## THALES

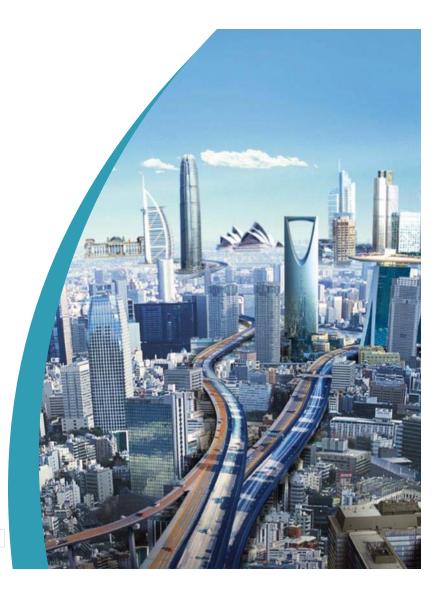
## Safety and Security in **Ground Transportation Systems**

Michael Paulitsch, Thales, Vienna, Austria

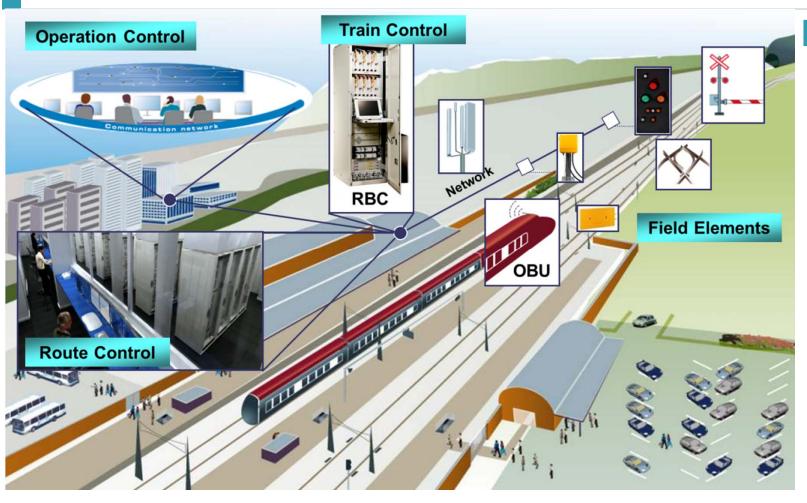
This work has been partially funded from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731456 (certMILS.eu).



www.thalesgroup.com



## 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 <u>operational disruption</u> (availability), access to <u>user confidential data</u>, and ensure <u>safety</u> is not impaired (system integrity).

M Paulitsch - Safety and Security in GTS



## Main CENELEC Standards for Signalling Applications – Safety

- EN 50126: The Specification and Demonstration of Reliability, Availability, Maintainability and Safety
- <u>EN 50128</u>: Communications, Signalling and Processing Systems – Software for Railway Control and Protection systems.
- <u>EN 50129</u>: Communications, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling.
- <u>EN50159</u>: 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 <sup>-9</sup> ≤ THR < 10 <sup>-8</sup>	4
10 <sup>-8</sup> ≤ THR < 10 <sup>-7</sup>	3
10 <sup>-7</sup> ≤ THR < 10 <sup>-6</sup>	2
10 <sup>-6</sup> ≤ THR < 10 <sup>-5</sup>	1

EN 50129:2003 excerpt – Safety Integrity Levels

THR ... tolerable hazard rate



- 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)

    Structure of Safety Case EN50129
  - **▶ Part 6** Conclusion *summarizes evidences*

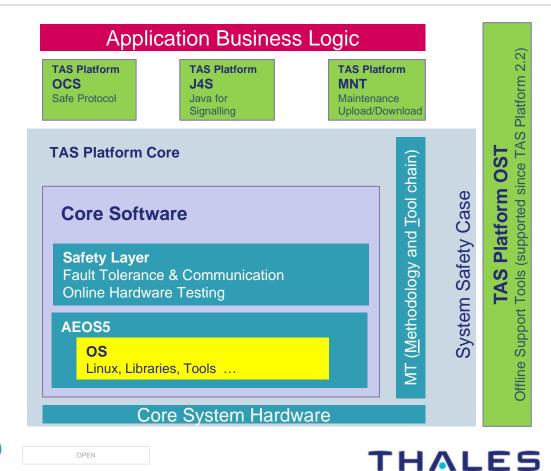
Chapter 1 Chapter 2 Chapter 3 Chapter 4 Chapter 5 Chapter 6

Definition of the system Management Report Report Report Report Cases

## TAS Platform - Safe Computation and Communication

Expandable Managed Critical Service Safe Execution Framework Life Cycle Support Functions gnalling ware independent Enables Tools for Sic ...ng applica AzLM Customer Development Safe Support Support Maintenance Communi-Ct cation Applications Manage Core Method & Tools Software (OS, J4S MNT&Download Safety Layers, S S OCS (Communication) 8 Packages) Support Deliver PLF Core (OS) velop. Managed Computing PLF Hardware (Boards)  $\geq 0$ Boards OPEN M Paulitsch - Safety and Security in GTS

- 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)



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

ETCS Interlocking On Board Field Elements

**TAS Platform System Safety Case Safety Application** TAS Platform Services Conditions TAS Platform Engineering & Environment **Safety Application** Safety Application **HW Core System** Core System TAS Platform SW Conditions (SAC) Conditions (SAC) Analyses Subsystems: OCS, MNT, J4S HW components SW components erification/Valid. Check of HW-CS SAC Analyses Analyses Safety Case Validation on HW-CS Verification Verification / Validation Manufacturing Approval with HW-CS Validation Manufacturing Approval

Distributed Development / Maintenance (Thales AT / TTS Germany)

## **Example: "TAS Platform in Used in Interlocking Configuration**



Interlocking

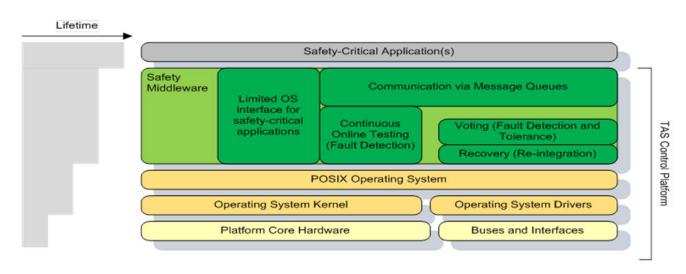


Onboard System (ETCS)



#### 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



## 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 <u>fixed</u> during their lifetime;
  - Category 2 consists of systems which are <u>partly unknown</u> or not fixed, however unauthorised access can be excluded;
  - Category 3 consists of systems which are <u>not under the control</u> of the designer, and where unauthorised access has to be considered.
- Categories implicitly address some security aspects



## 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.





## **Strategies**

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



Source: US dept of Homeland Security



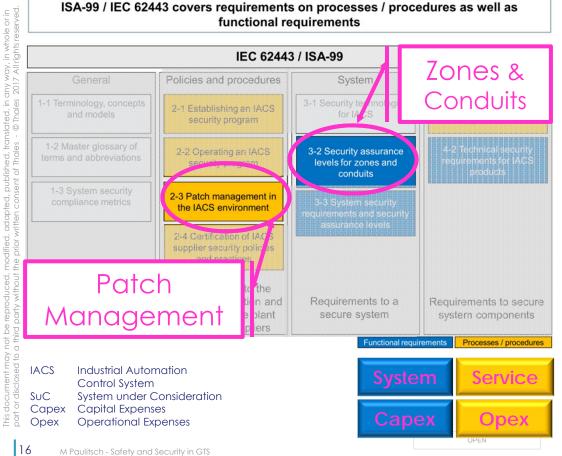
## IEC 62443 - An Applicable Security Standard

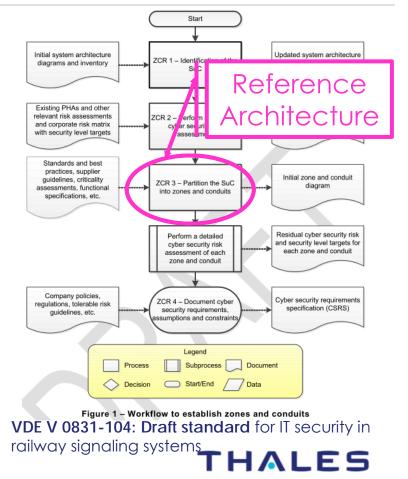
ISA-99 / IEC 62443 covers requirements on processes / procedures as well as functional requirements

IEC 62443 / ISA-99 Policies and procedures Component General System 1-1 Terminology, concepts 3-1 Security technologies 2-1 Establishing an IACS 4-1 Product development and models for IACS security program requirements 1-2 Master glossary of 4-2 Technical security 2-2 Operating an IACS 3-2 Security assurance terms and abbreviations requirements for IACS levels for zones and security program products conduits 1-3 System security 2-3 Patch management in compliance metrics 3-3 System security the IACS environment requirements and security assurance levels 2-4 Certification of IACS supplier security policies and practices Requirements to the Definitions security organization and Requirements to a Requirements to secure Metrics processes of the plant secure system system components owner and suppliers Functional requirements Processes / procedures Helpful in checking completeness



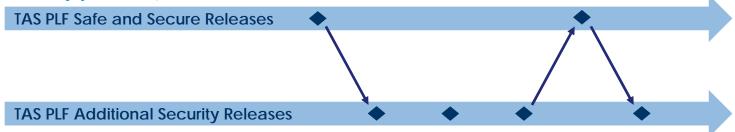
## Chances & Challenges - IEC 62443 for VDE V 0831-104





## 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 <u>balance between measures against systematic errors and measures against security</u> 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)
- **Bug Fix Release (on demand)** Last Maintenance Release **Maintenance Release** YEAR+1 Inputs from **Project Start** Closure Update "Developer Customers, CQDs Update Release Release" Release Roadmap Roadmap EQ2 each year Update **Update Meeting** Meeting
- 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 OS Objectives**

## **OS Objectives Security**

#### **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)

#### COTS software

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

#### Monitor vulnerabilities

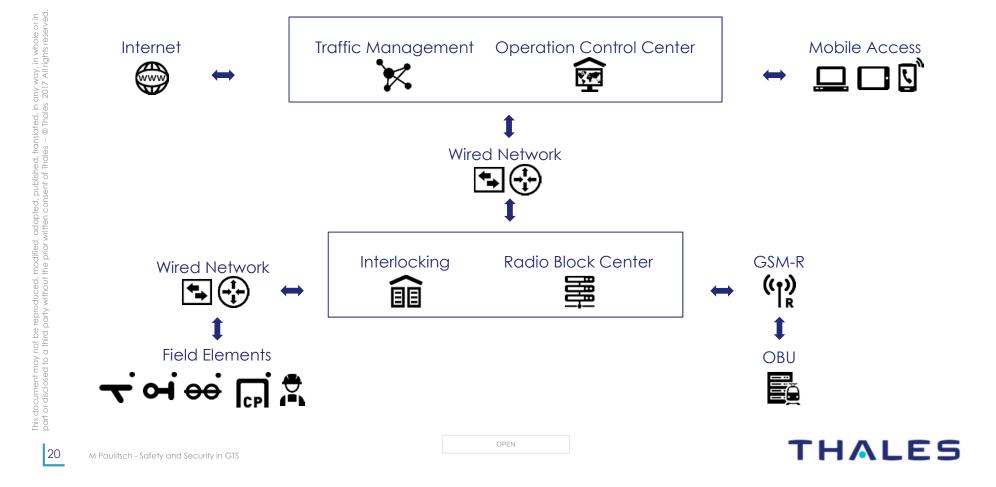
Identify bugs that could lead to security breach

### Least functionality

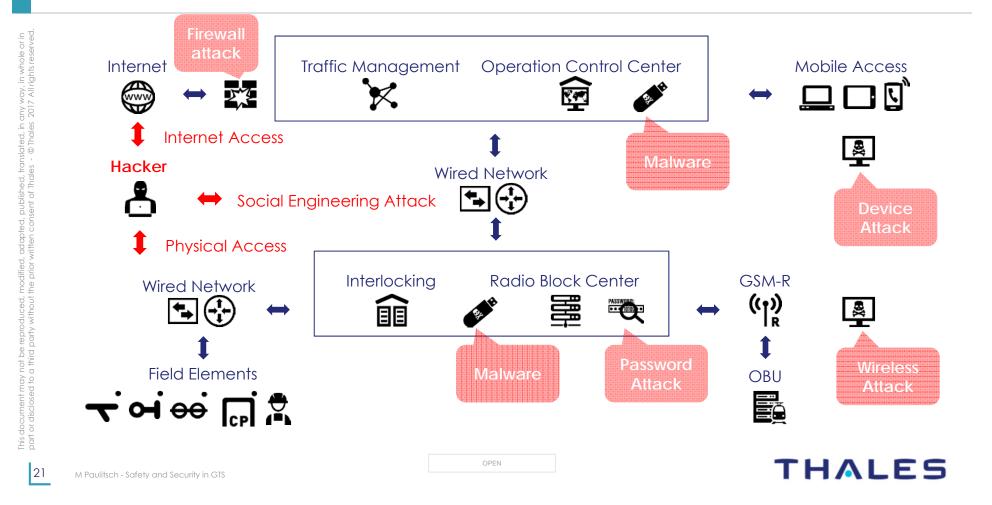
> Reduce attack vector

Some Objectives of Security and Safety Match

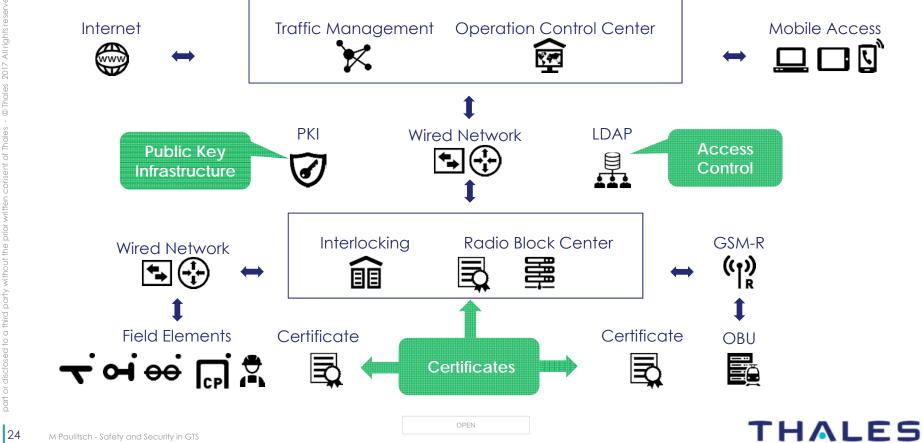
## Areas of Possible Vulnerabilities in Rail Systems ...



## Areas of Possible Attacks in Rail Systems...

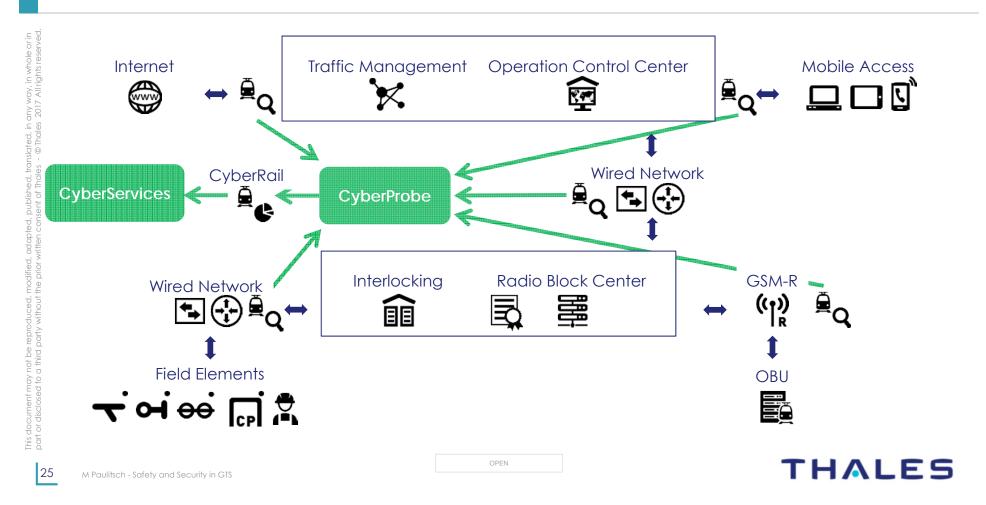


## **Examples of Areas to Protect Access in Rail Systems**

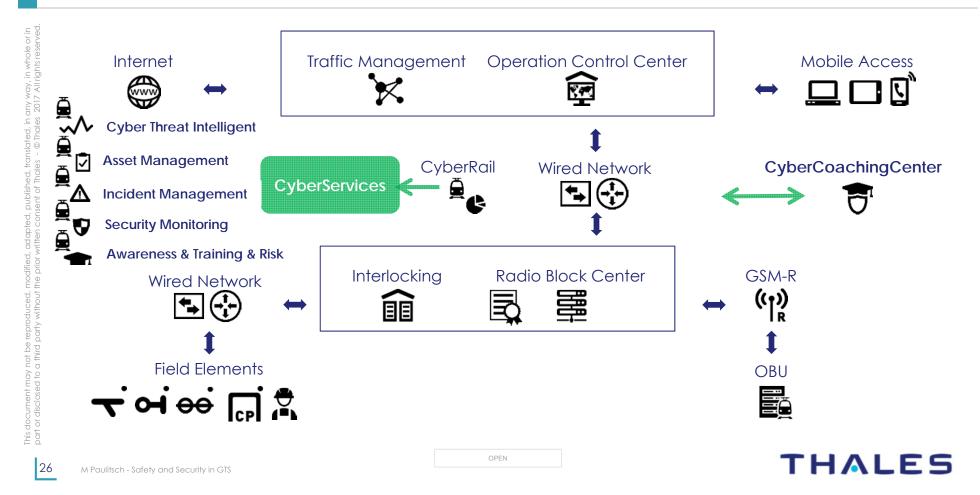


ns document may not be reproduced, modified, adapted, published, franslated, in any way, in whole of a disclosed to a third party without the prior written consent of Thales. - @ Thales. 2017 All riahts rese

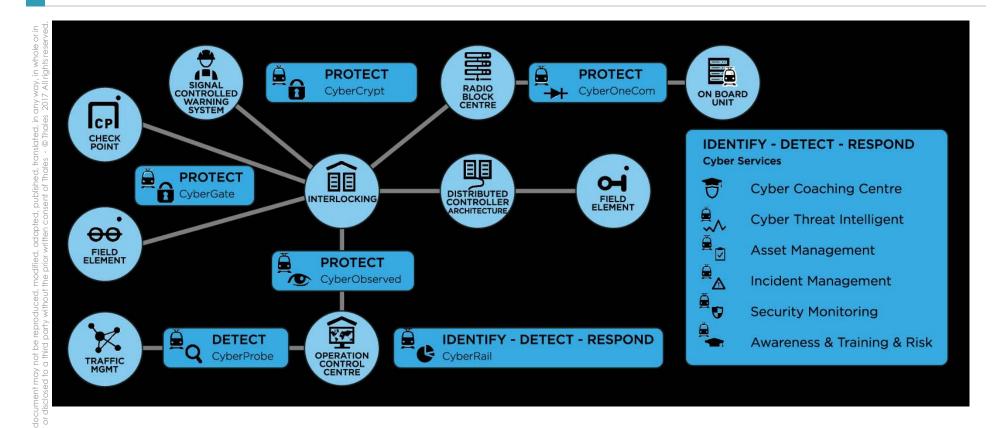
## **Examples of Areas to Monitor Security in Rail Systems**



## **Examples of Areas for Security Services in Rail Systems**



## Thales Cyber Security Reference Architecture CySecTrac



27 M Paulitsch - S



## 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

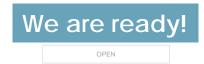




## **Summary**



- 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 extensionssimple 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 ...





## **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: <a href="mailto:coordination@certmils.eu">coordination@certmils.eu</a>

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.

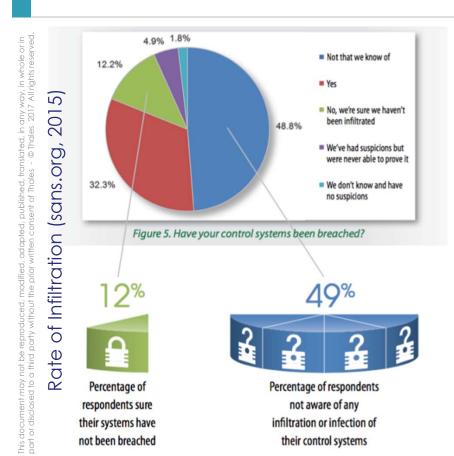


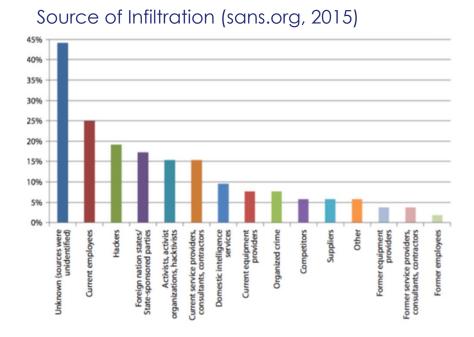
# THALES

# Backup

OPEN
THALES GROUP INTERNAL
THALES GROUP CONFIDENTIAL
THALES GROUP SECRET

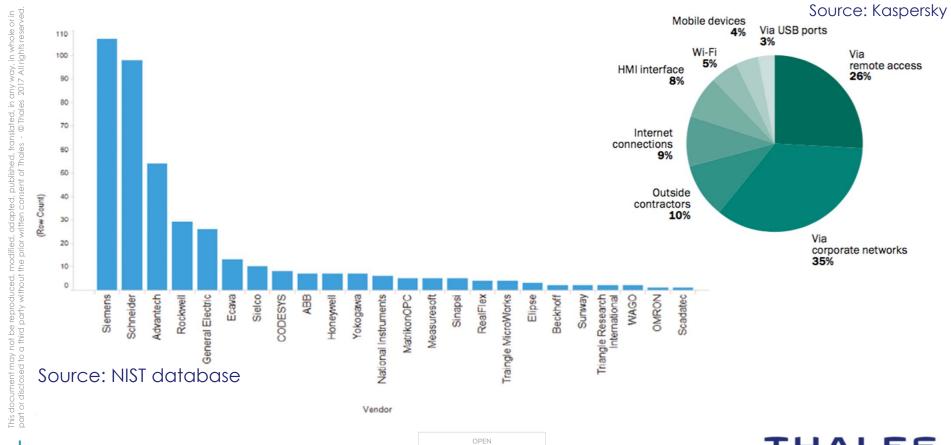
### **Infiltration Rate & Source**





THALES

## **Vulnerabilities**



## 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



