CYBERSECURITY

The Airbus Approach for Cyber Security in the Rail Sector

AIRBUS

SUMMARY

Introduction

Rail Reference Architecture

Threat Modelling for a Real World Scenario

- Attack on Train Control and Management System (TCMS)
- Attack on driver Human Machine Interface (HMI)
- Attack on train CCTV
- Attack on operation control centre (data centre)

Examples of the proposed counter measures

- Network Segregation
- Demilitarised Zone (DMZ)
- Hosts and Network intrusion detection systems
- Access Control
- Security management

The Airbus Approach for Cyber Security in the Rail Sector

Why Airbus CyberSecurity

- Our experience
- What makes us different
- Contact us

Introduction

The rail sector is shifting to a new paradigm of digitalisation to bring in efficiencies to counter the increased demands of travelling passengers and goods transport, while ensuring the highest safety and security of the infrastructure. To achieve this goal, Rail Operators have adopted modern systems combining IT and IoT technologies. Digital transformation strategies within the Rail sector include more connectivity for Industrial Control Systems (ICS), increasing their exposure and potentially making them more vulnerable and exposed to cyber-attacks.

The adoption of new IP-enabled devices within Rail systems and the need to run these new technologies alongside the existing legacy systems adds a new level of infrastructure complexity. Therefore, IT and OT networks within the rail sector could be made more vulnerable to cyber-attacks, and multiple types of cyber-attacks can be initiated by exploiting these vulnerabilities. For example, replay attacks, man-in-the-middle attacks, SQL injection, malware and ransomware attacks, DDoS, phishing, hacktivism, espionage and physical attacks. The impact of cyber-attacks could cause loss of safety, disruption on service availability, financial loss and harm to the reputation of the business and could even impact the national economy. As a result, protecting rail infrastructure is an essential activity which needs to be considered paramount in the Rail Operator's strategy. Alongside this, another key driver for cyber security is the compliance with regulations such as the NIS Directive and GDPR, which can also have major business implications.

The methodology to approach cyber security has to be holistic and consider people, processes, and technology. End-to-end security implementation comprises physical security, (such as CCTV, keys and access cards) network security (such as boundary enforcements, network segregation and detection of network anomalies) and application security (such as identification and access control, host-based intrusion detection and control code integrity). Other factors that need to be considered are security policies and procedures, training and awareness, as well as security analytics to correlate security related information and detect anomalies and potential cyber-attacks.

This whitepaper focuses on the Information and Operational Technology (IT and OT) domains within the rail industry. It aims to provide an insight into potential threats and vulnerabilities to rail ICS systems by demonstrating a case scenario example, model the cyber threats for that case scenario and then provide the mitigations to frame an holistic cyber security approach. The whitepaper will also demonstrate the Airbus CyberSecurity approach for building a cyber security programme and strategy for Rail Operators.

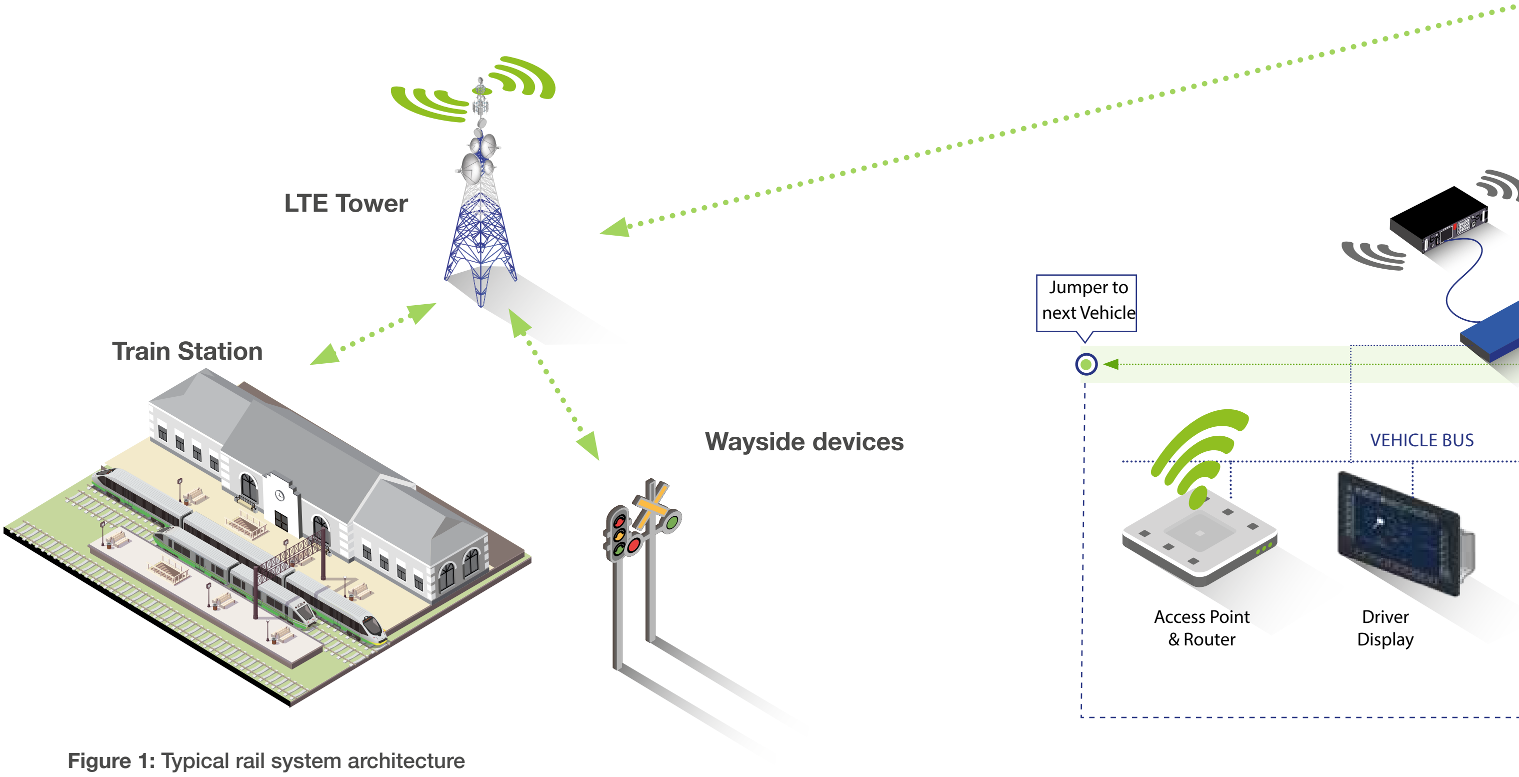


Figure 1: Typical rail system architecture

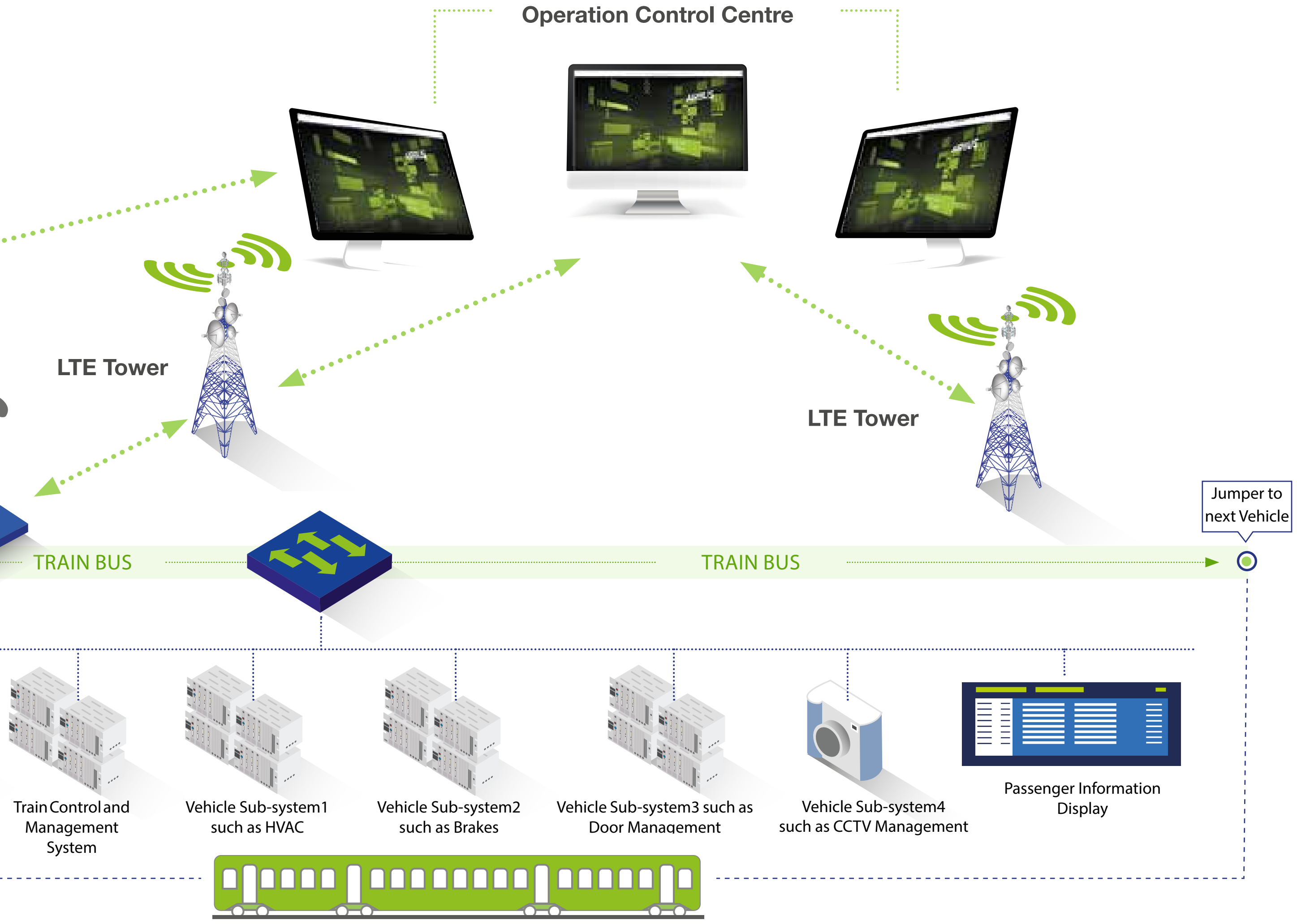
Rail Reference Architecture

A typical Rail architecture, as illustrated in Figure-1, consists of trains, railway stations, wayside devices such as signals and crossing gates as well as the operation control centre (or data centre). Trains, railway stations and wayside devices communicate with the operation control centre via LTE technology over IP/MPLS or GSM-R or microwaves. Trains communicate with wayside devices via Radio WLAN or LTE. The communications link between trains and railway stations is usually via Radio WLAN or LTE.

The Train Communication Network (TCN) consists of communication buses to exchange information between train vehicles. Within the vehicle, two main buses are utilised; the Train Bus and the Vehicle Bus. The Train Bus is used for a wide range of communications between the train vehicles - it uses Wire Train Bus (WTB) technology, which is a shielded twisted-pair wire cable with max of 1 Mbps transmission speed. However, the new technology adopts IP enablement, hence the train bus can utilise Ethernet backbone technology to get higher transmission speeds (up to 1 Gbps) and interconnecting up to 63 vehicles.

Alongside this, the Vehicle Bus is used for the internal communication of train systems such as the Train Control and Management System (TCMS), Passenger Information System (PIS)/PA, driver display, HVAC, lights, door and video surveillance. The Vehicle Bus utilises several technologies like Multifunction Vehicle Bus (MVB), CAN and serial links. MVB technology data transmission speed is 1.5 Mbps and can run over optical fibres, shielded twisted-pair wire cable and simple wire with no galvanic separation. However, improvements in technology are allowing newer trains to be IP enabled, which achieves greater bandwidth and leads to higher integration and efficiencies.

Figure-1 proposes that the Train and Vehicle Buses are Ethernet based technology to achieve interoperability and communication integration between sub-systems. However, some trains use several technologies like Ethernet, MVB, CAN, WTB and interfaces between them by using communication gateways.


Operation Control Centre
LTE Tower
LTE Tower
Jumper to next Vehicle
TRAIN BUS
TRAIN BUS
Train Control and Management System
Vehicle Sub-system1 such as HVAC
Vehicle Sub-system2 such as Brakes
Vehicle Sub-system3 such as Door Management
Vehicle Sub-system4 such as CCTV Management
Passenger Information Display

Threat Modelling for a Real World Scenario

The first step of implementing a holistic cyber security programme starts with understating the security posture and threat landscape of Rail systems. To achieve this, a comprehensive Risk Assessment (RA) should be conducted. The RA methodology considers people, processes and technology. The process starts with identifying threats and vulnerabilities on the target system(s) and its sub-system(s). Next would be to perform risk analysis and risk scoring based on the threats identified. Finally, proposal of counter measures and a roadmap to mitigate all identified risks.

The threats and vulnerabilities identification stage is the most important step during the risk assessment because it is the basis for the risk analysis. Vulnerabilities identification can be carried out by performing a Penetration Testing exercise on the target architecture/infrastructure. Threats identification, on the other hand, can be conducted by performing a threat modelling exercise.

There are several methods used for threat modelling purposes such as MITRE ATT&CK, Cyber Kill Chain, STRIDE, Attack Tree and many others. Airbus is experienced in using these methods and selects the most appropriate when performing a risk assessment for Rail systems. However, this whitepaper will utilise the newly released ICS MITRE ATT&CK to demonstrate how to model cyber threats to an actual real-world scenario.

Based on Airbus' experience in the rail sector, we are using a real-world use case scenario derived from a UK Rail Operator. This use case scenario considers the following assets; passenger WiFi, Train router, TCMS, CCTV and driver HMI. To demonstrate potential cyber-attacks for this case scenario, it has been considered that the adversary's initial access point is the public passenger WiFi. Figure-2 below shows the case scenario system architecture.

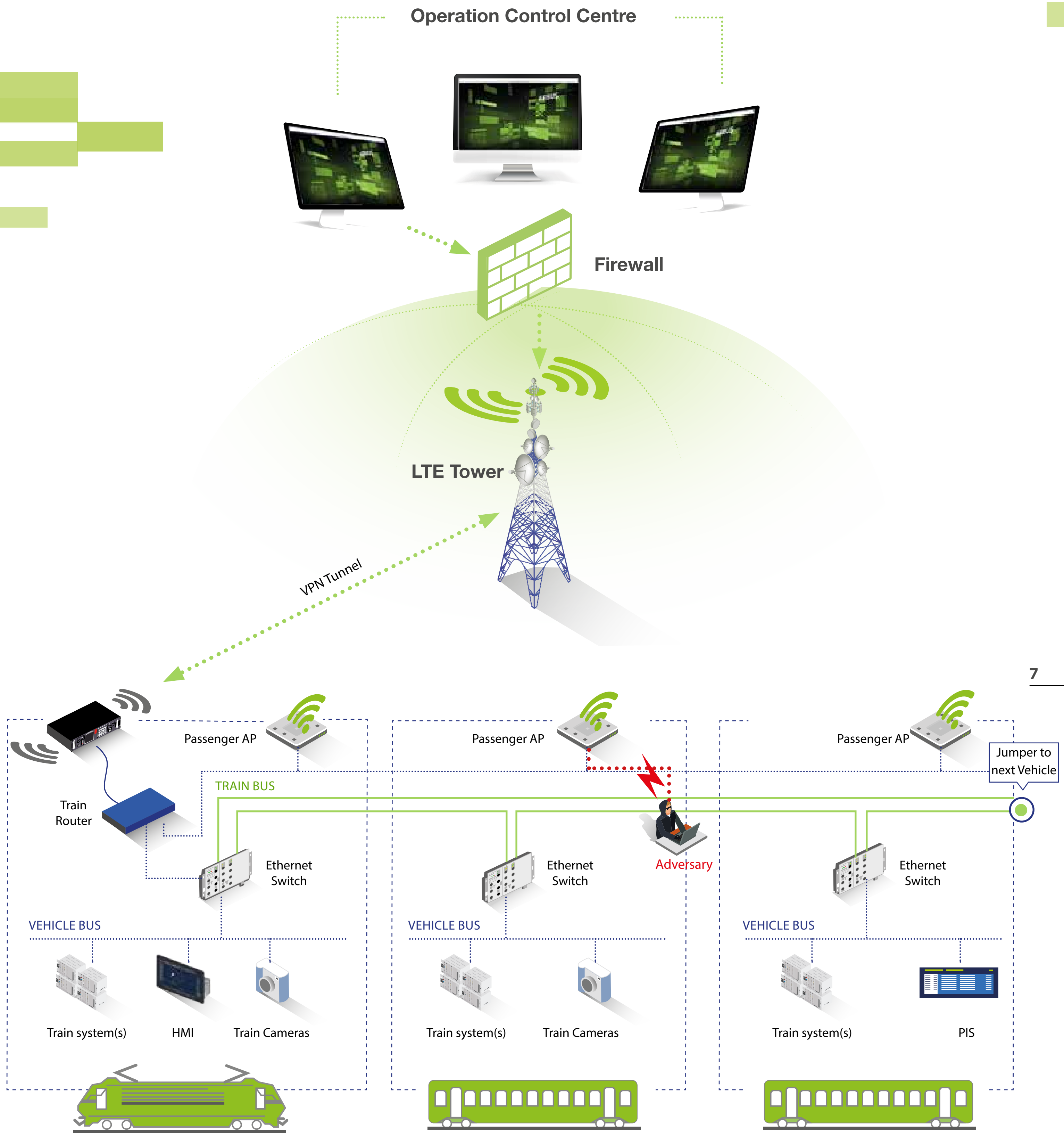


Figure 2: Case scenario example

Threat Modelling:

As mentioned before, this whitepaper uses ICS MITRE ATT&CK to model the threats for the given case scenario, the possible potential attacks are listed as the following:

1. Attack on Train Control and Management System (TCMS)

The adversary's objective is to modify the control logic for the TCMS controller in order to change a command value for certain train functionality such as acceleration.

The attack path is shown in Figure-3a and the MITRE ATT&CK model mapping is shown in Figure-3b below:

Initial Access	Execution	Persistance	Evasion	Discovery	Lateral Movement
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials
Drive-by Compromise	Command Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Dicovery	Exploitation of Remote Services
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	**Network Connection Enumeration**	External Remote Services
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	**Network Service Scanning**	Program Organisation Units
External Remote Services	**Man in the Middle**	System Firmware	Rootkit	Network Sniffing	Remove File Copy
Internet Accessible Device	Program Organisation Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	**Valid Accounts**
Replication Through Removable Media	Project File Infection		Utilise/Change Operating Mode	Serial Connection Enumeration	
Spearphishing Attachment	Scripting				
Supply Chain Compromise	User Execution				
Wireless Compromise					

Figure 3b: MITRE ATT&CK mapping on Train Control and Management System (TCMS)

The attacker initially gains access via the public passenger WiFi, then utilises some network discovery tools to discover all connected devices and their installed services on the network. Once a vulnerable service is discovered (such as a SNMP service) on the train router, the attacker can exploit this vulnerability to acquire a valid account (root or admin access) to the train router and move laterally over the network. Eventually, the attacker can access the TCMS system and modify the control logic. The impact will be on safety and control because this type of cyber-attack could lead to the changing of safety values such as increasing train acceleration, opening of train doors whilst moving or even blocking the braking system.

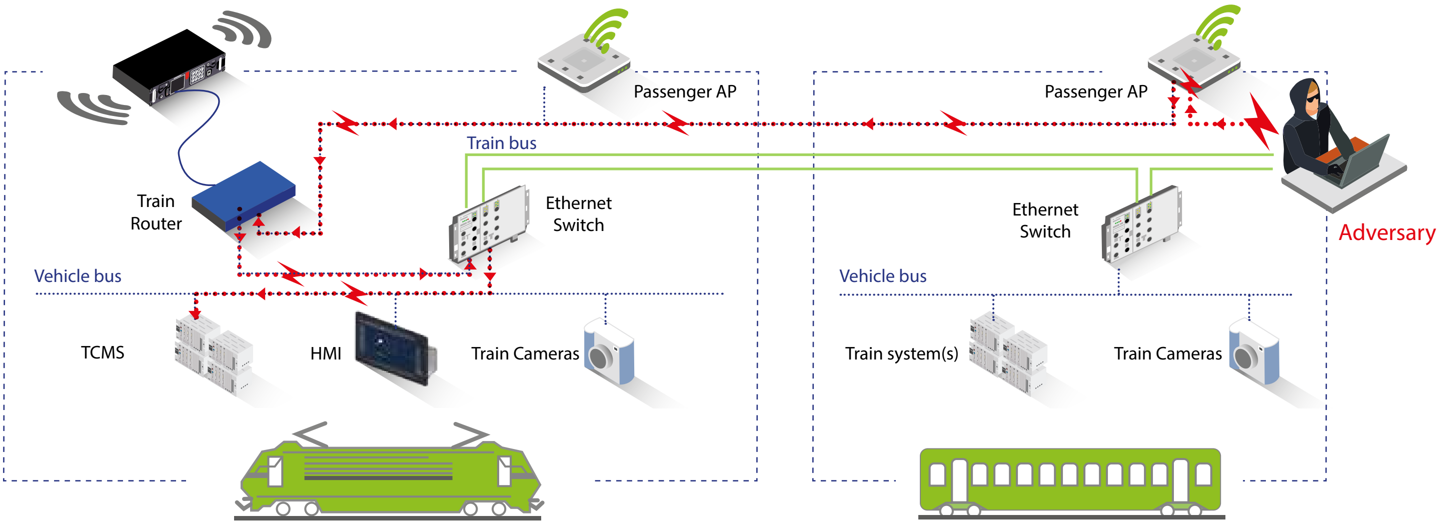


Figure 3a: Attack path on Train Control and Management System (TCMS)

Collection	Command & Control	Inhibit Response Function	Impair Process Control	Impact
Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/0	Damage to Property
Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Location Identification		Data Destruction	Module Firmware	Loss of Productivity & Revenue
Monitor Process State		Denial of Service	Program Download	Loss of Safety
Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Program Upload		Manipulate I/0 Image	Service Stop	Manipulation of Control
Role Identification		Modify Alarm Setting	Spoof Reporting Message	Manipulation of View
Screen Capture		Modify Control Logic	Unauthorised Command Message	Theft of Operational Information
		Program Download		
		Rootkit		
		System Firmware		
		Utilise/ change Operating Mode		

2. Attack on driver Human Machine Interface (HMI)

The adversary's objective is to act as the man-in-the-middle (MITM) between the train systems and driver HMI in order to initiate MITM and replay attacks. The attack path is shown in Figure-4a and the MITRE ATT&CK model mapping is shown in Figure-4b below:

Initial Access	Execution	Persistance	Evasion	Discovery	Lateral Movement
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials
Drive-by Compromise	Command Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Dicovery	Exploitation of Remote Services
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	**Network Connection Enumeration**	External Remote Services
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	**Network Service Scanning**	Program Organisation Units
External Remote Services	**Man in the Middle**	System Firmware	Rootkit	Network Sniffing	Remove File Copy
Internet Accessible Device	Program Organisation Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	**Valid Accounts**
Replication Through Removable Media	Project File Infection		Utilise/Change Operating Mode	Serial Connection Enumeration	
Spearphishing Attachment	Scripting				
Supply Chain Compromise	User Execution				
Wireless Compromise					

Figure 4b: MITRE ATT&CK mapping on driver HMI

The adversary gains access to the network by exploiting a vulnerability or several vulnerabilities to gain a valid account (root or admin access) and perform lateral movement into the network, which gives the adversary the ability to act as the man-in-the-middle and intercept the network traffic between train systems (like TCMS, DAS, PIS) and driver HMI to perform the cyber-attacks. The attacker could perform Alarm suppression, block command messages, cause data destruction and denial of service. The safety case in this context is important to consider and mitigate as losing the HMI view for DAS, PIS or TCMS systems could lead to having an out of control train within the fleet.

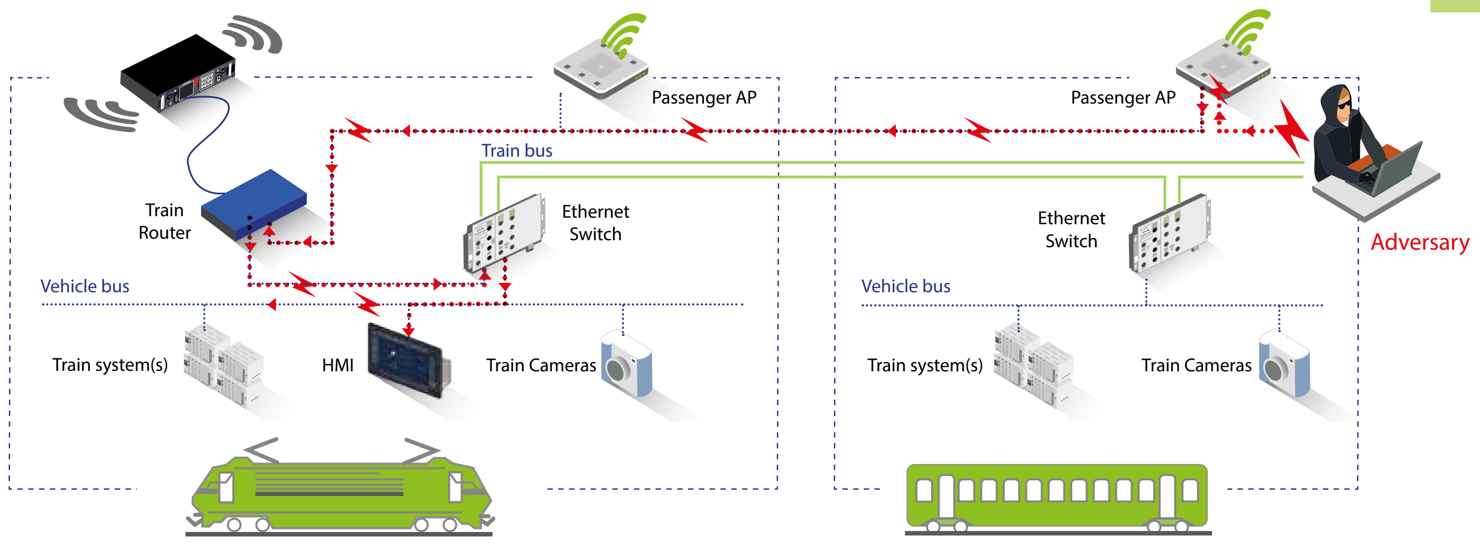


Figure 4a: Attack path on driver HMI

Collection	Command & Control	Inhibit Response Function	Impair Process Control	Impact
Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/0	Damage to Property
Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Location Identification		Data Destruction	Module Firmware	Loss of Productivity & Revenue
Monitor Process State		Denial of Service	Program Download	Loss of Safety
Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Program Upload		Manipulate I/0 Image	Service Stop	Manipulation of Control
Role Identification		Modify Alarm Setting	Spoof Reporting Message	Manipulation of View
Screen Capture		Modify Control Logic	Unauthorised Command Message	Theft of Operational Information
		Program Download		
		Rootkit		
		System Firmware		
		Utilise/ change Operating Mode		

AIRBUS

3. Attack on train CCTV

The adversary’s objective is to gain access to the train CCTV and video recording system.
The attack path is shown in Figure-5a and the MITRE ATT&CK model mapping is shown in Figure-5b below:

Initial Access	Execution	Persistance	Evasion	Discovery	Lateral Movement
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials
Drive-by Compromise	Command Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Dicovery	Exploitation of Remote Services
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organisation Units
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remove File Copy
Internet Accessible Device	Program Organisation Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts
Replication Through Removable Media	Project File Infection		Utilise/Change Operating Mode	Serial Connection Enumeration	
Spearphishing Attachment	Scripting				
Supply Chain Compromise	User Execution				
Wireless Compromise					

Figure 5b: MITRE ATT&CK mapping on CCTV and video recording system

The adversary gains access to the network via the compromised train router and performs lateral movement techniques in order to access the train cameras. The attacker could access the train cameras by performing a brute-force attack over standard application layer protocols such as HTTP. The attacker could also perform a denial-of-service for the cameras or theft of video recordings. The impact is on safety, confidentiality and loss of monitoring for the CCTV cameras.

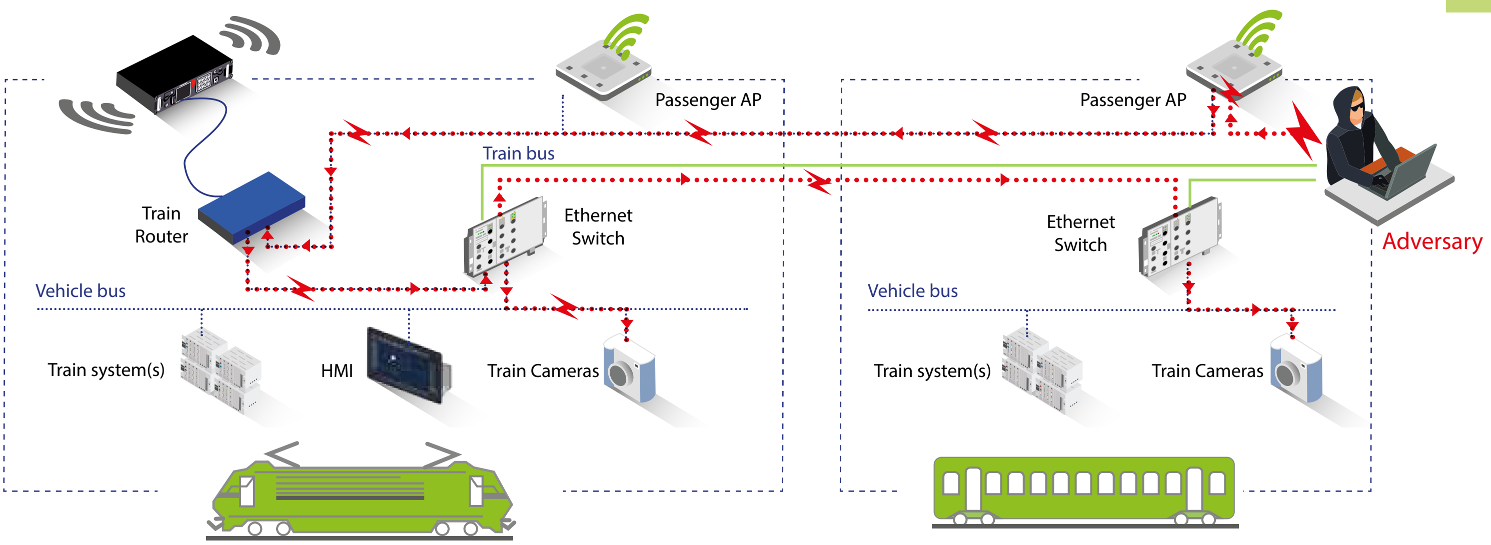
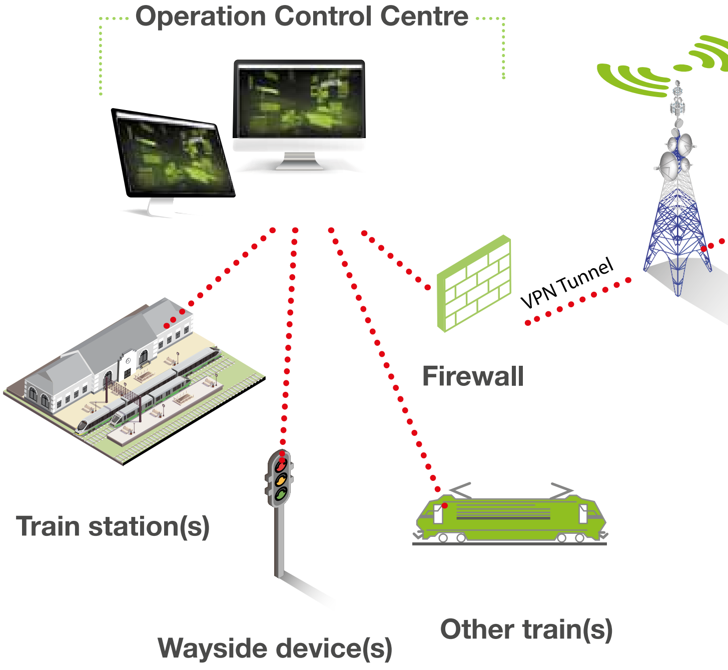


Figure 5a: Attack path on CCTV and video recording system

Collection	Command & Control	Inhibit Response Function	Impair Process Control	Impact
Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/0	Damage to Property
Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Location Identification		Data Destruction	Module Firmware	Loss of Productivity & Revenue
Monitor Process State		Denial of Service	Program Download	Loss of Safety
Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Program Upload		Manipulate I/0 Image	Service Stop	Manipulation of Control
Role Identification		Modify Alarm Setting	Spoof Reporting Message	Manipulation of View
Screen Capture		Modify Control Logic	Unauthorised Command Message	Theft of Operational Information
		Program Download		
		Rootkit		
		System Firmware		
		Utilise/ change Operating Mode		



4. Attack on operation control centre (data centre)

The adversary's objective is to gain access to the operation control centre systems such as SCADA, traffic management, maintenance system, etc. Moreover, the adversary aims to access the entire rail infrastructure including trains, wayside devices and train stations. The attack path is shown in Figure-6a and the MITRE ATT&CK model mapping is shown in Figure-6b below:

Initial Access	Execution	Persistance	Evasion	Discovery	Lateral Movement
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials
Drive-by Compromise	Command Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Dicovery	Exploitation of Remote Services
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organisation Units
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remove File Copy
Internet Accessible Device	Program Organisation Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts
Replication Through Removable Media	Project File Infection		Utilise/Change Operating Mode	Serial Connection Enumeration	
Spearphishing Attachment	Scripting				
Supply Chain Compromise	User Execution				
Wireless Compromise					

Figure 6b: MITRE ATT&CK mapping on operation control centre (data centre)

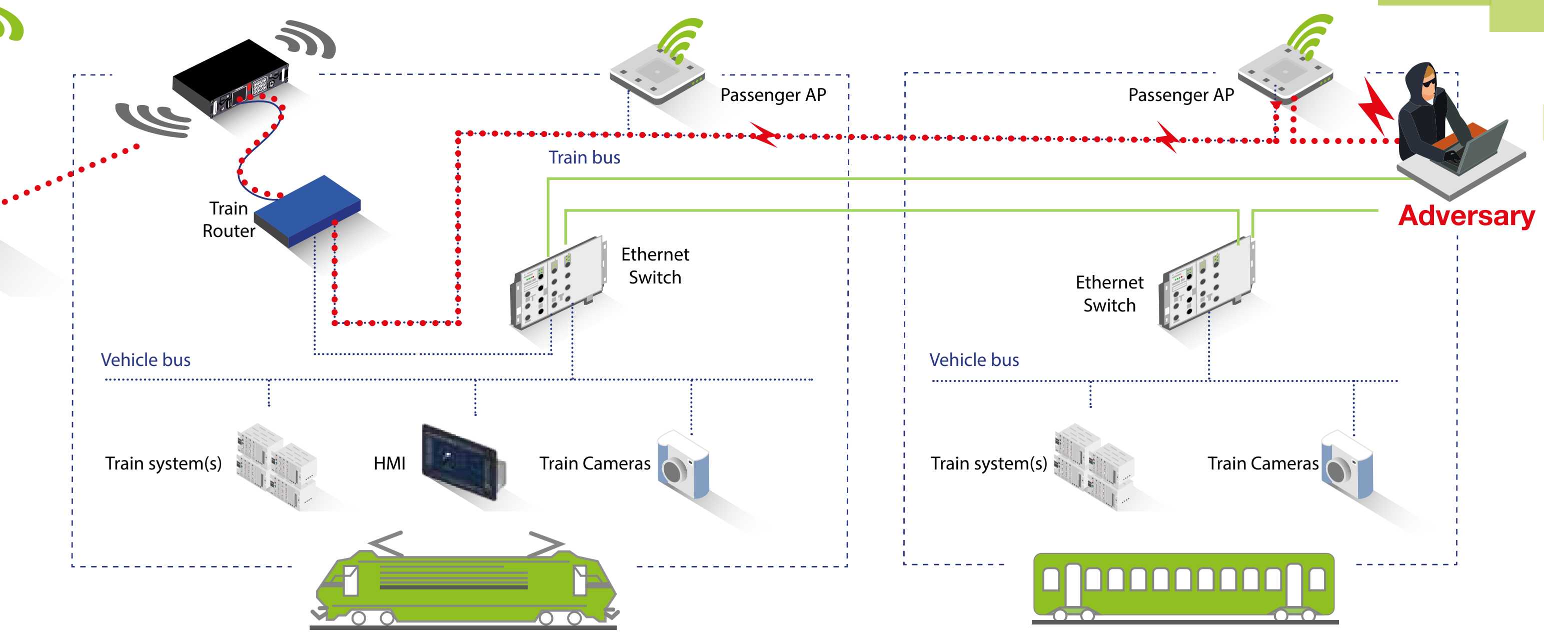


Figure 6a: Attack path on operation control centre (data centre)

Collection	Command & Control	Inhibit Response Function	Impair Process Control	Impact
Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/0	Damage to Property
Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Location Identification		Data Destruction	Module Firmware	Loss of Productivity & Revenue
Monitor Process State		Denial of Service	Program Download	Loss of Safety
Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Program Upload		Manipulate I/0 Image	Service Stop	Manipulation of Control
Role Identification		Modify Alarm Setting	Spoof Reporting Message	Manipulation of View
Screen Capture		Modify Control Logic	Unauthorised Command Message	Theft of Operational Information
		Program Download		
		Rootkit		
		System Firmware		
		Utilise/ change Operating Mode		

The adversary gains access to the network by exploiting a vulnerability and is able to access a valid account (root or admin access) over the train router. With access to the train router, authentication keys for VPN and SSH keys can be obtained to allow the attacker to perform further privilege escalations to gain access to the operation control centre. Compromising operation control centre systems could initiate highly damaging attacks on the train fleet, railway stations and wayside devices managed by the operation control centre. This damage could expand to national Rail Operators or even globally if the operation control centre has management over global train fleets. Hence, Rail Operators are highly recommended to conduct penetration testing across their complete rail infrastructure to identify all threats & vulnerabilities and possible cyber-attack paths.

Airbus' penetration testing partner organisation, Modux Ltd, are a NCSC-approved CHECK company and highly regarded in the industry and are highly experienced in penetration testing and vulnerability analysis across many types of infrastructure and industry verticals.

Furthermore, to help understanding the risks and attack paths, Airbus has developed a tool called icsModel which aims to model cyber threats for CNI. The tool models and simulates the risks associated with people, processes and technology and to determine the critical attack paths based on the dependencies between these risks. Figure-7 shows a snapshot from the tool and how the risks are related to each other.

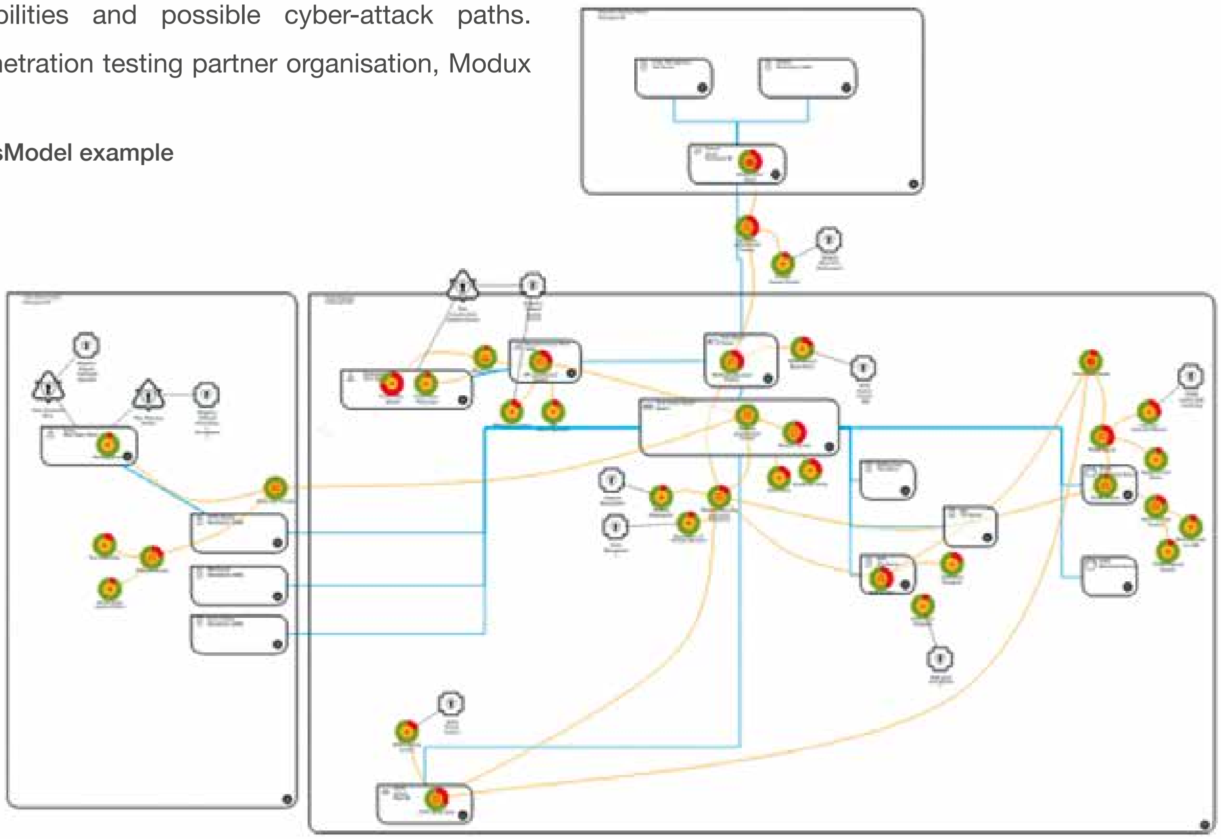


Figure 7: icsModel example

Examples of the proposed counter measures

The following mitigations are focused on the real-world case scenario and are based on Airbus' observations of the Rail industry:

- **Network Segregation:**
  One of the common findings in Rail infrastructure is the poor design of network architecture and the network devices not being configured to best practice, especially train router devices. The Train Communication Network should have physical segregation by utilising a dedicated switch for each network or logical segregation by configuring a dedicated VLAN for each network.

  The network design should also consider boundary enforcement by utilising enforcement devices such as Firewalls and implementing secure configurations over the network devices (switches, routers, proxy servers, firewalls, gateways and data diodes).

- **Demilitarised Zone (DMZ):**
  The DMZ is essential to air gap three different zones: trusted zone (Rail infrastructure), untrusted zone (Internet) and middle zone (Application layer). DMZ isolates trains, railway stations, wayside devices and the operation control centre from the Internet.

  To extend the private network between trains, train stations, wayside devices and the operation control centre, it is recommended to use a Virtual Private Network (VPN) to establish a secure connection. Several VPN types can be used within the Rail infrastructure such as IPSec VPN or MPLS-based Layer3 VPN. Depending on the security requirements and network technology used (such as IP/MPLS technology), the VPN type can be selected.

- **Hosts and Network intrusion detection systems:**
  Having security visibility and monitoring over the network and computer systems (IT and OT endpoints) is essential. Several Network IPS/IDS solutions are available for this purpose, the selection of security vendors should consider IPS/IDS for specific OT industrial protocols as well as consider the criticality of passive and active monitoring methods. Host IPS/IDS solutions can be utilised, such as blacklisting and whitelisting solutions, malware and spyware detections as well as system diagnostics monitoring

- **Access Control:**
  Access control is an authentication and authorisation mechanism for users and communication partners used in Rail systems. Access Control implementations need to be deployed based on the criticality of the device and consider least privilege and need-to-know basis. If possible, two-factor authentication (2FA) can be utilised, especially for gateways and proxy servers

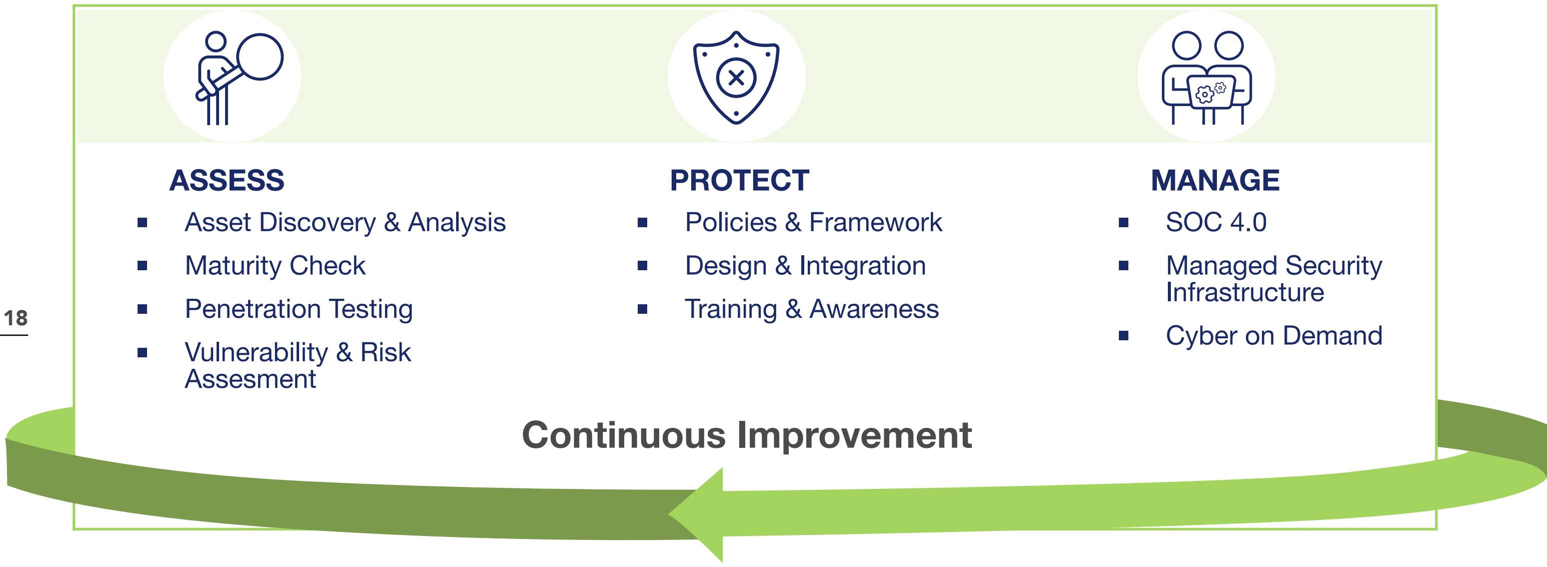
- **Security**
  This includes a protective and proactive security monitoring and management system. Solutions such as Security Information and Event Management (SIEM), security event collections and correlations, incident response, threat intelligence and disaster recovery can be utilised to monitor and manage the security posture of both IT and OT Railway infrastructure. A Security Operations Centre (SOC) is necessary to orchestrate and automate all of the aforementioned solutions.

Airbus provides SOC4.0 services as a Managed Security Service Provider (MSSP), where this service provides security management for IT and OT infrastructure for Rail Operators - further information about this service can be found in this link.

The Airbus Approach for Cyber Security in the Rail Sector

Rail Operators, infrastructure managers and other rail stakeholders need to take prompt action to start building their cyber security strategy and programme to tackle cyber issues. This initiative requires senior management and wider staff support and commitment. The cyber security programme should be in line with the business objectives and business continuity plan, as well as business availability during adverse conditions. Understanding the current security posture of the Rail infrastructure is essential to build the cyber security strategy. Many standards are available which can be used to determine a framework for cyber security. For example, the NIST framework is: "Identify, Protect, Detect, Respond, Recover". NIS Directive framework is: "Manage, Protect, Detect, Minimise the Impact". Airbus can work with Rail Operators to build the cyber security strategy and programme to meet their followed standard and best practices.

The cyber security programme starts with visibility of the infrastructure, including asset management for the information and operational technology (IT and OT) infrastructure, then understanding the current security state by conducting a comprehensive risk and vulnerability assessment. The outcome of this stage will list the IT and OT assets based on their criticality and score all the risks associated with these assets and thus, countermeasures can be proposed to mitigate the identified risks. Figure-8 below shows the Airbus services, which are derived from NIST and NIS frameworks: «Assess (or identify), Protect, Manage (detect & response), to build a cyber security programme for Rail Operators:



ASSESS

- Asset Discovery & Analysis
- Maturity Check
- Penetration Testing
- Vulnerability & Risk Assesment

PROTECT

- Policies & Framework
- Design & Integration
- Training & Awareness

MANAGE

- SOC 4.0
- Managed Security Infrastructure
- Cyber on Demand

Continuous Improvement

Figure 8: Airbus services for Rail Operators

The second stage of the programme should design the mitigation proposals and convert them into deployable solutions for IT and OT Rail infrastructure, where solutions should include people, processes and technology. Technology solutions include network security, access control, endpoint security, anomalies and intrusion detection, and physical security. Processes include review and development of cyber security policies and procedure such as change management policy, patch management policy, external service policy, etc. People aspects to consider are cyber security training and awareness for employees including rail related threats and cyber-attacks. The OT security team for Train Operators should also have a specialised training roadmap.

The final stage of the programme should manage and orchestrate the cyber security solutions deployed within the IT and OT Rail infrastructure. This is mainly represented by a Security Operations Centre (SOC) to monitor and detect all anomalies and possible cyber-attacks and respond to these events – the SOC can also orchestrate the rail systems recovery in case of an incident.

Airbus can support and work hand-in-hand with Rail Operators to develop their security programme and design these solutions.

In conclusion, Rail Operators should start their cyber security strategy and programme to ensure safety and security. They also need to build a roadmap to implement this programme, the roadmap could vary from months to years depending on the organisation size and scale. Moreover, Rail Operators need to create a platform for information sharing about cyber security and create a committee to involve different stakeholders from across the industry to be part of implementing cyber security in order to achieve the overall targets for the Rail sector within the nation or the region.

Why Airbus CyberSecurity

Our experience

Airbus CyberSecurity provides dedicated Cyber Security solutions to protect governments, national agencies, critical infrastructure, manufacturing and commercial organisations around the world from increasingly sophisticated cyber threats through a range of protective and responsive services.

Our cyber security solutions were developed to protect the Airbus business from cyber-attacks. Over a number of years, our methodologies, tools and processes have been continuously refined to protect us against the evolving cyber threat scenario. The same highly experienced individuals and technologies used to defend Airbus systems are made available to our commercial and Government customers, in order to ensure that their systems and networks are as well protected as those of Airbus.

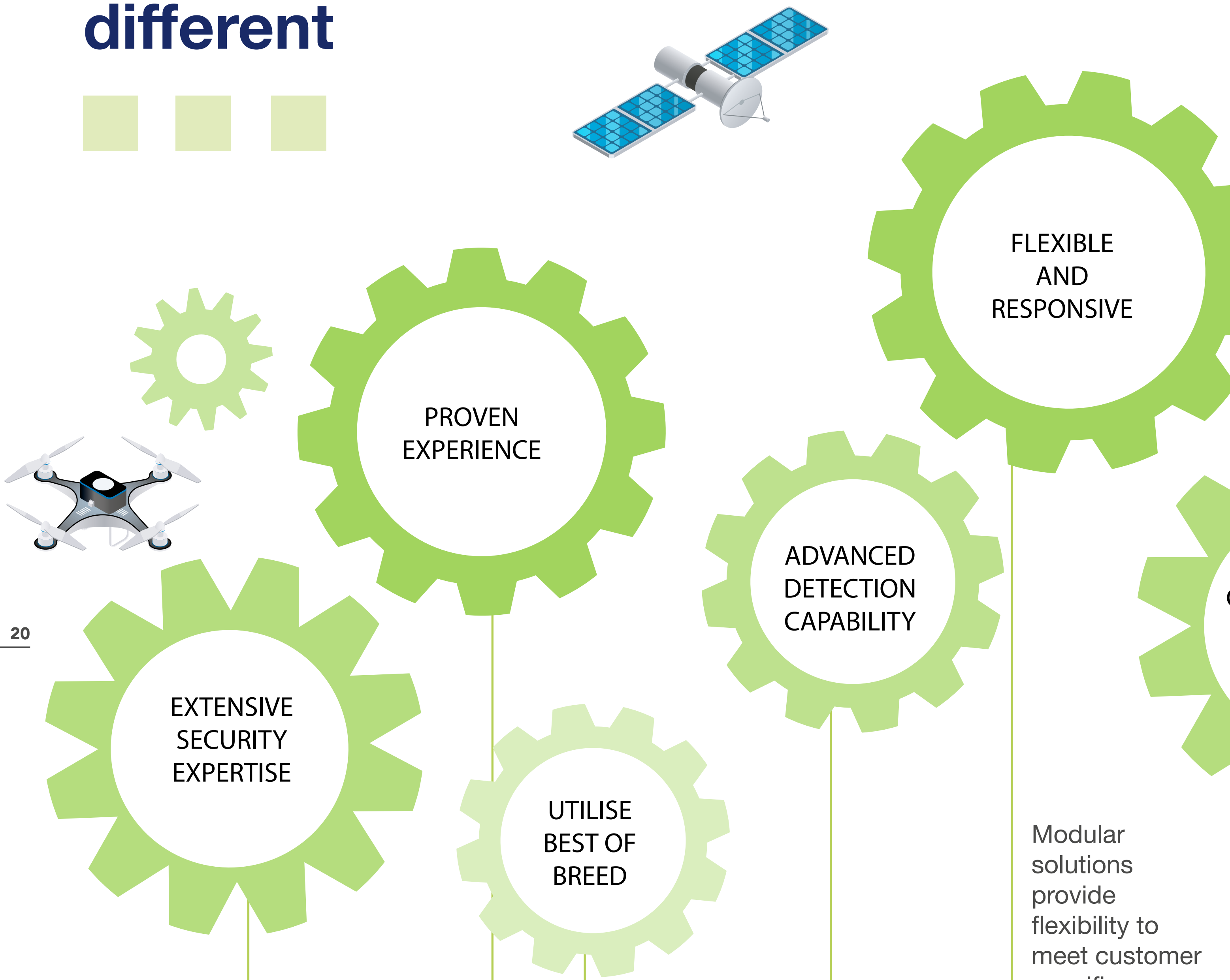
Based on our heritage, within the aviation, maritime, defence and space sectors, Airbus is well equipped to operate in a highly regulated, global and complex business environment. Operating on a 24/7 basis, our cyber security solutions can be adapted to the customer's specific requirements. Airbus continues to invest heavily in developing our cyber security solutions to ensure that we provide the best defence possible against current and future cyber threats.

Our ISO/IEC 27001 certified SOC services deliver highly accurate, near real-time detection and alerting against the world's most sophisticated threat actors and provides a global view across the business, all from a single management platform. This, combined with our powerful global Threat Intelligence (TI) and in-house developed malware analysis tools, means we can accurately and quickly identify even the most advanced cyber-attacks.

Airbus CyberSecurity		
Best of breed technologies configured to best meet our customers' specific requirements	Protecting critical IT and OT systems across a range of industries	Highly skilled security cleared experts across full spectrum of cyber capabilities
24x7 security monitoring with three levels of expertise, customised reporting and a Service Delivery Manager	Bespoke use cases and threat intelligence to detect cyber-attacks at all stages of the cyber kill chain enabling earlier identification and informed mitigation actions	Modular solutions provide flexibility to meet customer specific requirements and reuse customer existing equipment where possible
Accredited and trusted by national authorities to operate securely and confidentially	Experience in defending our own systems gives us unique insight in understanding the security threats and vulnerabilities facing safety critical industries	Continual service improvement by tuning system, using the latest threat intelligence, refining use cases and on-boarding additional devices

AIRBUS

What makes us different



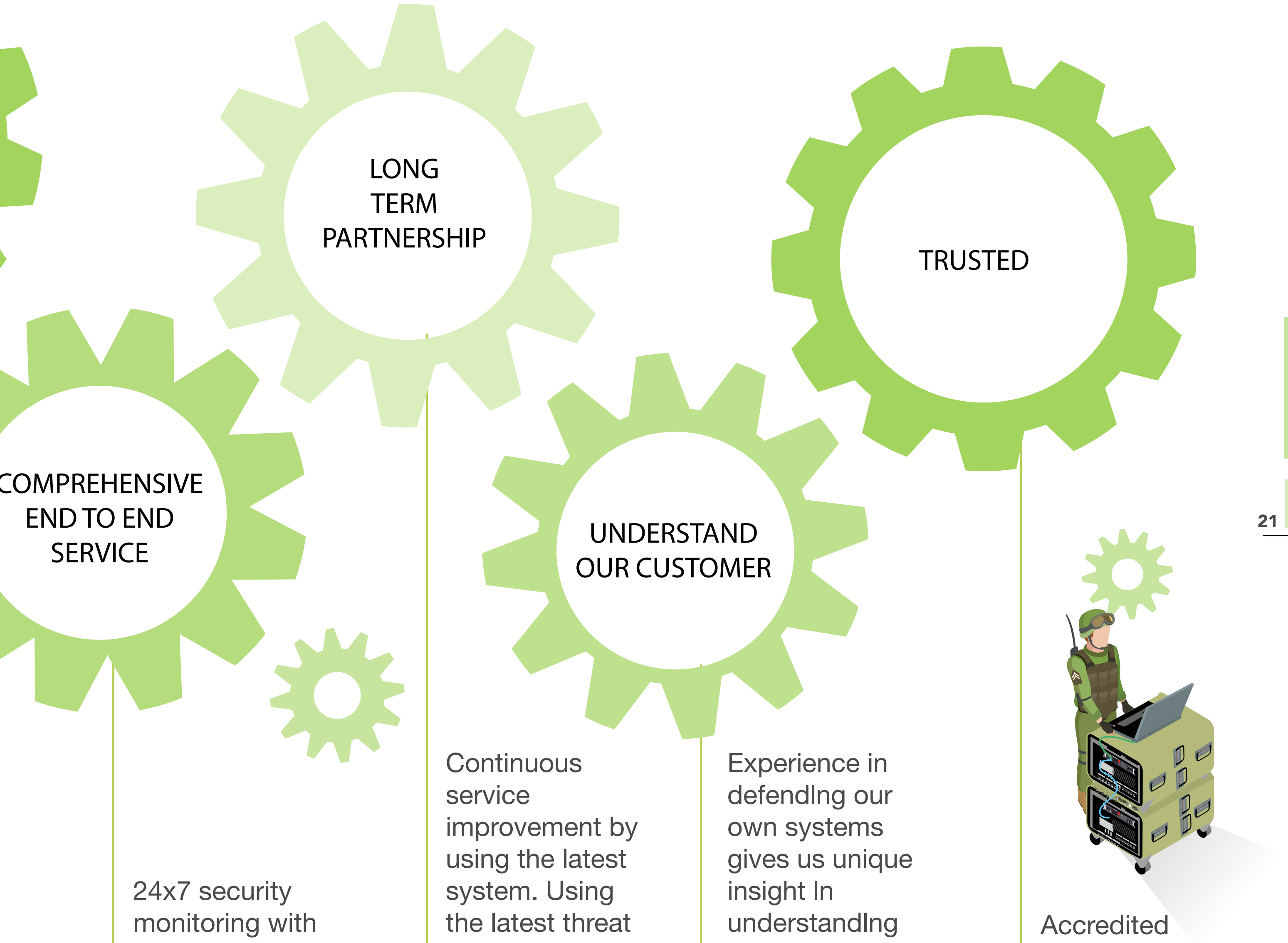
EXTENSIVE SECURITY EXPERTISE: Highly skilled, certified, security cleared experts across full spectrum of cyber capabilities

PROVEN EXPERIENCE: Protecting critical IT and OT systems across a range of industries

UTILISE BEST OF BREED: Choosing the best tools to effectively and cost-efficiently deliver results

ADVANCED DETECTION CAPABILITY: Leveraging Advanced Correlation and Anomaly Detection

FLEXIBLE AND RESPONSIVE: Modular solutions provide flexibility to meet customer specific requirements and reuse customer existing equipment where possible



COMPREHENSIVE END TO END SERVICE

LONG TERM PARTNERSHIP

UNDERSTAND OUR CUSTOMER

TRUSTED

24x7 security monitoring with three levels of expertise, customised reporting and a Service Delivery Manager

Continuous service improvement by using the latest system. Using the latest threat intelligence, refining use cases and on-boarding additional devices

Experience in defendIng our own systems gives us unique insight In understandIng the security threats and vulnerabilities facing safety critical industries

Accredited and trusted by national authorities to operate securely and confidentially

Contact us

FOR MORE INFORMATION:
Airbus CyberSecurity

FRANCE
Metapole 1, boulevard Jean Moulin /
CS 40001 / 78996 Elancourt Cedex/
France

GERMANY
Willy-Messerschmitt-Str. 1 /
82024 Taufkirchen / Germany

UNITED KINGDOM
Quadrant House / Celtic Springs
/ Coedkernew / South Wales
NP10 8FZ / United Kingdom

contact.cybersecurity@airbus.com
www.airbus-cyber-security.com

AIRBUS