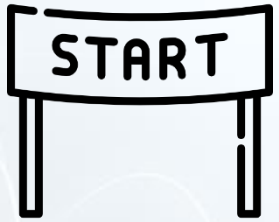
IEC PT 63452

Serge BENOLIEL, PT 63452 Leader
Railway Application, Cybersecurity

2nd ERA - ENISA Conference,
1st December 2022 – Lille, France

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
- Task: To develop the IS on cybersecurity for Railway

Goal

- **Establish an International Standard (IS) for handling Cyber Security for the whole railway sector**
- Cover Signalling, Rolling Stock, Fixed Installation
- Based on existing Industrial Cybersecurity security standards (i.e. IEC 62443 & **TS 50701**)

IEC TC9 / PT 63452

Project Team 63452

- 79 experts from 14 Countries and 3 Continents (Europe, Asia, America)
- Railway duty holders, system integrators, product providers, security solution providers, assessors

Time line

- 2022-07 Project Kick-Off
- 2023-07 Committee Draft (CD)
- 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 11 Subgroups

NC	Members
AT	4
CA	1
CH	3
CN	6
CZ	1
DE	11
ES	3
FI	4
FR	7
GB	9
IL	4
IT	17
JP	7
LU	1
Total	**78**

CLC TS 50701 - reminder

- **Established by the CENELEC TC9X / WG 26,**
- **Work started in July 2017, Technical Specification published in July 2021**
- **TS offered to IEC as input 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
  - Cyberseucrity 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 – targeted evolution

- **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 table usable as navigation tool
- Railway asset model improvement (dedicated zone for radio communications; clarify ATO position ..)
- Improve interface definition with other disciplines
- Risk assessment : improve part related to threat intelligence & threat landscape, optimization of IRA & DRA
- Cybersecurity requirement & legacy system
- **Operational, maintenance and disposal requirements**
  - **Maintain Security (vuln & patch management, protection of sensitive data,**
  - **Operate / administrate security (access right, thret 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, incident Management Plan, …)
- Description of Cybersecurity related roles

Quality criteria

- **Editorial quality**
  - Concept clearly defined, understandable by both rail and IT/OT security personnel
  - Text short and clear for normative part
- **Relevancy and applicability**
  - Applicable to greenfield and brownfield,
  - Technically and economically viable
  - Formal identification of requirements, compliance matrix,
  - Tailor, able and standardized, adaptable to Operator context
  - Complete
- **Guidance for implementation**
  - Non-normative part providing guidance on specific topic
  - Template for cybersecurity deliverables, define roles & needed competencies
- **To be consistent and compatible with ISA/IEC 62443 series**
- **To be maintainable through modular approach**

Take away

- **PT IEC 63452**
  - **Tasked to define an railway cybersecurity International Standard, based on TS 50701**
  - **Targeted content evolution defined**
  - **Subgroups activities organized and started**
  - **Committee Draft expected for July 2023**

- **Meanwhile …**
  - **Return on experience on TS 50701 usage welcome !**
  - **Additional participation welcome, especially from railway operators as one major evolution is related to the topic of cybersecurity during operation**

Thank you!

BENOLIEL Serge
serge.benoliel@alstomgroup.com

1st December 2022
Lille, FRANCE