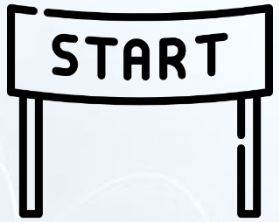
IEC PT 63452 - Towards the 1st International Standard dedicated to Railway Cybersecurity

Serge BENOLIEL, PT 63452 Leader
Railway Application, Cybersecurity

3rd ERA - ENISA Conference,
9th November 2023 – Athens, Greece

IEC TC9 / PT 63452



9/2835/RVN – IEC New work item proposal approved (05/2022)

- 23 Members voting, 100% approved
- Project assigned to Project Team **PT 63452**
- Title: Railway applications - Cybersecurity

Goal

- **Establish an International Standard (IS) for handling Cyber Security for the whole railway sector**
- Cover all TC9 scope: Signalling, Rolling Stock, Fixed Installation, Mainline, Urban, Freight, …
- Adaptation of the Industrial Cybersecurity security standards IEC 62443 to railway context

- Taking as input the TS 50701 from CENELEC

IEC TC9 / PT 63452

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

- 2022-07 65
- 2022-10 74
- 2023-05 93
- **2023-10 109**

From 4 Continents, 19 Countries
UITP & ERA Observers, ERJU & UNIFE liaison under discussion

NC	Count
AT	4
BE	3
CA	1
CH	4
CN	6
CZ	1
DE	11
DK	1
ES	5
ET	2
FI	4
FR	10
GB	13
IL	4
IT	19
JP	12
LU	1
SE	1
UITP	1
US	6

Time line

- 2022-07 Project Kick-Off
- 2023-08 Committee Draft (CD) (2023/08)
- 2024-07 Committee Draft for Vote (CDV)
- 2025-02 Final Draft International Standard (FDIS)
- 2025-07 International Standard (IS)

Organisation

- Alternance of hybrid workshops & conf. calls
- Structured in 10 Subgroups

CLC TS 50701 - reminder

- **Established by the CENELEC TC9X / WG 26,**
- **Work started in July 2017, TS published in July 2021**
- **TS offered to IEC as input to IEC to create a Railway Cybersecurity International Standard**
- **The TS 50701 is based on different sources :**
  - IEC 62443 (SL vector, risk assessment, cybersecurity requirements)
  - EN 50126 (life-cycle, threat log, cybersecurity case, SecRACs)
  - CSM-RA (risk acceptance principles)
- **Adapted to railway context**
  - Railway architecture model & zoning
  - Railway notes for Security Requirements
  - Cybersecurity Design principles
  - Cybersecurity & Safety interface
  - Handling Legacy System
  - Risk acceptance methods

- UNIFE report(1) promoting TS 50701 published end of 2021
- Report(2) by ENISA based on TS 50701 published end of 02/2022

(1) https://www.unife.org/wp-content/uploads/2021/09/UNIFE-Cybersecurity-position-paper.pdf

(2) https://www.enisa.europa.eu/news/building-cyber-secure-railway-infrastructure

PT 63452 – evolutions from the TS

- **Formal identification of normative clauses & recommendations, allowing to perform cybersecurity acceptance and/or certifications**
- **Interface of cybersecurity process with generic RAMS IEC life cycle 62278**
- Life cycle clause 6 usable as navigation tool
- Railway asset model improvement (dedicated zone for radio communications; clarify ATO position, etc.)
- Improved interface definition with other disciplines
- Risk assessment : improve part related to threat intelligence & threat landscape, optimization of IRA & DRA
- Update Cybersecurity requirement guideline & legacy system
- **Operational, maintenance and disposal requirements**
  - **Maintain Security (vuln & patch management, protection of sensitive data,**
  - **Operate / administrate security (access right, threat monitoring & detection, incident response, …)**
  - **Secure Decommissioning**
- **Additional description of typical expected content for cybersecurity deliverables**
  - e.g. Security context, Risk Assessment, Cybersecurity Requirement Specification, Cybersecurity Evaluation Plan, Cybersecurity guideline, Cybersecurity Maintenance Plan, …)
- Description of Cybersecurity related competences profiles

CD 63452 Ed 1

What we achieved

- Improvement and extension of the TS 50701
- 228 pages, half normative, half informative annexes
- 66 formal requirements (up to now)

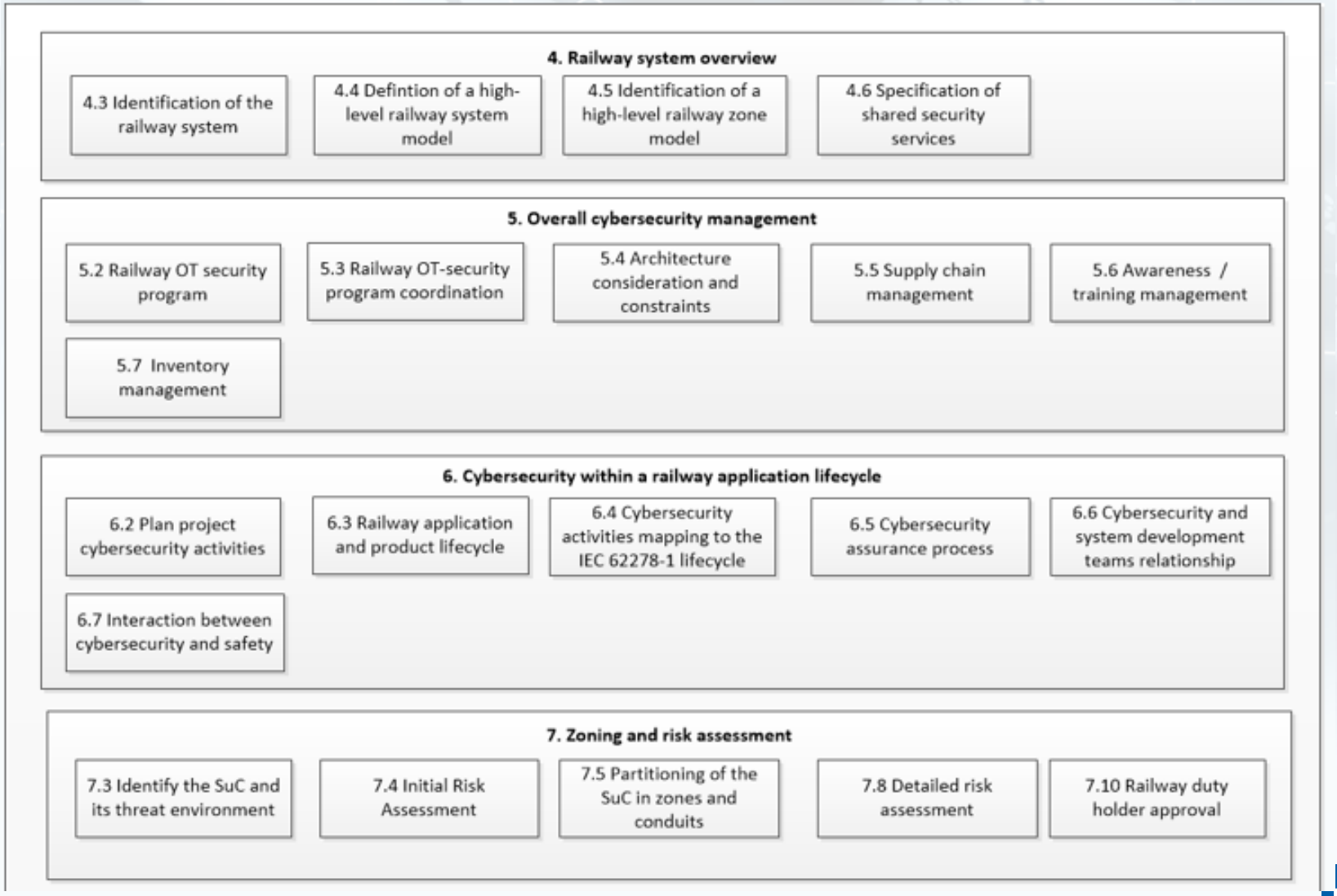
How we worked ?

- Sub-group focus on their respective parts
- Periodic workshops for subgroups progress sharing and alignment
- Once the first consolidated draft achieved
  - One dedicated workshop to address internal comments
  - Dedicated UK “polishing” task force to ensure English correctness
  - Working sessions for internal consistency check and finalization of clauses

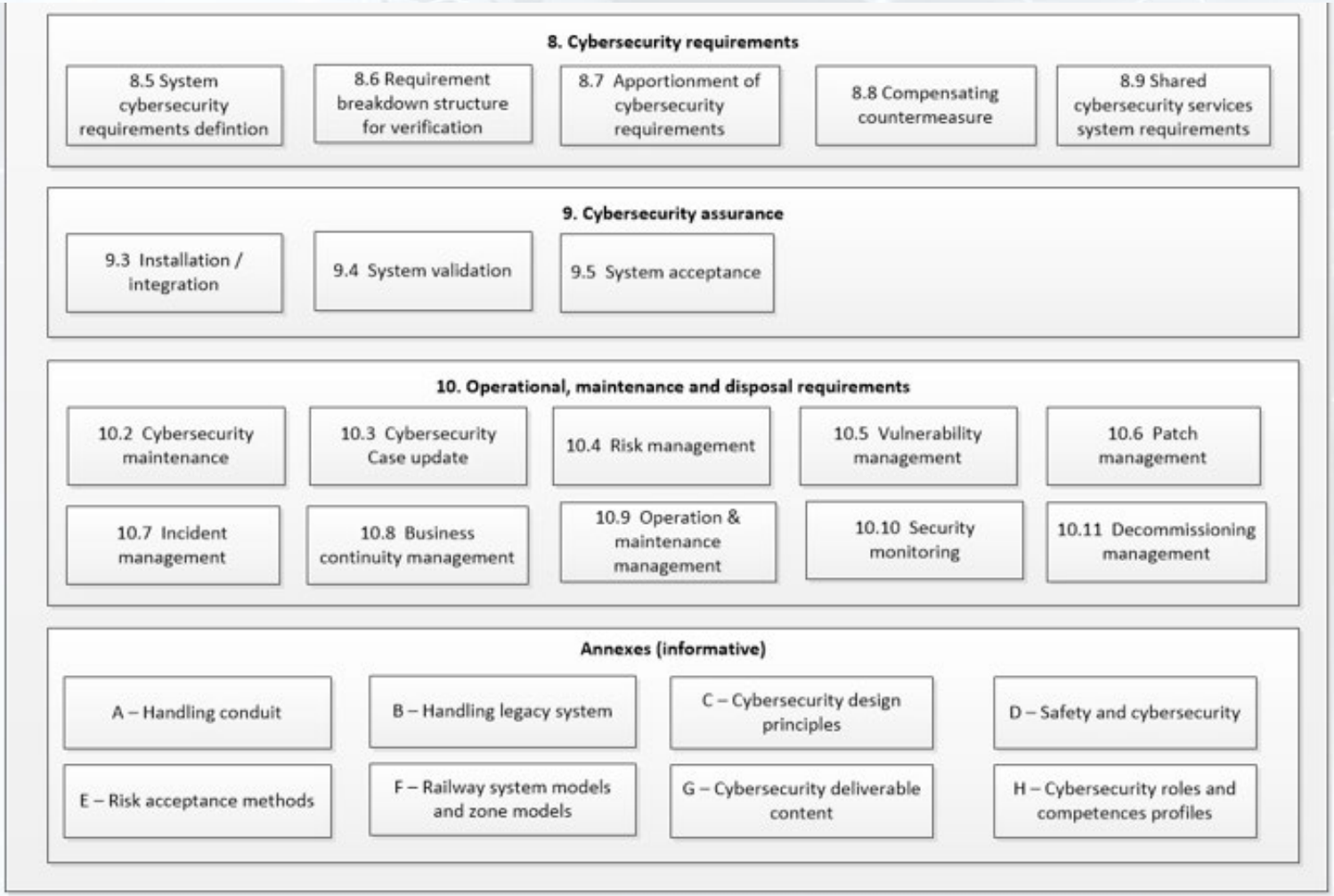
Next steps

- NC comments anticipated to be received mid-December
- Work is going-on: requirement internal review and open point decisions to anticipate answer to NC comments.
- Preparation and alignment of position on structural points.
- January – Start to NC comment analysis and answer

CD 63452 Ed 1 – Sneak peek



CD 63452 Ed 1 – Sneak peek



CD 63452 Ed 1 – Sneak peek – requirement

….

[CP-05-01] Awareness/training management

5.6.1 Requirement

The railway duty holder, integration service provider and maintenance service provider shall provide security training to internal and external personnel of their organisation who are participating in the lifecycle of the railway application.

The training programme shall include:
1) Cybersecurity awareness training on the basic security principles that personnel must apply in their daily work; and
2) Cybersecurity specialised training that is tailored to their responsibilities.

The contents of the security training shall be periodically reviewed and updated as necessary.

5.6.2 Rationale and supplemental guidance

Training and awareness are essential requirements in the railway duty holder's cybersecurity program because cybersecurity compromises are often at the end-user level, where personnel who are not aware of the security policies, processes and procedures are prone to fail to comply with them.

The cybersecurity awareness programme should be designed so that policies, processes and procedures related to the railway applications cybersecurity can be easily followed. There is also the need to reinforce the importance of compliance with both contractual and regulatory cybersecurity requirements.

Cybersecurity specialised training should equip the personnel with the skills needed to perform the tasks that are specific to their respective roles, and for training to be effective, it should be tailored to the specific railway system, application or solution and its operational environment.

…..

CD 63452 Ed 1 – requirement table

Clause	Req ID	Req Label	Requirement
4	SO-01-01	Identification of the railway system	The railway duty holder shall identify the scope of its railway system and railway application, identifying the OT (operational technology) systems and subsystems, segregating them from the IT (Information Technology) systems. The railway duty holder shall, where no clear assignment to IT or OT is apparent, decide if the subsystem is to be considered as IT or OT and inform the stakeholder in charge of IT cybersecurity.
4	SO-02-01	Definition of a high-level railway system model	The railway duty holder shall set out a high-level system model of the railway system
4	SO-03-01	Definition of a high-level railway zone model	The railway duty holder shall set out a high-level railway zone model of the railway system. The railway zone model is the grouping of assets in different zones and criticality.
4	SO-04-01	Specification of shared security services	The railway duty holder shall specify which shared security services shall be provided centrally by the railway system and which shared security services shall be provided as an inherent capability of the SuC itself.
			- - - - - - - -
6	LC-01-01	Establish and maintain a project cybersecurity management plan	A cybersecurity management plan shall be established and maintained, documenting all the cybersecurity activities and deliverable from 6.4. This requirement is applicable to all entities contributing to the SuC life cycle, on their respective scope as contractually agreed: railway duty holder, integration service provider and maintenance service provider.
6	LC-01-02	Life cycle conformity	a) All the listed activities in clause 6.4.shall be performed, delivering associated deliverables (outputs). b) Any deviation shall be recorded and justified in the project cybersecurity management plan. c) Deviations shall not be permitted if the deliverable or the activity is required in other clauses.

- - - - - - - -

- - - - - - - -

Thank you!

BENOLIEL Serge
PT 63452 Project Leader

November 9th 2023
Athens, Greece