Digitalization in Urban Transportation

A Cybersecurity Approach to Connected Urban Transport

Kees Pouw – Urban Rail Signalling

23 October 2017

Presentation Objectives

Discuss Digitalization in Urban Transport and the Drivers for Cybersecurity

Explain What Thales is doing to Address the cybersecurity challenge

Identify the Intersect of Functional Safety and Cybersecurity Disciplines

We are no longer confined to the Four Walls

It is all about enabling the business

Supporting the next generation of connectivity and technologies

- CBTC new features and innovation depend upon cybersecurity and the ability of leveraging public networks in a secure way. Examples Include:
  - Remote Terminals – web browser viewing of status information
  - Use of tablets by maintainers
  - Use of WiMAX and LTE as a secondary link to the private wireless network
- Cloud Computing
- Bid Data and Data Analytics (Cognitive Computing)

Supporting Clients High Assurance Needs

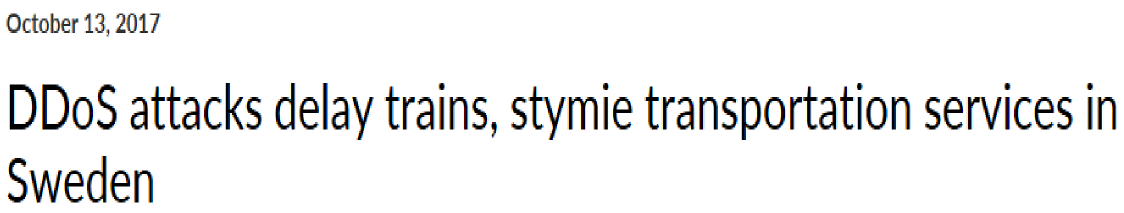
- Continuous risk assessment
- Disaster Recovery
- Patching

And the Threat Landscape has changed Significantly

Cyber threats are everywhere, more sophisticated, larger

« TV5 Monde knocked down by 'Russian based' hackers » April 2015

« FBI says hacker took over a plane through its in flight entertainment system » May 2015



October 13, 2017

DDoS attacks delay trains, stymie transportation services in Sweden

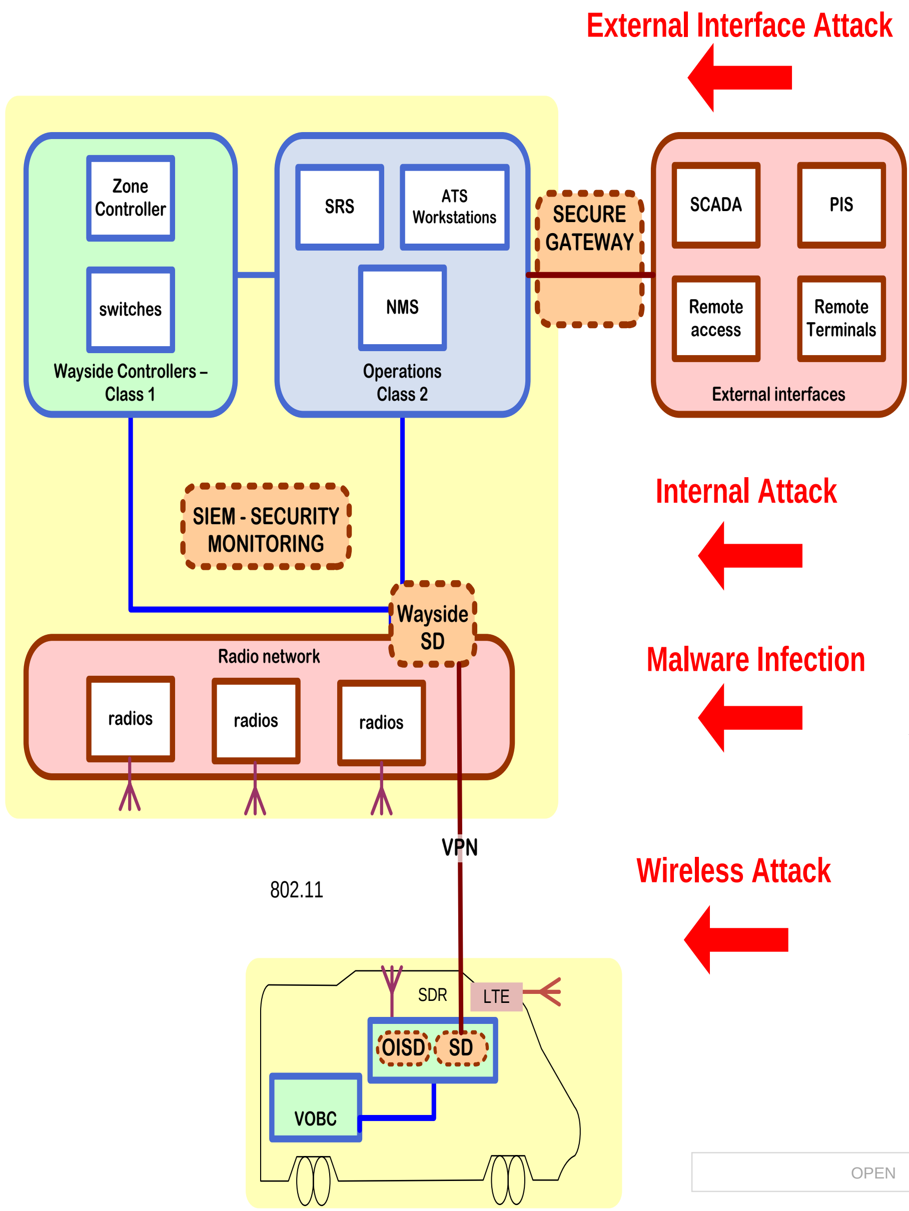
Cybercrime

« WannaCry»

Massive ransomware cyber-attack hits nearly 100 countries around the world

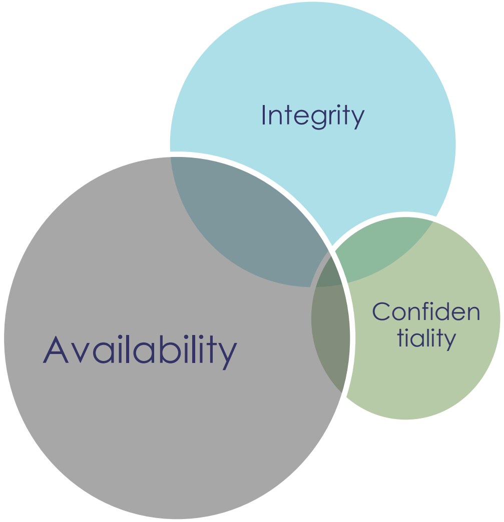
As the world becomes digital,
no safety or security without cybersecurity

Cybersecurity Threats – What does it mean to the Rail Signaling?



Safety Protection against EN 50159Threats: Repetition, Masquerading, etc.

Security Objectives



Prevent Impact to operations (localized virus infection) to complete shutdown (e.g. self propagating worm, full hacking compromise)

Protect Thales and customer reputation and public trust

OPEN

Digitalization in Urban Transport and the Drivers for Cybersecurity

What Thales is doing to Address the cybersecurity challenge

Intersect and common interest of Safety and Cybersecurity Disciplines

What Are We Doing About it?

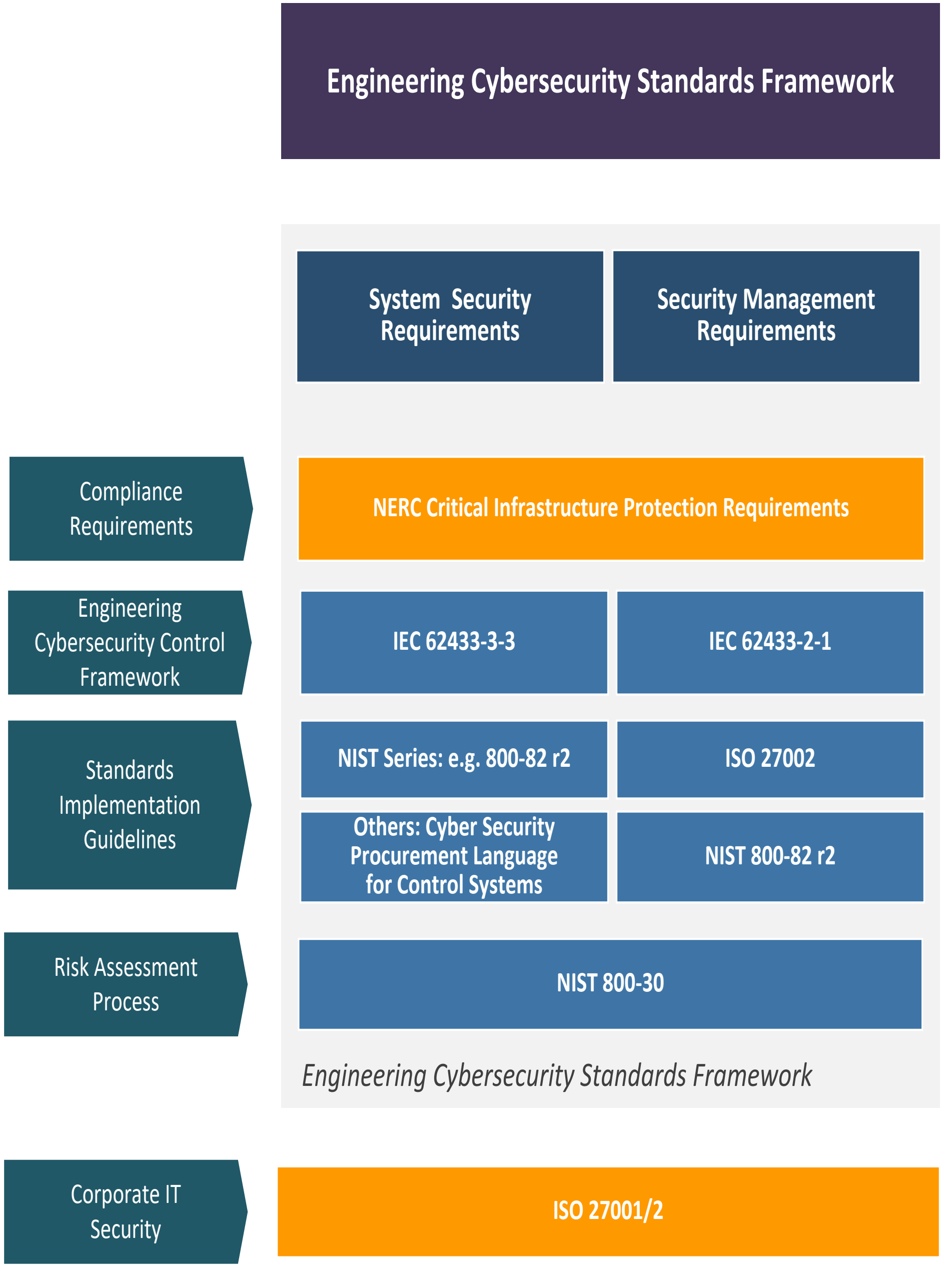
Cybersecurity Engineering Assurance Process

- Adopting Cybersecurity Standards
- Defining Policy and Procedures

Secure by Design

- Building Cybersecurity Building Blocks
- Developing Deployment Patterns

Cybersecurity Assurance – Adopting Cybersecurity Standards



Engineering Cybersecurity Standards Framework

System Security Requirements

Security Management Requirements

Compliance Requirements

NERC Critical Infrastructure Protection Requirements

Engineering Cybersecurity Control Framework

IEC 62433-3-3

IEC 62433-2-1

Standards Implementation Guidelines

NIST Series: e.g. 800-82 r2

ISO 27002

Others: Cyber Security Procurement Language for Control Systems

NIST 800-82 r2

Risk Assessment Process

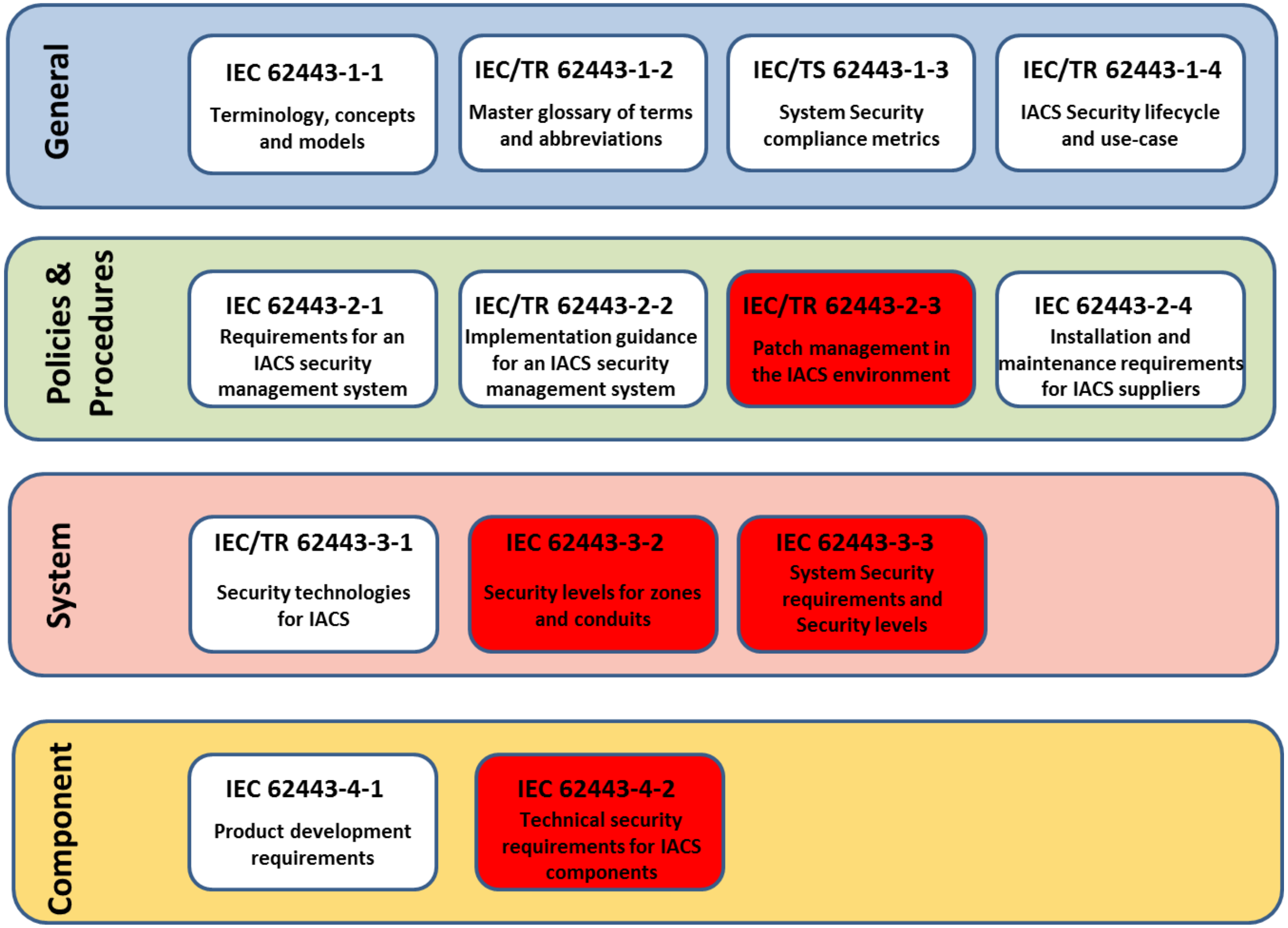
NIST 800-30

Engineering Cybersecurity Standards Framework

Corporate IT Security

ISO 27001/2

Cybersecurity Assurance – IEC Standard Framework



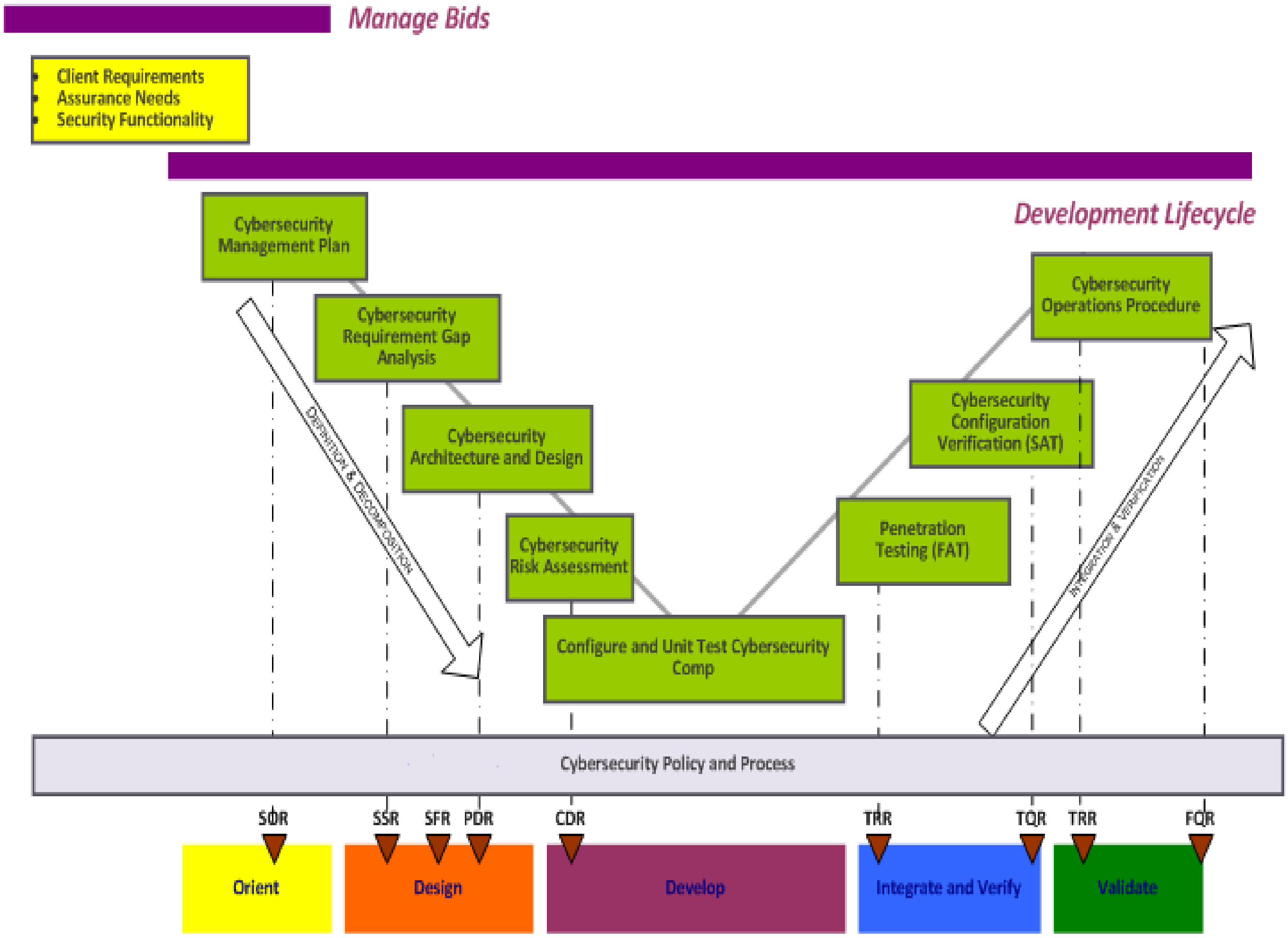
General	IEC 62443-1-1 Terminology, concepts and models	IEC/TR 62443-1-2 Master glossary of terms and abbreviations	IEC/TS 62443-1-3 System Security compliance metrics	IEC/TR 62443-1-4 IACS Security lifecycle and use-case
Policies & Procedures	IEC 62443-2-1 Requirements for an IACS security management system	IEC/TR 62443-2-2 Implementation guidance for an IACS security management system	IEC/TR 62443-2-3 Patch management in the IACS environment	IEC 62443-2-4 Installation and maintenance requirements for IACS suppliers
System	IEC/TR 62443-3-1 Security technologies for IACS	IEC 62443-3-2 Security levels for zones and conduits	IEC 62443-3-3 System Security requirements and Security levels	
Component	IEC 62443-4-1 Product development requirements	IEC 62443-4-2 Technical security requirements for IACS components		

- IEC/TR 62443-2-3 patch management *Because Security is a "moving target" patch management is essential (especially for systems developed without Security).*

- IEC 62443-3-2 and 62443-3-3 identifying the Security requirements for our system.

- IEC 62443-4-2: Detailed technical requirements for IACS components level. Helps finding the right Security products for the Security requirements defined above.

Cybersecurity Assurance – Cybersecurity Engineering Process


Manage Bids
Client Requirements
Assurance Needs
Security Functionality
Development Lifecycle
Cybersecurity Management Plan
Cybersecurity Requirement Gap Analysis
Cybersecurity Architecture and Design
Cybersecurity Risk Assessment
Configure and Unit Test Cybersecurity Comp
Penetration Testing (FAT)
Cybersecurity Configuration Verification (SAT)
Cybersecurity Operations Procedure
DEFINITION & DECOMPOSITION
INTEGRATION & VERIFICATION
Cybersecurity Policy and Process
SOR
SSR
SFR
PDR
CDR
TRR
TQR
TRR
FQR
Orient
Design
Develop
Integrate and Verify
Validate

DDQS - Design, Develop and Qualify the Solution

What Are We Doing About it?

Cybersecurity Engineering Assurance Process

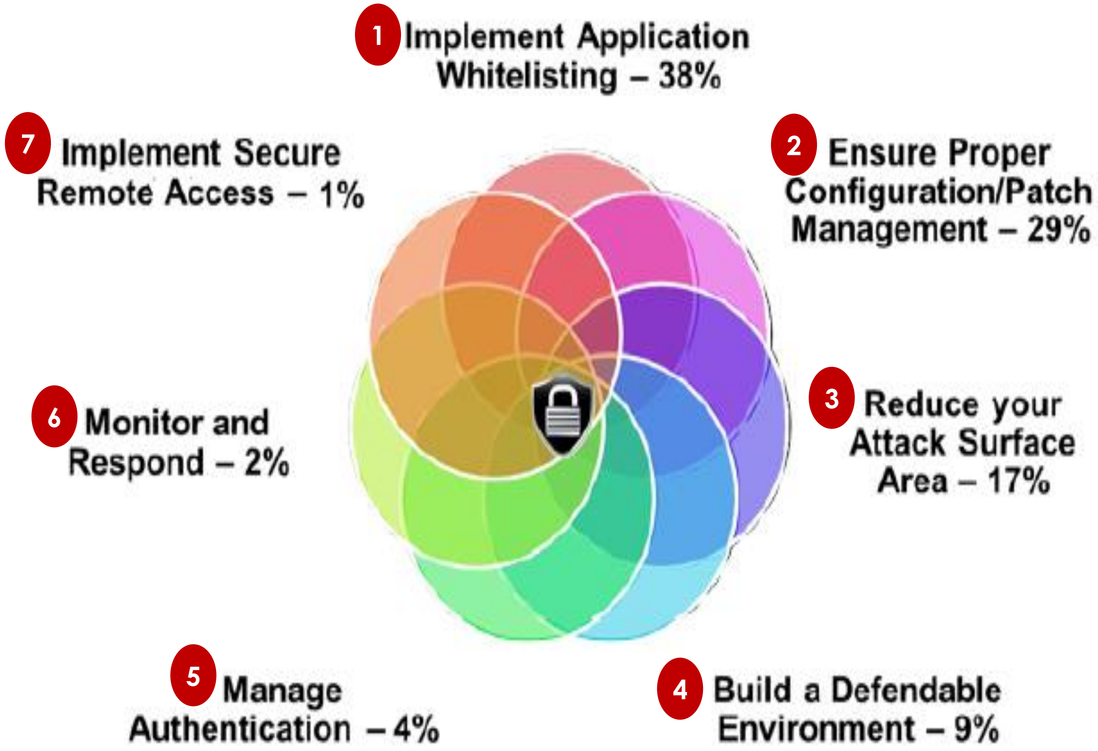
- Adopting Cybersecurity Standards
- Defining Policy and Procedures

Secure by Design

- Applying Design Patterns
- Developing Cybersecurity Building Blocks

Applying Design Patterns - 7 Cyber Defense Strategies for Control Systems

- Based on the incidents reported to ICS-CERT, the percentage of reported incidents in FY 2014/15 that can be mitigated by each strategy to counter common exploitable weakness in "as-built" control systems is concluded as below :



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

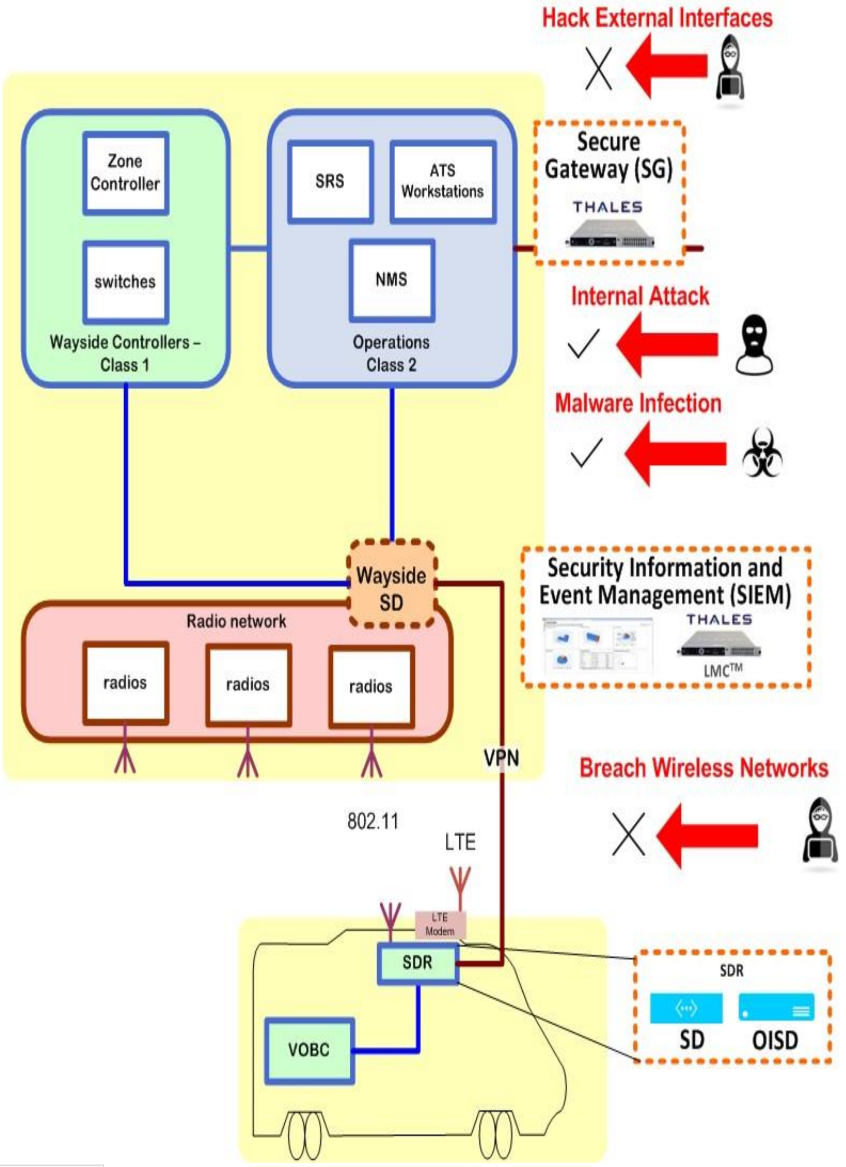
Source: Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) FY14/15 reported incidents research

Thales Cybersecurity Enhanced Solutions

- **Secure Interface Gateway (SIG) –** Provides secure application level filtering for interfacing with external system such as SCADA and PIS

- **rail Security Information and Event Management Solution (rSIEM) –** Provide logging and monitoring services and threat detection and prevention (multi- layer): cyberattacks, malware. A searchable central log repository with alerting capabilities to the NMS

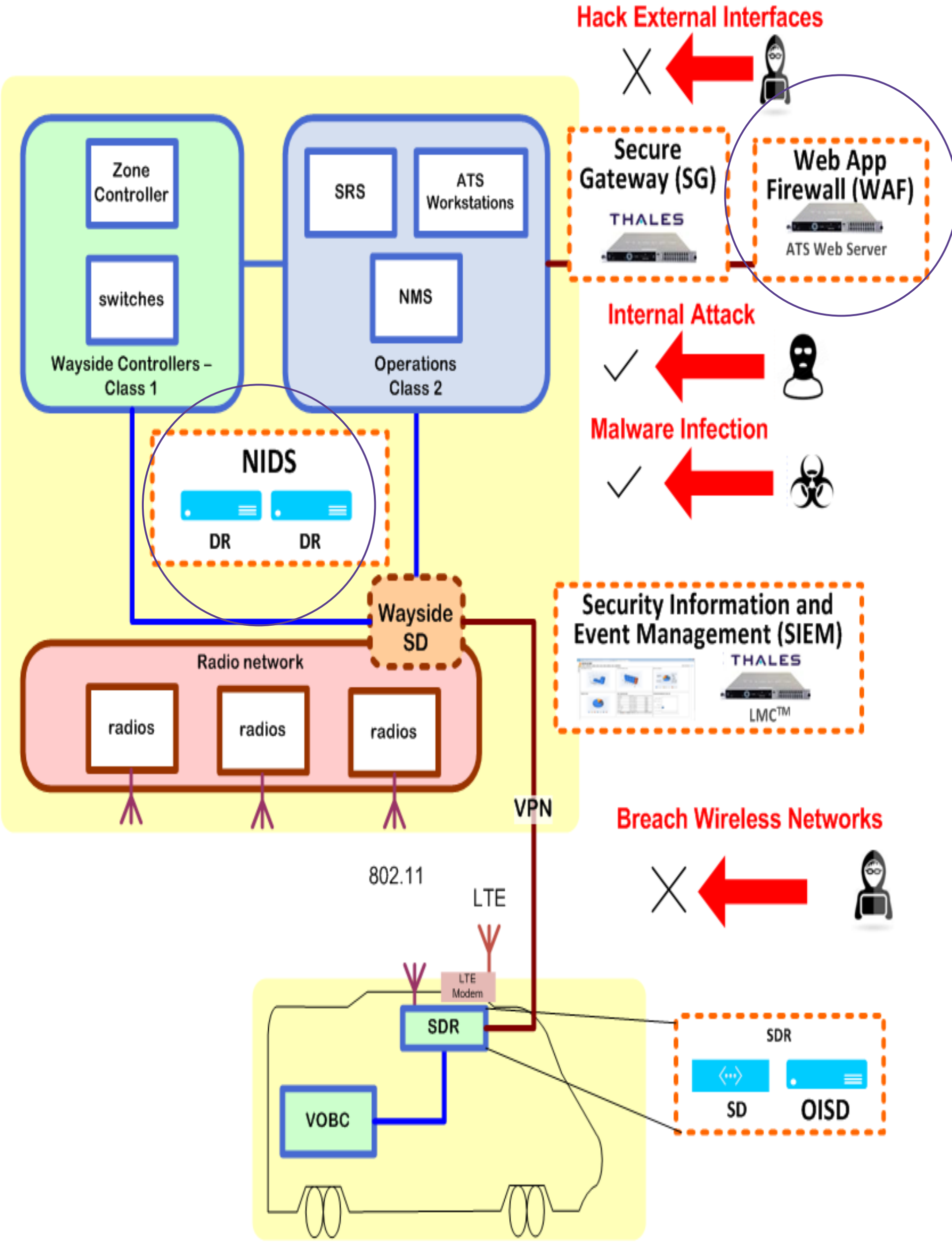
- **Onboard Internet Security Device (OISD)** – Additional SD (Encryption) functions such as multi-layer firewall and Hosting Intrusion Detection Prevention and remote logging to protect against public wireless networks



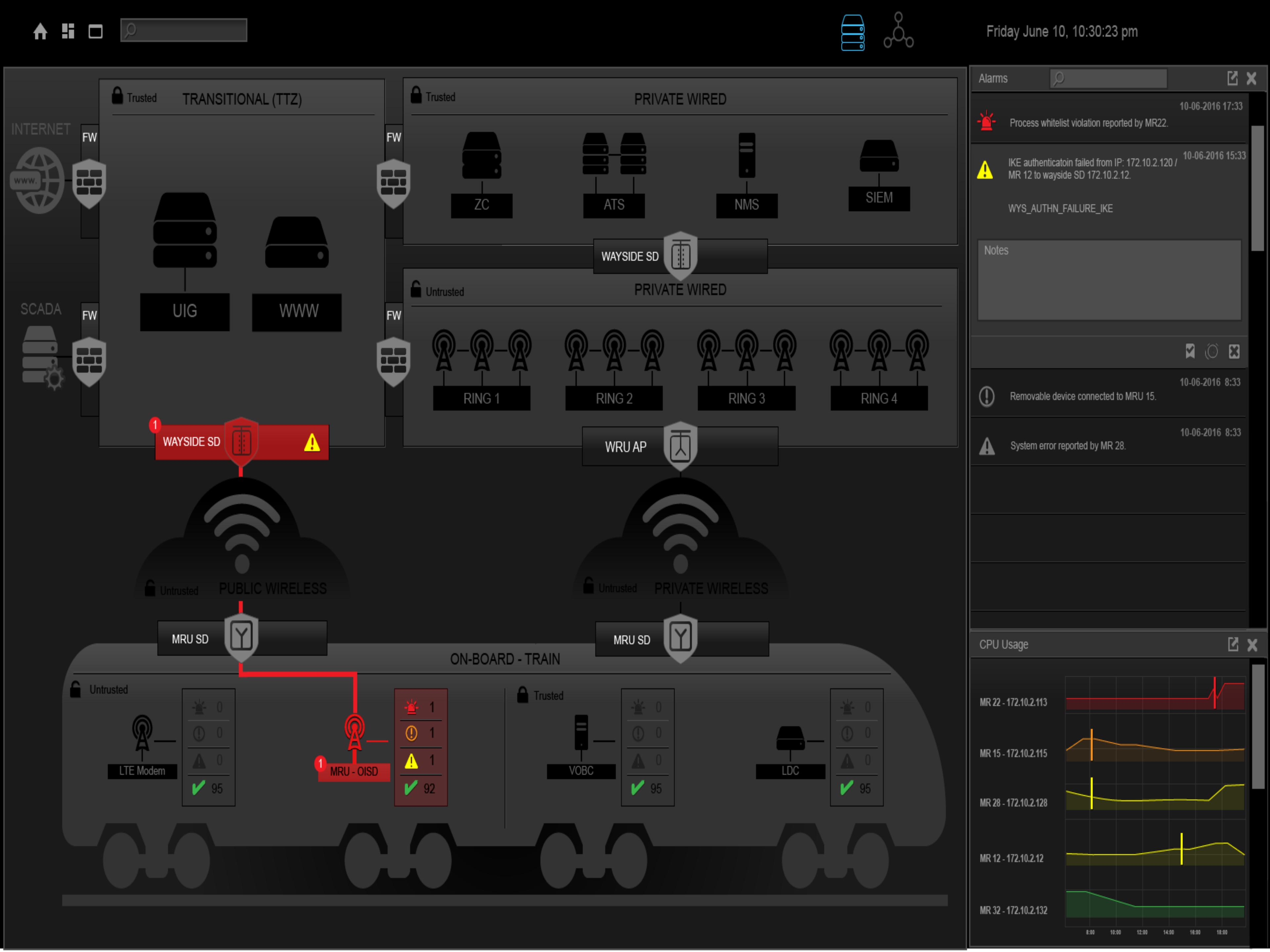
Thales Cybersecurity Enhanced Solutions

- **Web Application Firewall (WAF) –** Deployed in addition to the Secure Gateway (SG) when a web interface is exposed (ATS Web Terminal). It protects the web from defacement and adds an additional layer of protection (defense in depth).

- **Network Intrusion Detection (NIDS) –** The NIDS provides sophisticated detection capabilities in combination with the SIEM. It whitelists all network traffic and reports on any anomaly.



OP



Alarms

10-06-2016 17:33
Process whitelist violation reported by MR22.

10-06-2016 15:33
IKE authenticatoin failed from IP: 172.10.2.120 / MR 12 to wayside SD 172.10.2.12.

WYS_AUTHN_FAILURE_IKE

Notes

10-06-2016 8:33
Removable device connected to MRU 15.

10-06-2016 8:33
System error reported by MR 28.

CPU Usage

Digitalization in Urban Transport and the Drivers for Cybersecurity

What Thales is doing to Address the cybersecurity challenge

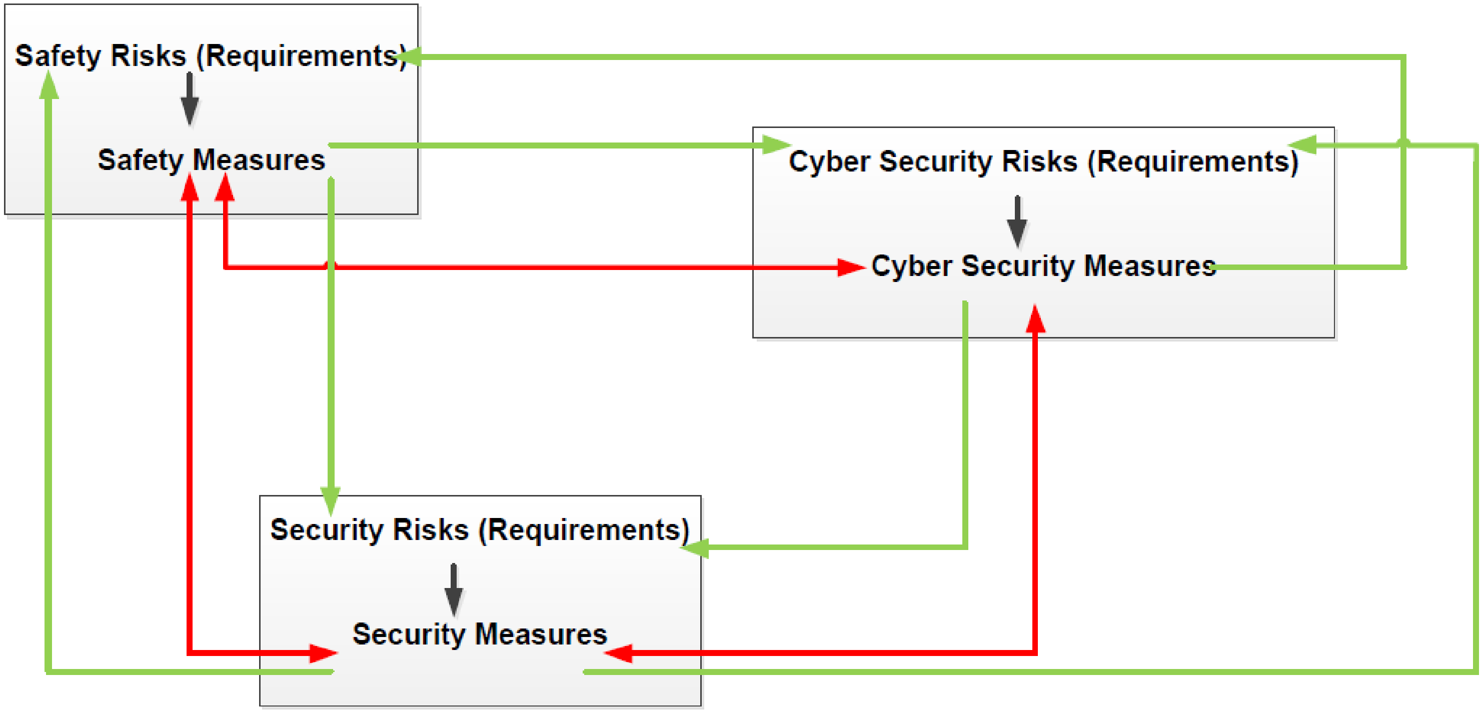
Intersect of Functional Safety and Cybersecurity Disciplines

Bridging the Gap of Functional Safety and Cybersecurity

	Functional Safety	Mapping Cybersecurity and Safety	Cybersecurity
Industrial Automation and Control	**IEC 61508** *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*	**IEC 63069** *IEC Framework for functional Safety and security*	**IEC 62443** *Security for Industrial Automation and Control Systems*
Rail signalling	**EN 50129** *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*		**EN ???** Cybersecurity for Rail

Interactions between Functional-Safety / Cybersecurity

- It is crucial to map security risk that affect safety controls into Safety Hazzards


Safety Risks (Requirements)
Safety Measures
Cyber Security Risks (Requirements)
Cyber Security Measures
Security Risks (Requirements)
Security Measures

Any measures corresponding to a specific set of requirements might affect other requirements : →

Measures might affect each other : ↔

Distinct Approaches

1- Functional safety is a near-hard science, Cybersecurity is more informal

- Functional Safety Assurance aims at exhaustiveness, and does widely resort to quantification
- Cybersecurity relies heavily on qualitative risk assessment (not quantitative).

2- Cybersecurity threat patterns are constantly evolving

- Safety Hazard initial causes and triggers are stable (and most of them standardized).
- Cybersecurity threats are evolving, and the operator has to define which level of threats he want to get protected against (from script-kiddies to state organizations) . Cost is here a key driver.

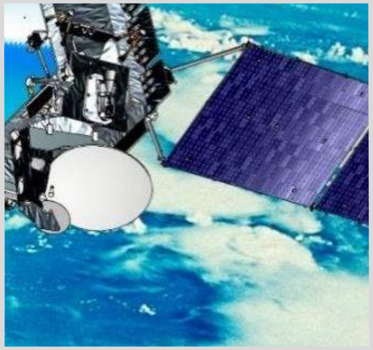
3- Cybersecurity permits more system level trade-offs than functional safety

- One could define not to protect the main safe operating system if there is a simple and robust fallback system (e.g. use manual driving and signals instead of CBTC
- Safety is not an option (thus it is already implemented in legacy systems)

Thales group

AEROSPACE

SPACE



GROUND TRANSPORTATION

DEFENCE

CYBERSECURITY

- 61,000 employees
- Revenues: 13 billion euros
- Over 20,000 engineers and researchers
- Operations in 56 countries

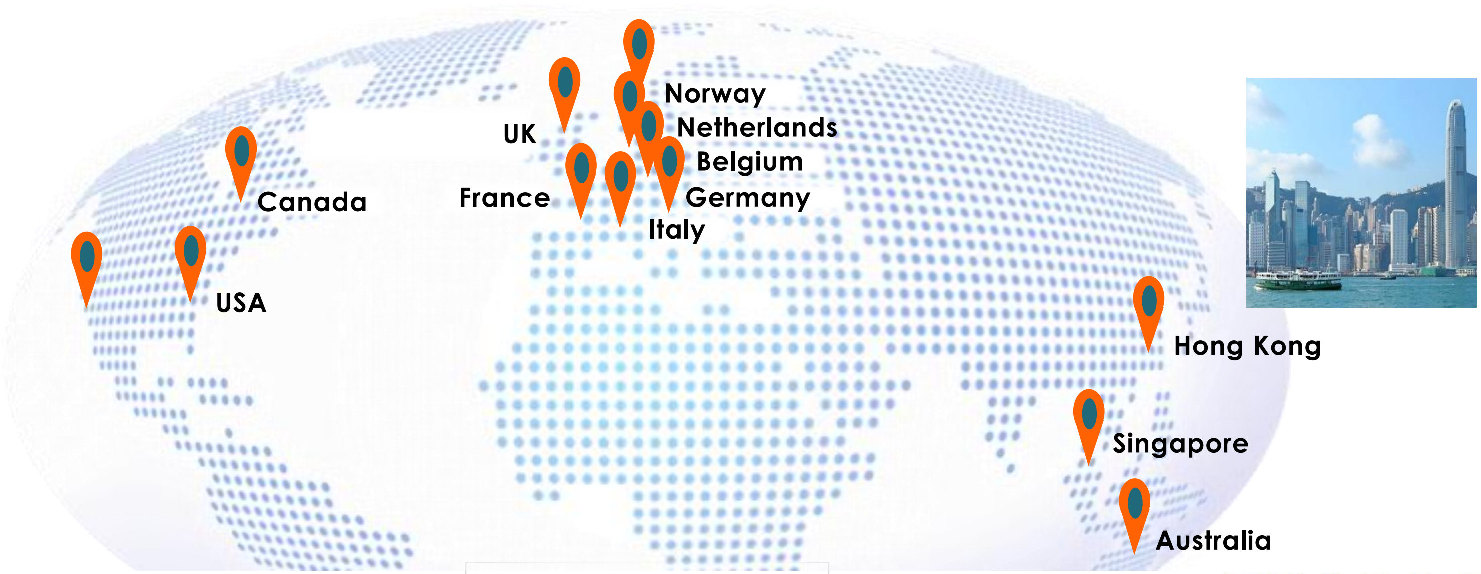
Wherever safety and security are critical, Thales delivers.
We innovate with our customers to build smarter solutions. Everywhere.

THALES

Together • Safer • Everywhere

Thales Critical Information and Cyber Security

- **5,000** IT and **security engineers,** including **1,500 cybersecurity experts**
- **5 Security Operation Centres:** 2 in France **(24/7)**, 1 in United Kingdom, 1 in Netherlands and 1 in Hong Kong
- **5** high-security **data-centres** in France and in the United Kingdom
- **High-grade security products** (confidential or top secret) for **50 countries**, including NATO countries
- Enterprise solutions and products for 200 customers, including protection of **80% of the world's banking transactions.** Security for **19 of the world's 20 largest banks**
- **Operation and supervision** of critical information systems for more than **100 customers**



Thank You
Questions

WHEREVER SAFETY AND SECURITY ARE CRITICAL, THALES DELIVERS