Railway Cyber Security
Threats and Resilient Measures

Alex Bishop

3rd June 2019
Introduction

- About me – background in safety critical systems engineering
- Threats to the railway – what is the problem?
- Resilience measures – how we are solving this problem?
Ricardo in the rail sector

We are rail industry specialists within the Ricardo group working to ensure that communities around the world are served by safe, resilient, high-performance railways.

Our expertise lies in understanding the complex and critical systems that underpin an efficient rail service, providing clients with all the technical skills and insight necessary to navigate the sector’s operational, commercial and regulatory demands.

In Denmark, amongst other projects, Ricardo Rail is acting as the General Independent Safety Assessor for the Banedanmark Signalling Programme.
Experts in critical and complex railway systems

By combining a deep understanding of the rail environment with specialist knowledge of its most critical technologies, we provide responses that deliver tangible outcomes for our clients and their stakeholders.

- **Systems engineering**
  Multi-disciplinary expertise that cuts across traditional industry silos.

- **Design and analysis**
  Expertise in producing cost-efficient responses to complex engineering challenges.

- **Asset management and optimisation**
  Specialist processes and technologies to improve efficiency across rail operations.

- **Independent assurance**
  Timely approvals for rail components, products and entire systems.
Introduction

In the past railways were mechanically **beautiful**, but **simplistic** from an cyber perspective.

Security is not new - UK Railways Act 1842 - ‘maintain and repair, good and sufficient fences throughout the whole of their respective lines’.
Introduction

To improve passenger experience and ease of operation modern railway systems have developed considerably:

- Each system can contain multiple data networks
- Almost every device is connected to a network

For example, many modern trains are now connected wirelessly through an on-board communication gateway.
Increased Connectivity

What does this connectivity mean?

- Improved reliability
- Better passenger experience
- Lower operating costs
- Reduced disruption

- Ease of mounting an attack
- Potential safety impact
- Service disruption
- Reputational damage
- Data theft
Cyber attack in practice

Roke
Part of the Chemring Group
Hypothetical Cyber Attack

SPEC5 Desktop 2.4GHz, 5GHz WiFi jammer - 10Watt

SPEC5 is the first ever jammer (and currently the only one on the market) with the ability to jam more advanced and more faster WiFi frequencies working on 5GHz spectrum. The 5GHz band operates at three standards: 802.11ac, 802.11a and 802.11n. 5GHz band becoming more and more popular nowada.

$840.00

More info
So what can we do about these threats?
We are working with a UK rolling stock manufacturer

We are helping them understand the security risk their train faces and develop resilience measures with them

This will help their customers, the railway undertakings, to be NIS compliant
Our Approach - List Assets and Their Criticality

1. List of Assets and their Criticality
2. Zonal Security Model
3. High Level Risk Assessment
4. Identify Threat Sources
5. Ranked List of Risks

Phase 1
Key to our approach, and what separates us from a traditional security company, is we understand what functions your railway system provides and are able to rate it in terms of safety, service disruption and data theft.

- The function an asset provides is identified
- The importance of that function is defined in terms of safety, service continuity and data theft
- This informs the appropriate level of security required for each asset
- An operational context is generated to understand how the train will be used
Our Approach - Threat Actor Identification

List of Assets and their Criticality → High Level Risk Assessment → Ranked List of Risks

Zonal Security Model → High Level Risk Assessment

Phase 1:

Identify Threat Sources
Our Approach - Threat Actor Identification

- Who are the threat actors?
- What are their motivations?
- What are their technical skills and resources?

Nation States

Information on threats actors are used to drive the level of security
Threat Actor Identification

- Analysis based on UK National Cyber Security Centre (NCSC)
- Rated potential threat actors in terms of motivation and capability
Our Approach - List Assets and Their Criticality

- List of Assets and Their Criticality
- Zonal Security Model

Phase 1

High Level Risk Assessment

Identify Threat Sources

Ranked List of Risks
Zonal Analysis

Following 62443-3-2: Security Levels for Zone and conduits:

- The system is divided into zones for the purposes of providing cyber security controls
- Each zone has an associated security level
- This is determined from the potential impact a cyber attack may have
- The security level defines the cyber controls which need to be in place
- We are using our clients exiting requirements process to implement these controls.
Our Approach – High Level Risk Assessment

- All of the previous work has then been used to analyse the system for threats
- This has resulted in a model of the system and a list of where we understand the great risks to be
- This will be used in the next phase – the detailed risk assessment
Our Approach – Detailed Risk Assessment

- In this phase we will dive into the details of the systems that have been identified to have the highest risk.
- We will validate if the security levels chosen are sufficient for the risk posed to assets and if additional controls outside of the ones defined by 62443 are required.
- Changes to the zonal model and further mitigation measures will also be explored at this stage.
- Validation will take place using:
  - Penetration testing, both of technology and processes
  - Checking if requirements have been implemented correctly though review of documentation
Our Approach – Independent Security Assessment (ISecA)

Testing witnessing of penetration activities on signalling control centre with Mike Ainsworth (Ricardo colleague) and myself
What Does Good Security Look Like? NIST Cybersecurity Framework

https://www.nist.gov/cyberframework
The Network and Information Security Regulations (NIS)

- Applicable to Operators of Essential Services (OES)
  - Managing Security Risk
  - Protecting Against Cyber Attack
  - Detecting Cyber Security Events
  - Minimising the Effects of Cyber Security Incidents

General Data Protection Regulation (GDPR)

- Securely processing and storing personal data
- Statutory reporting of data breaches
Standards

• ISO 27000: Information Security Management Systems Family of Standards – Collection of standards that covers organisational security policy and procedures; an essential starting point

• ANSI/ISA 62443: Security For Industrial Automation And Control Systems – This is the standard we are seeing specified in the UK to satisfy the engineering requirements NIS creates

• TS 50701: Cyber Security for Railway Applications – This is a technical specification being developed by CENELEC WG26. It is based on 62443 and will provide a tailored standard for the railway industry
Conclusions

New technology brings great benefits to the railways but we need to understand the risk.

This won’t be too different to how you understand risk at present; you already have half the answer. There are experts out there understand the security specifics. The key is linking the two.

• What can you do?
  – Educate yourselves – you don’t need to be an expert but this relies on everyone having an awareness
  – Ask questions – challenge things that don’t seem right or you aren’t happy with
  – Take a proportional approach – don’t dive into detailed analysis right away
  – Share your knowledge – working together we can create better solutions than we can alone
Alex Bishop  
Ricardo Rail  
5 St Mary’s Court  
Blossom Street  
York  
YO24 1AH  
United Kingdom  

Email: alexander.bishop@ricardo.com

Thomas Rasch  
Scandinavian Business Manager  
Certification  
Nørre Farimagsgade 11, 2. th.  
DK-1364  
København K  
Denmark  

Email: thomas.rasch@ricardo.com