Digitalization in Urban Transportation
A Cybersecurity Approach to Connected Urban Transport

Kees Pouw – Urban Rail Signalling

23 October 2017
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?

- **Security Objectives**
  - Integrity
  - Availability
  - Confidentiality

**External Interface Attack**

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

**Internal Attack**

- Malware Infection

**Wireless Attack**

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

**Operations Class 2**
- External interfaces
- Wayside Controllers – Class 1
- Radio network
- Zone Controller
- Switches
- SRS
- ATS Workstations
- NMS
- Operations Class 2

**Operations Class 1**
- Remote access
- Remote Terminals
- SCADA
- PIS

**External Interfaces**
- Wayside Controllers
- Radio network
- VOBC
- 802.11
- SD
- LTE
- SDR
- NMS
- Remote access
- Remote Terminals
- SCADA
- PIS

**Siem - Security Monitoring**

**Remote Access**

**Remote Terminals**

**Secure Gateway**

**Vpn**

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party, without the prior written consent of Thales – © Thales 2015 All rights reserved.
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
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.
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 systems 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 Hosted 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.
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

<table>
<thead>
<tr>
<th>Industrial Automation and Control</th>
<th>Functional Safety</th>
<th>Mapping Cybersecurity and Safety</th>
<th>Cybersecurity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rail signalling</td>
<td>EN 50129. Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling</td>
<td></td>
<td>EN ??? Cybersecurity for Rail</td>
</tr>
</tbody>
</table>
It is crucial to map security risk that affect safety controls into Safety Hazzards.
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)
Wherever safety and security are critical, Thales delivers.
We innovate with our customers to build smarter solutions. Everywhere.
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
WHEREVER SAFETY AND SECURITY ARE CRITICAL, THALES DELIVERS