Cyber security on track(s)

How to keep a modern digitalised train cyber secure

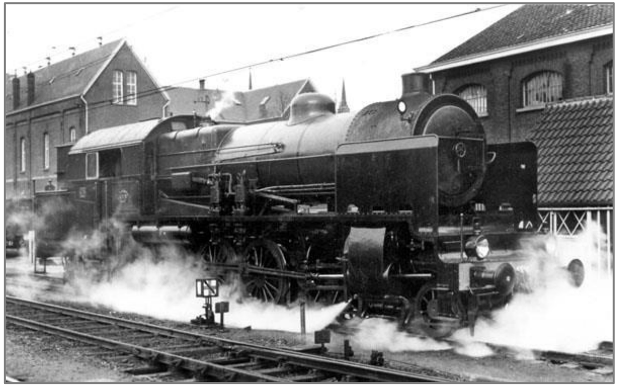
ISACA NL Square Table

Meinte Wildschut, Project Manager, NS

2 March 2022

Train digitalisation era’s

Mechanic



Stand-alone

Electro-mechanic

First external dependencies

Digital(-electro-mechanic)

Networked and connected

Digitalisation characteristics

1. IT is invisible
2. IT connections make the train part of a larger system
3. IT has a much higher change rate than a train
4. IT is vulnerable to attacks

Higher change rate - ICM compared to Apple

Introduction

Midterm overhaul

Replacement

1983 **2001** **2006** **2020** **2024**

Apple Lisa launch

iPod

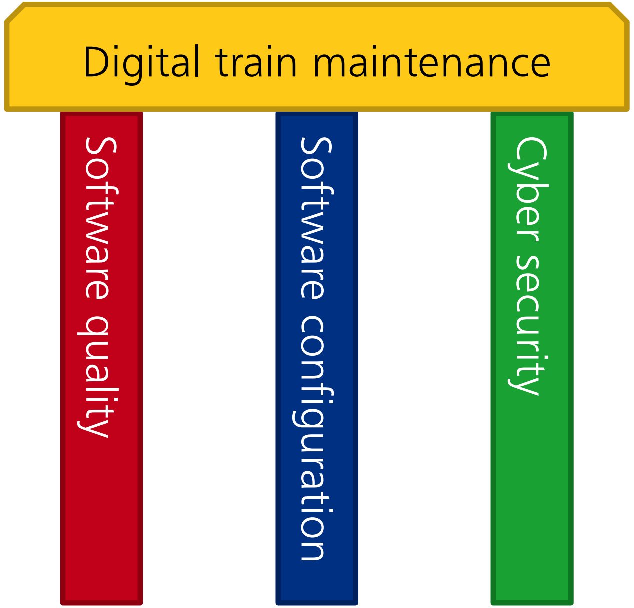
iPhone

iPhone 12 Pro

Project Titan

Key cyber security areas

- Software quality
  - Software has no form
  - How to ensure quality?
- Software configuration
  - High change rate - lots of software - lots of trains
  - Manage it, or you’re gone
- Cyber security
  - Impact on safety, operations, reputation, …
  - Know your risks



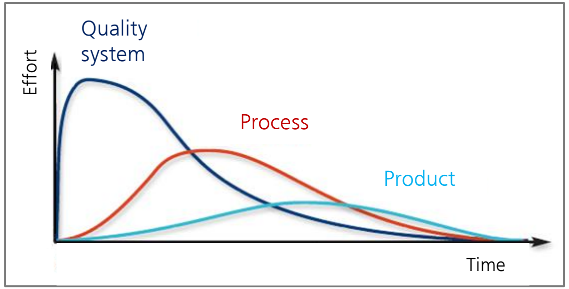
Digital train maintenance

Software quality

Software configuration

Cyber security

Software quality



- Quality system – Process – Product
- Testing
  - With known software configuration
  - Test plan - test report - release notes
  - Supplier test - focused integration on testbench - full integration test on train level
  - Single car - multiple car - connected with the shore - integrated in the system
- Software development style
  - Classical and iterative
- Release management
  - Roadmap - future releases - features & fixes

Software configuration

- Software configuration = current status of roadmap on train level
  - 100 trains = 100 copies of xxx software packages
  - Exact the same configuration for all trains of a fleet: utopia!
- Strict control on software uploaded to the train
  - Thorough verification and validation process before uploading
  - No cutting corners
  - Rolling Stock Software Desk
- Quite dynamic
  - Continuous drive for change, from operator, suppliers, ecosystem partners, etc.
  - Software is easily changed - risk

Cyber security

- Baseline: physical security
  - Compartmentalisation, fire-walls, encryption, …: useful, but second tier
- Continuously monitoring for vulnerabilities
  - Know your assets
  - Related to your assets, be aware of what’s going on out there
- Product requirements as well as system/process requirements
  - E.g. cyber security awareness/culture in the supplier ecosystem
- Risk based approach
  - Vulnerabilities and threats to be translated into risks
  - Uniform process for all trains

A few closing remarks

- Integration of IT and OT
  - Same stuff, but from different worlds, with different perspectives and cultures
- Monitoring vulnerabilities essential
  - Everyone on its own or aaS?
- Digitalisation is complex *and* promising
  - Internet of Things - learning to know your train
  - Predictive maintenance
- Modern trains are part of an ecosystem
  - Many dependencies, even between organisations (ERTMS)
  - An attack anywhere on the system is an attack on the train (Log4J)

Any questions ….

meinte.wildschut@ns.nl
+316 1087 4391