Safety and Security in Ground Transportation Systems
Michael Paulitsch, Thales, Vienna, Austria

This work has been partially funded from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 731456 (certMILS.eu).

www.thalesgroup.com
Overview Railway - Signal Control

Trends

- Removal of some field elements (signals, ...)
- Remote moving authority
- Central operation centers

RBC ... remote block center
OBU ... on-board unit
Safety & Cyber Security

Safety: « The state of being free of risk or danger and the means/actions to obtain this state ».

Cyber Security: « The protection of information systems from theft or damage, as well as from disruption or misdirection of the services they provide ».

The «digital transformation» of Rail Systems requires increased attention on Cybersecurity, to avoid operational disruption (availability), access to user confidential data, and ensure safety is not impaired (system integrity).
Main CENELEC Standards for Signalling Applications – Safety

- **EN 50126**: The Specification and Demonstration of Reliability, Availability, Maintainability and Safety
- **EN 50128**: Communications, Signalling and Processing Systems – Software for Railway Control and Protection systems.
- **EN 50159**: Communication, Signalling and Processing systems - Safety-Related Communication in transmission.

### Table A.1 – SIL-table

<table>
<thead>
<tr>
<th>Tolerable Hazard Rate</th>
<th>Safety Integrity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^{-5} \leq \text{THR} &lt; 10^{-4}$</td>
<td>4</td>
</tr>
<tr>
<td>$10^{-4} \leq \text{THR} &lt; 10^{-7}$</td>
<td>3</td>
</tr>
<tr>
<td>$10^{-7} \leq \text{THR} &lt; 10^{-6}$</td>
<td>2</td>
</tr>
<tr>
<td>$10^{-6} \leq \text{THR} &lt; 10^{-5}$</td>
<td>1</td>
</tr>
</tbody>
</table>

**EN 50129:2003 excerpt – Safety Integrity Levels**

THR ... tolerable hazard rate
Safety Case

The Safety Case contains the documented safety evidence for the system/sub-system/equipment, and shall be structured as follows:

> **Part 1** Definition of System (or sub-system/equipment)
> **Part 2** Quality Management Report
> **Part 3** Safety Management Report
> **Part 4** Technical Safety Report
> **Part 5** Related Safety Cases (includes dependencies of sub-systems Safety Application Conditions)
> **Part 6** Conclusion summarizes evidences
**TAS Platform - Safe Computation and Communication**

- **Managed Life Cycle**
- **Customer Support**
- **Expandable Safe Execution**
- **Critical Service Support Functions**
- **Tools for Development Support**
- **Manage Core Software (OS, Safety Layers, Packages)**
- **Managed Computing Boards**

**Method & Tools**

- **PLF Core (OS)**
- **PLF Hardware (Boards)**
- **MNT&Download**
- **OCS (Communication)**

**Support & Maintenance Framework**

- **Support Tools**
- **Deliverable Tools**
- **Life Cycle Tools**

**Open Source**
Overview TAS Platform - A Closer Look

- **Safety approval according to CENELEC 50129 SIL 4**
- **Safety layer**
  - Fault tolerance
  - Health monitoring
- **Board support package**
  - Communications interfaces / drivers
  - Some are very specific
- **Based on COTS hardware / operating system**
  - Kernel patches to address safety and maintainability
- **Support 25 years of application business logic (with changing underlying hardware and software)**

**Application Business Logic**

- **TAS Platform Core**
  - **Core Software**
    - Safety Layer
      - Fault Tolerance & Communication
      - Online Hardware Testing
  - **AEOS5**
    - OS
      - Linux, Libraries, Tools ...
- **TAS Platform OCS**
  - Safe Protocol
- **TAS Platform J4S**
  - Java for Signalling
- **TAS Platform MNT**
  - Maintenance Upload/Download

---

M Paulitsch - Safety and Security in GTS
TAS Platform - A Generic Safety Case

TAS Platform-based products MLS (Main Line Signaling)

TAS Platform-based products URS (Urban Rail Systems)

Generic TAS Platform
Generic CENELEC approval

TAS Platform System Safety Case
TAS Platform Engineering & Environment

Safety Application Conditions

Core System TAS Platform SW
Subsystems: OCS, MNT, J4S
• Check of HW-CS SAC
• Validation on HW-CS
• Approval with HW-CS

SW components
• Analyses
• Verification
• Validation

TAS Platform Services

Safety Application Conditions (SAC)

HW Core System
• Analyses
• Verification/Valid.
• Safety Case
• Manufacturing
• Approval

Field Elements

ETCS
Interlocking
On Board

Distributed Development / Maintenance (Thales AT / TTS Germany)
Example: “TAS Platform in Used in Interlocking Configuration”
TAS Platform is Based on Linux

- In addition to safety layer and functional services (communication)
- Reuse existing COTS security packages of Linux
  - Encryption
  - Access control
  - etc.

Layered safety approach allows integration of security functions
Safety Meets Security - a “First Date” in “Standard” Setting

**EN50159-2011 (excerpt)**

A safety-related equipment connected through an open transmission system can be subjected to many different IT security threats, against which an overall program has to be defined, encompassing management, technical and operational aspects.

In this European Standard however, as far as IT security is concerned, only intentional attacks by means of messages to safety-related applications are considered.

This European Standard does not cover general IT security issues and in particular it does not cover IT security issues concerning

- ensuring confidentiality of safety-related information,
- preventing overloading of the transmission system.
Example Communication in Railway Standards

Citation from EN 50159:2011

The safety requirements depend on the characteristics of the transmission system. In order to reduce the complexity of the approach to demonstrate the safety of the system, transmission systems have been classified into three categories:

- **Category 1** consists of systems which are under the control of the designer and fixed during their lifetime;
- **Category 2** consists of systems which are partly unknown or not fixed, however unauthorised access can be excluded;
- **Category 3** consists of systems which are not under the control of the designer, and where unauthorised access has to be considered.

Categories implicitly address some security aspects

- First time mentions IT security explicitly as concern

Excerpt:

- There are two kinds of threats resulting from unauthorized access to signalling equipment:
  - 1) Physical security threats. [...]
  - 2) IT-Security threats.

- Modern IT communication concepts result in the need to protect those systems also against logical access via IT systems. [...]

- IT-Security is a rapidly evolving field. There is no doubt that IT-Security can affect not only the service but also functional safety of a signalling system. [...]

- This **European Standard does not specify the requirements** for the development, implementation, maintenance and/or operation of security policies or security services, for which appropriate IT-Security standards are applicable.
7 strategies and their percentage of incidents potentially mitigated by each strategy

- Implement Application Whitelisting – 38%
- Ensure Proper Configuration/Patch Management – 29%
- Reduce your Attack Surface Area – 17%
- Manage Authentication – 4%
- Build a Defendable Environment – 9%
- Monitor and Respond – 2%
- Implement Secure Remote Access – 1%

Source: US dept of Homeland Security

Safety management helps here achieving security properties
## IEC 62443 - An Applicable Security Standard

**Summary:**

<table>
<thead>
<tr>
<th>ISA-99 / IEC 62443 covers requirements on processes / procedures as well as functional requirements</th>
</tr>
</thead>
</table>

### IEC 62443 / ISA-99

<table>
<thead>
<tr>
<th>General</th>
<th>Policies and procedures</th>
<th>System</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1 Terminology, concepts and models</td>
<td>2-1 Establishing an IACS security program</td>
<td>3-1 Security technologies for IACS</td>
<td>4-1 Product development requirements</td>
</tr>
<tr>
<td>1-2 Master glossary of terms and abbreviations</td>
<td>2-2 Operating an IACS security program</td>
<td>3-2 Security assurance levels for zones and conduits</td>
<td>4-2 Technical security requirements for IACS products</td>
</tr>
<tr>
<td>1-3 System security compliance metrics</td>
<td>2-3 Patch management in the IACS environment</td>
<td>3-3 System security requirements and security assurance levels</td>
<td></td>
</tr>
<tr>
<td>Definitions/Metrics</td>
<td>2-4 Certification of IACS supplier security policies and practices</td>
<td>Requirements to a secure system</td>
<td>Requirements to secure system components</td>
</tr>
</tbody>
</table>

**Helpful in checking completeness**
Chances & Challenges - IEC 62443 for VDE V 0831-104

IEC 62443 / ISA-99 covers requirements on processes / procedures as well as functional requirements.

- **General**
  - 1-1 Terminology: concepts and models
  - 1-2 Master glossary of terms and abbreviations
  - 1-3 System security compliance metrics
- **Policies and procedures**
  - 2-1 Establishing an IACS security program
  - 2-2 Operating an IACS security program
  - 2-3 Patch management in the IACS environment
  - 2-4 Certification of IACS supplier security policies and practices
- **System**
  - 3-1 Security terminology for IACS
  - 3-2 Security assurance levels for zones and conduits
  - 3-3 System security requirements and security assurance levels
  - 4-2 Technical security requirements for IACS products
- **Requirements to a secure system**
  - Requirements to secure system components

---

**Zones & Conduits**

**Reference Architecture**

**Patch Management**

---

**Figure 1 – Workflow to establish zones and conduits**

VDE V 0831-104: Draft standard for IT security in railway signaling systems
TAS Platform Security - Patch Management

- **Following standards:** IEC TR62443 2-3 for Patch Management
- **Separate safety and security life-cycles**
  - Using suitable architectures and processes or physical separation of security and safety functions
- **Provide safety and security releases (security releases verified only according to security process)**
  - TAS PLF Safe and Secure Releases
  - TAS PLF Additional Security Releases

**Comment in draft norm (prEN50129: 2016)**

**Safety and Security Life Cycle is Different**

**NOTE 3** Sometimes it can be necessary to balance between measures against systematic errors and measures against security threats. An example is the need for fast security updates of SW arising from security threats, whereas if such SW is safety related, it needs to be thoroughly developed, tested, validated and approved before any update.
Safety and Security Observations

- **COTS Observation for security and safety-relevant topics (already standard at regular intervals)**
  - Example monitored objects: kernel, glibc, gcc
  - Update cycle of Core Software is based on Service Level Agreement program
  - On demand security updates (non-safety-related) possible (business purpose)
    - similar safety defect management and associated response actions (emergency release)

- **TAS Platform is based on monitored COTS components (embedded usage)**
**TAS Platform OS Objectives**

- **COTS software**
  - Reduce development effort
  - Increase quality due to large user base

- **Monitor errata lists, etc.**
  - Identify bugs that could affect safe functionality
  - Required by CENELEC

- **Least functionality**
  - Safety argumentation
  - Deterministic runtime behaviour

- **Small footprint (down to 256 Mbyte RAM, 32 Mbyte ROM, 266 MHz)**

**Some Objectives of Security and Safety Match**

- **COTS software**
  - Reduce development effort
  - Increase quality due to large user base

- **Monitor vulnerabilities**
  - Identify bugs that could lead to security breach

- **Least functionality**
  - Reduce attack vector
Areas of Possible Vulnerabilities in Rail Systems …
Areas of Possible Attacks in Rail Systems...

- **Internet Access**
- **Social Engineering Attack**
- **Physical Access**
- **Wired Network**
- **Field Elements**
- **Firewall attack**
- **Hacker**
- **Malware**
- **Password Attack**
- **Wireless Attack**
- **GSM-R**
- **OBU**
- **Mobile Access**
- **Device Attack**

**Locations:**
- Traffic Management
- Operation Control Center
- Radio Block Center
- Interlocking
- Wired Network
- OBU
Areas of Possible Impact on Rail Systems …

- Traffic Management
- Operation Control Center
- Radio Block Center
- Interlocking
- Wired Network
- Mobile Access
- Internet
- Hacker
- Wired Network
- Field Elements
- GSM-R
- OBU
- Time Bomb
- Trojan
- Bad Code
- Spam
- Doc Malware
- Worm
Examples of Areas to Protect Rail Systems

- Traffic Management
- Operation Control Center
- Internet
- Mobile Access
- CyberObserved
- Wired Network
- CyberCrypt
- Encryption
- Wired Network
- Interlocking
- Radio Block Center
- Application Layer Firewall
- CyberGate
- Field Elements
- GSM-R
- CyberOneCom
- Data Diode
- OBU
- Mobile Access
Examples of Areas to Protect Access in Rail Systems

- Operation Control Center
- Traffic Management
- Radio Block Center
- Interlocking
- Field Elements
- Wired Network
- Certificate
- Certificate
- GSM-R
- OBU

Public Key Infrastructure

Access Control

Internet

Mobile Access

Wired Network

LDAP

PKI

Certificate

THALES
Examples of Areas to Monitor Security in Rail Systems

- Operation Control Center
- Traffic Management
- Internet
- Mobile Access
- CyberRail
- Wired Network
- Field Elements
- Interlocking
- Radio Block Center
- CyberServices
- CyberProbe
- GSM-R
- OBU
- Wired Network
- Mobile Access
- Internet
Examples of Areas for Security Services in Rail Systems

- Internet
- Cyber Threat Intelligence
- Asset Management
- Incident Management
- Security Monitoring
- Awareness & Training & Risk
- Wired Network
- Field Elements
- Traffic Management
- Operation Control Center
- CyberRail
- Wired Network
- Interlocking
- Radio Block Center
- GSM-R
- OBU
- Mobile Access
- CyberCoachingCenter

CyberServices
Cyber Reference Architecture - Example: Data Diode

- **Goal:** Non-Interference
- **Solution:** one channel communication, "data diode"
- **Thales 6838 CyberOneComm enables**
  - One channel communication over network
  - Multiple data connections
  - Use for diagnosis purposes
  - E.g. ETCS on-board system
Summary

- Security is becoming a real concern
- Multiple security assessments and customers have driven and are driving improvements of Thales applications and TAS Platform
- TAS Platform architecture has already been ready for security extensions - simple integration of security functions
- Overlaps in processes in achieving security and safety
- Thales security reference architecture & implementation of components augment overall architecture
- But never stop improving ...

We are ready!
“This work has been partially funded from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 731456.”

If you need further information on certMILS, please contact the coordinator:

Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55    Fax: +43 4242 233 55 77
E-Mail: coordination@certmils.eu

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author’s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.
Infiltration Rate & Source

Rate of Infiltration (sans.org, 2015)

Source of Infiltration (sans.org, 2015)
Vulnerabilities

Source: NIST database

Source: Kaspersky
Standards

Requirements for critical infrastructures firmed up by Public Authorities

- European commission: ENISA, Europe 2020 NIS
- Most National NSAs introducing guidelines

Active standards and working groups

- Generic ICT: NIST SP800-53; ISO/IEC2700x
- Industrial Control Systems: NIST SP800-82 (US), ISA(IEC) 62443
- Rail specific: APTA, CENELEC SC9XA-SG16 WG, UITP WG, UNIFE WG