Rolling Stock Cyber Security Strategy: An Overview

Written By: Lee Clough

Pride Solutions Derby

Pride Solutions Derby

Rolling Stock Cyber Security Strategy

Table of Contents

Introduction

Pride Solutions Derby | Rolling Stock Cyber Security Strategy

As the use of connected technology in rolling stock increases, it is essential to ensure that these systems are protected from new and emerging cyber threats. To this end, there is a need to create a culture that considers cyber security a critical part of fleet safety. This will require the creation of currently absent standards and frameworks for rail operators and industry stakeholders to follow when developing their own cybersecurity strategies.

This paper aims to explore the current state of rolling stock cyber security around the world, identify areas where improvements can be made, and present potential strategies for creating robust frameworks that will protect new digitally enabled trains from malicious actors.

In order to create a comprehensive strategy for rolling stock cyber security, it is important to consider all potential threat vectors. This includes physical security, software and hardware vulnerabilities, user access controls and privilege management, data encryption and authentication protocols, securing of controlled documents, patching and updating of systems, malware protection and other measures. Each of these elements will need to be addressed by suitably experienced experts through every level of seniority in order to create a secure platform that meets industry standards.

Additionally, rail operators should be encouraged to collaborate with industry stakeholders such as technology vendors and government agencies in order to share information on the latest threats and best practices. By having open communications channels between the various parties involved in rolling stock operations, vulnerabilities can be identified quickly and resolved without disruption.

Finally, there must be clear guidance on how to respond in the event of an attack. This includes identifying the source, determining which systems were impacted, and enacting countermeasures to contain any damage and prevent future attacks. Ongoing monitoring should also be carried out to ensure that all systems remain secure and to detect new threats quickly.

This white paper examines all of these points and suggests points of thought for the industry when evaluating their fleet security posture.

A Message From Our Director

Lee Clough | Pride Solutions Derby | Rolling Stock Cyber Security Strategy

"The industry is not only ill-equipped to detect and respond to current threats, it doesn't even know they exist"

I have worked in the railway in some form for approaching 10 years now. In that time I have had the pleasure of working on both traditional legacy stock and cutting edge new builds. Over that period I have also carried out extensive work in the enterprise IT world, from designing and implementing sprawling industrial automation systems from scratch, to supporting complex systems in light rail settings.

What has become clear over the last decade is how quickly the railway industry is digitising and our cyber security knowledge and capability is not keeping pace. The next generation of Rolling Stock is more connected than ever before, making use of Remote Condition Monitoring, TCMS, IP CAN-Bus systems and other technologies to make maintenance easier.

With this new technology, however, comes new threat and risks to manage. The problem? The industry is not only ill-equipped to detect and respond to current threats, it doesn't even know they exist

Overview of Rolling Stock Cyber Security

At present, the railway industry is significantly lagging behind other transportation sectors in terms of cyber security. Specifically, fleet cyber security. Modern fleets have extensive digital command and control systems on board that present a new set of threats that could ultimately compromise the operation and safety of the railway.

For example, in 2015 a supplier of connected equipment to British rolling stock were alerted to a flaw in their system that allowed an attacker (in this case an authorised security consultant) to connect to the on-board passenger Wi-Fi, compromise the suppliers main system management servers, and gain remote access to the network on any train currently powered on with that suppliers equipment fitted, anywhere in the world. Some of these were isolated 'Blue' networks with limited capabilities, others were more critical 'Red' networks, allowing potential breaching of on-board systems.

Elaborating on that a little more, suppose that was not a security consultant, but rather a foreign adversary of the UK, electing to attack national infrastructure. The attacker may be successful in gaining access to the Automatic Selective Door Operation (ASDO) database on a fleet of trains and manipulate that data to alter the side of the train the doors open on at a particular station, or compromise the CAN-Bus controller on a unit and generate unsolicited commands to on-board systems.

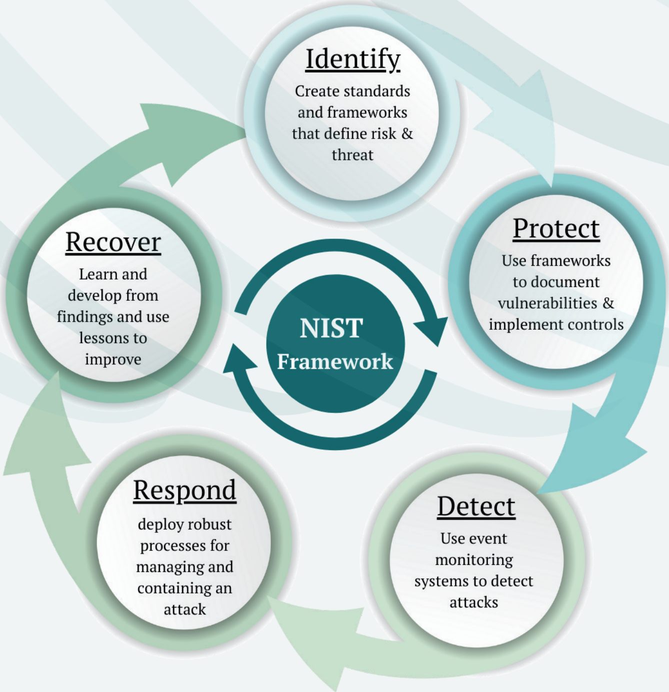
There are currently no Railway Group Standards for cyber security, and, On the whole, the ageing workforce in the railway does not have the required level of understanding and comprehension of modern digital systems to be able to tackle these issues robustly, leaving many railway operators vulnerable from the outset when introducing new digital technologies onto their networks. This lack of preparation exposes rolling stock to a variety of cyber threats, from simple malicious attacks to more complex and sophisticated campaigns.

In order to improve the security of connected trains, industry stakeholders need to take the lead. regulators such as the ORR & RSSB should look to adopt best practices from accepted global standards such as the National Institute for Standards and Technology (NIST) 800-82 'Guide for Industrial Control System (ICS) Security and the National Cyber Security Centre (NCSC) Cyber Security Framework and combine these into a comprehensive suite of frameworks and standards that are suitable for the railway.

These existing frameworks provide detailed guidance on how to identify and mitigate potential threats, as well as on how to respond in the event of an attack. NIST 800-82 recommends implementing layered defences with multi-factor authentication protocols and encryption techniques while NCSC stresses on user access controls, privilege management, and patching/updating systems regularly. By adopting best practice from these standards, the industry can create a secure environment that defends against the ever evolving threat landscape.

Rolling stock owning companies need to take whole life ownership of these digital assets and work with vendors to provide robust support mechanisms that become a part of the rolling stocks existing maintenance regimen. Minimum update and security support periods need to become the norm, underpinned by a requirement to meet industry standards for encryption, intrusion detection and vulnerability patching.

Rail operators should also take steps to manage the emerging risks through development of their existing safety management systems. Digital security is no longer a nice to have, it is a safety critical obligations. Mandatory training and education of staff members on good cyber hygiene practices such as using unique passwords for each system and avoiding downloading unauthorised software onto their devices is key. Additionally, they should consider extensive hardware security mechanisms, including investing in tools such as intrusion detection systems (IDS) that can detect when malicious actors attempt to gain access or compromise data security. Finally, they must ensure that all equipment, train and wayside, is patched regularly to protect against known vulnerabilities that hackers could exploit.


Identify
Create standards and frameworks that define risk & threat
Protect
Use frameworks to document vulnerabilities & implement controls
Detect
Use event monitoring systems to detect attacks
Respond
deploy robust processes for managing and containing an attack
Recover
Learn and develop from findings and use lessons to improve
NIST Framework

Identifying Potential Threat Vectors

We don't always think of the Railway and Rolling stock as critical national infrastructure from a cyber security viewpoint. However, due to its 4 million daily passenger journeys, increasingly digitalised nature and reliance on connected systems that is exactly what it has become. If a successful attack were to occur on the UK rail network, it could bring the entire system to a complete standstill, with potentially catastrophic consequences for passengers and train crew. This is why it is vitally important that the whole railway industry understands the threats posed by malicious actors and take steps to mitigate them.

The challenge of identifying the threat landscape for an industry wide mix of fleets with differing systems on board but that all connect together through common hubs cannot be under-estimated. This will require cyber security personnel to work closely with rolling stock engineers, third party vendors, software developers, vehicle manufacturers and operations staff to understand exactly what hardware is fitted to the vehicles, what the equipment does, how it all connects together, what the capabilities are of the system as a whole and what vulnerabilities may lie therein.

One of the most effective tools for supporting this process is frameworks such as Mitre ATT&CK. This provides an in-depth understanding of different attack vectors that could be used against digital systems and networks, from simple malicious attacks such as those targeting on-board Wi-Fi, to more complex campaigns like those involving remote condition monitoring systems, edge computing devices or exploiting zero-day vulnerabilities to take unauthorised remote control of whole trains. The staff conducting the assessments need to be able to correctly use the design and configuration documentation to identify possible vectors such as cross site scripting or SQL injection for database systems with web interfaces, API vulnerabilities for remote monitoring systems and hardware specific vulnerabilities for CAN-Bus based systems.

Staff also need to have a good understanding of computer network topology, with a working comprehension of VLANs, subnetting, firewalls and the OSI model to be able to make informed decisions about any network level vulnerabilities which could impact how widespread any potential breach could become.

When discussing threat and risk, in any industry, early detection is critical to the containment and mitigation of any incident.

In order for stakeholders to identify potential threats early on, they need to have in-depth visibility into their whole networks at all times; not just when an incident has already occurred. Real-time monitoring tools should be deployed throughout the organisation in order to detect suspicious activity as soon as possible and spot any anomalies that could indicate a breach has taken place. The information gained from these systems then needs to be analysed against updated threat intelligence feeds by experienced and well trained staff who understand how the relevant systems work, the potential consequences of a breach and the realistic mitigations that could be applied.

Additionally, each system, including 'benign' items such as maintenance equipment, must be configured securely with appropriate detection systems in place to alert the organisation to any suspicious activity. This configuration needs to be based on controls identified in industry codes of practice, with regular security patching being applied across all train units and wayside equipment in order to prevent exploitation of known vulnerabilities.

When analysing threats within the context of rolling stock cyber security strategy, there are some key areas that need consideration including user authentication & access control at all levels from maintenance personnel up; secure data handling and storage processes; asset management & configuration; threat intelligence & identification; incident response & recovery processes; and governance & compliance frameworks.

Once identified, threats and vulnerabilities need to be assessed in the same manner as engineering changes to a vehicle. Formal recording of any potential safety and operational risks, graded and documented with supporting risk assessments and mitigations to ensure continued protection and, where necessary, those mitigations may include widespread fleet disruption while appropriate corrective actions are put in place.

By taking these steps, railway organisations can better prepare themselves against potential cyber threats and ensure their rolling stock remains safe from malicious actors.

Collaboration with Industry Stakeholders

Organisations operating within the railway industry must be aware of the potential cyber threats that could compromise assets, and take steps to ensure they have a robust security posture. Stakeholders such as the Office of Rail and Road (ORR), Department for Transport (DFT) and Railway Safety & Standards Board (RSSB) will play a leading role in this process, providing guidance on how organisations can best protect themselves against potential attacks.

These regulating authorities are ideally positioned to draw best practices together from other industries and generate the frameworks and guidance the industry will use to protect against threats, as well as recommendations for standards that should be met in order to ensure safety and compliance with regulations. They also have access to up-to-date threat intelligence information on a global stage which can help organisations identify vulnerabilities before they are exploited. Working together, these stakeholders can help create secure systems of work to support the wider industry.

There is a desperate need for much closer working with other stakeholders too, such as vehicle owners, operating companies, third party system vendors, vehicle builders and advanced cyber security partners to develop regular self testing mechanisms that validate the continued effectiveness of implemented controls and feed findings into the development process so the industry is always improving its security posture.

System vendors need to be held accountable for better defining and supporting the design life of their product at point of manufacture. Vendors need to be positioning themselves to conduct regular testing of their equipment against existing and emerging threats and offer regular patching to ensure detected vulnerabilities are eradicated as well as ensuring that critical operating system patches are rolled out to fleets. I have come across too many on-board systems running outdated and unsupported versions of Windows, such as Windows 7, which no longer receive security updates and patching or maintenance laptops running Windows XP because there is not the knowledge to update these systems whilst maintaining operational capability.

Permitting devices that interface with a train to lapse in terms of security has not been a problem historically as these systems were largely offline with a pure monitoring position only. With the next generation of rolling stock, however, this kind of approach is a significant security risk to vehicle systems and these security flaws need to be identified and managed to minimise risk, not just at the point of vehicle introduction, but as an ongoing endeavour through the vehicles life.

As discussed earlier, of equal importance is the need to define how digital systems will be maintained over their designed life. Collaborative working between OEMs and asset owners/operators with the sharing of information will identify what steps need to be taken. The periodic security scanning of systems needs to become a regular item on routine maintenance exams for vehicles, backed up with detailed procedures on what to do with identified vulnerabilities and, where required, the upgrade of equipment may be necessary in order to overcome hardware vulnerabilities.

The industry also needs to develop closer ties with external Cyber Security practitioners in order to conduct targeted security assessments and penetration testing on a periodic basis. These kind of controlled attacks are what identified the vulnerability discussed in the introduction that allowed an adversary to compromise any train in the world with the same equipment fitted, through the Wi-Fi on one train. Had the security company not been employed to conduct that test, the first time the vulnerability came to light may well have been in the hands of a malicious actor.

Now the development of these relationships, as is the case with the frameworks and supporting guidance, training and detection systems is not a quick process to implement. To develop a robust security posture for the industry is going to take exceptional levels of commitment, collaboration, humility and, most importantly, funding for several years to come. Hence, the development and adoption of any posture needs to be led from the top down.

Create a Comprehensive Framework

We have now established that the development of an effective cyber security strategy for rolling stock requires the active participation and cooperation of many stakeholders. This includes collaboration between industry bodies such as the RSSB, railway operators, vehicle owners, third party system vendors and advanced cyber security partners. Parliamentary working groups can also play an important role in developing frameworks to ensure that appropriate measures are established and implemented across the sector.

The framework needs to include requirements for the secure configuration of on-board systems, using pre-hardened images where applicable, and protocols to ensure that these configurations remain 'secure' during the vehicles life. It should also identify what kind of information needs to be shared between stakeholders, such as sharing threat intelligence and vulnerability data from third parties, or cyber security practitioners. It must also define how any identified vulnerabilities will be managed and tracked through their remediation process and documented in vulnerability databases.

Finally, it is essential that any adopted framework ensures that all stakeholders are working towards a common goal with clearly articulated objectives and timelines. This will help ensure everyone is working together efficiently and effectively while ensuring that security posture remains at an acceptable level.

The development of an effective cyber security framework should include a number of key elements:

- Draw upon existing best practice from other industries and frameworks to identify the most applicable methods for threat assessment, intelligence led vulnerability analysis and any applicable laws and standards already in place. An ideal starting point would be NIST SP 800-82 and ISA/IEC 62443 which are both existing systems for implementing cyber security principles to industrial control systems.

- A standardised and harmonised risk assessment process across all stakeholders. This should consider the risks posed by digital threats to both physical and information assets, as well as the impact on customer safety, privacy, data protection and asset integrity.

- Detailed security requirements which define what needs to be done in order to protect rolling stock systems from attack. These requirements will then be used to develop appropriate management and containment measures that will be deployed on the operational railway.

- Robust policies and procedures that cover the secure deployment, maintenance and disposal of rolling stock systems in accordance with contractual obligations between stakeholders

- Monitoring and auditing of systems on a regular basis to ensure that security measures are effective and up to date. This should include the adoption of periodic penetration testing in order to identify weaknesses within the system which can then be rectified

- The development of an appropriate cyber governance structure, with clear lines of communication between stakeholders, and appropriate escalation paths for any identified issues and reporting mechanisms into the relevant national security agencies to allow adaptable practices based on evolving international threats.

These elements will form the foundation upon which all aspects of rolling stock security can be developed, assessed, tested and monitored over time. Adopting such a framework provides assurance that the necessary steps have been taken by all parties in order to protect against potential threats from malicious actors, allowing confidence to be placed in new digital technologies as they are introduced to the railway.

The framework should be owned and maintained by the industry as a whole to encourage adaptability and flexibility of the framework to work with different systems. It is worth noting, however, that the overall security posture of the whole railway will be dependant on a unified adoption and implementation of core security principles. Whilst it is not practical to apply the same level of adoption and protection mechanism to every element of the industry, peace meal implementation and compliance to a standardised security convention cannot be optional. Such practice would allow for more Advanced Persistent Threats (APTs) to leverage weaker protected assets as a pivot point within the network, to carry out attacks on better protected systems over a longer period of time, potentially undermining the safety of the railway.

Consequently, the core ideals and intention of the framework, with a minimum compliance level in terms of risk assessment and documentation should be mandated within a supporting Railway Group Standard. In this way, the practices that underpin the safety of the railway will be applied across all areas of the industry.

Detecting & Responding to Attacks and Ongoing Monitoring

Detecting and responding to attacks on rolling stock systems is essential for the security and safety of the railway. The first step is to be able to detect an incident when it occurs. This involves identifying and deploying various detection systems to alert an incident response team to an issue.

A range of detection techniques should be selected and deployed in order to identify threats and vulnerabilities in real time, including both automated monitoring of system behaviour as well as manual assessments undertaken by skilled personnel. Automated monitoring can include log analysis, behavioural analytics and anomaly detection software, all of which should be regularly tested and updated in order to stay one step ahead of attackers. These systems can be configured to report to a central location to allow the alerting of, and responding to incidents in a prompt manner. Manual security assessments should include tactics such as network scanning, black box testing and the use of ethical hacking tools in order to identify any potential vulnerabilities that could be exploited by malicious actors.

The next link in the chain is to create a process for managing and responding to an incident. Incident Management and Incident Response are two distinctly processes with overlapping elements.

The aim of Incident Management (IM) is to oversee, communicate, engage support, escalate, report and notify the incident to other functions and agencies.

The IM will determine who in the organisation will have ultimate oversight and accountability for an incident, to what extent the organisation will communicate the progression of the incident response team, what additional support will need to be on standby during the various stages of the incident, signposting for escalation to internal and external agencies (including law enforcement where necessary) and how the outcome of the report will need to be documented.

The aim of the Incident Response and Handling (IHR) process is to triage the incident, analyse the extent of the compromise, contain the risk, eradicate the vulnerability, recover service and review the findings of the incident.

The IRH process will outline the path an investigation must take, setting criteria for triaging the incident to determine the scale of the response required, the key roles within the Cyber Security Incident Response Team (CSIRT), who must fill those roles and how the incident must be documented and reported. The hierarchy of personnel within the incident response process does not necessarily have to reflect the hierarchy of roles within the organisation. It is more important to have the correct person in the role, no matter their seniority within the organisation outside of incident response.

The CSIRT may require a number of roles in order to ensure that incidents are managed and coordinated effectively. These could include:

- Government and law enforcement
- Senior / Executive management
- Incident manager
- Technical lead / Evidence recovery manager
- Crisis management, business continuity, disaster recovery
- Investigators and analysts, cyber security specialists
- IT and infrastructure
- Other departments including legal, PR, HR and customer services

In response to any identified threats or vulnerabilities, or during the introduction of, or change to a system, a risk assessment should be undertaken in order to determine the most appropriate course of action. This may require containment measures such as quarantine or deactivation of affected systems and vehicles, followed by patching if available or replacing with up-to-date secure equipment. Where possible, existing cyber security principles should be applied throughout this process, including vulnerability management systems such as NIST SP 800-82 and ISA/IEC 62443. The development and implementation of cyber security policies should also be a priority to ensure all personnel are made aware of their roles and responsibilities for the protection of rolling stock systems.

In addition, regular auditing and testing of monitored systems must take place in order to ensure that any system changes, deployed mitigations, patches or updates have been applied correctly with no further vulnerabilities present, as well as maintaining the currency of such processes over time. This can include desktop exercises to test the effectiveness of processes, or the use of penetration testing services which are designed to simulate an attack on a system before they occur in real life. Such tests allow organisations to test their defences in advance and gain feedback on areas which may need improvement or additional controls. They can also provide assurance that existing security measures are up-to-date, effective and compliant with industry standards

Conclusions on Creating a Secure Environment for Connected Trains

The next generation of rolling stock is arriving and bringing with it a plethora of new, interconnected digital systems. These systems come with inherent operational risk to the operation and safety of rolling stock and the industry as a whole is woefully underprepared for the emerging cyber security risks. Creating a secure environment for modern connected trains is an important challenge that the railway industry must endure and overcome in order to ensure continued passenger safety and provide reliable services. It requires developing industry led standards, frameworks, policies, procedures and processes that address all avenues of cyber security risks associated with train operations. By following adopting applicable standards such as NIST SP 800-82 and ISA/IEC 62443, the industry will benefit from existing elements of best practice whilst developing solutions that work in the operating railway.

To achieve this will require close collaboration between government and industry stakeholders and a long term commitment to funding and development. Operators and vehicle owners should then build on these frameworks to create risk assessment processes and incident response plans as well as conduct regular auditing of systems, testing of controls, patching of vulnerabilities where possible or replacing insecure equipment. Additionally, personnel within each organisation must be suitably knowledgeable and experienced to assess this new generation of risk. Technical staff must be aware of their role and responsibility for protecting rolling stock systems in the same way they approach safety on a day to day basis.

By incorporating these measures throughout the vehicle and systems expected life, the industry will begin to create more robust solutions which can protect against future threats while ensuring reliability at every its operational life cycle. With adequate planning and implementation strategies in place it's possible to create environment for connected trains that provides passengers with peace of mind when travelling on them each day.

Recommendations

To ensure a secure environment for connected trains, we recommend the following measures be taken by railway organisations:

1. Conduct regular risk assessments and vulnerability scans to identify any potential threats or vulnerabilities.

2. Develop policies and procedures that address all cyber security risks associated with train operations including; incident response plans, testing & validation of security controls, auditing of systems and patching vulnerabilities.

3. Follow applicable standards such as NIST SP 800-82 and ISA/IEC 62443 for guidance in order to ensure maximum protection against cyber
4. Ensure personnel are aware of their roles and responsibilities when it comes to protecting rolling stock systems.

5. Incorporate security measures into design stages of development to create more robust solutions which can protect against future threats and ensure reliability.

6. Use penetration testing services to simulate an attack on a system before they occur in real life, allowing organisations to test their defences in advance and gain feedback on areas which may need improvement or additional controls.

7. Implement appropriate frameworks for managing risk, as well as provide guidance for responding to potential cyber-attacks or incidents.

8. Regularly monitor systems to ensure any system changes, deployed mitigations, patches or updates have been with no further vulnerabilities present and that processes remain up-to-date, effective and compliant with industry standards.

Pride Solutions Derby

Pride Security

Contact

Pride Solutions Derby Ltd

11 The Greenway,
Elvaston,
Derbyshire,
DE72 3UL

01332 949706

PrideSolutions.co.uk
enquiries@PrideSolutions.co.uk