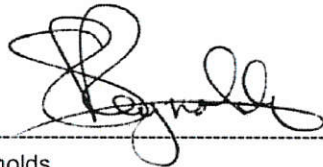


RDG Guidance Note Cyber Security – Advice on Working Practices from a Rolling Stock Perspective

Written by



Steve Reynolds
ERTMS Fleet Engineer, RDG

Written by



Chris Masson
ERTMS Systems Specialist, RDG

Submitted by:



Phil Barrett
New Technology Introduction Team Leader, RDG

Sponsored by:



Simon Holmes
Head of Technology (RSP), RDG

Synopsis

This document provides guidance to train operators and owners on mitigating the high-level risks associated with Cyber Security relating to maintenance of rolling stock, maintenance facilities and associated operational practices.

Applicability

This Guidance Note has been prepared for operators. However, its content may also be of use to others.

Issue record

Issue	Date	Comments
One	July 2017	First issue

Contents

Part 1 About this document.....	4
1.1 Responsibilities.....	4
1.2 Explanatory note.....	4
1.3 Guidance Note status	4
Part 2 Purpose and Scope.....	5
2.1 Purpose	5
2.2 Scope.....	5
Part 3 Background and Approach	6
3.1 Background.....	6
3.2 Approach	6
Part 4 Considerations	7
4.1 People Considerations	7
4.2 Process Considerations.....	8
4.3 Technology Considerations	9
Appendix A Glossary (Abbreviations).....	12
Appendix B Further Resources	13

Part 1 About this document

1.1 Responsibilities

- 1.1.1 Copies of this Guidance Note should be distributed by RDG members to persons within their respective organisations for whom its content is relevant.

1.2 Explanatory note

- 1.2.1 RDG produces Guidance Notes for the information of its members. RDG is not a regulatory body and compliance with RDG Guidance Notes is not mandatory.
- 1.2.2 RDG Guidance Notes are intended to reflect good practice. RDG members are recommended to evaluate the guidance against their own arrangements in a structured and systematic way. Some or all parts of the guidance may not be appropriate to their operations. It is recommended that this process of evaluation and any subsequent decision to adopt (or not to adopt) elements of the guidance should be documented.

1.3 Guidance Note status

- 1.3.1 This document is not intended to create legally binding obligations between railway duty holders. This note is provided for guidance only.

Part 2 Purpose and Scope

2.1 Purpose

- 2.1.1 Cyber Crime is an ever-increasing problem for the industry. The transport industry is part of the UK's Critical National Infrastructure (CNI) and therefore is an attractive target for hackers and is potentially vulnerable to cyber threats. This document is intended to provide practical advice for operators and owners of rolling stock to help them address this risk as part of their overall security assurance risk assessment.
- 2.1.2 The railway industry has become more reliant on digital technologies, computer systems and wireless networks. The industry has seen a growing interest in the field of Cyber Security, and what action is needed to protect assets and operations from Cyber Incidents. These incidents could be either malicious, where persons deliberately try to access information which they should not have access to, or accidental, when people misuse a system or pass on a virus or enter incorrect data. Whether deliberate or accidental, the result of such an incident is most likely to cause delay and disruption to the rail network and could provide the person concerned with a commercial benefit, at worst putting our staff and customers at risk of harm. The industry is working to mitigate this risk.
- 2.1.3 This Guidance Note is designed to complement existing tools and provide generic practical advice for operators and owners of rolling stock, to help them understand what they need to do about Cyber Security risks in their day to day business.
- 2.1.4 This guidance is not exhaustive and is not intended to replace any formal approach to:
- Delivering the Rail Cyber Security Strategy,
 - Meeting the EU's Network and Information Security (NIS) Directive,
 - Implementing the UK's National Rail Security Programme, when available,
 - Implementing other industry or government advice or regulations.
- 2.1.5 It should be considered alongside train operators own arrangements in a structured and systematic way, including any prevailing adoption of related standards, such as:
- Information Security Management: ISO 27001 & ISO 27002,
 - Cyber Essentials Certification (UK Government Endorsed),
 - Industrial Automation and Control Systems Security: ISA/IEC 62443,
 - European General Data Protection Regulation (GDPR).

2.2 Scope

- 2.2.1 This Guidance Note has been produced for the benefit of rolling stock operators and owners. It provides some common recommendations for managing Cyber Security risks and should be considered for the operation of new and existing rolling stock and associated facilities.

Part 3 Background and Approach

3.1 Background

- 3.1.1 RSSB have developed a Rail Cyber Security Strategy for the industry, which has been passed to the Rail Delivery Group (RDG) for delivery. In addition, RDG have developed a cyber maturity model in the form of a Self Assessment Questionnaire (SAQ) to help the industry and its suppliers to identify concerns that need to be addressed. Network Rail (NR) has gone a stage further and are developing a detailed risk assessment process to undertake analysis of railway assets. This process is known as the Security Assurance Framework (SAF) and will allow individual Duty Holders to assess their security risks.
- 3.1.2 Cyber Security discussions have been held at a high level within the Digital Railway programme through the Cyber-Security Steering Group (CSSG). As there was confusion about what action the train operators fleet engineers needed to take, it was decided to implement a sub-group work stream to answer the operators question 'what do we actually need to do?'. A workshop was held with a selection of operator rolling stock representatives to try and identify the specific Cyber Security issues that could affect traction and rolling stock engineering, including the depot environment.

3.2 Approach

- 3.2.1 Workshop attendees were supplied with six worksheets split into separate subject areas. These were designed to capture some early thoughts on the issues they thought were relevant. The responses were used to find common areas and steer the conversation on the day.
- 3.2.2 Notes taken during the workshop were consolidated into a draft document and arranged in a format similar to a risk log. This was subsequently provided to the Digital Railway Cyber Security Subject Matter Experts (SME's) to analyse and provide guidance based on the information provided by operators, and their current cyber security concerns.
- 3.2.3 The objective of this work stream was to produce a set of recommendations that can be used by all train owners and operators, to improve their understanding of ERTMS cyber security risks in the traction and rolling stock environment and to provide guidance as to how risks can be mitigated. This document is the final output from this work. As the work stream identified that the risks were not limited to ERTMS, it addresses the subjects of people, process and technology as generic rolling stock cyber security risks, noting that all are a source of vulnerability and therefore an opportunity for improved security.
- 3.2.4 It is important to understand that references to security in this document are not just IT Security but also about the behaviours of people and processes. There is an opportunity, through people, to improve cyber security by adopting a 'cyber-aware' culture. Likewise, good processes provide an opportunity to prevent basic security breaches.
- 3.2.5 The raw data generated by the work stream during the process is not included in this document for the purposes of clarity. That information is available as a separate document which details the output of the initial workshop and further work, and can be sent on request by contacting the Rail Delivery Groups New Technology Introduction team.

Part 4 Considerations

4.1 People Considerations

- 4.1.1 Identify a single point of accountability for the security risk associated with operational assets, in compliance with a suitable security policy. This is often the Finance Director as they also control the corporate risk register and the organisation's insurances.

***Suggested Action:** For security to be effective it is essential that a single person is allocated the accountability to ensure that the correct risks are identified and mitigated. This is sometimes an Information Technology (IT) responsibility, but is best held at board level to ensure it fully supports the people and process aspects of cyber security.*

- 4.1.2 Develop and document an operational asset security governance model linked to job descriptions, roles and responsibilities for those with access to operational assets, particularly IT and engineering personnel.

***Suggested Action:** Develop a matrix of those Responsible, Accountable, Consulted and Informed (RACI) because it is unlikely that the single point of accountability for cyber security can always undertake and oversee all security activities. Development of a RACI will enable a company to identify all employee responsibilities with respect to maintaining the security of an operator's assets.*

- 4.1.3 Develop new or revised facility induction security awareness material.

***Suggested Action:** Cyber security should be included in site inductions for all new staff and contractors. It should also be considered when facilities and operations are altered in a way that changes their cyber-attack vulnerability/risk.*

- 4.1.4 Provide targeted training for individuals whose role includes access to operational assets.

***Suggested Action:** All staff who use computer-based devices at facilities that are responsible for operating, maintaining and overhauling rolling stock, should be adequately trained in the correct use of the equipment and software including the implications and prevention of cyber-attack.*

- 4.1.5 Raise awareness of cyber security pertaining to operational asset information; including the need for data classification, (aligned with an IT policy), the identification of phishing/spear phishing attacks, and the risks associated with unauthorised use of cloud storage facilities or inappropriate use of technology.

***Suggested Action:** All staff who use company IT systems in their role should undertake formal awareness training to enable them to use company IT systems in a secure and responsible manner compliant with company IT policies. This should include but not be limited to:*

- Raising awareness of the dangers of phishing and spear-phishing email attacks,*
- Use of confidential data,*
- The risks associated with using removable media and cloud-based storage,*
- Appropriate use of IT systems,*
- Supporting each other in delivering these policies and practises.*

4.2 Process Considerations

- 4.2.1 Develop a physical security policy that ensures only registered, authorised and trained users are issued with access keys, codes and equipment.

Suggested Action: *Use of equipment, access codes and access keys (including T keys) should be reviewed and monitored to ensure that only authorised employees have access to work areas that are required for them to carry out their duties. Common keys and codes should always be avoided. All keys and access codes should be changed from factory default at the point of installation or retrospectively if necessary. Multiple access layers are recommended for maximum security where required. This applies equally to operational assets at facilities and on rolling stock.*

- 4.2.2 Develop a removable media policy that restricts and manages the use of USB devices, including ‘sheep-dip’ testing prior to use on operational assets. Wherever possible ensuring the USB is encrypted.

Suggested Action: *A policy of routine testing USB devices prior to use should be implemented. USB devices, if used in an uncontrolled manner, represent a serious threat to operational equipment and IT systems due to their ability to transfer malware across the system boundary.*

- 4.2.3 Develop a password policy for operational assets based on IT good practice.

Suggested Action: *Ensure that passwords are changed regularly, that they are secure in format and that they are not displayed on the asset concerned or other location where they could be used by unauthorised persons. Ensure that software or operating asset passwords are not shared through uncontrolled media, or available in general documentation such as Vehicle Maintenance Instructions (VMI) of Maintenance Procedures (MP).*

- 4.2.4 Implement a security risk assessment and management process to ensure all digital operational assets are secure.

Suggested Action: *At a business level, an RDG Self-Assessment Questionnaire is available to help identify and prioritise areas of poor maturity. Network Rails’ SAF can be applied to investigate in much greater detail, the operational asset risks in compliance with a Common Safety Methodology and UK Rail Safety Management System approaches. All systems should be subject to such reviews every 1-3 years depending on the level of change both in the threat environment and systems itself.*

- 4.2.5 Develop a security change control policy, or update existing safety change control mechanisms, to ensure that, when an operational asset is modified, security is considered in relation to the requested change.

Suggested Action: *When an operational asset is updated or modified any safety implications should be carefully considered and analysed as part of a change control process. Change control processes should be updated to include a security assessment to ensure the security and safety of the asset is not compromised by the change, the NR SAF could be used as the risk assessment process to be triggered by the change control request.*

- 4.2.6 Apply an ISO27001: Information security management approach through a security control policy that ensures appropriate information assurance, from Lanyards to base IT security. This will help protect operational data assets throughout their lifecycle.

Suggested Action – IT Department: *Where the extraction of personal or maintenance data is required from an operational asset; the use of the ISO27001 Standard should be applied to ensure that the data is protected in transit compliant with a recognised Standard. Management of all personal data must also comply with the European Union's General Data Protection Regulation (GDPR) by May 2018. Consider implementing a Data Processing Agreement (DPA) with the data owner/controller, by liaising with your organisation's Data Protection Office (DPO).*

Suggested Action – Maintainer: *No personal data should be visible or accessible to the user when accessing train systems for maintenance, this includes passenger systems such as Wi-Fi because it would be a breach of GDPR and non-compliant with the principles of ISO27001. If the user finds any personal data, such as names, email addresses or passwords, while accessing train systems and extracting any system data, they must report the incident to the IT Department for immediate security action.*

- 4.2.7 Develop a Security Procurement Language policy and ensure supplier, leasing and maintenance contract requirements include the appropriate security policy clauses for both information and system protection.

Suggested Action: *When specifying new assets, it is important to place security requirements within supplier contracts prior to contract award. RDG is working across the industry and key suppliers to develop a common commercial schedule that can be adapted to suit these circumstances. Until this is available a good document to obtain requirements from is the "United States (US) Department of Homeland Security ICS Procurement Requirements Guidance", which is available via the US Department for Homeland Security website.*

- 4.2.8 Develop interlinked Human Resources (HR) and IT Security processes that ensure all personnel accounts and access are removed at the point of contract termination.

Suggested Action: *A change of job role or responsibilities generally results in a change of accountability. It is therefore important that there is a process for an employee's IT account to be reviewed for security requirements whenever a change of job role occurs. When a member of staff leaves a company, it is essential that all accounts associated with that employee are terminated with immediate effect to prevent ongoing unauthorised access to company systems.*

4.3 Technology Considerations

- 4.3.1 Ensure that operational system passwords comply with the principle of least rule of privilege; ensuring engineering access is limited to required functionality.

Suggested Action: *Users should only be given access to the minimum amount of software they are expected to use. Additional access should be subject to formal request and review. A further review would be required for a change of job role.*

- 4.3.2 Where possible restrict administrator rights to specified asset managers and IT managers.

Suggested Action: *Users should not be able to make changes to configuration settings on computer systems, except where required as part of their duties when connecting to and communicating with traction and rolling stock components during maintenance.*

- 4.3.3 Legacy maintenance PCs whose operating systems cannot support vulnerability patching should be scheduled for replacement with IT supported hardware.

Suggested Action: *All PCs should support Operating System (OS) vulnerability patching, if they are too old to support modern anti-virus protection they should be replaced as a priority.*

- 4.3.4 Where the requirements of 4.3.3 are not possible, machines should be regularly Anti-Virus scanned using controlled removable media.

Suggested Action: *If a PC is unable to support vulnerability patching it should be regularly Anti-Virus scanned using removable media to ensure malware is not present on the PC.*

- 4.3.5 Dedicated laptops should be used for maintenance functions and conform to an IT hardened build specification, with all superfluous media and applications disabled or removed, such that it meets ISA/IEC 62443.

Suggested Action: *Laptops represent a significant threat to operational systems if equipped with IT media applications such as email and internet. If a laptop is to be used in the maintenance environment it should only have the maintenance applications required for that specific function, and should not be used or connected in relation to general IT activities. Email or internet connection facilities should be removed or securely disabled.*

- 4.3.6 Laptops should be password protected and stored in a secure environment, ideally with end-point encryption to ensure confidential data is secure when at rest.

Suggested Action: *Operators should keep maintenance laptops in a secure local environment when not in use and not allow employees to use them as personal equipment. All laptops should have individual passwords that are maintained compliant with a strong password policy as recommended in Process Considerations above.*

- 4.3.7 Develop and implement ISA/IEC 62443: Industrial Automation and Control Systems Security – *Network and system security* compliant operational asset architectures that ensure the appropriate network segregation between systems; e.g. proportionate passenger Wi-Fi, Remote Condition Monitoring and safety system segregation.

Suggested Action – System Design: *To ensure security by design, asset network architectures should be layered and segregated to minimise the possibility and effect of a cyber security attack. ISA/IEC 62443 is the leading standard for assessing and architecting operational technology to secure from, and in the event of, a cyber security incident.*

Suggested Action – Maintainer: *While undertaking maintenance activities users may be required to modify train networks, either to make the train serviceable, or as part of an improvement activity. to meet security requirements. Because vital safety networks and non-vital passenger networks are required to be segregated, care should be taken when modifying train system networks to ensure that the integrity of this segregation is maintained. Connections between vital and non-vital networks should always be avoided. In addition, where installed, internal trains system firewall configurations should be regularly checked, validated and maintained to ensure sub-system segregation is compliant with the system design and security requirements.*

- 4.3.8 Avoid direct vendor connections for remote downloads; develop an ISA/IEC 62443 staged patch management architecture that includes a robust DMZ design and associated IT security ruleset. This should also comply with ISO27001.

Suggested Action: *Vendor upload/download connections represent a significant threat to operational asset security because they bypass company security Firewalls. To reduce this risk to a minimum, direct connections should be prohibited and access should be routed through a unified security gateway controlled and monitored by the company IT Security function.*

- 4.3.9 Physically block media ports on critical assets to prevent access.

Suggested Action: *Key or tool accessed covers should be fitted to prevent access to serial/parallel/USB /RJ connections on operational assets. Where this is not possible ports should be physically decommissioned or an alternative secure location should be provided.*

- 4.3.10 Restrict use of “homemade or modified” connectors or cables that could cause damage to equipment or corrupt data being used.

Suggested Action: *Manufacture of bespoke cables and connectors needs to be carefully controlled and assessed. It may be possible to unwittingly damage equipment, corrupt data or reconfigure functionality if plug and socket wiring configurations are not as originally designed.*

Appendix A Glossary (Abbreviations)

Asset Architecture	The communication network architecture that connects operational asset equipment, and third party and enterprise networks.
AV	Anti-Virus
Controlled Removable Media	Typically, a USB or Maintenance laptop used to interact with an operational asset, but used in compliance with a policy that heavily restricts its use to its core function
CREST	The Council for Registered Ethical Security Testers.
CSSG	Cyber Security Steering Group (Digital Railway)
DFT	Department for Transport
DMZ	Also known as a Demilitarised Zone or a Perimeter Network – used between an organisations external facing network and larger untrusted networks, such as the internet.
Facilities	Stations, Depots and Sidings.
Network	Communication network or data bearer.
NR	Network Rail
Operational Asset	A rolling stock asset maintained by engineering rather than an IT function.
Phishing	Non-specific email containing a virus or web-link, requesting an inappropriate response.
RACI	A matrix that maps the terms ‘Responsible Accounted Consulted Informed’ to specific roles or job descriptions with the aim of mapping an effective security organisation.
RDG	Rail Delivery Group
RSSB	Rail Safety & Standards Board
SAF	Security Assurance Framework (Network Rail)
Sheep Dip	A process of checking a USB or Maintenance laptop by connecting to an IT asset with up to date AV signatures to ensure that the USB or laptop is not infected with malware prior to connecting it to an operational asset
Spear Phishing	Socially-engineered/target email containing a virus or web-link, requesting an inappropriate response.
Vulnerability Patching	A process whereby AV updates are applied to a PC or laptop to ensure malware signatures are up to date

Appendix B Further Resources

National Cyber Security Centre (NCSC)

The NCSC, as part of GCHQ, seek to oversee the UK's cyber security and offer some useful advice, especially the "10 Steps to Cyber Security":

1. Risk Management Regime
2. Secure configuration
3. Network security
4. User privileges
5. User education and awareness
6. Incident management
7. Malware prevention
8. Monitoring
9. Removable media controls
10. Home and mobile working

These affect every one of us, every day, and worth checking with every change within our environment and can be found on the UK Government website.

Open University: Introduction to Cyber Security

A course has been developed by The Open University with support from the UK Government's National Cyber Security Programme:

"This free online course, Introduction to cyber security: stay safe online, will help you to understand online security and start to protect your digital life, whether at home or work. You will learn how to recognise the threats that could harm you online and the steps you can take to reduce the chances that they will happen to you.

With cyber security often in the news today, the course will also frame your online safety in the context of the wider world, introducing you to different types of malware, including viruses and trojans, as well as concepts such as network security, cryptography, identity theft and risk management."

This course can be accessed via the Open University's website.