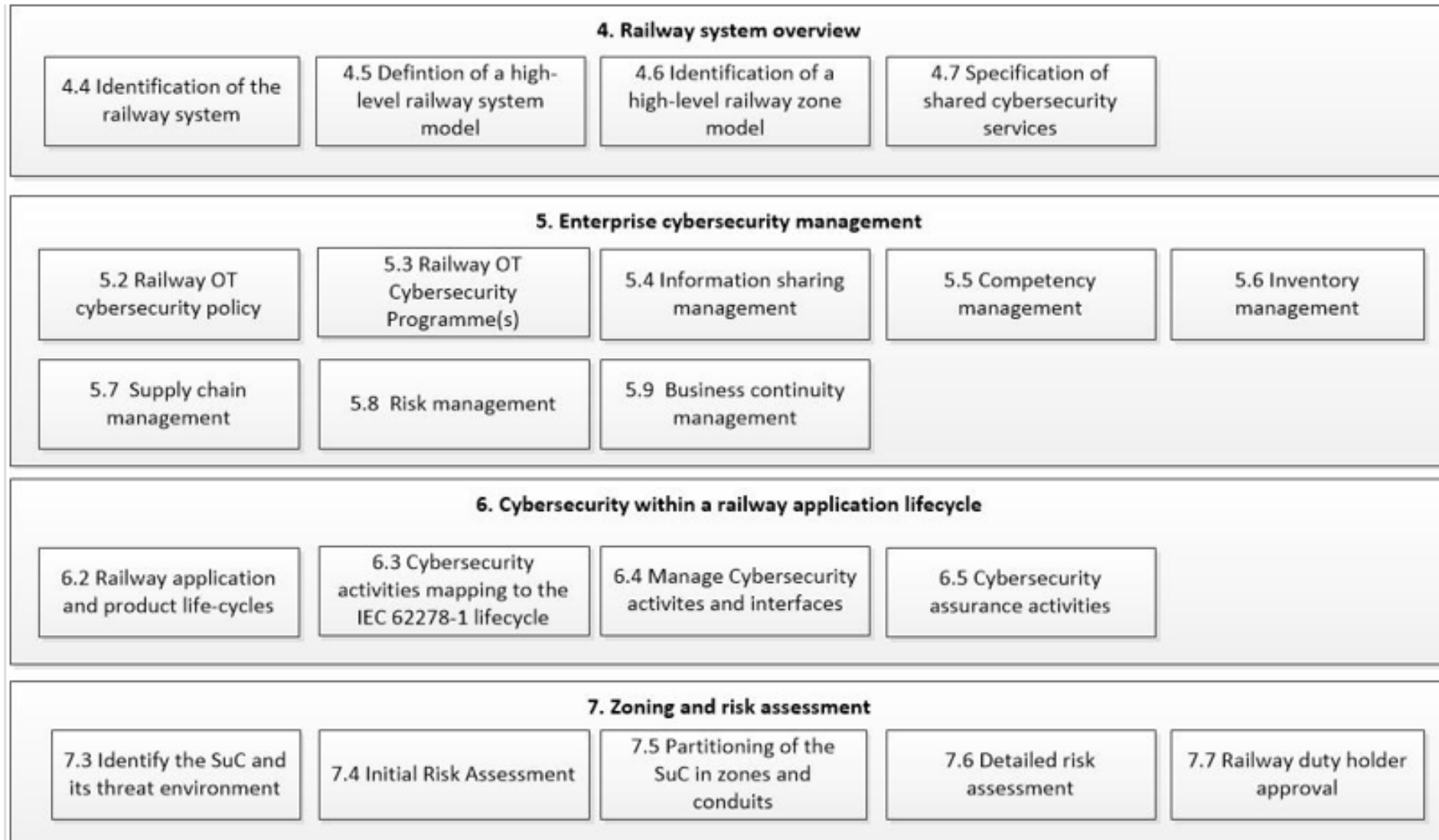
Tentative mapping for Railway Duty Holder, for their railway OT systems



NIS article 21 – requirement impacting essential and important entities	Related clauses in IEC 63452
f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	<ul style="list-style-type: none">- 5.8 Risk Management (entreprise level)- Clause 7 Zoning and risk assessment- 10-6 Continuous cybersecurity verification
g) basic cyber hygiene practices and cybersecurity training	<ul style="list-style-type: none">- 5-5 competencies management- 5-6 information sharing management- Annex H - cybersecurity roles and competencies profiles
h) policies and procedures regarding the use of cryptography and, where appropriate, encryption	<ul style="list-style-type: none">- Annex C – Cybersecurity design principles and system req. (guidance on application of 62443 3-3 in a railway context)
i) human resources security, access control policies and asset management	<ul style="list-style-type: none">- 5.6 Inventory management- 10-3 Consistent access management for O&M
j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate	<ul style="list-style-type: none">- Annex C – Cybersecurity design principles and system requirements (guidance on application of 62443 3-3 in a railway context)

**If you are a bit more curious of 63452
content ...**

IEC 63452 draft – current structure sneak peek



IEC 63452 draft – current structure sneak peek

8. Cybersecurity requirements

8.5 System cybersecurity requirements definition

8.6 Requirement breakdown structure for verification

8.7 Apportionment of cybersecurity requirements

8.8 Compensating countermeasure

8.9 Shared cybersecurity services system requirements

9. Cybersecurity assurance

9.3 Cybersecurity verification and validation

9.4 Railway solution acceptance

10. Operational, maintenance and disposal requirements

10.3 Consistent access strategy for O&M

10.4 Protection of critical data

10.5 Cybersecurity maintenance

10.6 Continuous cybersecurity verification

10.7 Cybersecurity case update

10.8 Risk assessment update

10.9 Vulnerability management

10.10 Vulnerability advisories

10.11 Patch management process

10.12 Patch management supply chain

10.13 End-of-life & security update capabilities

10.14 Incident management

10.15 Security monitoring

10.16 Decommissioning management

Annexes (informative)

A – Handling conduit

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 deliverable content

H – Cybersecurity roles and competences profiles

I – Cybersecurity for O&M activities - Operational guidance

J – Vulnerability management - Operational guidance

K – Cloud Security

Q & A



Thank you!

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

PT 63452
ERA / ENISA conference – Lille, 2024 10 02