CENELEC prTS 50701
(Railway applications – CyberSecurity)

ENISA-ERA Conference: Cybersecurity in Railways

16th of March 2021
Railway CyberSecurity challenges

Railway-specific challenges need to be addressed
- Attackers have fairly easy physical access
- The train is only one part of an diverse cross-border eco-system
- There are safety-critical and non safety-critical systems in the environment

Commercially viable methods for operators, manufacturers and vendors are needed

Synchronization points between stakeholders as well as safety and security required
WG 26

- Working Group on “Railway Applications – Cybersecurity”
- Covers Signaling, Rolling Stock, Fixed Installation
- ~90 experts (20-30 experts participating to F2F meetings)
- Experts from 13 countries (+ SBS, ERA and ENISA as observer)

Goal

- Establish a TS for handling CyberSecurity in an unified way for the whole railway sector
- Based on already existing Industrial CyberSecurity security standards (e.g. IEC 62443)

Timeline

- July 2017: Creation of TC9X – WG 26 to produce a Technical specification (TS 50701)
- June 2019: First enquiry on prTS 50701 draft
- Dec 2020: Final version submitted to NC vote
- In European Voting process since 8th of January 2021

Next steps

- End of Voting: 2nd of April 2021
- TS expected to be available in Summer 2021
prTS 50701 overview

The TS is an innovative standard that takes inspiration from different sources ...
- IEC 62443 (SL vector, Risk assessment, list of requirements)
- EN 50126 (life-cycle, threat log, cybersecurity case, SecRACs)
- CSM-RA (risk acceptance principles)

... adapted to railway context
- Railway architecture model & zoning example
- Railway notes for Security Requirements
- Cybersecurity Design principles
- Cybersecurity & Safety interface
- Handling Legacy System
- Risk acceptance methods

In 3 years the TS shall be re-examined and possibly transformed into an EN
- The success of this upgrade will depend on its capability to intercept the needs of the users
- One key element is the availability of a simple and easy-to-implement process
Business enterprise zone
(IT for planning, logistics, sales, engineering)

eg ISO 27001

ER TS 50701
Railway system

IEC 62443
IACS

Applicable cybersecurity law and regulation
EN 50126-1:2017 - Figure 7 — The V-cycle representation
prTS 50701 overview – Reference Arch.

Operational control and maintenance

- Train Operation
- Timetable
- Technical Management
- Maintenance
- NMC / SOC

Network (centralized in one or more control centers)

Train on a journey

- Public Services (WLAN, Video on Demand, ...)
- Train Control (PS, HVAC, ...)
- Auxiliary (EMS, DAS, Diagnostics, ...)
- Signaling/ATP (OBU, emergency brake, ...)
- Train Driver
- Goods
- Passengers
- Switch Post
- Electric Supply and Traction Mains

Network Devices
- Firewall, Gateway or Router
- Network
- Public Network

Network (for trackside and decentralized compartments)

Abbreviations
- ATP: Automatic Train Protection
- CCTV: Closed circuit television
- DAS: Driver Assistance System
- EMS: Energy Metering System
- HVAC: Heating, Ventilation and Air Conditioning
- JRU: Juridical Recording Unit
- MCG: Mobile Communication Gateway
- NMC: Network Management Center
- OBU: Onboard Unit
- PA: Public Adress
- PIS: Passenger Information System
- SOC: Security Operation Center
- TCMS: Train Control Management System
- WLAN: Wireless Local Area Network

Public Services
- WLAN, Video on Demand, Train Comfort (PIS, HVAC, ...) Control/Command (Traction, Breaking, Doors, ...)

Signaling/ATP
- OBU, emergency brake, ...

Colour legend
- Track
- Signal
- Station
- Public Services
- Auxiliary
- Comfort
- Public
- Auxiliary
- Colour

Christian Schlehuber, Convenor - Serge Benoliel, Secretary - TC 9X/WG 26
## prTS 50701 overview – Lifecycle

<table>
<thead>
<tr>
<th>Phase (EN 50126-1)</th>
<th>Synchronization points and deliverables</th>
<th>Cybersecurity activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Concept</td>
<td>SuC Identification:</td>
<td>• Review of the degree of security achieved up to now</td>
</tr>
<tr>
<td></td>
<td>→ Operational environment incl. existing security-related controls &amp; High-Level zone model (see ch. 4)</td>
<td>• Analysis of the project’s security implication and context (incl. generic threats) <em>(see ch. 5.3)</em></td>
</tr>
<tr>
<td></td>
<td>→ Applicable security standards</td>
<td>• Alignment with railway operator / asset Owner and stakeholder’s security goals</td>
</tr>
<tr>
<td></td>
<td>→ Purpose and scope</td>
<td>• Consideration of security lifecycle aspects (patch management, monitoring etc.) <em>(see ch. 10)</em></td>
</tr>
<tr>
<td></td>
<td>← Project cybersecurity management plan (incl. cybersecurity context, goals and lifecycle activities)</td>
<td></td>
</tr>
<tr>
<td>2 System definition and operational context</td>
<td>System definition:</td>
<td>• Review of the logical and physical network plans</td>
</tr>
<tr>
<td></td>
<td>→ System boundaries</td>
<td>• <em>Initial Risk Assessment for the SuC (see ch. 6.3)</em></td>
</tr>
<tr>
<td></td>
<td>→ Initial system architecture, incl. list of functions, interfaces and generic systems</td>
<td>• <em>Partitioning of the SuC into zones and conduits (see ch. 6.4)</em></td>
</tr>
<tr>
<td></td>
<td>→ Logical &amp; physical network plans</td>
<td>• <em>Documentation of components, interfaces and characteristics for each zone and conduit (see ch. 6.5)</em></td>
</tr>
<tr>
<td></td>
<td>← Logical &amp; physical network plans review</td>
<td>• - This activity and the corresponding synchronization point may also be conducted in phase 3.</td>
</tr>
</tbody>
</table>
**prTS 50701 overview – Lifecycle**

<table>
<thead>
<tr>
<th></th>
<th>Operational context and criticality:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>→ Essential functions</td>
</tr>
<tr>
<td></td>
<td>← Initial risk analysis results</td>
</tr>
<tr>
<td></td>
<td>← Zones &amp; Conduits</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>Risk analysis and evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>DRA:</strong></td>
</tr>
<tr>
<td></td>
<td>→ Functional Requirements (linked to essential functions)</td>
</tr>
<tr>
<td></td>
<td>← Initial Threat Log</td>
</tr>
<tr>
<td></td>
<td>← Potential Updates (Zones &amp; Conduits, network plans)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>Specification of system requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>CRS release:</strong></td>
</tr>
<tr>
<td></td>
<td>← System Cybersecurity Requirements Specification incl. security-related application conditions</td>
</tr>
</tbody>
</table>

- Detailed Risk Assessment (DRA) *(see ch. 7)*:
  - Derive technical (e.g. SL-T), physical and organizational countermeasures or assumptions for zones and conduits
  - Consider business continuity aspects (incl. incidence response and recovery) for the SuC

- SuC-specific refinement of normative requirements *(see ch. 8)*
- Definition of organizational and physical requirements
- Definition of security-related application conditions *(see ch. 7)*
The process needs to take into account also legacy solutions or standards, this may be handled by reference systems or codes of practice, that need to be integrated with the SL approach.

The process is carried out by zone/conduit and by threat.

Finally the requirements for a zone/conduit are consolidated.

This allows a non-disruptive move to 62443 but also preserves legacy solutions.

**CSM-RA, Risk Acceptance Principles**

*For each zone and conduit*

*For each threat and vulnerability*

**For each threat and vulnerability**

**Derive the SL-T vector**
How is a SL assigned?

- SL can be viewed as a qualitative means of risk reduction. It is assumed that each organization has a risk matrix with appropriate acceptance criteria.

- To obtain SL, the zone/conduit is evaluated taking into account all measures that a particular (candidate) SL vector implies.

- If the risk is acceptable then the SL-T is found. If not, add additional countermeasures (increase SL-T) and try again.
<table>
<thead>
<tr>
<th>Req</th>
<th>SL</th>
<th>Title</th>
<th>Railway notes (informative)</th>
<th>Relevant design principles</th>
<th>Stakeholder</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR 1.1 RE(1)</td>
<td>2</td>
<td>Unique identification and authentication</td>
<td>-</td>
<td>6 - Authenticate requests 13 - Precautionary principle</td>
<td>Sys Sup</td>
<td>Tech</td>
</tr>
<tr>
<td>SR 1.1 RE(2)</td>
<td>3</td>
<td>Multifactor authentication for untrusted networks</td>
<td>The feasible multifactor authentication solutions outside the IT system in railways are generally external and could comprise a badge or a physical recognition of presence for the human user e.g. by a phone call. This could equally apply to regularly planned maintenance activities.</td>
<td>6 - Authenticate requests 12 - Proportionality principle</td>
<td>Sys Sup</td>
<td>Tech</td>
</tr>
<tr>
<td>SR 1.1 RE(3)</td>
<td>4</td>
<td>Multifactor authentication for all networks</td>
<td>The feasible multifactor authentication solutions outside the IT system in railways are generally external and could comprise a badge or a physical recognition of presence for the human user e.g. by a phone call. This could equally apply to regularly planned maintenance activities.</td>
<td>6 - Authenticate requests 12 - Proportionality principle</td>
<td>Op Sys</td>
<td>Tech</td>
</tr>
<tr>
<td>SR 1.2</td>
<td>2</td>
<td>Identification and authentication of software processes and devices</td>
<td>Note that in the equivalent requirement IEC 62443-2-1/62443-2-4 USER-07 &quot;sw services are considered instead of &quot;sw processes&quot;; USER-07: All software services shall be identified and authenticated prior to their execution. Identification of internal software processes/services and devices are not a common practice in railway applications or railway systems. White list application management supports integrity of systems.</td>
<td>4 - Grant least privilege 6 - Authenticate requests 7 - Control access</td>
<td>Op Sup Sup</td>
<td>Tech Proc</td>
</tr>
</tbody>
</table>
Usually there exist (a few) high-level security requirements that are safety-related.

In the Cybersecurity Case these are either

- shown to be fulfilled, or
- fulfilled under assumptions that have to be exported as SecRAC, or
- partially fulfilled (compensating countermeasures have to be defined)

Safety Case references the Cybersecurity Report.

Cybersecurity Case can be updated without change of the safety case.
Content of CyberSecurity Case 1/2

Introduction (could be a set of references to other documents)
- System under Consideration definition (incl. Zones and Conduits)
- Threat and risks assessment
  - Assumptions
  - List of threat intelligences sources
  - List of threat Scenarios
  - List of sufficiently mitigated risks (with explanation)

Cybersecurity Requirement Specification (CRS) (could be a set of references to other documents)
- Assumptions
- Cybersecurity needs (including safety-related high level objectives)
- Cybersecurity requirements
- List of open risks (with explanation)

Cybersecurity management (could be a set of references to other documents)
- Cybersecurity policy
- Cybersecurity plan
- Cybersecurity process
- Vulnerability assessment and management

Cybersecurity fulfilment (could be a set of references to other documents)
- Implementation of cybersecurity measures - evidences of fulfilment of CRS
- Evidence of application of cybersecurity process
- Verification & validation results
  - Testing of security measures (e.g. V&V, Penetration testing)
  - Traceability to cybersecurity requirements
- Related cybersecurity cases (from included components or subsystems, if any)

Security-related application conditions (could be a set of references to other documents)
- Installation
- Maintenance
- Operation

Conclusion
- Cybersecurity claim
- Residual risks status
Next steps

- Dissemination of the TS 50701
- Capture return on experience to improve the TS and transform it into an European Norm (EN)
- Collaboration with other standardization committee (IEC AHG 20, ...)
- Preparation of submission of a NWIP to complete the TS with additional material (e.g. topics related to cybersecurity during operation and maintenance phases as security monitoring and security incident response)
Thank you for your attention!

christian.schlehuber@deutschebahn.com
serge.benoliel@alstomgroup.com
Q & A