THALES

Safety and Security in Ground Transportation Systems

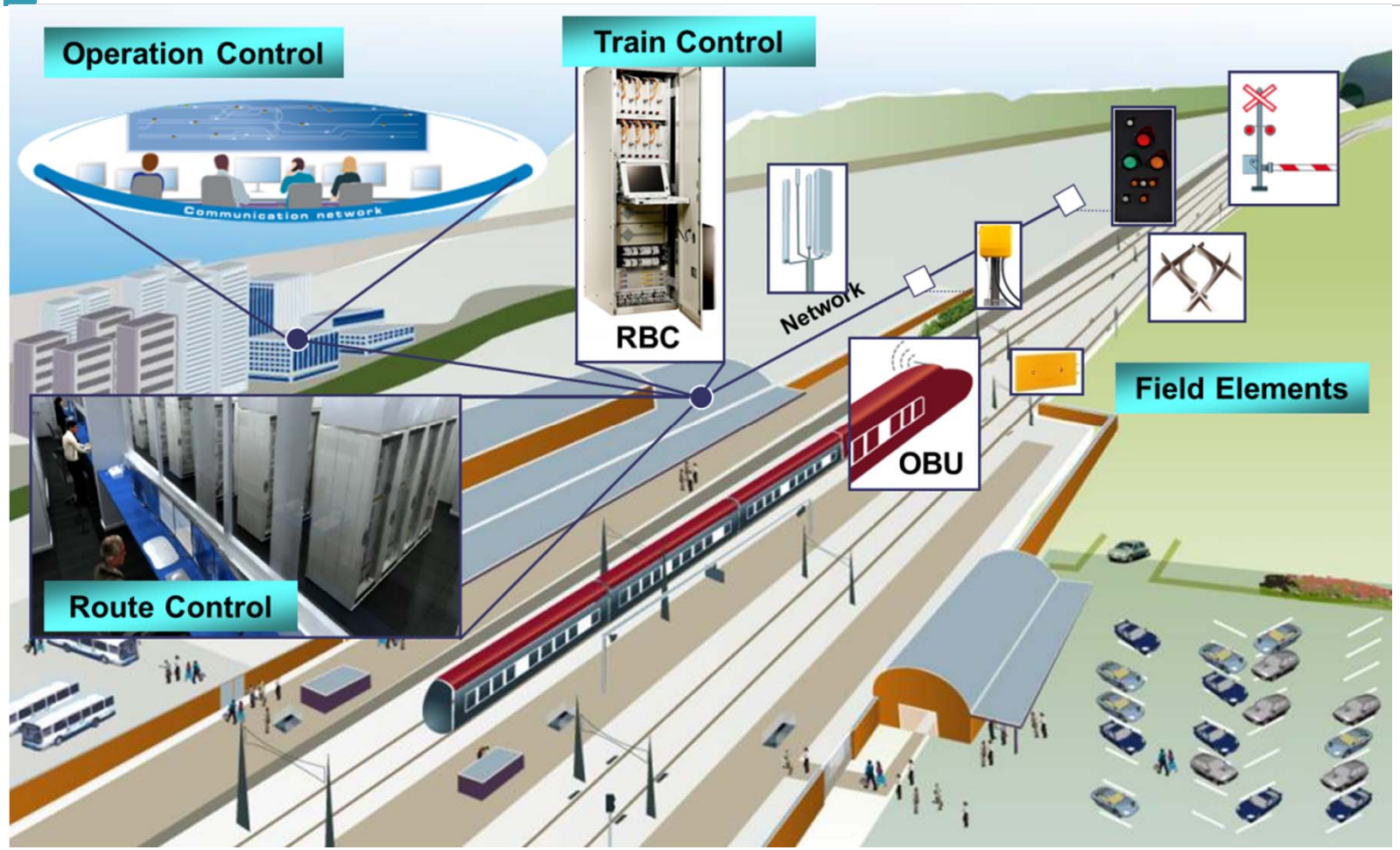
Michael Paulitsch,
Thales, Vienna, Austria

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

OPEN

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).

THALES

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 50129: Communications, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling.
- EN50159: Communication, Signalling and Processing systems - Safety-Related Communication in transmission.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Table A.1 – SIL-table

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

EN 50129:2003 excerpt – Safety Integrity Levels

THR … tolerable hazard rate

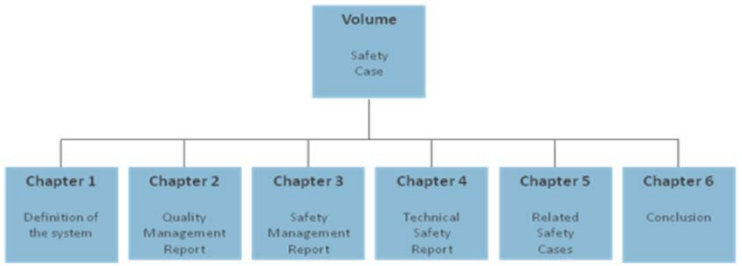
THALES

Safety Case

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

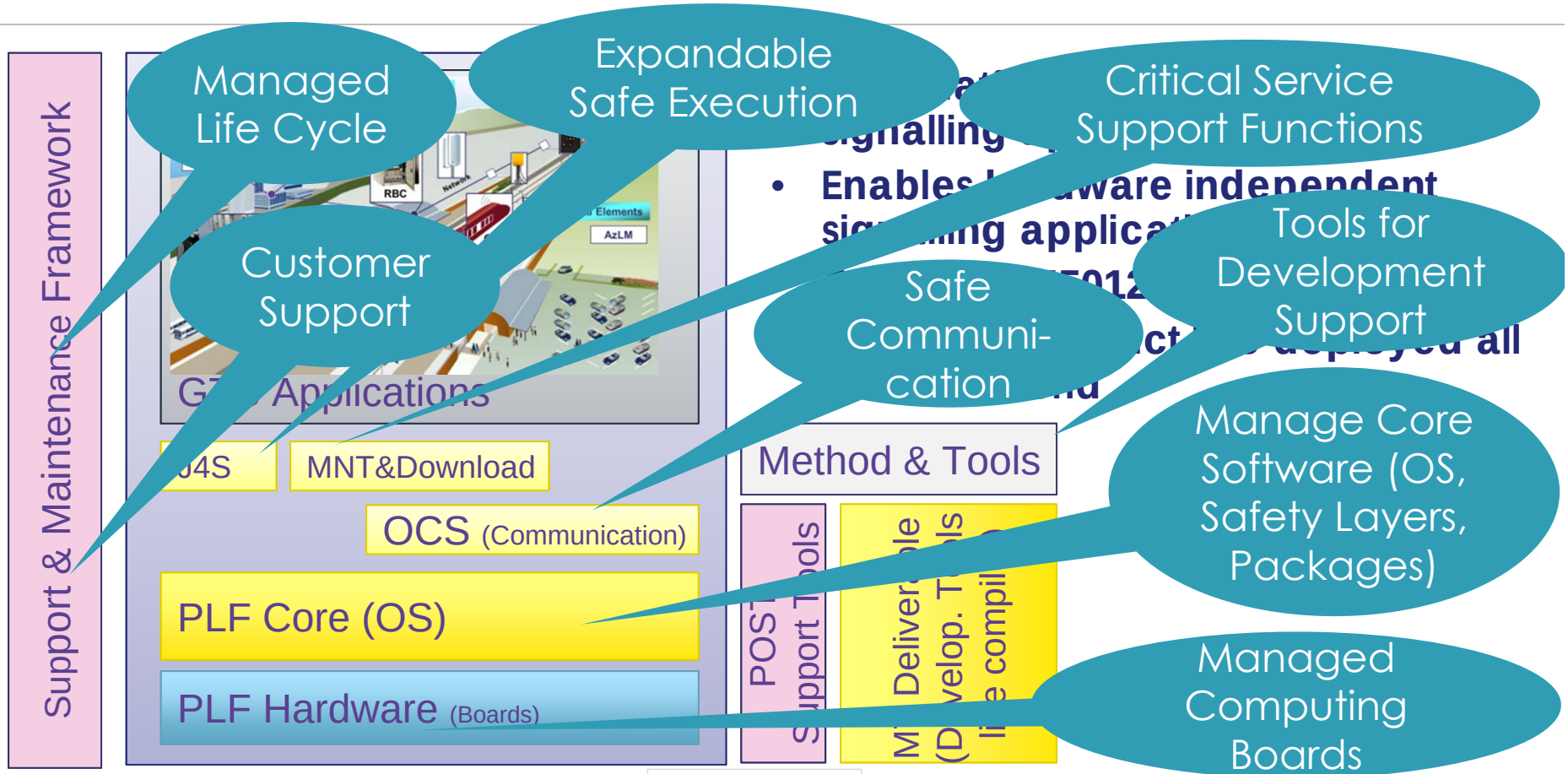
- **Part 1** Definition of System (or sub-system/equipment)
- **Part 2** Quality Management Report
- **Part 3** Safety Management Report
- **Part 4** Technical Safety Report
- **Part 5** Related Safety Cases *(includes dependencies of sub-systems Safety Application Conditions)*
- **Part 6** Conclusion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

Structure of Safety Case – EN50129



THALES

TAS Platform – Safe Computation and Communication



Overview TAS Platform – A Closer Look

Safety approval according to CENELEC 50129 SIL 4

Safety layer

- Fault tolerance
- Health monitoring

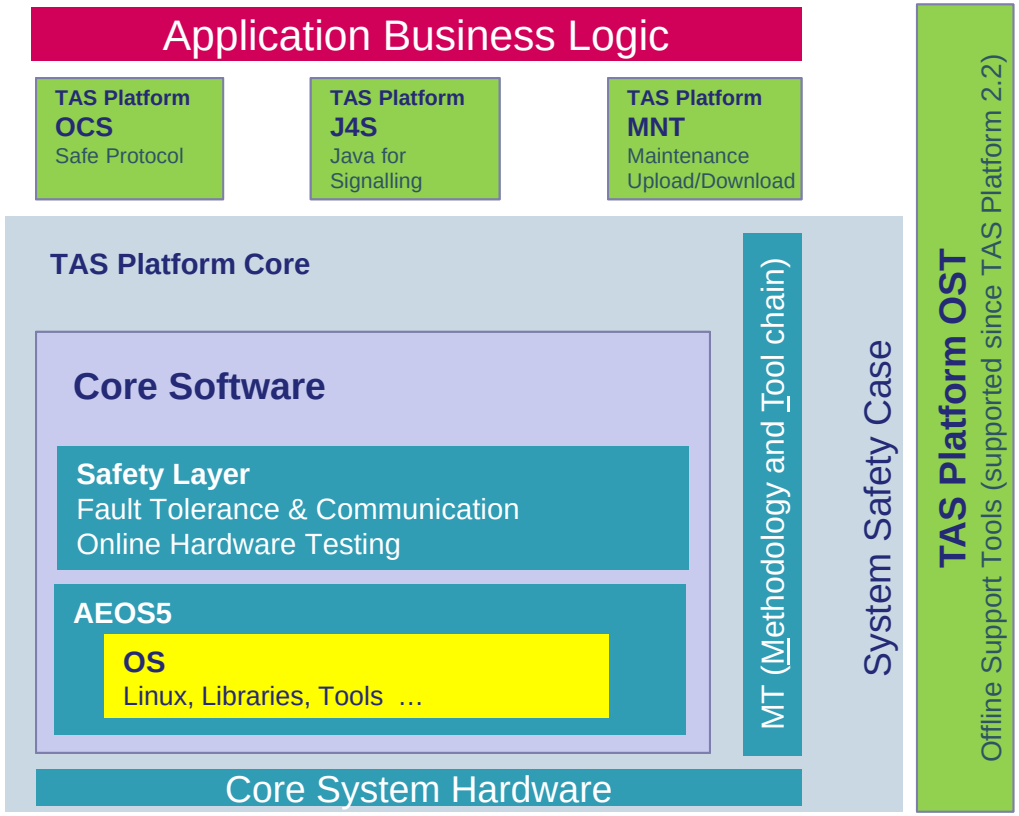
Board support package

- Communications interfaces / drivers
- Some are very specific

Based on COTS hardware / operating system

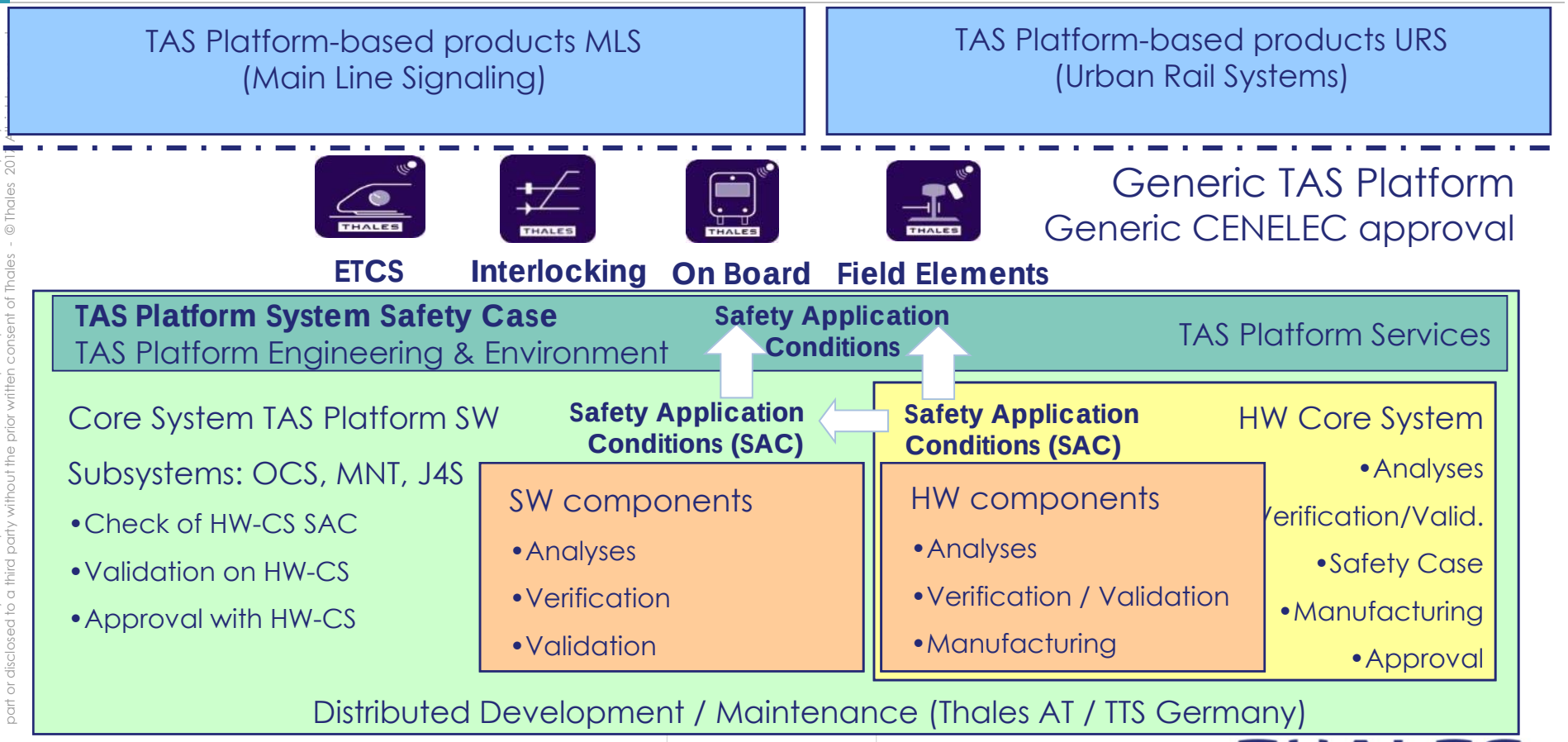
- Kernel patches to address safety and maintainability

Support 25 years of application business logic (with changing underlying hardware and software)



THALES

TAS Platform – A Generic Safety Case



Example: “TAS Platform in Used in Interlocking Configuration

Interlocking

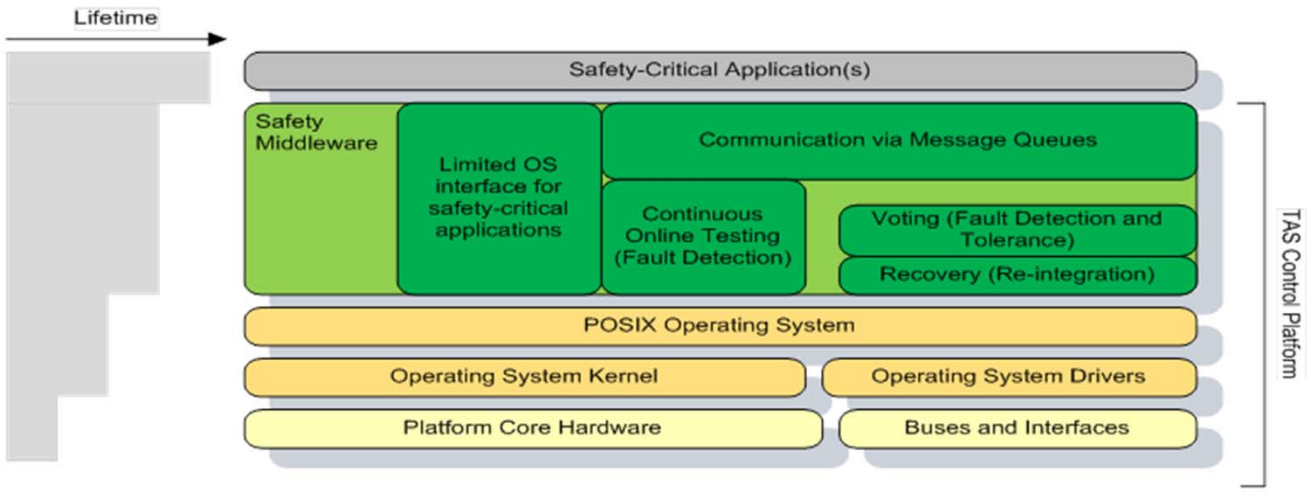
Onboard System (ETCS)

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

THALES

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

THALES

Security Meets Safety: Draft Standard - prEN50129:2016

First time mentions IT security explicitly as concern

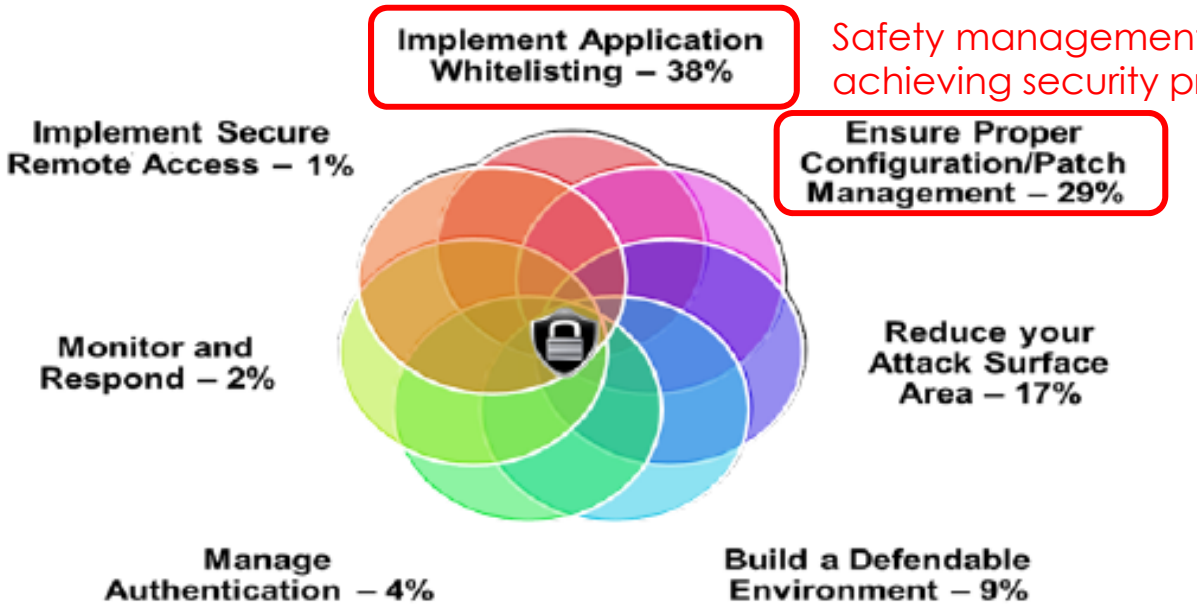
Excerpt:

- 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.

THALES

Strategies

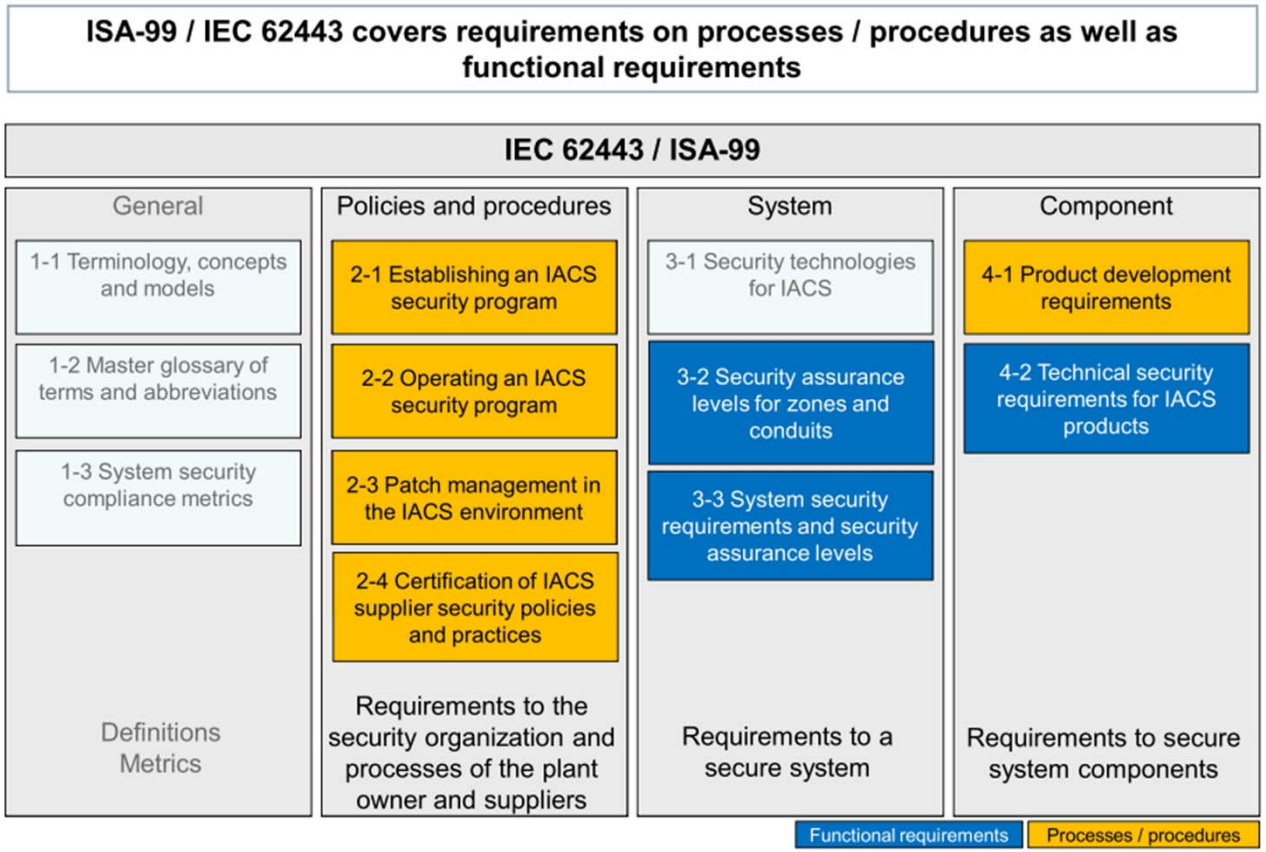
7 strategies and their percentage of incidents potentially mitigated by each strategy



Safety management helps here achieving security properties

Source: US dept of Homeland Security

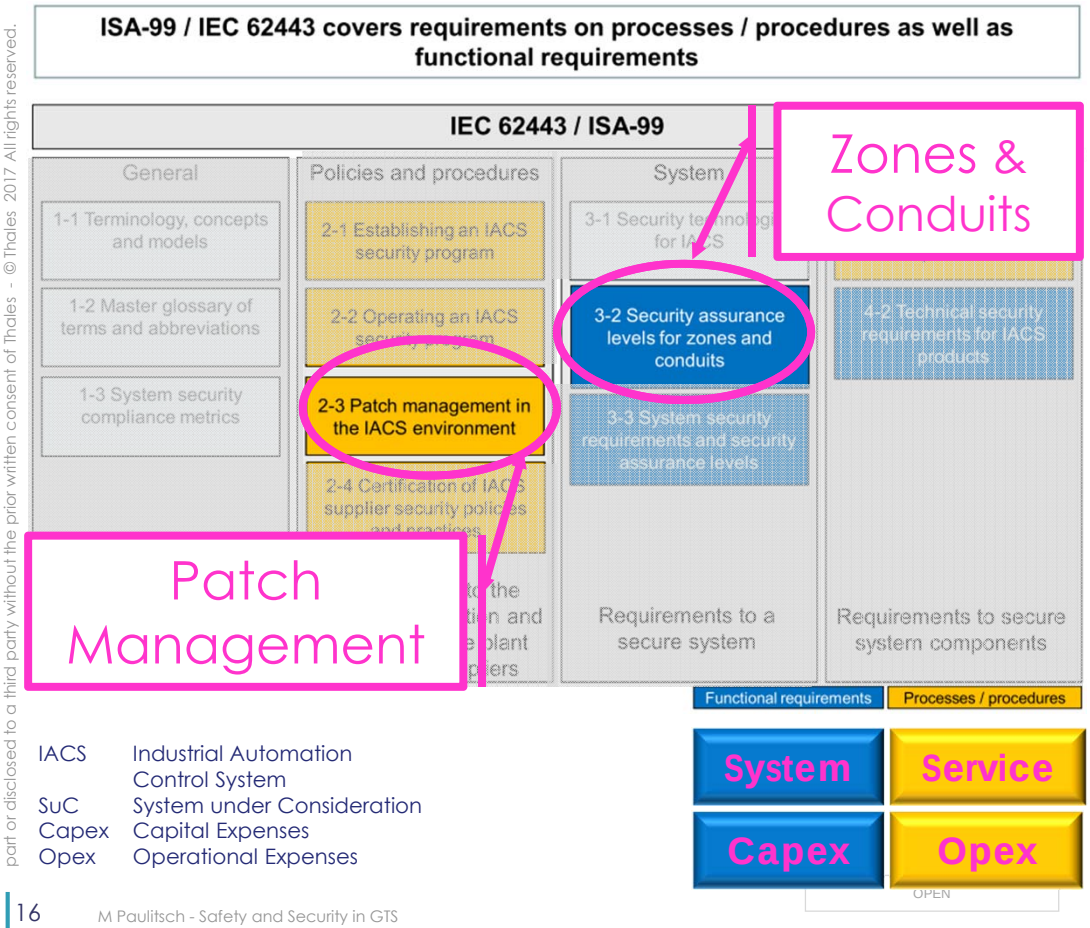
IEC 62443 – An Applicable Security Standard



Helpful in checking completeness

THALES

Chances & Challenges - IEC 62443 for VDE V 0831-104



IACS	Industrial Automation Control System
SuC	System under Consideration
Capex	Capital Expenses
Opex	Operational Expenses

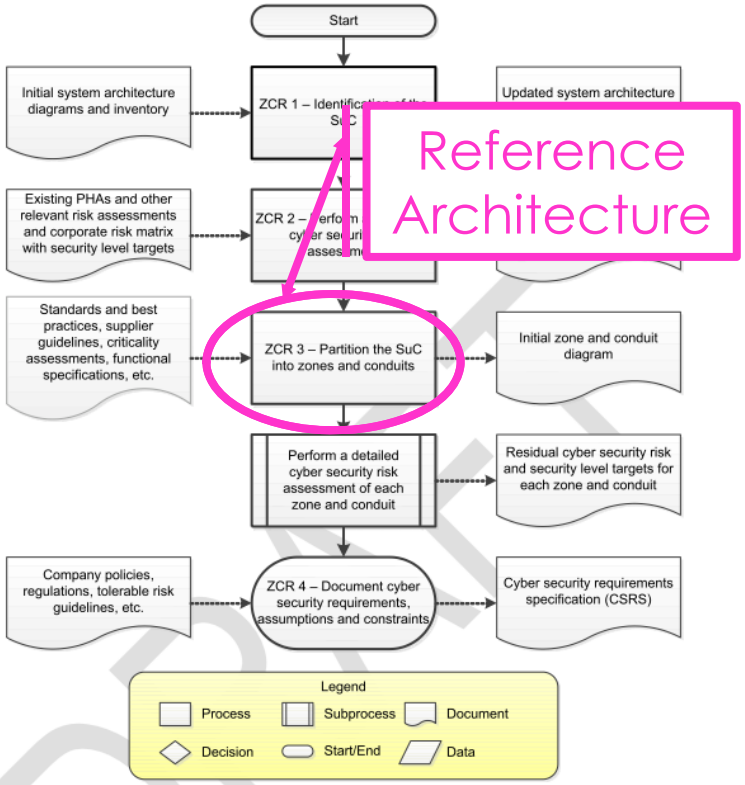


Figure 1 – Workflow to establish zones and conduits

VDE V 0831-104: Draft standard for IT security in railway signaling systems

THALES

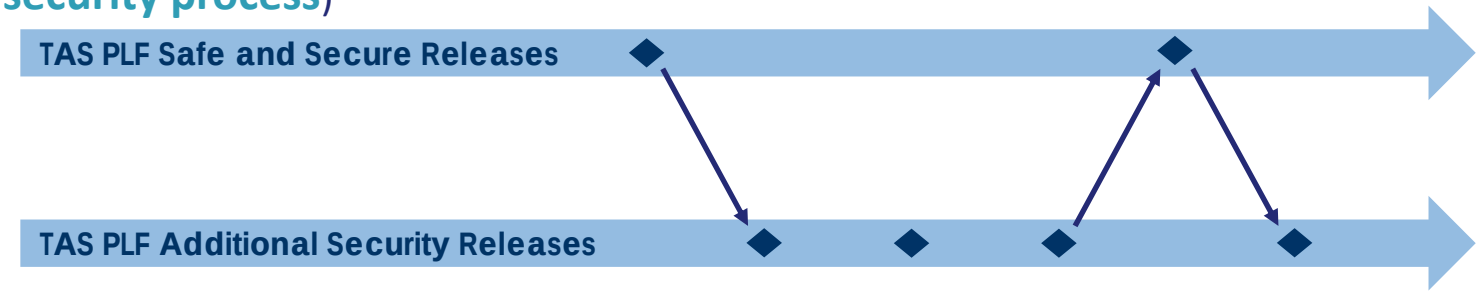
TAS Platform Security – Patch Management

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)



Comment in draft norm (prEN50129: 2016)

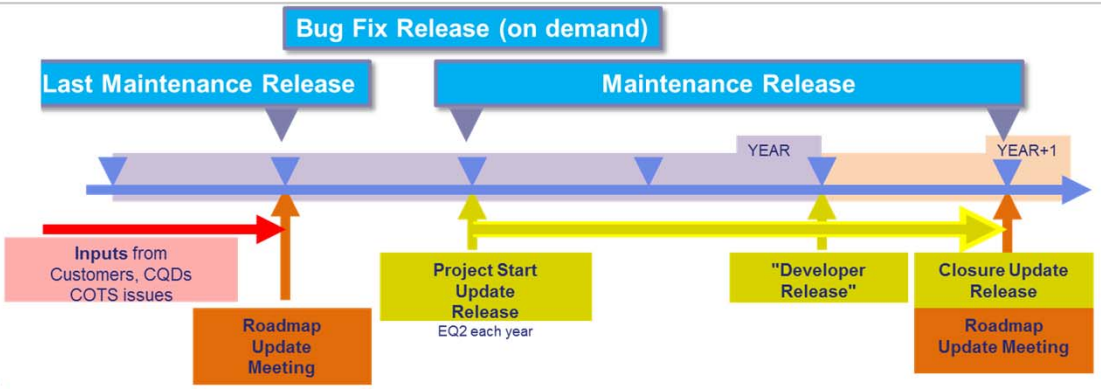
NOTE 3 Sometimes it can be necessary to balance between measures against systematic errors and measures against security threats. An example is the need for fast security updates of SW arising from security threats, whereas if such SW is safety related, it needs to be thoroughly developed, tested, validated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

Safety and Security Life Cycle is Different

THALES

Safety and Security Observations

COTS Observation for security and safety-relevant topics (already standard at regular intervals)



TAS Platform is based on monitored COTS components (embedded usage)

- 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)

THALES

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)

OS Objectives Security

COTS software

- Reduce development effort
- Increase quality due to large user base

Monitor vulnerabilities

- Identify bugs that could lead to security breach

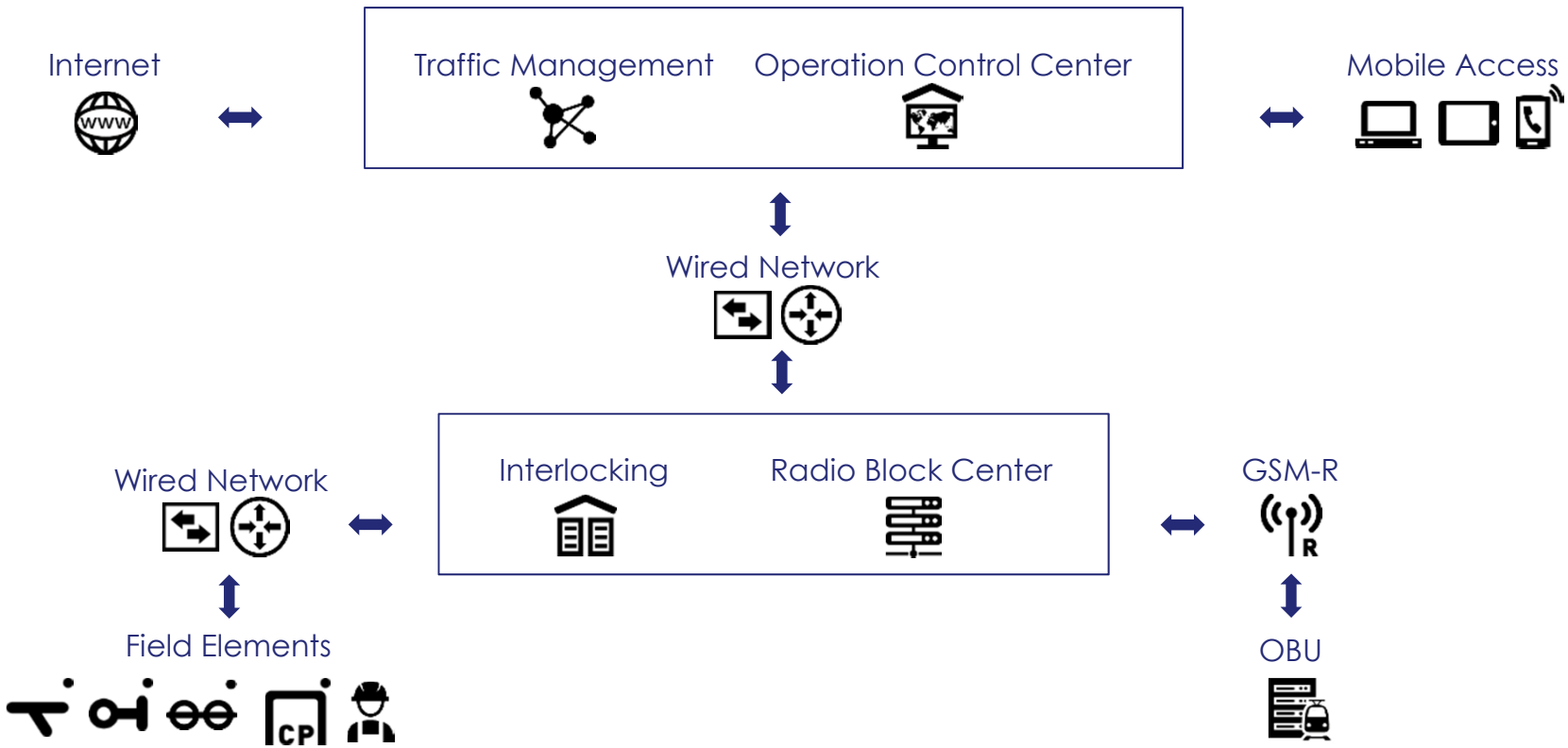
Least functionality

- Reduce attack vector

Some Objectives of Security and Safety Match

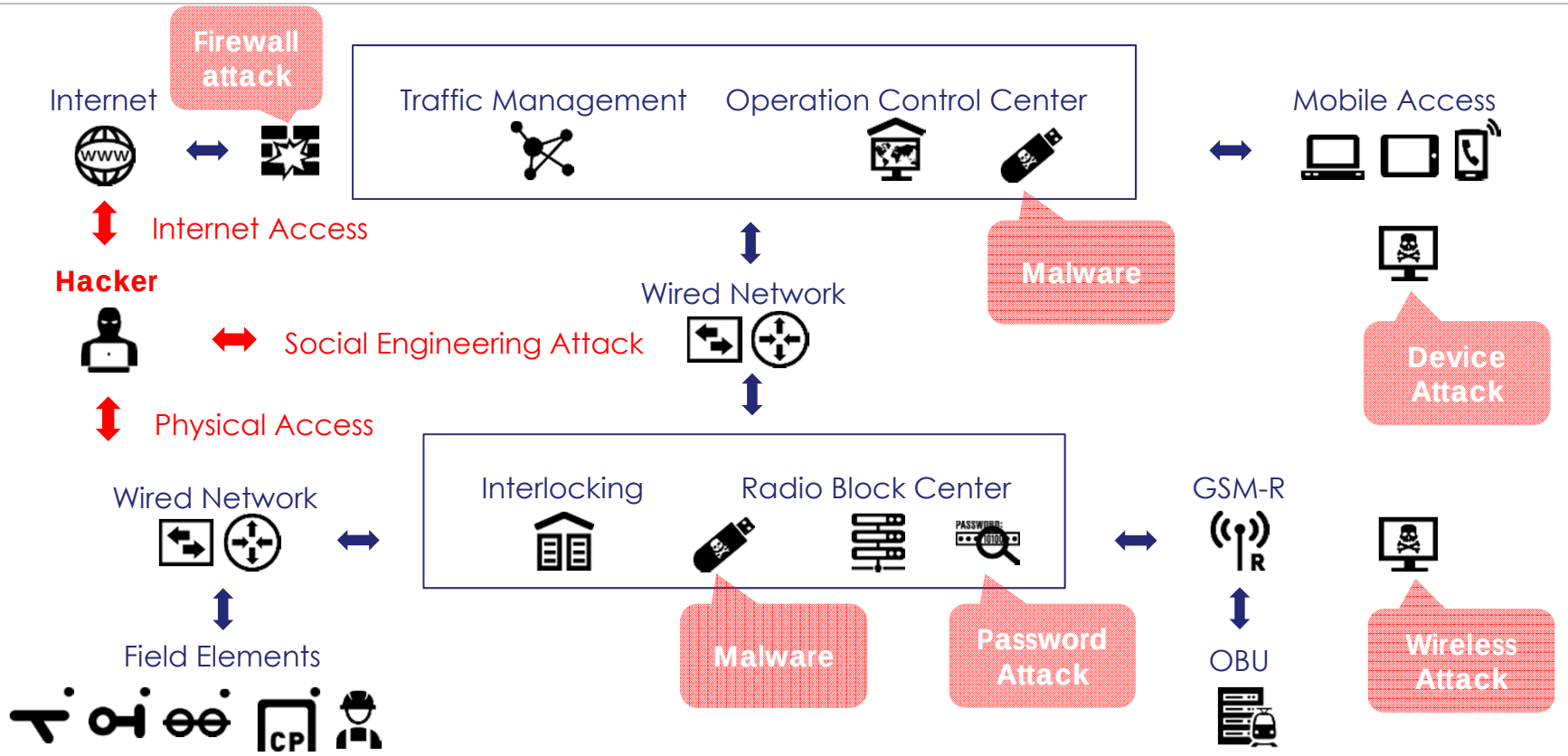
THALES

Areas of Possible Vulnerabilities in Rail Systems …



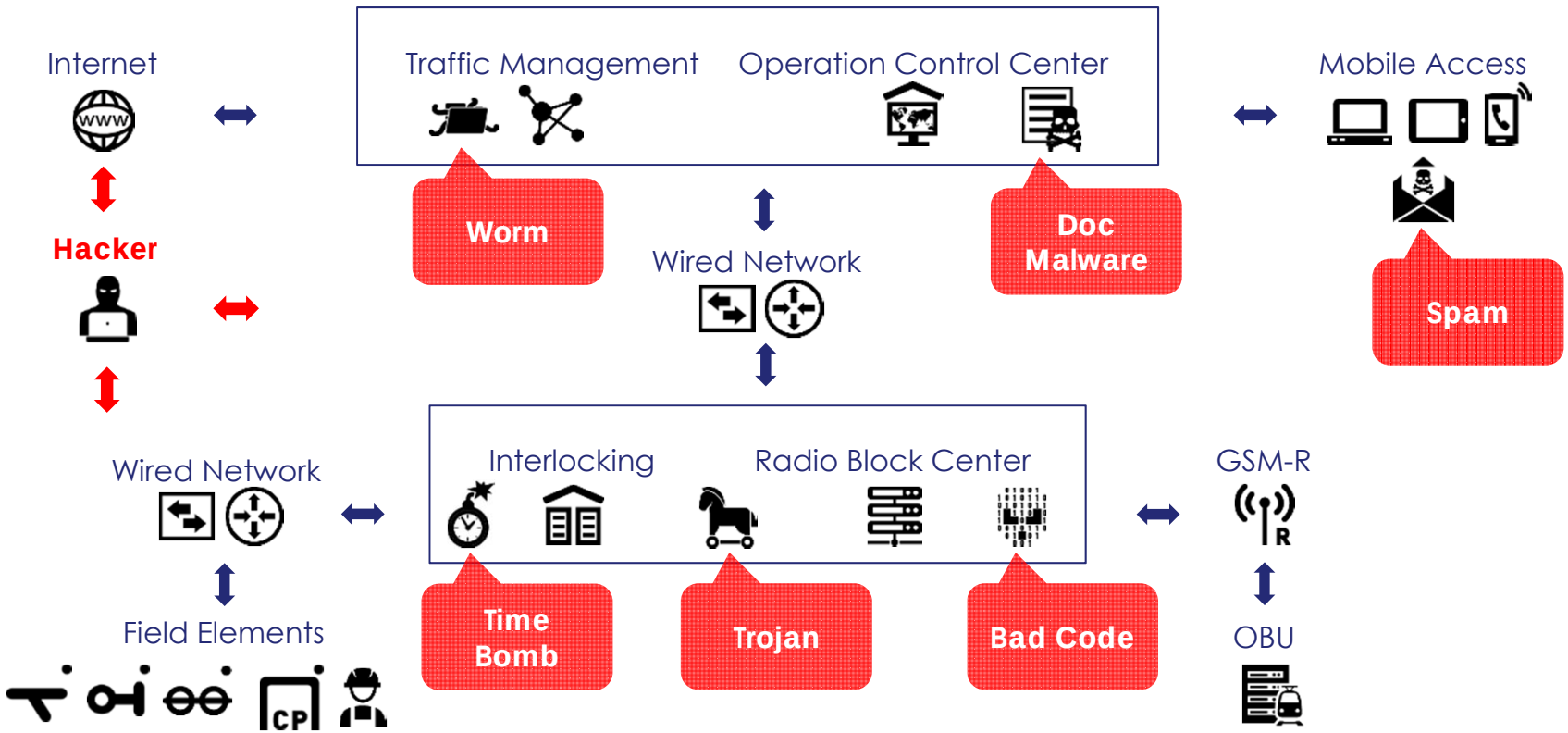
THALES

Areas of Possible Attacks in Rail Systems...



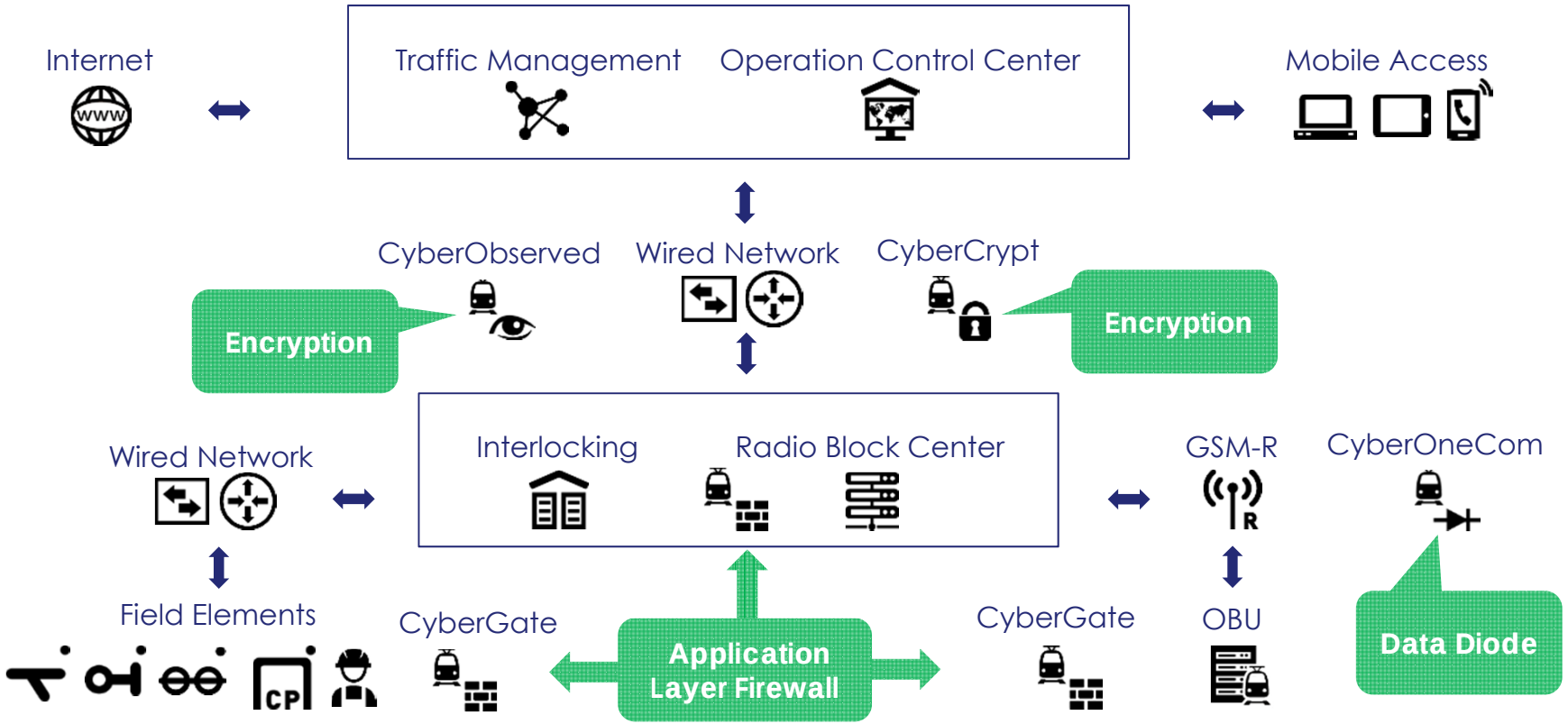
THALES

Areas of Possible Impact on Rail Systems ...



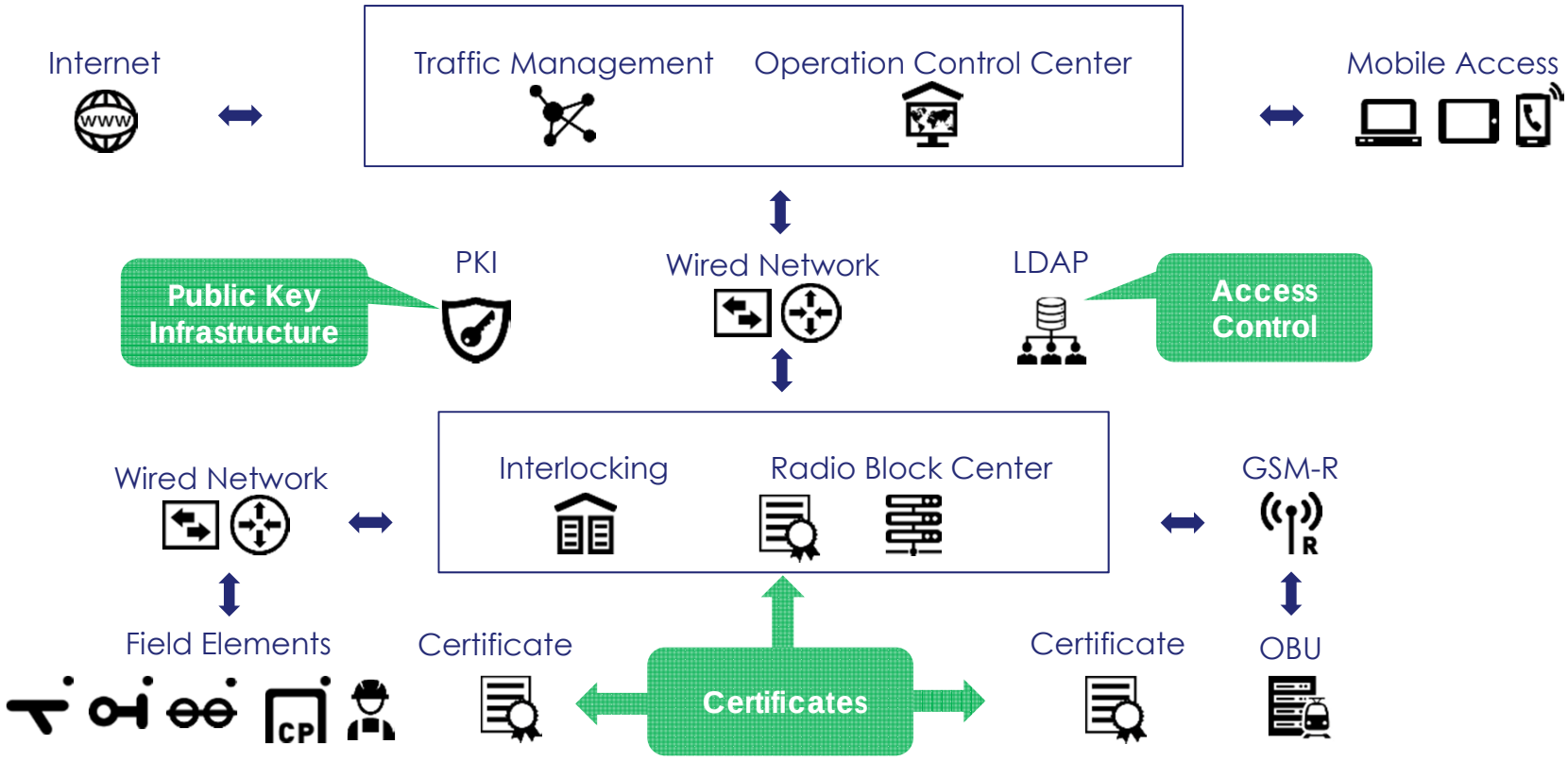
THALES

Examples of Areas to Protect Rail Systems



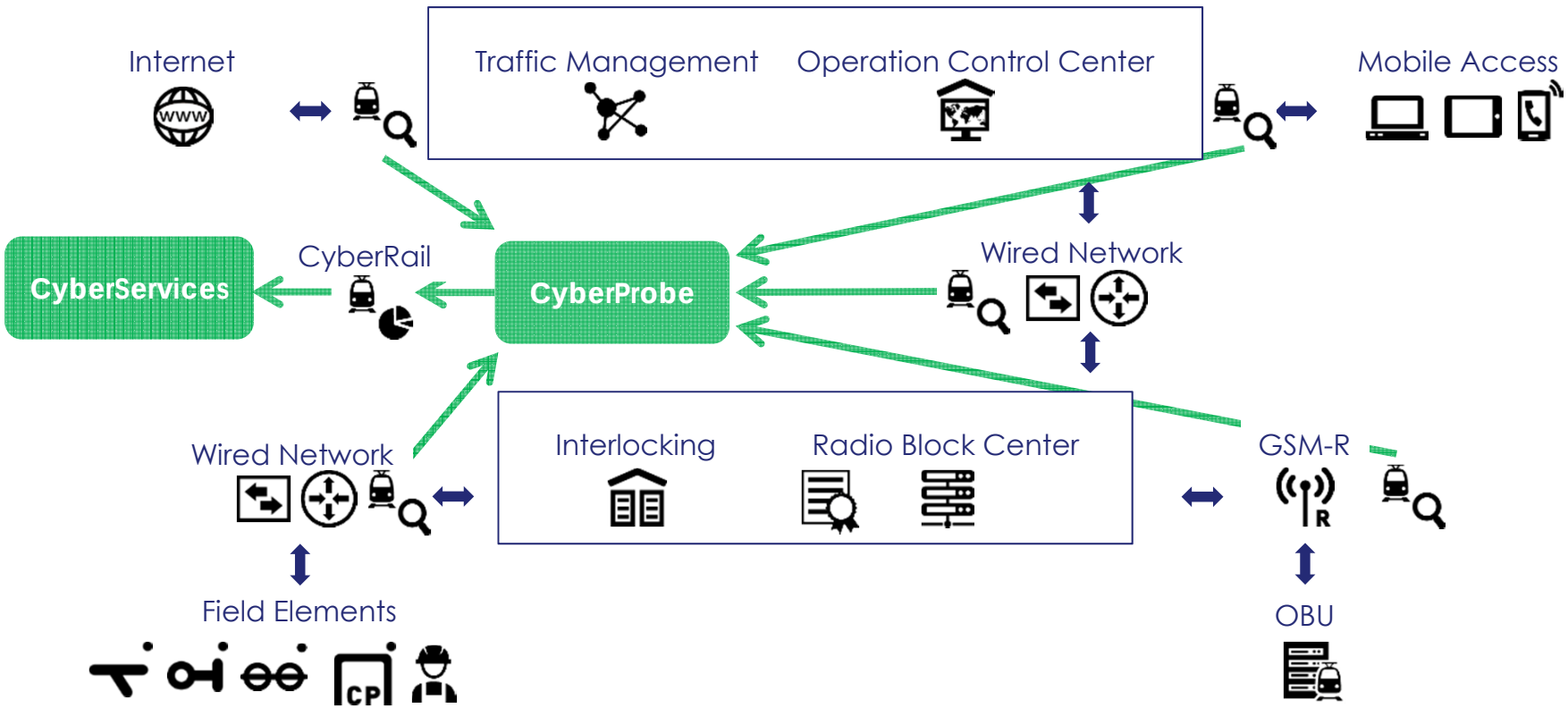
THALES

Examples of Areas to Protect Access in Rail Systems



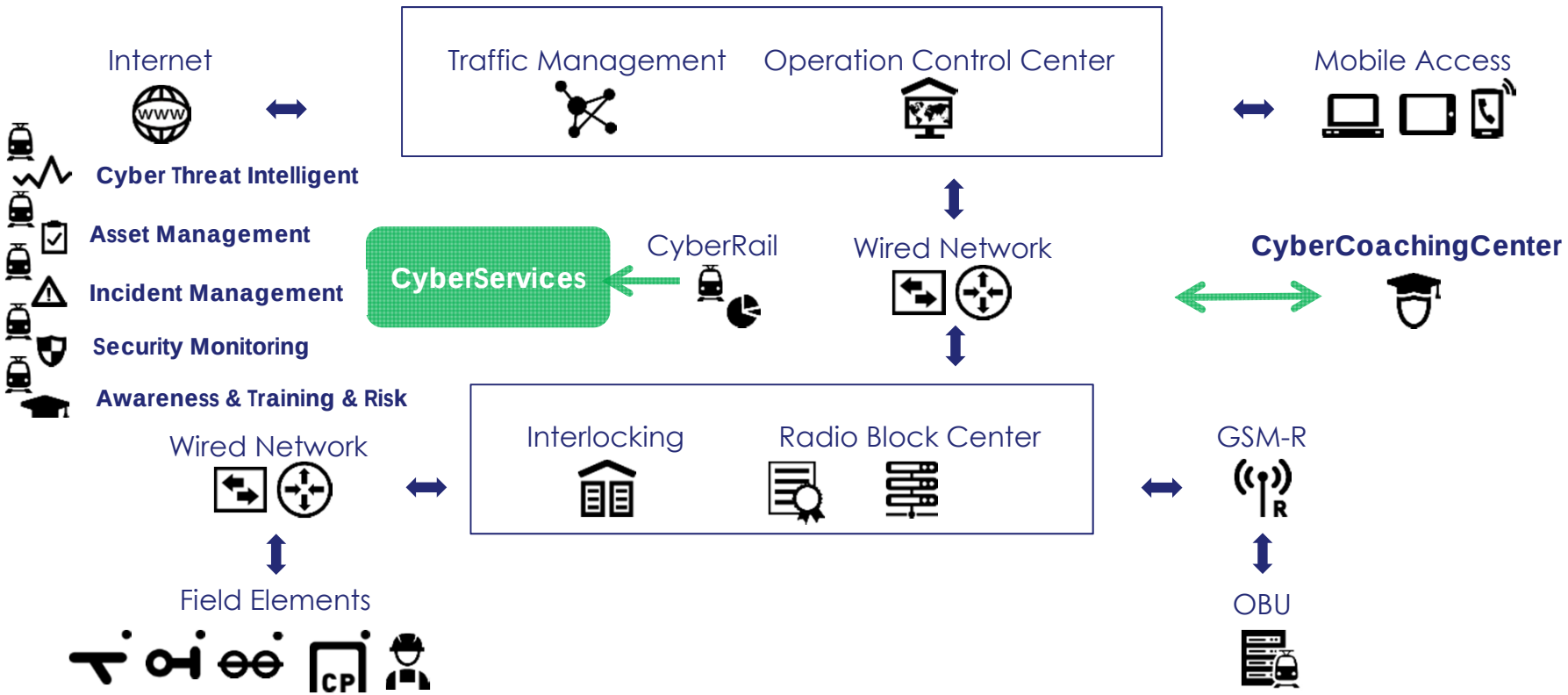
THALES

Examples of Areas to Monitor Security in Rail Systems



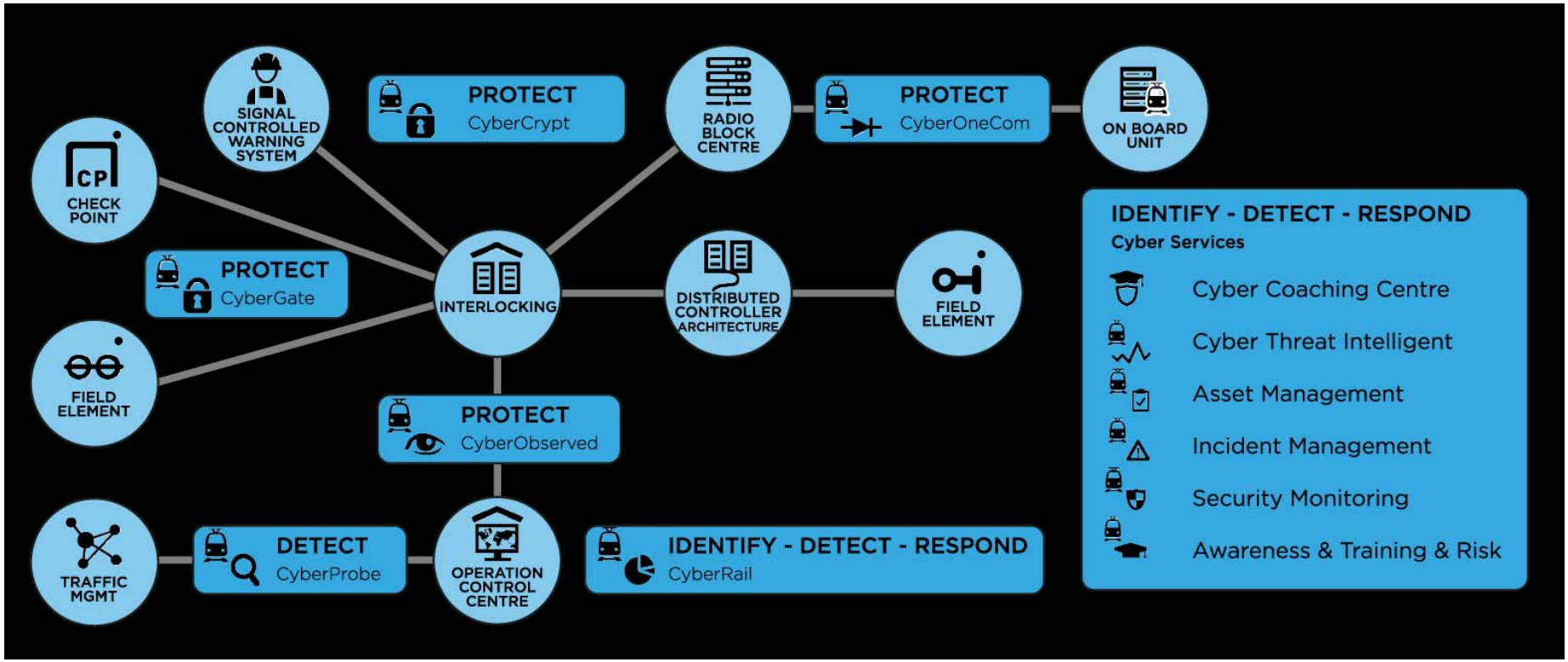
THALES

Examples of Areas for Security Services in Rail Systems



THALES

Thales Cyber Security Reference Architecture CySecTrac



THALES

Cyber Reference Architecture – Example: Data Diode

Goal: Non-Interference

Solution: one channel communication „data diode“

Thales 6838 CyberOneComm enables

- One channel communication over network
- Multipe data connections
- Use for diagnosis purposes
- E.g. ETCS on-board system

THALES

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!

OPEN

THALES

Funding Notice: CERTMILS Contract No: 731456

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

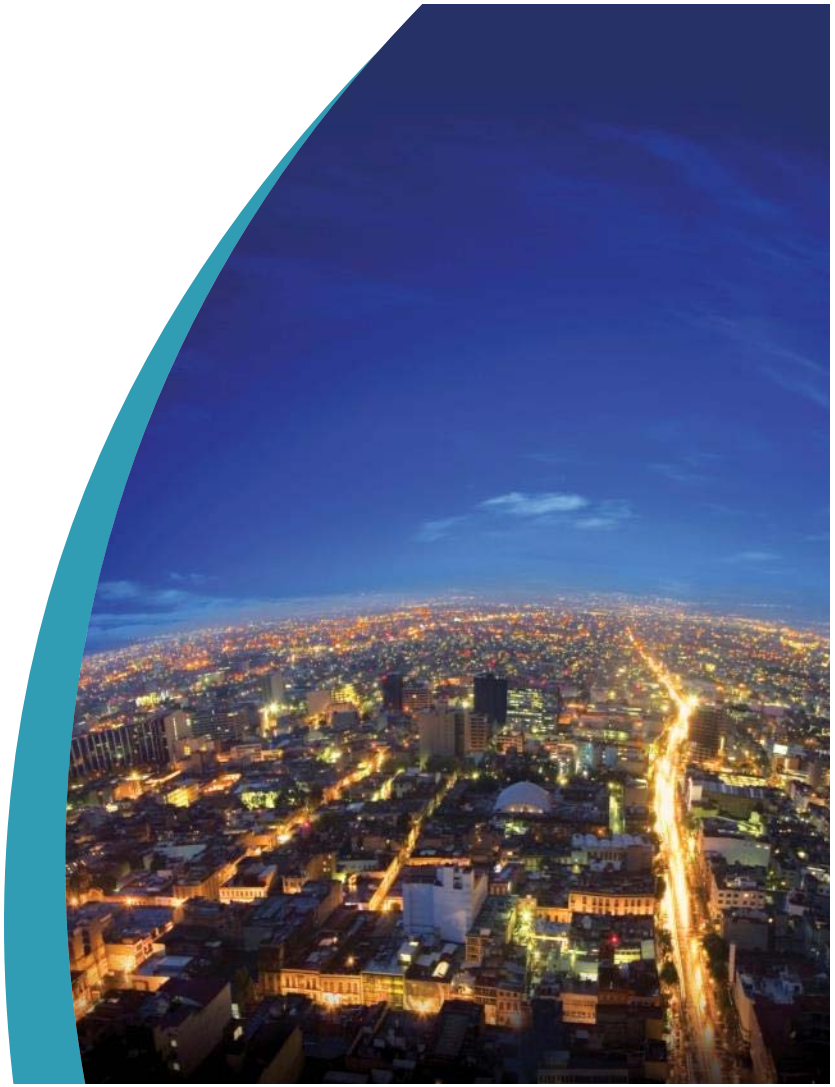
If you need further information on certMILS, please contact the coordinator:

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

THALES

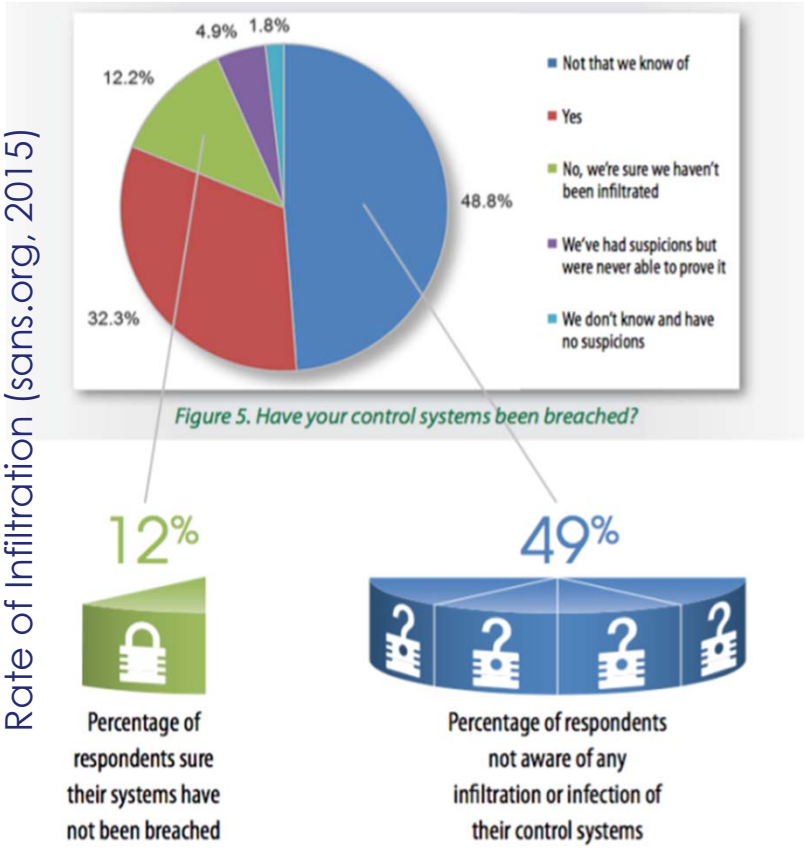
THALES

Backup

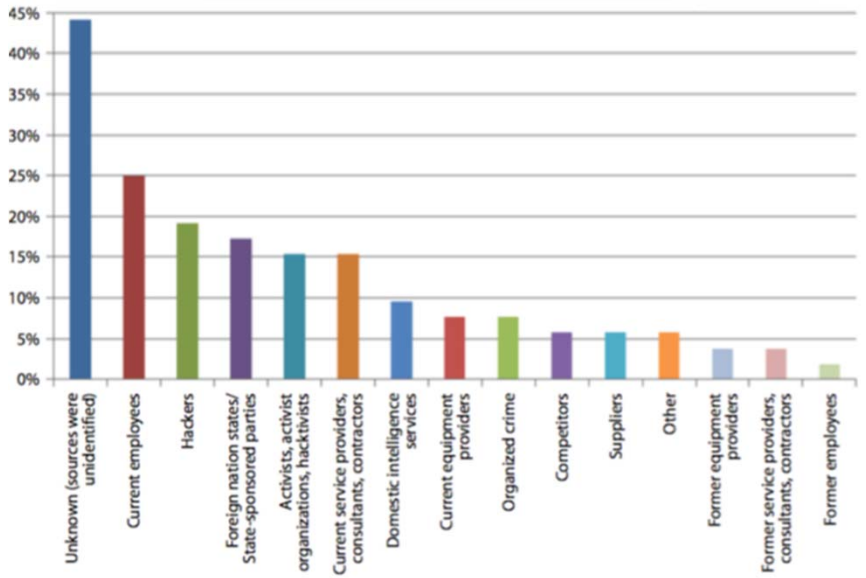


Infiltration Rate & Source

Rate of Infiltration (sans.org, 2015)

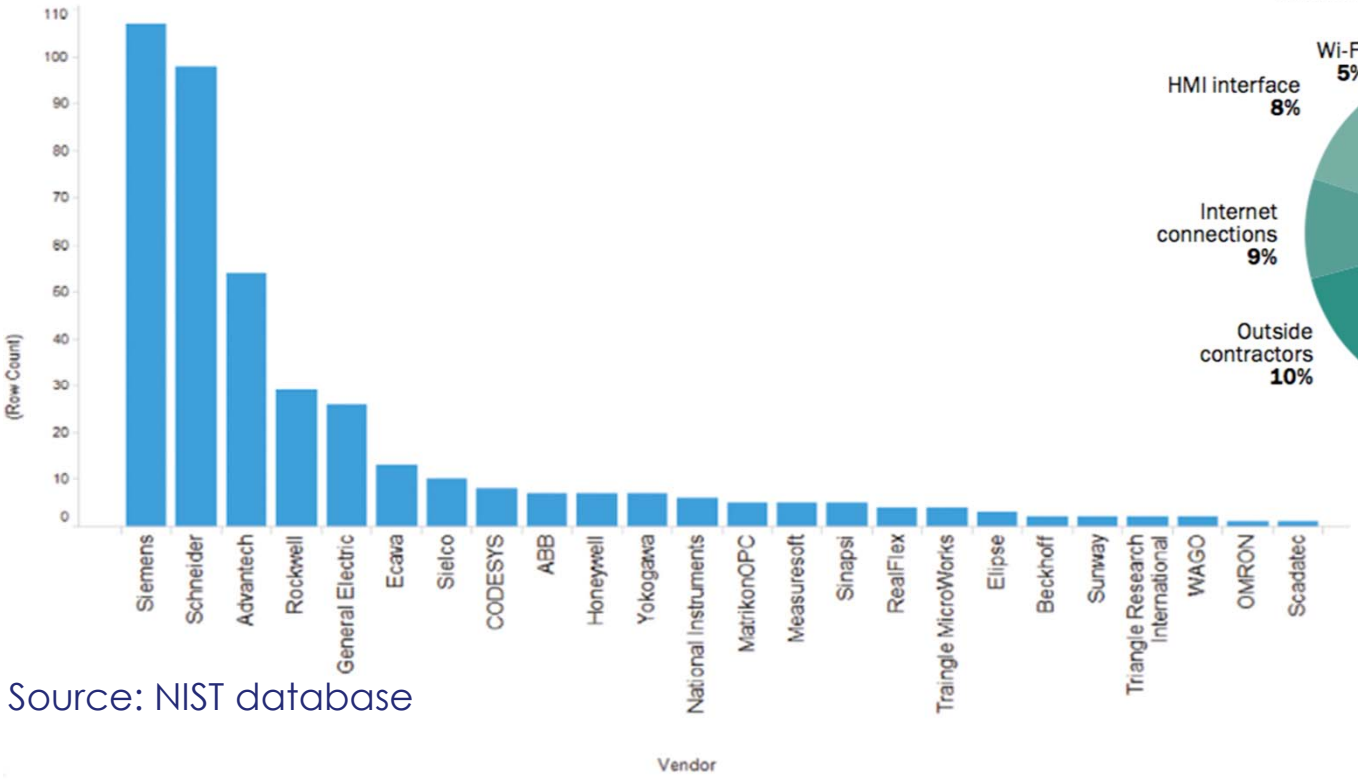


Source of Infiltration (sans.org, 2015)



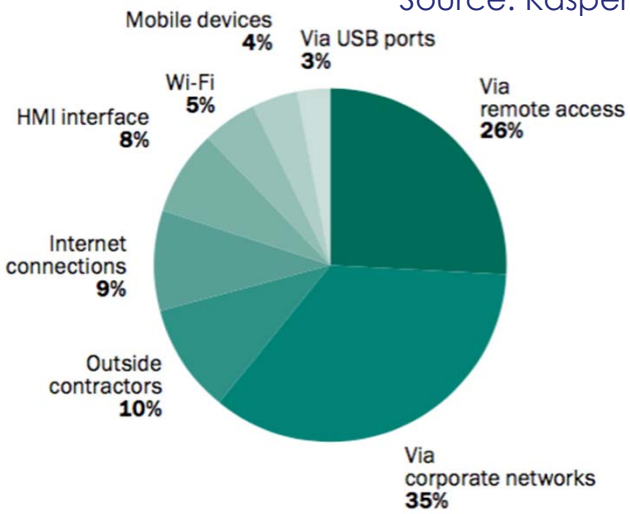
THALES

Vulnerabilities



Source: NIST database

Source: Kaspersky



THALES

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