# IT Risk Management and Security Architecture in Trains

Gertjan Tamis, Information Security Officer

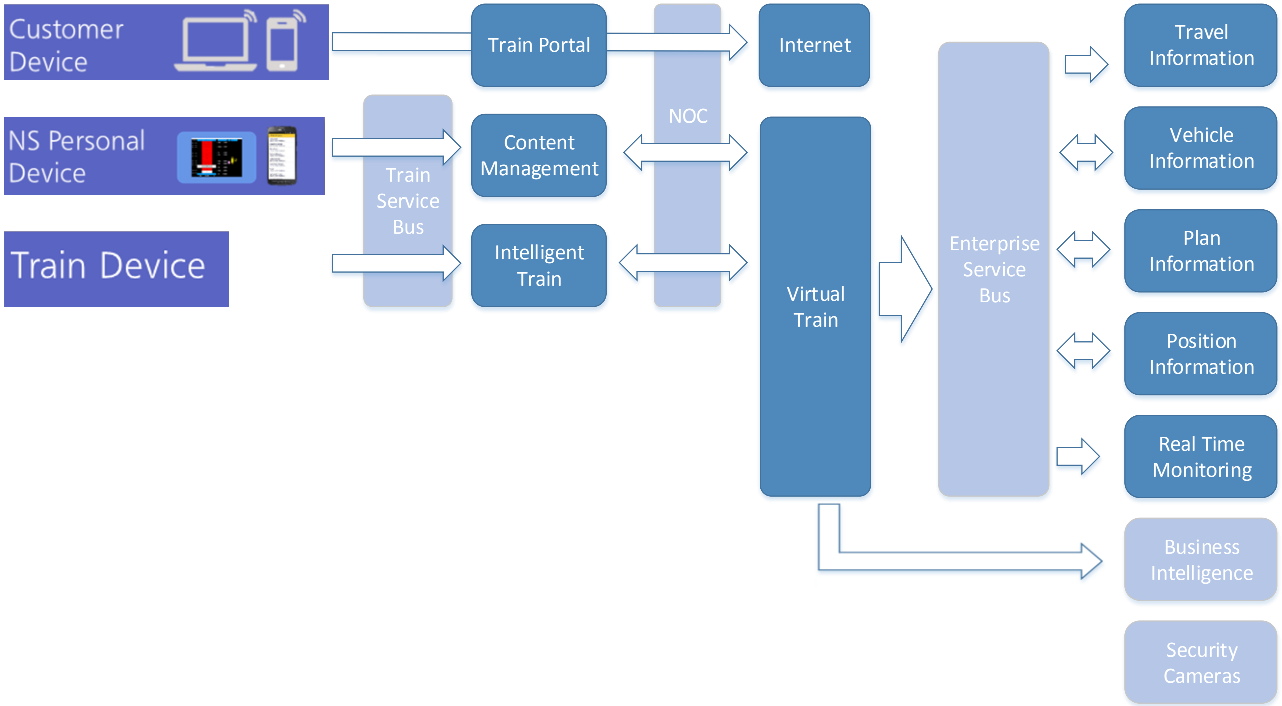
Nederlandse Spoorwegen

**CyberSecurity4Rail Conference**
**Brussel, 2017**

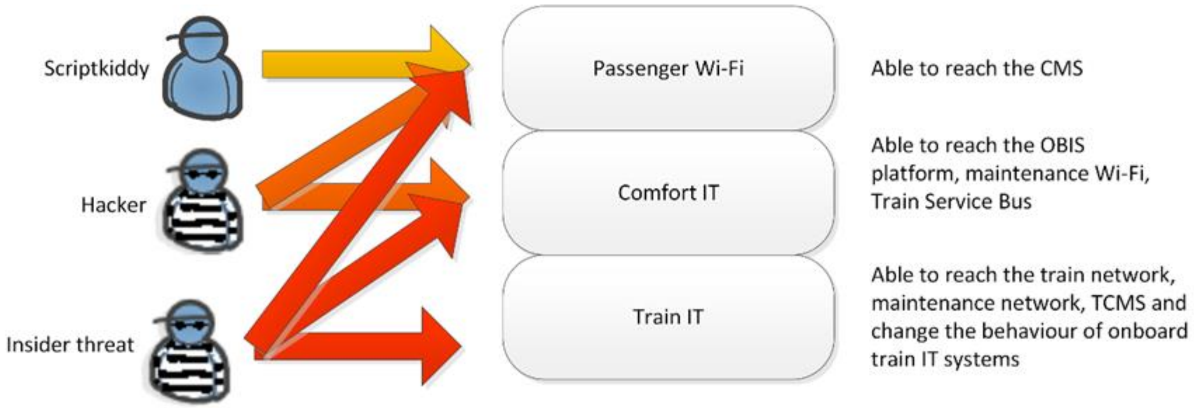
# Agenda

- Setting the scene
- Where is the risk
  - Mitigation strategies
- Prevention is key
  - Secure train architecture
- Lessons learned
- Conclusion

# Setting the scene – Computers on Rails



# Where is the risk - Risk analysis for trains



Scriptkiddy

Hacker

Insider threat

Passenger Wi-Fi

Comfort IT

Train IT

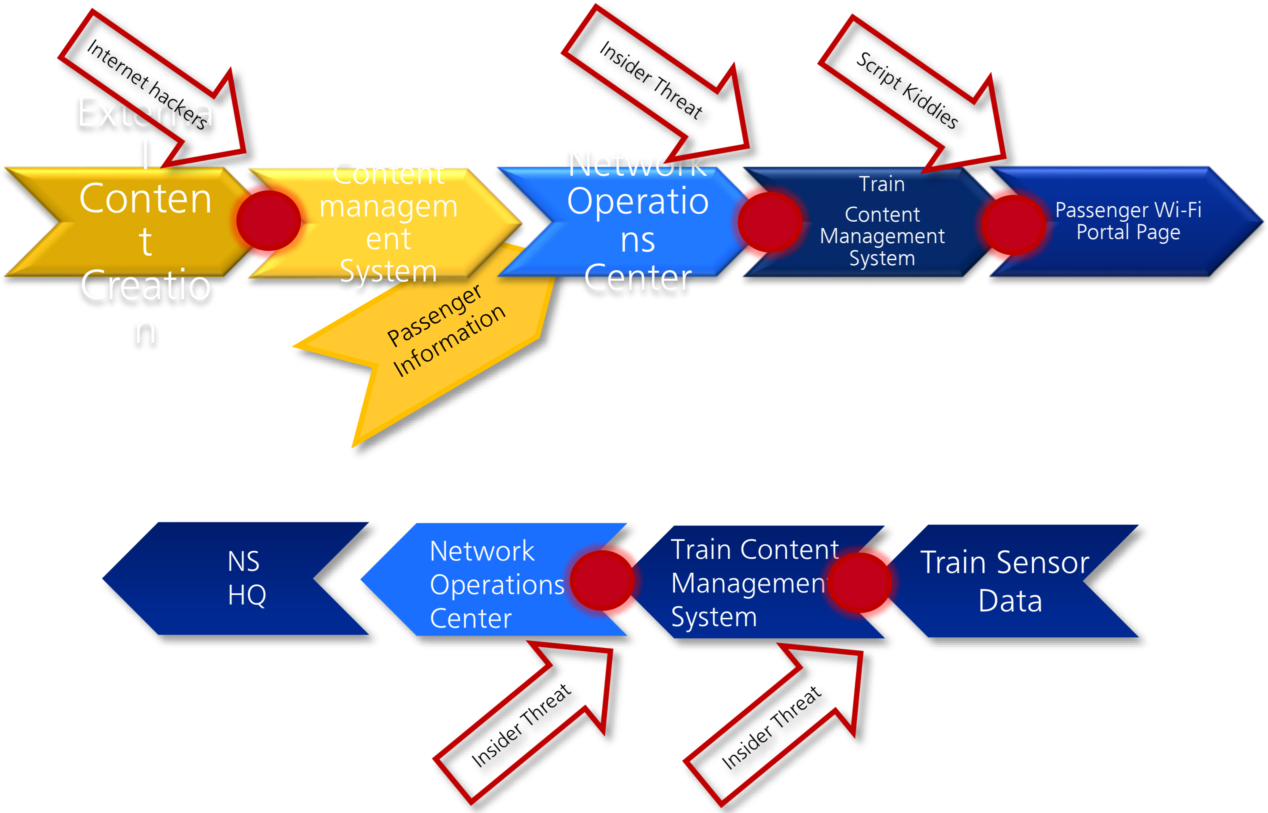
Able to reach the CMS

Able to reach the OBIS platform, maintenance Wi-Fi, Train Service Bus

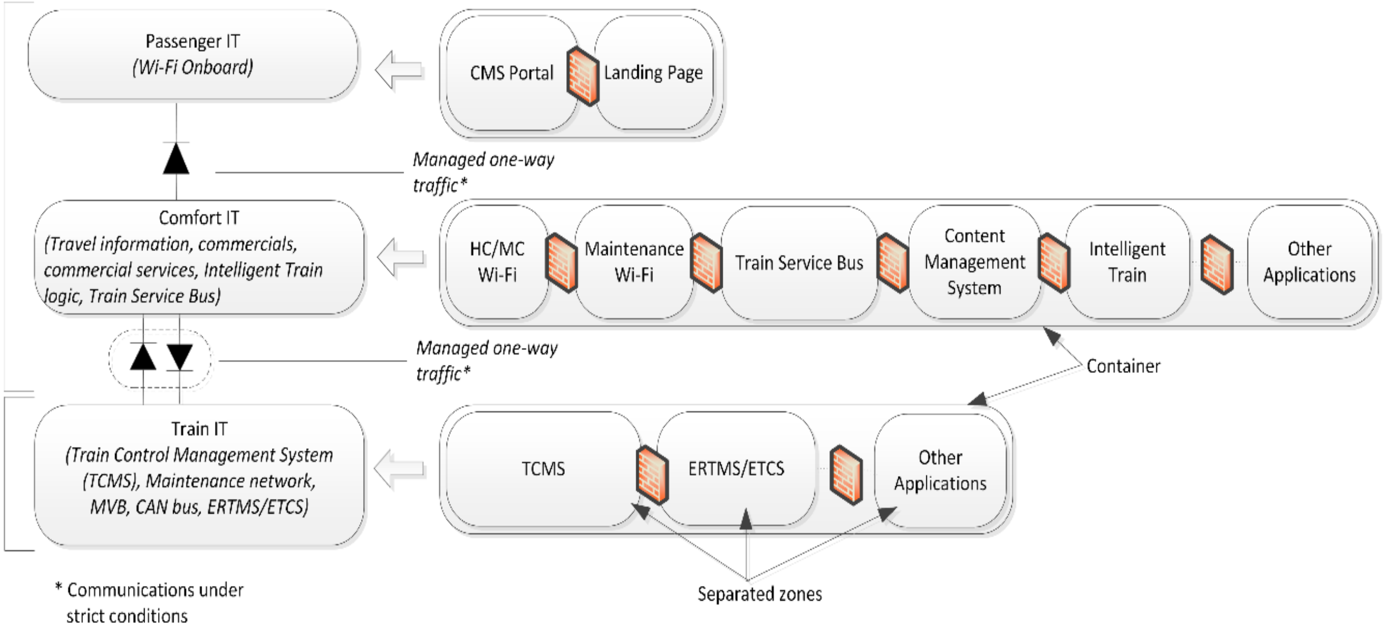
Able to reach the train network, maintenance network, TCMS and change the behaviour of onboard train IT systems

**Legenda**
CMS: Content Management System
OBIS: Onboard Information Systems
TCMS: Train Control Management Systems

# Where is the risk – Information flows


Internet hackers
External Content Creation
Content management System
Passenger Information
Insider Threat
Network Operations Center
Script Kiddies
Train Content Management System
Passenger Wi-Fi Portal Page
NS HQ
Network Operations Center
Train Content Managemen System
Train Sensor Data
Insider Threat
Insider Threat

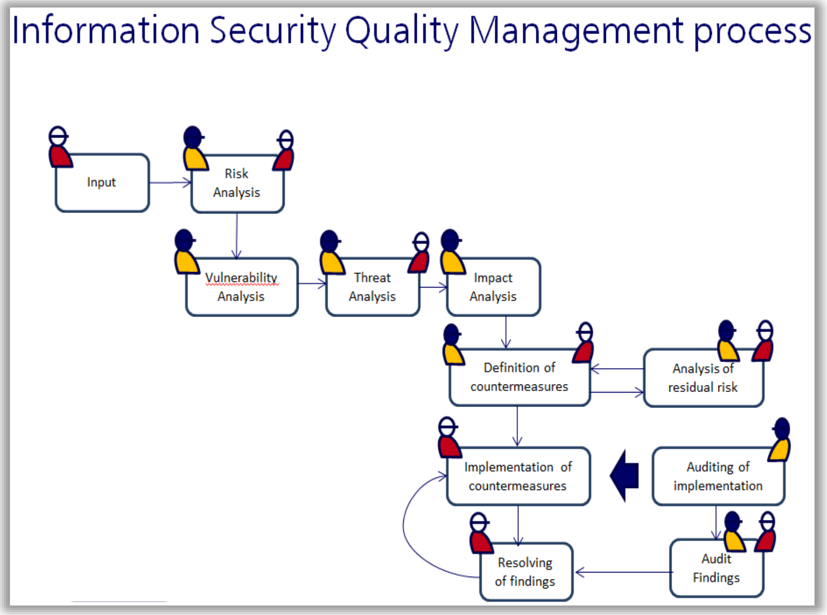
# Prevention is key - Target architecture



* Communications under strict conditions

# Prevention is key - External challenges

- Train suppliers
  - Include security requirements in RfI and RfP
  - Assist in interpretation of requirements
- Continuous communication and open exchange of information
- Create a common understanding of risks using a standard process
  - Business Impact Analysis
  - Threat and Vulnerability analysis
  - Determine Risk
  - Select and implement controls
  - Check implementation
  - Accept remaining risks


Information Security Quality Management process
Input
Risk Analysis
Vulnerability Analysis
Threat Analysis
Impact Analysis
Definition of countermeasures
Analysis of residual risk
Implementation of countermeasures
Auditing of implementation
Resolving of findings
Audit Findings

# Key take-aways

- Specify Information Security Requirements beforehand
- All software must be protected (logical and physical) and up to current levels of security standards
  - Comfort IT
    - Media player, content management system, passenger Wi-Fi, etc
  - Train IT
    - HMI software, train personnel Wi-Fi, RTM, etc
  - TCMS
    - Train computer, PLC’s, CAN bus/MVB/Train ethernet, etc
- Physical security is an important aspect (safety versus cyber)
- Train builders are willing to comply on process level. It is harder to improve hardware level when buying off-the-shelf trains
- Define an internal process to manage residual risk including stakeholders and ownership

# Conclusion

- Information technology enables new business and operational models
- Information security for Train IT is relative new but key in keeping trains safe in the (very) near future
- Threat analysis provides a good basis  for mitigating risks efficiently
- Close co-operation is needed
  - Rail Operators
  - Suppliers and
  - Maintenance Companies and
  - Regulators

**Gertjan Tamis**

*Information Security Officer*

**E** gertjan.tamis@ns.nl

**NS** | IT BAS | CoE Information & Risk Management
Laan van Puntenburg 100
Postbus 2025, 3500 HA Utrecht