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

Legenda
CMS: Content Management System
OBIS: Onboard Information Systems
TCMS: Train Control Management Systems
Where is the risk – Information flows
Prevention is key - Target architecture
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
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 relatively 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