NORTH AMERICA TRANSIT CYBERSECURITY CONSORTIUM

OPERATIONAL TECHNOLOGY PROCUREMENT REQUIREMENTS

CONTENTS

Revision History

Date	Version	Change
10/19/2022	1.0	Original draft.
10/21/2022	1.1	Rearranged sections. Edited content for clarity and completeness.
10/24/2022	1.2	Updated content and syntax.
5/16/2023	1.3	Added additional references to 62443
6/1/2023	1.4	Minor changes in Security patching and mitigation governance
8/16/2023	1.5	Minor changes in Documentation and definition section
11/16/2023	1.6	Minor changes in Vulnerability Discovery section
1/31/2024	1.7	Alignment with the key aspects of the NIST 800-82 R3

1 OVERVIEW AND SCOPE

This Agreement specifies Cybersecurity Operational Technologies (OT) Procurement Requirements as a guideline for members of the North America Transit Cybersecurity Consortium.

It establishes a consistent management approach to leverage security protocols across railway infrastructures and provides essential information necessary to navigate the ever-evolving sophisticated threat landscape across the Railway sector.

A consensus on the threat landscape between all Stakeholders is crucial to building a centralized cybersecurity strategy that detects, identifies, prevents, circumvents, recovers, and manages the various levels of cybersecurity threats that can jeopardize the railway system.

To counter these threats, all Stakeholders are encouraged to participate in a process as defined in this Agreement and to agree on a generally accepted threat landscape that is based on recognized and accepted threat libraries and reports.

This Agreement is designed to serve as a baseline for all stakeholders, specifically railway operators, system integrators, and product suppliers. The scope of the agreement covers the implementation of the system under consideration (SuC) as a system of systems and its integration with other systems in an Authority's operational landscape. The SuC shall be designed and implemented based on this agreement's provisions. The SuC may be any system that participates in providing services to the transportation environment including but not limited to signaling, communication, processing, operational technology, SCADA and rolling stock. In some cases, the SUC may integrate within existing system to form a system of systems. In other, the SUC may only interface with other systems and processes within the existing environment. In most cases, the SUC will need to perform both functionalities.

This Agreement is compliant with industry TS-50701, NIST 800-82r3 and government standards that govern cybersecurity processes and controls including ANSI/ISA 62443 and NIST 800-53 current revisions. While adhering to this Agreement, should any conflicts between standards arise, ANSI/ISA 62443 recommendations shall take precedence.

The North America Transit Cybersecurity Consortium comprises the following organizational entities tabulated in alphabetical order.

North America Transit Cybersecurity Consortium Organizations	
Transit | State | Authority	**Serving Authority**
AC Transit, Oakland, CA	Central Ohio Transit Authority
Centro Syracuse, NY	Chicago Transit Authority
Dallas Area Rapid Transit ((DART), TX	
Go Metro Cincinnati, OH	Southwest Ohio Regional Transit Authority
Golden Gate Bridge	Highway and Transportation District CA
Greyhound Lines North America	Greyhound Lines
Hampton Roads Transit, VA	Transportation District Commission of Hampton Roads
Long Beach Transit (LBT), CA	
Massachusetts Bay Transportation (MassDOT) Authority	Massachusetts Department of Transp ortation Board
Metra Commuter Rail (Metra) WI, IL	Regional Transportation Authority (RTA)

North America Transit Cybersecurity Consortium Organizations	
Transit | State | Authority	**Serving Authority**
Metropolitan Atlanta Rapid Transit Authority, GA	
Metropolitan Council Minneapolis, MN	
Metropolitan Transit Authority of Harris County, Houston, TX	
New Jersey Transit	The New Jersey Department of Transportation's Office of Fixed Guideway
Northern Indiana Commuter Transportation District (NICTD)	
Orange County Transportation Authority, CA	
Pace Suburban Bus, Chicago, IL	
Port Authority Pittsburgh, PA	
Port Authority of NY/NJ	
Regional Transportation Authority, Chicago, IL	
RTC Southern Nevada	
Sacramento Regional Transit District	
San Diego Metropolitan Transit System	
San Francisco Municipal Transportation Agency	
Santa Clara Valley Transportation Authority, CA	
Société de transport de Montréal, Canada	
Sound Transit Seattle, WA	
Southeastern Pennsylvania Transportation Aut hority, Philadelphia, PA	
Southern California Regional Rail Authority	
Toronto Transit Commission, Canada	
Transbay Joint Powers Authority, San Francisco	
TransLink Vancouver, Canada	
TriCounty Metropolitan Transportation District of Oregon, Portland	
Utah Transit Authority	

2 CYBERSECURITY SUC AGREEMENT REQUIREMENTS

This Agreement stipulates Security Contract Terms and Conditions for System(s) Under Consideration (SuC). The cybersecurity requirements stated herein are to be implemented by the Vendor responsible for providing SuCs that will be operated by the Authority or operated by the Vendor.

A SuC is defined as a collection of Integrated Administration and Control System (IACS) assets, subsystems and components including network infrastructures, that provide complete automated solutions. A SuC can be deployed into one or more zones and related conduits. All assets within a SuC belong to a zone or a conduit.

Upon completion of the Risk Assessment Process, the vendor shall submit a cybersecurity plan for the review and approval of the Authority. The plan shall cover, at a minimum, how the vendor will address cybersecurity risks and establish the programs described in this agreement. The cybersecurity plan and material produced or exchanged in connection with this agreement shall be classified as restricted data. Data classified as Restricted shall be encrypted at rest and in motion. The Vendor shall apply necessary rules and controls to prevent unauthorized disclosure of such material.

3 SUC RISK ASSESSMENT

3.1 SUC DOCUMENTATION & DEFINITION

The Vendor shall provide documentation detailing the SuC and its components as follows:

1. Definition document that defines the overall scope, functionality, features and boundaries of the SuC.
2. The SuC objective and mission profile comprised of SuC functions, boundaries, and interfaces.
3. Description and functionality of each essential function, internal and external dependencies, and subsystems contributing to each essential function, physical and network interfaces, and the actors interacting or interfacing with the SuC. The actors may be adjacent systems, hardware, software, processes, communications or subsystems.
4. SuC integration to other railway systems; whether the SuC incorporates other systems, is part of a larger system, or both. The Authority shall provide the Vendor with the necessary information for the Vendor to develop dependency diagrams representing SuC relationships to affiliated/integrated systems.
5. The boundaries and interfaces of the systems, the zones and conduit environments the SuC will operate in.
6. Additional documentation summarizing the SuC's security features and security-focused instructions on product maintenance, support, and reconfiguration of default settings.
7. Documentation shall include use-case operational scenarios that define how the SuC will be used and constraints by the environment in which the SuC operates.
8. The planned lifetime and necessary lifecycle system updates for Hardware and Software.
9. Roles and responsibilities for maintaining cybersecurity features and activities for the SuC.
10. The initial draft of the Supply Chain Security requirements defined in section 20 of this document.

3.2 PHYSICAL AND ENVIRONMENTAL IMPACT ANALYSIS

As part of the risk assessment, the Vendor shall analyze and document the potential physical and environmental impact of cybersecurity risks associated with the SuC including the potential safety risks resulting from a cybersecurity compromise. As a part of the safety case, the vendor shall evaluate and document the larger context the SuC's operational environment and that of the Authority's railway system as a whole. How could a cybersecurity compromise of the SuC result in physical impacts on the SuC's operational environment or other railway processes? Specifically, the vendor shall analyze and document the following:

1. Define how a cybersecurity incident could manipulate the physical environment and other railway operations, including operational downtime caused by denial-of-service type attacks.
2. Document how a cybersecurity event on the SuC could cause a cascading physical impact on other OT systems and railway operations.
3. Design features of the SuC to mitigate or prevent the associated physical risks.

3.3 RISK ASSESSMENT DOCUMENTATION

The Vendor shall perform the necessary risk assessment activities to securely deploy the SuC into railroad operations as detailed in the following subsections.

3.3.1 Initial Risk Assessment

The Vendor shall perform an Initial Risk Assessment (IRA) documenting the cybersecurity threat risk assessment and related threat risk treatment and protection. The IRA shall consider the potential impact of cyberattacks on safety functions, forecast potential worst-case impact scenarios to railway operations in terms of human health and safety, operational availability, financial impact, and develop the following:

1. Cybersecurity impact assessment based on the Authority's risk matrix.
2. Likelihood assessment for cybersecurity risks, risk evaluation and assessment of protection requirements

The Authority shall approve the Initial Risk Assessment documents.

The IRA will lead to the definition and agreement of the Security Level Targets for the SuC, subsystems, and components based on the ISA-62443-3-2-2020 Standard for each zone and conduit as determined by the Zone and Conduit Requirement (ZCR).

3.3.2 Zones and Conduits Design

As part of the risk assessment process, the Vendor shall complete the initial design of the zones and conduit documents for the SuC. The design shall ensure that Operational Technologies systems can continue to function safely in the event that a related Information Technology system has been compromised. The Vendor shall submit for approval the Zones and Conduit design to the Authority detailing the following categories:

1. Type of interfaces or connections to other components of the SuC
2. Physical or logical location(s)
3. Access requirements
4. Operational function(s)
5. Organizational responsibilities for each asset
6. Physical separation of safety systems in dedicated zones
7. Separation between Operational Technologies Zones and IT Zones.
8. Categorize zones and conduit assets in hierarchical groups wherein the highest security requirement is enforced as the security requirement for all components in the zone.
9. The design shall follow the Purdue Enterprise Model (PEM) principles categorizing each zone according to the model and detailing how the separation between zones will be configured.

3.4 DETAILED CYBER RISK ASSESSMENTS

The Vendor shall perform a Detailed Cyber Risk Assessment (DCRA) in collaboration with the Authority's cybersecurity, safety, and operational staff in accordance with the Authority's risk matrix. The DCRA shall take into consideration the zones and conduit design, essential and nonessential functions, and the operational requirements of the SuC. The vendor shall deliver a documented DCRA as listed below.

1. Evidence-based assurance that cybersecurity functions shall not negatively impact safety functions or other essential functions.
2. Define threat landscapes, use cases, and potential cybersecurity threats based on the MITRE ATT&CK framework for individual and grouped zones.
3. The applicable security controls and countermeasures to address identified threats. Based on the nature of the vulnerability and threat, security controls may be both digital or physical.
4. List of all unmitigated cybersecurity risks categorized by potential impact
5. Validate Security Level Target
6. Document how the failure of IT components supporting the SuC impact operations and safety.
7. Document how a security incident on a component of the SuC may propagate to other components and connected systems both within and outside of the Authority's OT environment. Document how cascading impacts could occur as the result of both physical and logical dependencies.

8. Proof that implementation of the suggested ISA-62443-3-3 Standard Security Level Target measures will result in the required risk reduction; risk shall be reduced to the target risk level as defined by the Authority. By default, all components shall meet Security Level 3 unless otherwise detailed by the DCRA and approved by the Authority.
9. Deliver risk evaluation reports after the application of the Security Level Targets and additional compensating controls/countermeasures
10. Demonstrate the iterative process of risk identification and application of security controls and countermeasures. The design shall demonstrate that the application of security controls and countermeasures shall reduce the residual SuC cybersecurity risk to an acceptable level. The process shall be repeated at the interval the Authority defines.
11. The Vendor may request a risk acceptance for specific risks. The Authority shall grant or deny the request. The Authority shall review and approve the DCRA prior to proceeding with the SuC's implementation. The Vendor shall update the DCRA annually once the system is deployed.
12. In the event that the SuC processes or stores data with potential privacy implications, or may so in the future, the Vendor shall document and manage the privacy risk as guided by the NIST Privacy Risk Assessment Methodology (PRAM).

4 SECURE SYSTEM DEVELOPMENT

Based on the Detailed Cyber Risk Assessment (DCRA) Reports, the Vendor shall collaborate with the Authority to define the appropriate Security Levels and Security Level Targets (SL-T) that the Vendor shall comply with during the system development process. The Vendor and its suppliers participating in providing the SuC shall obtain certification from a recognized certification third-party to demonstrate compliance with agreed-upon Security Level Targets based on ANSI/ISA-62443 4 1 2018 requirements, Security For Industrial Automation And Control Systems Part 4-1: Product Security Development Life-Cycle Requirements **and** ANSI/ISA 62443 3 3 (99.03.03)-2013 Security for industrial automation and control systems/Part 3-3: System security requirements and security levels**.** The Vendor's subcontractors and suppliers participating in providing the SuC shall comply with all cybersecurity provisions within the National Defense Authorization Act (NDAA). Suppliers who are not able to obtain ISA-62443 certifications may be granted, at the Authority's discretion, an additional period to obtain the required certification. Such exception shall not be granted to the prime vendor providing the SuC.

SuC third-party components and subsystems shall comply with the same security requirements as the Vendor.

5 VULNERABILITY DISCOVERY, REPORTING, AND ASSESSMENT

The Vendor shall implement a vulnerability detection and remediation program that covers the SuC, its subsystems and components. The program shall be consistent with industry standards such as ISO-27417 and NIST 800-53 current revisions. The Vendor shall develop, document, and implement policies and procedures to address the disclosure and remediation by the Vendor for vulnerabilities and material defects related to the products and services provided to the Authority under this Agreement. The vendor shall provide the Authority with the documentation detailing the program policies and processes. At a minimum, the Vulnerability Management Program shall include the following:

1. Prior to the delivery of the procured SuC, the Vendor shall provide or direct the Authority to available sources that contain a summary of documentation of publicly disclosed vulnerabilities and material defects, the potential impact of such vulnerabilities and material defects, the status of the Vendor's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and the Vendor's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds. The Vendor shall perform an initial report of the active vulnerability scan during each phase of the implementation.
2. The Vendor shall provide or direct the Authority to available sources that contain a summary of documentation describing vulnerabilities and material defects in the SuC within thirty (30) calendar days after such vulnerabilities and material defects become known to the Vendor. The summary documentation shall include a description of each vulnerability and material defect and its potential

impact, root cause, recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds (e.g., monitoring). The Vendor shall categorize the vulnerabilities based on impact and system criticality.

3. The Vendor shall disclose the existence of all known methods for bypassing system authentication in the SuC, often referred to as *backdoors*, and provide a written attestation that all such backdoors created by the Vendor, or its suppliers have been permanently remediated.
4. The Vendor shall report to the Authority, all newly discovered vulnerabilities, and provide severity ratings and sufficient details describing the vulnerabilities to assess potential operational and safety impacts on the SuC. The Vendor shall report all vulnerabilities within 14 days of discovery/at or prior to public disclosure, or when reported on the National Vulnerability Database (NVD) site. The vendor shall provide security patches and implement remediation procedures at the earliest timeframe to the Authority in compliance with requirements stated in **Section 6: Security Patching and Mitigation Governance** of this document.
5. The Vendor shall disclose vulnerabilities that may impact the safety of critical systems to the Authority within 1 day of discovery. The vendor shall provide a patch or a countermeasure within 14 days of discovery.
6. If the Vendor assesses that the discovered vulnerability may have a safety impact, the Vendor shall make available, patches or countermeasures for the vulnerability to the Authority prior to its public disclosure.
7. The Vendor shall perform vulnerability discovery and enumeration once every 14 days. When feasible, the Vendor shall perform authenticated vulnerability discovery procedures.
8. The Vendor shall document and limit discoverable information on the SuC to prevent an attacker from gaining knowledge of system components and versions.
9. The Vendor will assess the effectiveness of existing security controls implemented to mitigate the risk of known vulnerabilities quarterly.
10. The Authority or a third party appointed on its behalf may perform vulnerability scanning testing on the SuC. Testing shall be performed in coordination with the Vendor and shall be carried out within 30 Days of notifying the Vendor. The Vendor acknowledges that during the testing phase, it may be necessary to circumvent security controls to obtain accurate test results. The vendor agrees that it owns or controls all the necessary rights, licenses, or permissions to facilitate the testing procedures.
11. The Vendor shall perform risk assessments on all known or discovered vulnerabilities. The Vendor shall score vulnerabilities that are not already scored in the National Vulnerability Database (NVD) using the same methodology as the NVD's CVSS 3.0 rating system. The scoring shall classify the vulnerabilities with one of the following ratings: Low, Medium, High, or Critical. At the approval of the Authority, the scoring can be modified to reflect the exploitability of the vulnerability. Patching or mitigating the vulnerabilities shall follow requirements stated in **Section 6: Security Patching and Mitigation Governance** of this Agreement.

6 SECURITY PATCHING AND MITIGATION GOVERNANCE

The Vendor shall establish a patch deployment and compensating control (mitigation or countermeasure) deployment program for the SuC, its subsystems and components. At the request of the Authority, tooling to facilitate the deployment of patches and mitigations shall be deployed to facilitate the process. The Authority may make tooling available to the Vendor, in which case the Vendor shall leverage the Authority's existing tools.

1. In cases where the SuC is distributed across more than three locations, the Vendor shall provide documentation on the methods for deploying patches remotely without breaching zone separation logic over the Authority provided secure connectivity to the assets.
2. The Vendor shall provide patch deployment plans that minimize the risk of operational disruption to an acceptable level.

3. All patches and mitigation methods shall be tested in nonproduction environment(s). Test results shall be documented. Test results shall be combined into a patch risk analysis and approved by the Authority prior to making any changes in operational systems.
4. Patch authenticity and integrity shall be validated before deployment onto the operational network.
5. The Vendor shall provide detailed documentation and adequate tooling to empower the Authority to patch the SuC (including third-party hardware, software, and firmware). This documentation shall include the required resources and technical capabilities to sustain the SuC and related processes.
6. The Vendor shall retain previous versions of software and firmware. Vendor shall make available an authoritative list of all versions and updates with dates and related release notes.
7. When feasible, all patch deployment in production environments shall be automated to prevent operator errors.
8. The Vendor shall verify and provide documentation for integrated products and sub-products (including third-party hardware, software, firmware, and services) with appropriate updates and patches installed prior to delivery of the SuC to the Authority, or within 30 days prior to the system going live.
9. The Vendor shall make patches and mitigation methodologies available to third parties authorized by the Authority to receive such items.
10. The vendor shall provide patches that can be rolled back if required and provide a recovery plan for the component or system being patched. Vendor shall supply the rollback step by step process. Rollback process shall not wipe out configuration.
11. The Vendor shall provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses based on the requirements stated in **Section 17: System Lifecycle Management** of this Agreement.
12. Updates to remediate critical vulnerabilities shall be provided within the period agreed upon during the risk assessment process. If updates cannot be made available by the Vendor within the designated timeframe, the Vendor shall provide mitigations and/or workarounds within the period defined in **Section 5: Vulnerability Reporting, Discovery, and Assessment** of this Agreement.
13. When the Vendor provides third-party hardware, software, and firmware to the Authority, the Vendor shall provide appropriate hardware, software, and firmware updates to remediate newly discovered vulnerabilities or weaknesses according to the Risk Rating Deadline Patching Schedule. If the third-party updates cannot be made available by the Vendor within the designated timeframe, the Vendor shall provide mitigations and/or workarounds within the schedule's deadlines.
14. The Vendor shall supply the Authority with procedures and processes to validate patching or mitigation results that confirm that the intended goal of remediating the target vulnerability(ies) has been achieved. The application of the patch or mitigation shall reduce the risk to a tolerable risk level.
15. The Vendor shall exercise due care in ensuring that patches do not introduce new vulnerabilities.
16. Patch deployment shall not change the Security Level achieved by the SuC.
17. Patch deployment shall adhere to the requirements stated in **Section 7: Operational Governance** of this Agreement.
18. The Authority shall dictate the manner and date; the patches or compensating controls will be deployed.
19. Patches and mitigation timeframe shall adhere to the schedule tabulated below.

Risk Rating Deadline Patching Schedule	
Risk Rating	**Patching/Mitigation (Compensating Controls) Availability Deadline**
Low	180 Days
Medium	60 Days
High	45 Days
Critical	30 Days

20. The patching or mitigation shall lower the overall risk of the SuC to a tolerable risk level within the deadlines tabulated above.

7 OPERATIONAL GOVERNANCE

The Vendor shall comply with the Authority's Operational Governance procedures. Once the SuC is operational, the Vendor shall adhere to the Authority's internal control processes including but not limited to, Change Management, Release Management, and Configuration Management. At the Authority's request, the Vendor shall develop detailed processes for system operations governance. All SuC changes shall maintain the SuC's achieved Security Levels (SL-A) which define the actual levels of security that are commissioned and in operation.

8 SUC INVENTORY

The Vendor shall establish a program to manage and report on the current systems inventory detailing all hardware and software components with versions including third-party subsystems and components, change registers, and unique identifiers for each component. The Vendor shall provide the following:

1. The Vendor shall integrate the configuration management processes into the Authority's Configuration Management Database (CMDB). At the request of the Authority, the Vendor shall provide a CMDB system in use with the SuC.
2. The Vendor shall maintain a detailed asset inventory of the SuC's components. The Vendor shall provide the Authority with the inventory at least 30 days prior to the SuC going live. The asset inventory shall include details on all hardware assets and all required software components. The inventory shall include information about the physical location of the assets, the hierarchical relationship between systems, subsystems and components and their respective OEMs.
3. Hardware, software, and firmware versions shall be tracked as part of the systems inventory.
4. The Vendor shall update the system inventory upon maintenance or change events. The Vendor shall follow the Authority's process to maintain an updated system inventory.
5. Assets shall be mapped to the SuC functions documented in Section 3: SuC Risk Assessment of this Agreement. The asset's role in providing the function shall be described in detail.
6. Asset inventory shall detail all subsystems and systems components. The Vendor shall provide the Authority with a listing of necessary network connection details and detailed network diagrams.
7. The Vendor shall supply the Authority with a list of all hardcoded accounts in the SuC including hardcoded accounts in subsystems.
8. The Vendor shall supply the Authority with a list of all accounts and roles necessary to operate the SuC.
9. For network segments under the management of the Vendor; the Vendor shall utilize asset discovery tools to discover assets on the network at least once every seven days.
10. The Vendor shall investigate and document all unknown assets discovered on the network.
11. The Vendor shall utilize the updated system inventory to perform vulnerability discovery as detailed in **Section 5: Vulnerability Discovery, Reporting, and Assessment** of this Agreement.

12. The system inventory shall include information describing the criticality of the systems, subsystems and components on safety and role(s) in the railway ecosystem (signaling, safety, rolling stock, communications, comfort, etc.).
13. The system inventory shall include all virtualized components.
14. The Vendor shall categorize the SuC, its subsystems and components based on the Authority's systems categorization policy. The Authority shall review and approve the SuC categorization.

9 SECURE SYSTEM CONFIGURATION

9.1 HARDWARE CONFIGURATION REQUIREMENTS

1. The Vendor shall institute and follow systems hardening processes according to the latest Security Technical Implementation Guide (STIG) and Center for Internet Security (CIS) benchmarks.
2. The Vendor shall password protect the BIOS from unauthorized changes unless it is not technically feasible, in which case the Vendor shall document the security deviation and provide mitigation measures.
3. The Vendor shall ensure that the hardware can support encryption according to FIPS 141-3 without impeding the hardware's ability to perform its intended function at the required availability and performance levels.
4. The Vendor shall provide physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alerting to protect the SuC device and configuration from unauthorized modification or use.
5. The Vendor shall identify the physical and cyber security features and provide the methodology(ies) for maintaining the features including the methods to change settings from Vendor-configured or manufacturer default conditions.
6. The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during SAT when connected to existing equipment.
7. The Vendor shall adhere to the principle of least functionality and remove or disable all software and hardware components and ports that are not required for the operation and maintenance of the SuC prior to deployment. Vendor shall provide a list of all disabled features and components.
8. The Vendor shall provide documentation on components that are removed and/or disabled.
9. The Vendor shall configure the system to allow the system administrators the ability to re-enable devices if the devices are disabled by software and provide documentation of the configuration change process.
10. The Vendor shall deliver all hardware free of backdoor accounts/access methods or security override processes. Hardcoded accounts shall have updated unique passwords according to the Authority's password standards. Default passwords shall be changed.
11. The Vendor shall provide, within a pre-negotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.
12. The Vendor shall verify and provide documentation that the Safety Instrumented System (SIS) is certified after incorporating the security devices.
13. The SuC shall be capable of integrating with the Authority's Public Key Infrastructure (PKI) and be able to perform certificate-based device authentication.
14. The Vendor shall protect hosts from loading drivers and applications that are not cryptographically signed by an approved software development entity.
15. Hosts shall be configured for secure boot using UEFI Secure Boot. If a TPM chip is available, the Vendor shall enable the TPM technology to assert a secure boot.
16. The Vendor shall recommend methods to the Authority to prevent unauthorized changes to the Basic Input/Output System (BIOS) and other firmware.

9.2 SOFTWARE CONFIGURATION REQUIREMENTS

1. The Vendor shall use the latest versions of supported software. OEM support for all incorporated software shall be expected to last for at least 3 years past the Authority's acceptance of the SuC.
2. The SuC shall enforce a software installation "allowlist" and only permit the installation of approved software.
3. The Vendor shall adhere to the principle of Least Functionality and only install software that is necessary to support the function of the SuC.
4. Software shall conform to the Least Privilege configuration principle and only be granted access that is necessary to support the function of the SuC. Software shall be configured to disable all unnecessary services and communication functionality by default. Installed software shall not open undocumented ports or permit access to the network which bypasses security controls.
5. Unless otherwise approved by the Authority in writing, the current or supported version of SuC components shall not require the use of out-of-date, unsupported, or end-of-life versions of third-party software (e.g., Java, Flash, Web browser, etc.).
6. Software shall use secure communication protocols and encryption when communicating on the network unless encryption is provided as the networking layer.
7. The Vendor shall document a software configuration baseline for Authority approval. The baseline will include version information and the software's intended purpose.
8. The Authority's configuration management system will be used to manage software on the operational SuC.
9. On the operational SuC, software shall only be installed by privileged users, or the automated software management system appropriately authenticated to the network.
10. All software and software updates will be tested in a non-production environment before deployment to the SuC.
11. Where feasible, software installation and updates shall be performed automatically using the Authority's configuration management application. Upon request, the Vendor shall provide an automated software deployment and updating system.
12. The Vendor shall configure software logging and forward logs to the Authority's centralized log storage and analysis system according to the log management section of this agreement.
13. Vendor produced, or OEM acquired software shall be cryptographically signed before installation on the SuC.
14. The Vendor shall preform a security impact analysis on all software and implement security controls to mitigate any vulnerabilities or security weakness introduced by the software.
15. If open-source software is utilized by the SuC, the vendor shall identify it and conduct code security analysis using industry standard code analysis tools. The Vendor shall establish process and procedures to monitor information sources for the public disclosure of vulnerabilities.
16. Vendor shall provide full configuration backup of fully functional SuC. The vendor shall provide documentation detailing the configuration and settings necessary for the SuC to function as intended.

9.3 OPERATING SYSTEM SECURITY

1. Upon the approval of the Authority of the Operating Systems choice for the SuC components, the Vendor shall follow the CIS Security Technical Implementation Guides (STIGs) to securely configure operating systems for all operating systems installations.
2. The Vendor shall be responsible for maintaining operating systems installation updates according to STIG requirements.
3. The Vendor shall deploy the Authority-provided Endpoint Protection Software supporting all instances of the operating system. At the Authority's request, the Vendor may provide and deploy Endpoint Security Protection software. The Authority shall review and approve the Endpoint Security Protection software and its configurations.

4. All alerts and detections generated by Endpoint Protection software shall be routed to the Authority's Security Operations Center.
5. Only required and secure ports and services shall be enabled.
6. All systems shall enforce software clear-listing rules.

9.4 VIRTUALIZATION SECURITY

If the SuC is an integrated system and requires a virtualized environment, the Vendor shall follow the CIS security benchmarks for the latest cybersecurity recommendations for the virtualization platform. If specific guidance is outdated or unavailable, the Vendor shall follow the latest cybersecurity best practices provided by the software vendor and recognized cybersecurity entities to protect the virtualization infrastructure. At a minimum, the Vendor shall perform the following actions to secure the installation of hypervisors and related infrastructure components:

1. The Vendor shall adhere to all applicable sections of this document to manage the security of the virtualization environment and its subcomponents.
2. The Vendor shall configure hypervisors to leverage single sign-on for authentication and authorization. Local accounts shall be minimized and used only in emergencies following break-glass procedures.
3. All authentications and authorizations shall follow the requirements stated in the Access Control section of this document.
4. Access directly to hypervisor hosts shall be limited to Secure Management Workstations. Access shall be logged and protected as privileged access. Access shall follow the Zones and Conduits security configuration. Vendors shall isolate hypervisor management traffic networks for their specific functions' networks.
5. The Vendor shall use the hypervisor's official client to administer the hypervisor's hosts. Direct access shall be limited to emergency scenarios.
6. The Vendor shall only run hypervisor vendor-approved software packages.
7. Virtualization environment components shall adhere to the requirements stated in this section of the Agreement.
8. The Vendor shall ensure that hypervisor architecture is fault-tolerant following the Authority's recovery point and time objectives (RTOs and RPOs)
9. The Vendor shall validate and document startup tasks regularly.
10. Virtualized networks shall be integrated into the Authority's network management fabric.
11. All hosted components on the virtualized system shall follow the zone and conduit restrictions.
12. API keys and service accounts passwords should be vaulted in an industry-standard key vault/ key management service.

9.5 SECURING ACTIVE DIRECTORY

If the SuC is an integrated component of a system and requires a dedicated Active Directory installation, the Vendor shall follow the latest cybersecurity recommendations to protect the Active Directory installation. At a minimum, the Vendor shall perform the following actions to secure the installation.

9.5.1 Active Directory Security

The Vendor shall establish a program with related processes and procedures to protect Active Directory installations. The program shall be updated to reflect the latest threat intelligence, industry guidance, and Microsoft's recommendations. Additionally, the Vendor shall implement the following controls:

1. Maintain individual complex passwords for Privileged Accounts on all computers with membership in the domain/forest.
2. Refrain from giving individual users explicit rights to Active Directory containers.
3. Implement processes to alert if permissions on any Active Directory containers have changed.
4. Configure GPO not to cash credentials on all domain member computers.

5. Remove downstream clients from the domain.
6. Ensure that PowerShell logs are captured and analyzed by EDR tools.
7. Disable SMB when feasible. At a minimum, disable SMBV1 and SMBV2 protocols.
8. When feasible, disable the ability to run obfuscated scripts.
9. Domain trusts shall be reviewed and validated quarterly. Cross domain authorization shall be minimized.

9.5.2 Securing Active Directory Domain Controllers

The Vendor shall adhere to all applicable sections of this Agreement to protect Active Directory domain controllers. Additionally, the Vendor shall adhere to the following security requirements:

1. Active Directory domain controllers shall be categorized as High in risk assessment ratings.
2. Administrative access to domain controllers shall only be permitted from a secure management workstation. All other RDP or remote management protocols and methods shall be denied at the network level.
3. Domain controllers shall be prevented from accessing the Internet with possible exceptions for EDR tools.
4. Domain controllers shall run a version of the operating system that is supported by Microsoft.
5. Application clear-listing shall be enforced on all domain controllers.
6. Full disk encryption shall be enforced on all domain controllers and on all desktops/laptops.
7. Active Directory databases shall be backed up on all domain controllers. Backups shall be encrypted and classified as the highest sensitivity data classification as per the Authority's Data Classification Policy. Backups shall be saved to an immutable storage backup system.
8. When feasible, domain controllers shall be deployed on a separate virtualization infrastructure.
9. Domain controllers shall be deployed in data centers and locations where physical access is restricted.
10. Access to the LSASS process shall be hardened.
11. Domain controllers shall not be excluded from any Endpoint Protection software or features.

10 CLOUD SECURITY

This Agreement applies to on-premise OT systems and networks. Although many of the security principles and controls outlined in this Agreement are also relevant to cloud environments, the primary focus of this Agreement is not on the cybersecurity implications associated with cloud infrastructure as a replacement for physical on-premise systems and networks. However, this Agreement does not restrict the use of cloud hosted services, provided that doing so does not adversely impact the Security Level Target of the SuC as documented in the Detailed Cyber Risk Assessment (**Section 4.3**).

11 AVAILABILITY

Availability in the context of cybersecurity is the ability of the SuC to operate reliably, contain, and "fight through" cyber-attacks and general OT and IT component failures. Resilient system architecture that incorporates redundant systems and other work arounds to compensate for failed components helps to assure system availability. Availability is managed at multiple levels including data, application OT infrastructure, IT infrastructure and the SuC itself. The goal is to prevent the failure of one component at one level from cascading to other components and other levels. The Vendor shall submit a High Availability architectural design that demonstrates the achievement of uptime and performance goals. At a minimum, the architecture shall demonstrate the following:

1. The Vendor shall eliminate single points of failures.
2. The Vendor shall maintain a critical spare inventory.
3. The Vendor shall design highly resilient Information Systems as described in **Section 22** of this document.

4. The Vendor shall design and implement a fault tolerant system with redundant communication pathways to ensure that a failure of one network segment does not limit the network as a whole. Self-healing network architecture and technology shall be preferred where feasible.
5. The Vendor shall incorporate system and data backups as described in **Section 22.1** of this document.
6. The Vendor shall implement resilient, fault tolerant data communication protocols.
7. SuC components with redundant systems shall include an automatic failover capability to limit the system downtime resulting from a mechanical or digital failure.
8. The Vendor shall implement real-time detection, alerting and logging of all system failures.
9. The vendor shall demonstrate competence in owning processes, tools, and the personnel needed to meet the uptime and performance goals set forth by the Authority for the SuC.

12 TIME SYNCHRONIZATION

If not available through the Authority, the Vendor shall use a GPS master station clock as a baseline reference for timestamps used for logs and systems generating logs. If GPS reference is not possible, the Vendor shall use a NIST authenticated time service. Public, unauthenticated, and unencrypted NTP pools shall only be used as an option of last resort, and only for as long as needed to begin leveraging other options.

If not available through the Authority, the Vendor will provide a centralized redundant primary and a backup time source.

The Vendor shall synchronize local time on all SuC components being leveraged at a protocol version with no known medium or high vulnerability.

13 DATA SECURITY

The Vendor shall establish and maintain a Data Management and Protection Program. The program shall be driven by a data classification process to enforce the appropriate controls based on data sensitivity.

1. The Vendor shall follow the Authority's data classification policy in creating an inventory of all data under the Vendor's management.
2. The Vendor shall maintain an inventory of datasets, descriptions, classifications, and owners.
3. The Vendor shall follow the Authority's data retention requirements.
4. The Vendor shall encrypt data at rest and in motion based on the Authority's classification requirements and in compliance with FIPS 141-3.
5. The Vendor shall ensure that encryption does not create unacceptable latency.
6. The Vendor shall follow SP 800-57 Part1 Rev. 5 for management of encryption keys.
7. The Vendor shall submit a Data Residency Plan detailing where data will be stored on the SuC components. Data residency shall follow the zone design based on zone security level and data classification.
8. The Vendor shall implement Data Loss Prevention systems and processes where applicable.
9. Access and modification of data shall be logged based on the data classification requirements.
10. Data shall be disposed of securely to prevent unauthorized disclosure.

14 IDENTITY AND ACCESS MANAGEMENT SECURITY

The Vendor shall develop, document and maintain an Identity and Access Management Program to ensure adherence to current cybersecurity best practices. The Vendor shall provide the Authority with documentation detailing the program's policies and processes. At a minimum, the program shall include the following.

14.1 ACCESS CONTROL

1. The Vendor shall establish and maintain an Access Control Program to ensure that only authorized access is allowed to the SuC, its subsystems and components. The program shall

ensure that all account changes and access activities are logged in a manner that enables auditing and incident response. All granted access shall follow an authorization process approved by the Authority. The Vendor shall provide the following:

2. The SuC, its subsystems and its components shall require authentication and authorization prior to allowing access.
3. The Vendor shall configure the SuC, its subsystems and applicable components with options for integration with the Authority's Single Sign-on System.
4. The Vendor shall configure each component of the SuC to operate using the principles of "Least Privilege" and "Separation of Duties." This includes operating system permissions, file access, device access, device user accounts, service accounts, and communications/data transfers.
5. The Vendor shall configure the SuC, its subsystems and applicable components with support for FIDO 2.0 U2F based authentication.
6. The Vendor shall configure the SuC, its subsystems and applicable components to support role-based access and authorization. The role-based configuration shall be approved by the Authority.
7. If the SuC is not connected to the Authority Single Sign-on System, the Vendor shall provide a centralized User Account Management System. User accounts for onboard systems shall be configurable by the Authority.
8. The Vendor shall establish identity management that uniquely identifies authorized persons, processes, and devices.
9. Field I/O level (Purdue Level 0) devices incapable of authentication requires mitigating security controls to detect incorrect or malicious data.
10. The concept of Least Privilege shall be employed with a user account hierarchy in place.
11. The Vendor shall provide documentation for the user, groups, and role management and define security privileges and permissions.
12. The Vendor shall perform account recertification and access reviews at least once every 30 days.
13. When feasible, access revocation and account de-provisioning shall be automated based on rules approved by the Authority.
14. The Vendor shall revoke access to accounts immediately upon termination of employees or change of roles.
15. All access from a less secure zone or network shall be challenged according to the FIDO 2.0-based authentication specification.
16. Access for processes from a lower security zone to a higher security zone shall be logged and controlled.
17. Where feasible, eliminate the use of shared accounts. If shared accounts are used, the Vendor shall take steps to minimize access to shared accounts. Credentials for shared accounts shall be rotated at least quarterly and when a person with knowledge of the credentials no longer needs to use the shared account.
18. The Vendor shall ensure that access enforcement shall not adversely impact the operational performance of the SuC.
19. The Vendor shall configure the SuC to log account usage to support monitoring of atypical account activity.
20. Access control shall be designed to not interfere with time-critical emergency duties.

14.2 PRIVILEGED IDENTITY AND ACCESS

The Vendor shall implement a program to govern privileged identities and access. The program shall include the following requirements:

1. The Vendor shall follow the Least Privilege principle when granting privileged access.
2. All privileged access shall follow the request/evaluation /approval/denial process.

3. All privileged access authorization shall be documented in a manner that allows auditing of all changes and provides non-repudiation.
4. Identity proofing to verify account ownership shall be completed every 6 months for privileged users and system account owners.
5. Privileged access and privileged escalation shall be challenged by Authority-approved MFA methods.
6. Any changes to privileged groups shall be monitored with corresponding alerting.
7. Users shall use separate accounts for privileged access and business functions access.
8. Privileged account authentication requires additional safeguards such as stronger passwords, more frequent password changes or physical tokens.
9. When feasible, Privileged Accounts shall be denied access to the Internet.
10. Service Account credentials shall be vaulted. Scripts shall not have hardcoded credentials. The credentials will be requested from the vault at runtime. A service account is a special type of account used by applications, services, or automated processes to interact with systems, resources, or APIs. Unlike user accounts, service accounts are not associated with a specific person but are intended for use by software to perform tasks, manage access, and authenticate without human intervention.
11. The Vendor shall document procedures that define changing service account credentials according to the Authority's Password Policy.
12. All privileged activities shall be tracked in system logs or other mechanisms.
13. Systems shall be protected against unauthorized privilege escalation.
14. Service accounts shall be assigned to technical and business owners.
15. Services accounts shall be restricted to access only systems the accounts are intended for.
16. Service accounts shall be denied interactive access to systems.
17. Services accounts where passwords have not changed for 6 months shall be flagged to owners with requirements to change the password within 15 days.

15 SESSION MANAGEMENT

The Vendor shall not, unless specifically requested by the Authority, allow multiple concurrent logins using the same authentication credentials, allow applications to retain login information between sessions, provide any auto-fill functionality during login, or allow anonymous logins unless specifically requested by the Authority.

16 NETWORK SECURITY

The Vendor shall develop, maintain, and follow necessary procedures to protect the integrity and confidentiality of the information transmitted on any network as needed for the safe functioning of the SuC. The Vendor shall design and implement SuC communication to meet the availability and quality goals set forth by the Authority during the SuC design process. The Vendor shall implement communication security protocols that assume networks may already have unauthorized access. The implementation of the SuC network shall follow the Zones and Conduits security design detailed in the DCRA processes. All network systems and configurations shall adhere to all relevant sections of this Agreement. Additionally, the Vendor shall deploy the following controls:

1. The SuC shall not connect to public networks.
2. The Vendor shall document and provide a secure network architecture including but not limited to the cases where the higher security zones connect to less secure zones.
3. The Vendor shall document and provide the design for all communication paths between networks of different security zones and through a DMZ.
4. The Vendor shall provide a method for managing the network devices and changing addressing schemes.
5. The SuC shall be configured to integrate with the Authority's existing secure name/address resolution service.

6. The Vendor shall document interconnections between network devices and other external connections for IP and non-IP connections. When practicable, the vendor shall use one way gateways to connect between different layers of the Purdue Model.
7. The Vendor shall document data flows internal and external to the SuC.
8. The Vendor shall provide methods to monitor network data traffic and support the development of a network traffic baseline. Network monitoring shall alert the Security Operation Center upon the detection of unknown devices or services and be tuned to reduce alert “noise”.
9. The network shall be architected to support securely monitoring data at key points where most of the data flows through and is not encrypted.
10. The Vendor shall verify and provide documentation that the network configuration management interface is secured.
11. The Vendor shall provide ACLs, port security address lists, and enhanced security for the port mirroring.
12. The Vendor shall ensure that security capabilities are not dependent on the network capabilities.
13. The Vendor shall deliver a security design allowing the usage of cable and radio-based networks.
14. The Authority shall define network requirements concerning availability and performance (bandwidth and latency).
15. All devices shall authenticate to the network prior to participation in sending and receiving safety-related communications.
16. The Vendor shall implement capabilities to log and audit access from less secure networks to secure networks. Logs shall be stored in a centralized location.
17. The network shall have capabilities to perform packet capture as needed (PCAP).
18. Devices participating in safety-critical networks with the ability to support certificate-based authentication shall support the following:
    a. X.509 certificates for identification with 802.1x authentication integrating into Authority-provided PKI infrastructure.
    b. Device certificates shall be manageable remotely where feasible.
    c. A method to remotely and securely install a signed X.509 certificate on the device is required along with installing the CA certificate.
    d. A secure method must be available to programmatically install certificates on each device via automation without physical access to the device, and the Authority may, at its discretion, rotate certificates frequently (e.g., 24 hours).
    e. Device certificates shall be manageable from a centralized system that allows updating certificates remotely in a controlled manner.
    f. Certificate rotations shall not require outages or operational impacts (e.g., reboots). The device shall receive accurate time as defined in the Time Synchronization clause of this Agreement.
19. The Vendor and Authority shall agree on acceptable encryption protocols and secure communication processes appropriate for each Security Level Target. Encryption keys shall be rotatable and updated remotely without impacting availability.
20. The Vendor shall not deploy deep packet inspection capabilities on safety-critical networks.
21. Where applicable, the Vendor shall prioritize safety-critical communications.
22. The SuC, its subsystems, and components shall support access control systems that validate the system’s security posture prior to admission onto the network.
23. The Vendor shall implement a deny-all, permit-by-exception policy on firewalls separating network segments and on permitter devices.
24. Network permitter devices shall restrict communication both into and out of the network.
25. Network perimeter device configuration shall be reviewed quarterly and reconciled against change management records.

26. Network device configuration shall be monitored for changes. Changes shall be validated immediately.
27. Network device configurations shall be backed up daily to a centralized location.
28. All access to network device configuration shall be treated as Privileged Access.

16.1 WIRELESS NETWORKS SECURITY

1. Wireless access points shall be established within their own network segments and work with boundary protection devices to restrict unauthorized communication.
2. Authority SSIDs shall not be broadcasted by default and shall be pre-configured on wireless clients.
3. Wireless communications within rolling stock shall be encrypted and authenticated.
4. Wireless clients accessing secure zones shall authenticate to wireless controllers using 802.11x and WPA2-Enterprise.
5. Guest wireless networks shall be restricted to accessing the Internet only.
6. The wireless network manager shall be “allowlist” authorized devices to prevent connection by rouge devices.
7. Wireless controllers shall be configured to detect rogue access points, and rogue deployment locations and alert the Vendor and the Authority of the same.
8. Rate-limiting shall be configured on wireless controllers to prevent Denial of Service failures caused by excessively large authentication attempts or volume of traffic.
9. Wireless networks for secure zones shall have signal strength range minimized to the required coverage area.
10. Wireless access points’ wiring to switches shall be concealed.
11. All wireless access points shall be deployed with static IP addresses, on a separate management network, and have switchport security enabled and postured utilizing the Authority’s NAC.
12. Third-party carrier based wireless networks shall be secured in collaboration with the carrier.

    The vendor shall provide a security plan to the Security Level Target according to the Zones and Conduit design for such networks. The Authority shall approve or request changes to the Vendor’s plan prior to connecting the Authority’s asset to such networks. The Authority shall have the right to audit the implementation of the plan or have an authorized third party perform the audit.

16.2 SEGMENTATION/MICRO SEGMENTATION

1. The Vendor shall verify and document that disconnection points are established between network partitions and provide the methods to isolate subnets to continue limited operations.
2. The Vendor shall provide and document tailored filtering and monitoring rules for all security zones and alert for unexpected or anomalous traffic.
3. The Vendor shall deliver capabilities enabling the Authority to configure its components to limit access to and from specific locations (e.g., security zones, business networks, and demilitarized zones [DMZs]) on the network to which the components are attached and provide documentation of configuration as delivered.
4. The Vendor shall retain a qualified third-party entity to perform security testing to verify that network separation is enforced.

16.3 PHYSICAL SECURITY

1. The Vendor shall design communication networks assuming that physical local manipulation of equipment is possible. The Vendor shall build sufficient redundancy and separation for the network to withstand the physical failure of communication paths without causing operational disruption.
2. The Vendor shall document physical environment conditions required operating the SuC including HVAC, and power requirements.

3. Where feasible the Vendor shall implement physical access control to prevent unauthorized access to SuC components.
4. The Vendor shall submit a fault tolerance design for the approval of the Authority.
5. The Vendor shall ensure that wired networks are concealed and not exposed to the elements or human tampering.
6. The Vendor shall restrict access to information related to the location of critical infrastructure, interconnections, and fallback scenario descriptions.
7. The Vendor shall employ different redundancy technologies, such as a combination of wired and wireless communication between sites.
8. The Vendor shall provision a redundant wired connection, and consider different deployment topologies (such as mesh, ring, etc.).
9. The Vendor shall ensure that central services are locally replaceable to avoid overall service interruption by considering different options such as Island Mode deployment.
10. The Vendor shall monitor physical equipment for unauthorized access, tampering, and degradation of performance.
11. The Vendor shall develop maintenance processes and a spare inventory, to respond to physical network disruptions.

16.4 REMOTE ACCESS

Limited, secure remote access can be utilized to perform maintenance and system checks. The Vendor shall submit a request to the Authority to enable temporary remote access that securely traversers the Purdue Model Layers of the Authority's OT environment to establish communication with the target system. Virtual Private Network (VPN) technology with strong encryption and authentication shall be used to protect remote communication and prevent unauthorized access. The following controls shall be implemented to secure remote access capability.

1. Remote access shall not circumvent or negate safety or security controls, any control such as a firewall that must be modified to permit remote access will have a compensating control to ensure the overall Security Level of the Authority's OT environment is not adversely impacted.
2. VPN encryption shall be compliant with the FIPS 141-3 encryption standard.
3. Unique usernames and passwords shall be established for each user requiring remote access.
4. All logins and logouts shall be logged in the Authority's centralized logging system including all meta data associated with the access transaction.
5. Remote logins shall require the use of Strong Multifactor Authentication.
6. Remote access shall only be possible from pre-defined clear-listed set of IPs.
7. Default remote login credentials shall be removed from the system before deployment of the SuC.
8. Remote sessions shall automatically terminate upon client disconnection or time-out and terminate after 5 minutes of inactivity.
9. Remote access activity shall be monitored and logged in the Authority's centralized logging system.
10. Remote access shall be limited to secure management systems that are not used for other purposes.
11. All remote access software, and firmware shall be updated and maintained at their latest versions.
12. In the event that a vulnerability is disclosed that impacts remote access technology or protocols, remote access shall be disabled until the affected software is patched or replaced.
13. The Vendor shall document and provide the Authority with a process to quickly disable remote access on the SuC in the event of unauthorized access. The Authority shall be able to disable remote access without needing any external assistance.

17 ROLLING STOCK SECURITY REQUIREMENTS

The Vendor shall establish and maintain up-to-date Cybersecurity Program(s) to protect all onboard SuC's in a rolling stock. The program will be reviewed and approved by the Authority. All onboard

systems shall adhere to all sections of this Agreement. The Vendor shall update the Detailed Cyber Security Risk Assessment for rolling stock components at least annually, taking into consideration the threat landscape evolution and technological updates.

Additionally, the following controls shall be applied:

1. Penetration tests (on a grey-box basis) shall be conducted annually by a provider selected by the Authority. The scope of this test shall include all onboard systems and wayside systems.
2. Physical security controls shall be inspected for integrity and signs of tampering.
3. The concept of Defense in Depth shall be applied to the security design of the system(s), such that failure in a single security mechanism shall not result in a compromise of the system or network.
4. A system for securely collecting, storing, and retrieving log files from onboard systems shall be in place. All log files, including security logs, shall be routed to the Authority's log management system. The local log management systems shall be redundant and capable of storing a minimum of 30 days of logs.
5. All onboard networks must be monitored by a threat detection system, providing detections that include but are not limited to, unauthorized hardware, anomalous network traffic, reconnaissance activity, DOS attempts, and endpoint-based attacks. Threat detection alerts shall be routed to the Authority's Security Operations Center.
6. End devices at particular risk of compromise, due to their function, or level of accessibility, including but not limited to Mobile Communications Gateways/Routers, and PIS controllers (with external access), shall be monitored by a Host Intrusion Detection System.
7. On-board networks shall be segmented and segregated using a firewall according to a Zone and Conduit model developed during an ISA 62443-3-2 Risk Assessment. Firewall rulesets shall be reviewed by the Authority on an annual basis.
8. Separate physical networks shall be established for 1) train control and safety critical systems: 2) Operational systems; and 3) passenger-facing systems (such as WiFi and media).
9. Access to hardware from passenger-accessible areas shall be secured with a unique physical key. Access panels shall not be in concealed locations (e.g., toilets) and must be observable by a video surveillance system.
10. Risk Assessments conducted on onboard systems shall, at a minimum, consider threats from:
    a) Passengers (via wireless networks or physical access)
    b) Bystanders
    c) The Authority's staff (whether train crew or maintenance staff)
11. Patching, system maintenance, and other system maintenance activities shall be performed from trusted service laptops. The use of USB devices shall be strictly prohibited.
    a) Service laptops shall not be used for other purposes including administration or general control of the SuC.
    b) Only service tools developed and tested by the Vendor or provided by the OEM and cryptographically signed by the developer shall be utilized.
    c) Service laptops shall be updated with the most recent Operation System and software patches with host-based protection installed and enabled leveraging a process that does not expose the laptop to cyberattacks during the update process.
    d) Service laptops shall not connect to public networks.
    e) The service laptop shall be disconnected from the SuC when not in use, temporary connection configurations shall be removed.
    f) Service laptops shall be sanitized or destroyed before disposal.

18 FAILURE MODE

The Vendor shall configure the system's failure mode to guarantee safety if the system fails. The failure mode may be open or closed, based on the safety case of the SuC and its components. Failure mode

shall not impact the integrity of the system. The Vendor shall submit a risk assessment for the failure condition per component to the Authority.

19 SYSTEM LIFECYCLE MANAGEMENT

The Vendor shall create a program to manage the SuC, its subsystems and components lifecycle. The program shall ensure that all components of the SuC remain under the available support of the Original Equipment Manufacturer(s) (OEM). Throughout the Design Life of the SuC, the Vendor shall be responsible for maintaining all components including those provided by second and third-party providers.

Planned obsolescence found in IT components may not extend to SuC components.

1. The SuC, its subsystems, and components shall not reside on end-of-life operating systems, or any components, including embedded software that is expected to be deemed end-of-life by the OEM within 24 months from the date of deployment into production.
2. Embedded systems shall run software covered by OEM support for at least 10 years from the date of deployment.
3. The SuC shall support the latest versions of operating systems on which vendor-provided hardware and/or software functions within twenty-four (24) months from the official public release of that operating system version.
4. Digital systems shall have an assumed design life of 12 years with plans for a technology refresh over the lifetime of the system. The vendor shall provide documentation, including typical tasks and timelines for a successful technology refresh while minimizing operational disruption.
5. The Vendor shall provide security patches throughout the Design Life.
6. Device configuration shall be verified after maintenance and software patching, as some features may have inadvertently been reenabled or disabled or new features installed.
7. The vendor shall provide evidence of through regression testing to ensure that updated components shall work as expected when introduced to the operating environment.
8. Vendor shall perform security testing and validation after components have been replaced included software components and embedded systems.
9. Systems or components that become obsolete and unable to be patched shall be replaced with a system of identical or superior functionality, as determined by the Authority.
10. Throughout the System lifecycle, the Vendor shall notify the Authority of any changes in supply chain components.
11. The Vendor shall maintain an inventory of critical system components in corresponding nested systems in order to supply replacements quickly in the event of an emergency or supply chain disruption. The Vendor and the Authority shall mutually agree on acceptable critical component inventory and storage location(s) and levels.
12. The Vendor shall provide guidance and template documentation to the Authority for implementing maintenance tracking capability specific to the SuC. These materials shall include at least:

    Processes for local and remote repairs, in accordance with existing Authority policies and other sections of this document.

    Identification of maintenance tracking tools that facilitate scheduling, authorizing, monitoring, and auditing repair activities for the SuC.

    The vendor shall leverage Authority provided maintenance tracking or configuration management systems where feasible.
13. The vendor shall provide the Authority with a disposal plan for all software that has reached the vendor's stated end-of-life. This plan shall include, at a minimum, but may not be limited to:

    Enumeration of all potential performance issues related to transitioning from old software to supported software and plans to mitigate all identified performance issues.

    Description of when and how the old software will be decommissioned.

    Description of which, if any, software components, including library files, and/or data will be preserved.

Description of which, if any, documentation related to the old software will be preserved.

Description of disposal processes for old software documentation.

Identification of Vendor primary and backup points of contact for all service and support during the disposition timeline.

14. The Vendor shall ensure that:

    Security functionality shall be updateable without negatively affecting safety functions.

    The lifetime of the safety system shall be 25 years minimum.

    The security-relevant functionality shall be replaceable without replacing the full safety system.

15. The Vendor shall deliver a safety and a security case for the components and systems. The safety and security cases will contain all evidence, including documented information on the verification and validation activities undertaken during the development and delivery of the SuC.

20 SUPPLY CHAIN SECURITY

The Vendor shall institute a program to ensure that supply chain risks are managed in a manner that guarantees the integrity, confidentiality of components, and conformance to relevant laws and regulations governing imports and exports. The Vendor shall ensure that all parts and components are sourced in a manner that guarantees the integrity of the components against accidental or intentional tampering, manipulation, and unauthorized access. The Vendor shall submit documentation detailing their supply chain security to the Authority. The Authority maintains the right to request changes to the processes to ensure tolerable risk levels. The Vendor shall maintain compliance with the National Defense Authorization Act at all times.

At a minimum, the Vendor shall perform the following security functions that apply to all entities participating in the supply chain process:

1. The devices shall be stored in a secure and monitored facility with limited access following Identity and Access Management and personal identification protocols.
2. The hardware (housing) shall be sealed to indicate tampering attempts.
3. If the outdoor cabinet is delivered pre-configured, the cabinet is to be delivered to the Authority and installed sealed.
4. All seals shall be recognizable if tampered with.
5. The information-processing devices must provide a secure boot including Field Programmable Gate Arrays (FPGA) devices.
6. The Vendor shall oversee sealing procedures and ensure that components can be checked against manipulation after a power interruption or loss of continuous monitoring.
7. All imported components shall have a valid Certificate of Origin.
8. Chain of Custody documents shall be maintained and shall be provided at the request of the Authority.
9. The vendor shall document tracking serial numbers, digital certificates/signatures or other identifying features to verify the authenticity of SuC components.

The Authority has the right to audit the supply chain between the Vendor and its suppliers. The Authority may assign a qualified third-party entity to perform supply chain audits on its behalf.

20.1 NATIONAL DEFENSE AUTHORIZATION ACT COMPLIANCE

1. The Vendor shall maintain compliance with all provisions of the National Defense Authorization Act.
2. The Vendor shall ensure that the acquisition of components or subcomponents shall not infringe on Section 7613 or future provisions, limiting the use of Federal Transit Administration (FTA) funds or local funds to procure rolling stock.
3. The Vendor shall not source any material, components or subcomponents from suppliers “owned or controlled by, is a subsidiary of, or is otherwise related legally or financially to a corporation based in” a country that meets the statutory criteria. U.S. International Trade Administration’s list

of designated nonmarket economy countries, available at https://www.trade.gov/nme-countries-list. For criteria (ii) and (iii), recipients should consult the latest version of the U.S. Trade Representative's Special 301 Report for a list of countries included on the priority watch list and whether such countries are subject to monitoring under Section 306 of the Trade Act of 1974. Changes to the NDAA provisions will override the provisions of this agreement.

20.2 SOFTWARE ORIGINS

The vendor shall specify the software development languages used to create all system components along with versions and compilers.

20.3 SOFTWARE BILL OF MATERIAL (SBOM)

1. The Vendor shall provide an initial and updated SBOM whenever the system software components change with new releases or patches. This includes but not limited to Operating Systems, Open Source components, libraries with utilized versions; any third party commercial components -; communication protocols; and any infrastructure components such as virtualization and containerization systems
2. The Vendor shall provide an updated SBOM to the Authority prior to the deployment of updates or patches that change the original SBOM. If due to emergency patching or bug fixes the Vendor must deploy software different from the SBOM, the Vendor shall supply the Authority with a revised SBOM within 7 days of the deployment of the emergency patch.
3. The Vendor shall provide a SBOM for procured (including licensed) products consisting of a list of components and associated metadata that make up a component. The SBOM shall cover all nested components within third party components.

20.4 HARDWARE BILL OF MATERIAL (HBOM)

The Vendor shall identify or provide the Authority with a method to identify the country (or countries) of origin of the Vendor procured products and components (including hardware, software, and firmware). The Vendor will identify the countries where the development, manufacturing, maintenance, and service for the SuC were provided. The Vendor will notify the Authority of changes in the list of countries where product maintenance or other services are provided in support of the SuC. This notification in writing shall occur at least 180 days prior to initiating a change in the list of countries.

21 NONPRODUCTION ENVIRONMENT

Unless directed otherwise, the Vendor shall deliver a non-production environment that includes at least one instance of each unique component in the SuC. The non-production environment shall represent the SuC in a manner sufficient to enable the training of personnel, testing of system updates, security testing, and security-related scanning. The Vendor shall maintain the nonproduction environment to remain an accurate representation of the operational SuC in the railway environment. The non-production environment shall be available for Authority validation at least 60 days prior to the SuC going live. The Authority shall approve the non-production environment.

The non-production environment shall be completely isolated from the production environment. The environment shall be used only for the purposes explicitly mentioned above in this section.

22 INCIDENT RESPONSE READINESS

The Vendor shall establish and maintain incident response readiness and threat detection processes that integrate into the Authority's Incident Response Program. The Vendor shall assist the Authority with all threat detection and incident response activities related to the SuC. The Vendor shall fulfill the following requirements:

1. Incident response documentation shall adhere to TSA Security Directive 1680-21-01.
2. The Vendor shall assist the Authority in post-incident response activities including but not limited to, root cause analysis and forensic investigations.
3. The Vendor shall deploy cybersecurity controls and processes to prevent the expansion of the incident and limit the adversaries' lateral movement from an impacted component to a non-impacted system.

4. The Vendor will consider how an incident involving the SuC could propagate to a connected system and system components. Propagation points shall be documented and provided to the Authority.
5. At the request of the Authority, the Vendor shall obtain a Retainer Agreement with a recognized industry leader in the Operational Technology Cybersecurity domain.
6. Where feasible, the Vendor shall provide the Authority with documentation and training for manual overrides or intervention when the SuC's confidentiality, integrity or availability is impacted by a suspected cybersecurity incident. The documentation shall cover all components tracked in the system inventory. The impact of overriding action shall be documented to inform the Authority of such potentials.
7. The Vendor shall provide the Authority with documentation and necessary material to recover the SuC to its normal operational state in post-cybersecurity incidents.
8. The Vendor shall incorporate lessons learned from incidents to strengthen the SuC's security posture.

22.1 AUDITING

The SuC, its subsystems and components shall be configured to generate audit trails that document system access, authentication, system changes, account changes, administrative events, and system condition change events in a manner that enables a qualified incident responder to reconstruct an event under investigation and assemble a timeline. Such events may be a security incident or a system change.

1. Custom scripts developed by the Vendor to help with the deployment and operation of SuC shall generate audit trail telemetry.
2. The SuC shall have defined event criticality thresholds that qualify an event to trigger an alert based on its sensitivity.
3. The SuC shall support verbose/detailed, machine readable event logging when required which enables detailed troubleshooting and diagnostics.
4. The vendor shall provide and update as needed the Authority with the log schema and format documentation to enable the Authority detection systems to properly parse the SUC logs.
5. Events shall be triggered and forwarded in real time.
6. Log events shall be timestamped based on ISO 8601 Standards.
7. Logs generated by the SuC shall follow the Common Event Format (CEF) Standard.
8. The Vendor shall provide documentation that describes how logs can be ingested into the Authority's Log Management System including log schema, log transport, and API definition when applicable.
9. Logging facilities and log content shall be protected from tampering and unauthorized access by Authority-approved cryptographic methods.
10. Security log access shall be controlled and authorized by the Authority on a need-to-know basis.

22.2 LOG COLLECTION

Logs shall be collected that identify the device, the timestamp of the event, and the user or system account that generated the event.

1. The SuC shall support forwarding logs to multiple audit log storage repositories distributed across multiple regions for redundancy and fault tolerance.
2. Event timestamps will be synchronized across logging systems to ensure events can be effectively correlated.
3. Logs generated by the SuC shall be collected into the Authority's centralized log data collection database.
4. If logs are forwarded into a less secure network than the forwarding component, the Vendor shall deploy unidirectional gateways to support the transfer of logs. If unidirectional gateway capacity is available, the Vendor shall leverage existing gateways.

5. The SuC shall have the capacity to store logs locally for a minimum of 14 days.
6. The SuC shall generate an alert whenever the logging service encounters an error, or log desk/quota nears its limit by 2 days remaining out of the 14-day requirement or 80% of its storage limit, whichever occurs first.
7. Secure authentication and transmission protocols for log capture and log forwarding shall be leveraged for all SuC components.

22.3 LOG ANALYSIS AND THREAT DETECTION

1. The Vendor shall provide defined procedures to continuously analyze logs to detect cybersecurity threats. The procedures shall follow the MITRE ATT&CK framework to define detection use cases.
2. The Vendor shall provide documentation detailing use cases for detection and mitigation for all relevant tactics and techniques based on the MITRE ATT&CK ICS framework.
3. Vendor-provided log analysis procedures and use cases shall focus on minimizing false negatives, true negatives, and false positives while maximizing true positives.
4. Results from security testing and penetration testing shall be used to develop additional use cases as applicable.
5. Industry threat intelligence services shall be leveraged to keep threat detection capabilities up to date with the industry's knowledge of the threat landscape.
6. New indicators of compromise based on threat intelligence shall be provided to the Authority's Security Operations Center.
7. The Vendor shall notify the Authority within 1 day if a system similar to the SuC, deployed in other environments, has been impacted by a cyberattack.
8. The Vendor shall develop a baseline of normal SuC operation to enable the detection of abnormal conditions. The Authority shall have the ability to tune the baseline.
9. The Vendor shall instrument the SuC, its subsystems and components to enable threat and anomaly detections which perform the following functions:
    a. Detect and prevent unauthorized system intrusion.
    b. Detect and prevent unauthorized system modification.
    c. Detect denial of service attack.
    d. Detect unplanned shutdowns
    e. Detect unexpected remote logons
    f. Detect unauthorized internal or external system communication
10. The SuC's operations shall not be impacted by the introduction of detective and preventative controls.

22.4 TABLETOP EXERCISES

1. At the request of the Authority, the Vendor shall make available personnel with expertise in SuC's cybersecurity and operational aspects to participate in Tabletop Exercises for training and validation of incident response readiness purposes.
2. The Vendor shall develop and perform tabletop exercises to cover potential negative events local to the SuC at least once annually.

23 USER AWARENESS AND TRAINING

The Vendor shall develop and maintain a user awareness training program to educate its employees and contractors on secure practices to carry out their duties. The program shall cover the following areas:

1. Necessary security and safety policies, standards, and procedures.
2. A new employee cybersecurity awareness training program covering both general IT and OT relevant security topics.

A yearly plan to train and maintain personnel necessary to fulfill SuC implementation and operational duties in a structured, secure, and measurable manner.

3. Labs and methods to train personnel on SuC functions and services in a controlled and supervised manner before deployment to Authority's service.
4. User awareness and training programs shall include the following activities:
    a. Safety protection principles and safe change management of technologies' configuration.
    b. Security incident and anomalous activity reporting.
    c. Data security and privacy standards.
    d. Insider threat and insider threat reporting
    e. The Social Engineering threat and how to detect it
    f. Physical security protection of OT infrastructure and systems.
    g. When and how to safely connect and disconnect the SuC from external security domains.
    h. Principles of multiple security teams utilizing shared file and data exchanges, and working with contractors and third parties.
    i. Secure practices at sensitive locations and sites.
    j. Secure use of messaging, email, web, browser, networks, and removable media.
    k. Secure and safe Do's and Don'ts.
    l. Personal and corporate encryption for sensitive data.
    m. Incident response training and confidential reporting of illegitimate/unsafe/insecure behaviors noticed by others.
    n. Developed roll-out procedures that educate Vendor employees and Authority-approved contractors on secure and safe workplace and remote work behaviors.
    o. Methods to gauge users' understanding of fundamental security practices, address, and monitor laggers (i.e.: users who show weak/poor understanding of their security responsibilities) progression over time.
    p. Reiterate users' responsibility to abide by the NDAs signed by them which necessitates the protection of the Vendor, Authority, and Vendor-associated client information disclosed to them before, during, and after onboarding.

24 INFORMATION SYSTEM RESILIENCE

The SuC shall be designed to meet the Authority's reliability, availability, and performance goals. The vendor shall design and implement a program to minimize the operational impact of potential threats and systems failures to meet the Authority's recovery objectives. The system design shall respect the rail system resiliency requirements with the primary goal of keeping the system operating safely. In collaboration with the Authority, the Vendor shall develop target values for the SuC and its components to define Mean Time Between Failure (MBTF) and Mean Time to Recovery (MTTR). The vendor shall define and submit for approval all assumptions considered while developing the values of MTBF and MTTR.

The vendor shall demonstrate competence in owning processes, tools, and the personnel needed to meet the uptime and performance goals set forth by the Authority for the SuC.

24.1 BACKUP AND RESTORATION

1. As part of the initial design, the Vendor and the Authority shall define the Recovery Time Objective (RTO) for the SuC.
2. The Vendor shall provide guidance based on comparable systems to assist the Authority with determining the RTO of the SuC.
3. The vendor shall implement backup strategies that guarantee the ability to meet the RTO and RPO (Recovery Point Objective) for the SuC.
4. The vendor shall maintain or provide guidance to the Authority on the methods to maintain backups of all necessary data including operating systems, device configuration, security configuration and data collected and stored by the SuC during operation.

5. The Vendor shall incorporate a “backup-in-depth” model in which recent local backups are ready for immediate implementation while full restoral backups needed to recover from an enterprise-wide incident such as a Ransomware attack are available at a secure facility.
6. The Vendor shall ensure it has the personnel with the expertise necessary to perform the restoration process of the SuC when necessary. Additionally, the vendor shall adhere to the following requirements:
    a. Develop and maintain detailed restoration runbooks for the SuC.
    b. Maintain list of required installation media with version, license keys and configuration information.
    c. Provide SuC relevant information, processes, and policies to aid in the maintenance of the Authority’s Disaster Recovery Plan (DRP) in accordance with NIST SP 800-34 Rev1, when requested by the Authority.
    d. Conduct data restoration tests.
    e. Conduct disaster recovery tests at least once, annually.
    f. Develop and deploy processes to protect backups against tampering, unauthorized encryption or destruction.

25 SYSTEM ACCEPTANCE

The Vendor shall adhere to the system acceptance process instituted by the Authority. Prior to acceptance by the Authority, the Vendor shall provide evidence of compliance with the requirements stated for the SuC. Evidence may include:

1. System documentation detailing:
    Detailed, as built system documentation
    Operational and functional requirements of the system
    Performance and capacity requirements
    Standard and safe operating thresholds
2. Evidence of compliance with defined target security levels.
3. Perform a full scope penetration test of the fully built SUC and share the test results with the Authority.
4. Current results of DCRA, including:
    Assumptions
    Threat intelligence sources
    Threat scenarios
    Risks mitigated
    Results of independent penetration or controls testing to demonstrate the effectiveness of current security countermeasures.
    Results of testing the resiliency of countermeasures.
    Training of Authority personnel and knowledge transfer.
    Standard operating policies, procedures, and playbooks.
    Status of residual risks.
    Enumeration of accepted risks and associated justifications.

26 SYSTEM RETIREMENT

26.1 MIGRATION OF SYSTEM FUNCTIONALITY

1. At the end of the SuC lifecycle, all in-service system functionality will be documented, or existing documentation will be reviewed, updated as necessary, and verified by the Vendor and the Authority that current documentation of system functionality is complete and accurate. Essential functions and associated dependencies on other systems shall be documented to develop a detailed plan for the complete migration of desired system functionality.

2. Operational impact as a result of system retirement must be documented. Operational impact as a result of system retirement should be tested, in a non-production environment, to the extent practicable.

26.2 HARDWARE DISPOSAL

All retired hardware will be disposed of in a manner consistent with local, state, and federal laws.

26.3 DATA HANDOVER AND DESTRUCTION

Any stored data related to a system being retired shall be enumerated and provided to the Authority in a format mutually agreed upon. The Vendor shall not maintain any Authority data except at the written request of the Authority. Any data related to the system being retired that remains on the system or in possession of the Vendor shall be completely erased, verified, and attested to by the Vendor.

27 THE AUTHORITY RIGHT TO AUDIT

1. The Vendor shall conduct a comprehensive audit of its compliance with ISA 62443-4-1 and the Security Level agreed upon with the Authority for the SuC development process annually at a minimum. The Vendor shall provide audit findings to the Authority. The Audit shall be performed by a qualified third-party entity.
2. The annual audit shall include an operational impact analysis of all changes made to the system to ensure changes did create an unintended impact on the Security Level of the SuC.
3. The Authority shall maintain the right to audit the Vendor and Vendor suppliers to validate compliance with clauses of this Agreement. The Authority shall perform the audit at its own cost.

28 EXCEPTION PROCESS

The Vendor may request an exemption from the Authority from delivering some of the controls listed in this Agreement. The Vendor shall submit the following information in an exemption request:

1. Details of the exemption(s) requested.
2. The reason for the exemption request.
3. If the exemption request is for a limited period, the date the exemption expires.
4. A risk assessment detailing the residual risk exposure that may be caused by the absence of controls.
5. A plan for deploying the necessary compensating controls and countermeasures to mitigate the residual risk created by the exemption.

Appendix 2

List of Tables

List of Figures

List of Abbreviations

Abbreviations	Description
AC	Air Conditioning
ANSI	American National Standards Institute
APR	Application Protection Requirements
AVS	Air and Ventilation System
CAP	Corrective Action Plan
CBTC	Communication Based Train Control
CENELEC	European Committee for Electrotechnical Standardization
CISA	Cyber Security & Infrastructure Agency
CMDB	Configuration Management Database
CP	Control Panel
CS	Control System
CVE	Common Vulnerabilities and Exposure
CVSS	Common Vulnerability Scoring System
DC	Data Confidentiality
DoS	Denial of Service
DRA	Detailed Risk Assessment
FR	Fundamental Requirement
HMI	Human Machine Interface
HS	Heating System
HVAC	Heating Ventilation and Air Condition
IAC	Identification and Authentication Control
IAM	Identity and Access Management
ICS CERT	Industrial Control System Cyber Emergency Response Team
IEC	International Electrotechnical Commission
IRA	Initial Risk Assessment
ISA	Interconnection Security Agreement
iSL-T	Initial Security Level Target
LDAP	Lightweight Directory Access Protocol
LRA	Local Root Account
NDA	Non-Disclosure Agreement
NIST	National Institute of Science and Technology
NTP	Network Time Protocol
OC	Operation Center
OT	Operational Technology

PKI	Public Key Infrastructure
POAM	Plan of Action and Milestones
PTC	Positive Train Control
RA	Resource Availability
RAMS	Reliability Availability Maintainability and Safety
RDF	Restricted Data Flow
RDP	Remote Desktop Protocol
SI	System Integrity
SIEM	Security Information and Event Management
SL	Security Level
SL-T	Security Level Target
SOP	Standard Operating Procedures
SR	System Requirement
SS	Sensor System
SuC	System under Consideration
TMS	Train Management System
TRE	Timely Response Events
TS	Technical Specification
UC	Use Control
UI	User Interface
VLAN	Virtual Local Area Network
WIFI	Wireless Fidelity

Appendix 2 Table- 1 List of Abbreviations

Assumptions

ID	Assumption
A_01	HVAC system is remotely managed and monitored by the HVAC control center
A_02	HVAC has its own control and communication network across the vehicle (category one network according to EN 50159)
A_03	HVAC sensors are in each wagon of a train (incl. driver car/cab) to measure the actual temperatures
A_04	HVAC thermostats are in each wagon of a train (incl. driver car/cab) to adjust temperature in each wagon of a train independently
A_05	Each wagon of the train has its own temperature zone (climate zone), which is monitored by the corresponding sensor and is controlled by the corresponding thermostat
A_06	Driver (driver HMI) and HVAC operation center have control over each individual wagon of a train
A_07	A fleet is remotely controlled by the HVAC operation center
A_08	The driver has permeant monitoring possibilities for all individual zones from the train he is operating.

Appendix 2 Table- 2 List of Assumptions

INTRODUCTION

Appendix 2 is added to the NATCA agreement as an aid to vendors and system builders following the agreement to deliver a System under Consideration (SuC) to a contracting authority. This Appendix contains a partial demonstration “The Example” of how a vendor who has been awarded the contract to

provide an HVAC system (the SuC) for deployment into rolling stock can supply the SuC in compliance with the agreement.

The Appendix covers the agreement sections three (3) through section six (6). These sections were chosen for detailed coverage to illustrate a real-life simplified example of the activities necessary for a vendor to comply with the intent of the agreement. The agreement draws on IEC 62443 and TS- 50701 to specify the desired cybersecurity outcomes for the SuC based on its specific risk profile. This example also aims to demonstrate the processes needed to achieve the desired cybersecurity outcomes.

To avoid a misperception that this appendix endorses certain products, fictitious product names were used in the narratives, these products are imagined as fulfilling roles in real-life conditions that a vendor may encounter while working with an Authority on the provisioning of the HVAC SuC.

Many details in this example are omitted or significantly abridged to focus on the cybersecurity aspect of the example and keep the appendix reasonably sized. Additionally, some details may not represent realistic system characteristics or requirements, however, such details were added to the appendix to demonstrate the compliance process via hypothetical examples. An actual implementation shall vary in detail and scope depending on the actual system supplied.

The IEC 62443 standard defines the specifications for a plannable and assessable design of security for all types of OT systems against cyber-attacks. Since the end of 2021, it has been supplemented in the railway sector by the technical guideline TS 50701, which was developed in Europe and specifies the application of IEC 62443 in the railway sector.

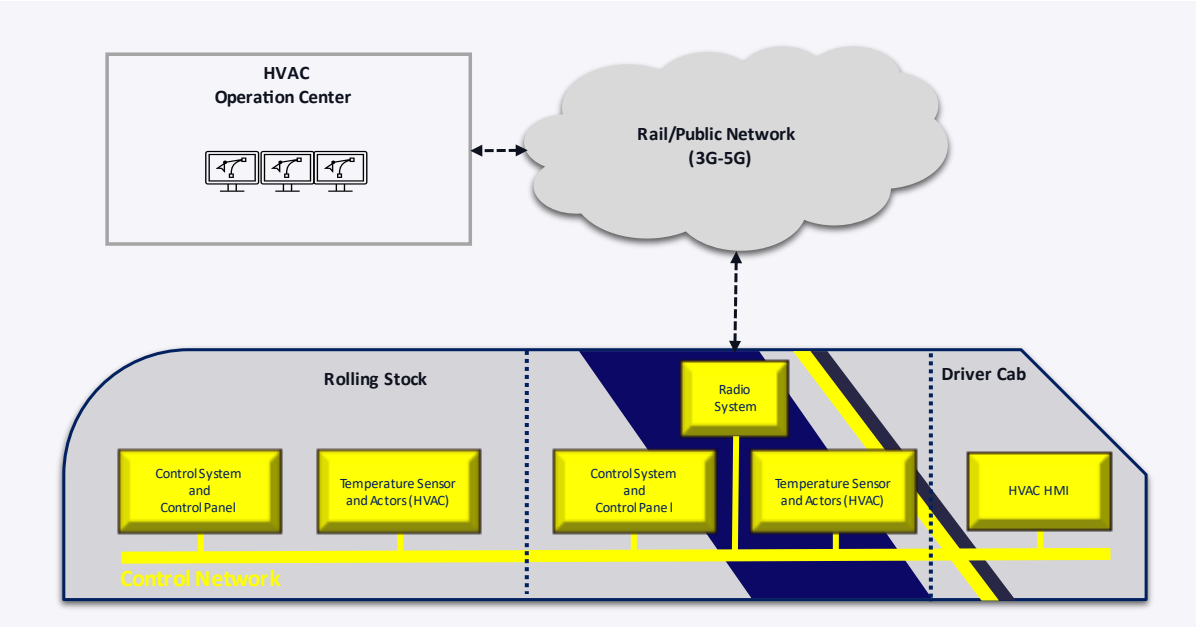
1 Process Definition

In this chapter, the process for the first three phases according to the Agreement and in alignment with TS 50701 (CENELEC Phase 1 to 3) including the detailed risk assessment is defined, which is based on the decision to use TS 50701 as the basic standard.
The following process steps based on IEC 62443, TS 50701, and best practices are used:

- Define System under Consideration (SuC)
- Assessment of the Protection Requirements (APR)
- Initial Risk Assessment (IRA)
- Initial Zoning Concept
- Detailed Risk Assessment (DRA)
    - Attacker type definition (maximum iSL-T)
    - Threat catalog definition
    - Relevance and impact evaluation (delivers iSL-T)
    - SL-T vector determination
    - Select system requirements (SR) to mitigate risk.
    - Perform a second risk assessment including selected SR.
    - Select additional compensating measures to mitigate the risk further (if necessary)
    - Perform final risk assessment (residual risk)
    - Check if residual risk can be accepted (compared to target risk)
        - Provide a reason for accepting the final risk.
        - Check if additional measures are necessary.
    - Define explanations for unused SR and perform a completeness check.

2 System under Consideration

In this scenario, the System under Consideration (SuC) is a Heating, Ventilation, and Air Conditioning System (HVAC System) installed in rolling stock. An HVAC system is essential for maintaining a comfortable and safe environment for passengers and crew. The following figure provides an overview of the main functions of the SuC.



Appendix 2 Figure- 1 System Under Consideration

The SuC includes the following functions (components):

Component	Description
HVAC HMI	Heating, Ventilating and Air Conditioning control unit for the driver
AC	Air conditioning system
HS	Heating System
AVS	Air ventilation and distribution system including air intakes, exhaust air unit and pressure protection system.
SS	Sensor system capturing environmental conditions and system information relating to the function
CS	Control System for a coordinated management of the subsystems AC, HS and AVS based on control panel input or to adjust to predefined environmental parameters.
CP	Control Panel to control a climate zone locally
RS	Radio System to enable remote control and monitoring via the HVAC Operation Center
CN	Control Network to connect all subsystems
OC	HVAC Operation Center to control and monitor the fleet of rolling stock.

Appendix 2 Table- 3 SuC Components

In this CENELEC phase, only the main functions are considered. The actual system composition (components and subsystems) is defined in a later phase (CENELEC phase 5) of an actual development project.

2.1 Scope, context, purpose, and Environment of the SuC

SuC Overview	
Scope	Regulate climatic conditions inside of a rolling stock by the vehicle staff and remotely by a dedicated operation center
Context	Functions during operation of a rolling stock and is maintained when the rolling stock is in the depot
Purpose	Maintain a comfortable and safe environment for passengers and crew in a rolling stock during train operation
Environment	Primary location of the SuC is in a rolling stock

Appendix 2 Table- 4 SuC Overview

2.2 System boundaries

The SuC is a closed onboard HVAC network with a radio-based remote connection to an operation center. The SuC and its subcomponents will not interface, nor have the ability to impact safety critical systems such as PTC or CBTC. The SuC will not be accessible from passenger comfort systems such as guest WIFI or entertainment systems.

2.3 Functionalities provided by the SuC

The main functionalities of the SuC are heating, cooling, ventilation, and control over these functionalities inside of rolling stock. Additionally, remote monitoring and control is possible via an operation center.

2.4 Interfaces (external and internal)

External:

- Radio System interface via a rail/public radio network to the HVAC Operation Center
- Maintenance Laptop(s)

Internal:

- Each functional block (component or subsystem) has an interface to a dedicated HVAC onboard network.

A complete list of all interfaces shall be developed during the development of the system (up to CENELEC phase 5). In this scenario, a communication matrix will be created to identify potential interfaces for all zones.

2.5 Presentation of the security policy used.

The Authority security policy is used.

2.6 Presentation of the security legislation

US security legislation.

2.7 List of assumptions and justifications for the SuC

For the full list of assumptions please refer to *Table- 2 List of Assumptions* .

3 ASSESSMENT OF THE PROTECTION REQUIREMENTS

The above information is used to develop the security requirements for the SuC.

3.1 APR DEFINITIONS

For the classification of the protection class covering the three security targets (confidentiality, integrity, and availability) the following definitions are used:

- Protection Class Definition Table- 5 Protection Class Definition .
- Predefinitions to cover relations between the security targets and safety Table 6 Predefinitions for the Application Protection Requirements Assessment .

Category / Protection class	Financial Impact:	Privacy violations:	Violation of laws, regulations, and rules:	Disruption of business activity:	Loss of reputation:	Health damage:
Definition	Loss of revenue, damages, additional personnel costs or investments, material damage, etc.	Handling personal data of customers, employees, and suppliers based on the applicable data protection laws and the guidelines applicable thereto. It is strongly recommended to coordinate the assessment with the relevant data protection organization.	For example: Group guidelines, company agreements, service regulations, legal ordinances, customs regulations, etc.	Delayed implementation, late delivery, additional expenditure, inadequate service, etc.	Negative reporting, loss of reputation, loss of confidence among customers and business partners, etc.	Injury or fatality
Low	None or only minor financial damage. Financial thresholds are defined by the CISO of the CEO taking into account 1:4 and external sales.	An impairment of the right of self-determination with regard to information has no effect on the personal rights of the person concerned. e.g., generally accessible data, address data within the scope of an employment contract or other contractual relationship, personnel number.	The risk occurrence comprises a single issue with politically/legally relevant sub-aspects. Note: The following aspects may be relevant for the assessment: contractual agreements, federal organizations for security, rail authority, network, right to personal self-determination and integrity.	Isolated limitations in operational activities with little or no impact on capabilities/processes. Note: The following aspect may be relevant in the assessment: - End customer service provision - Public supply	Local reporting on individual subject matter with critical aspects. Note: The following aspects may be relevant when assessing reputation: Employee Reputation, Employer Reputation, Strategic Goal Attainment at Risk, Customer or Market Share loss / Political Trust.	Individuals may suffer minor injuries if the system fails.
Middle	Tolerable financial damage. The financial thresholds are defined by the CISO of the CEO, taking into account 1:4 and external sales.	An impairment of the right to informational self-determination has a minor impact on the personal rights of the data subject. e.g., generally accessible data, address data within the scope of an employment contract or other contractual relationship, personnel phone number.	The occurrence of risk comprises a single issue that leads to a contractual, legal, or political audit with probable consequences (e.g., penalties). Note: The following aspects may be relevant for the assessment: contractual agreements, federal organizations for security, rail authority, network right to personal self-determination and integrity.	Increased constraints on operations with acceptable impact on capabilities/processes. Note: The following aspect may be relevant in the assessment: - End customer service provision - public supply	Country-wide and supra-regional (neighboring countries) critical reporting of sub-areas/individuals of the company. Note: The following aspects may be relevant when assessing reputation: Employee reputation, employer reputation, strategic target achievement at risk, loss of customers or market share / political trust.	If the system fails, individuals may suffer serious injuries. As a rule, inpatient hospitalization is required.
High	High financial damage. Financial thresholds are defined by the CISO of the CEO, taking into account 1:4 and external turnover.	An impairment of the right to informational self-determination has a significant impact on the personal rights of the person concerned or is a criminal offense. e.g., customer or employee profiles, qualification or scoring data, wage or salary data, bank data, health data, political and religious convictions, video surveillance and recording, telecommunication service data at the provider.	The occurrence of risk comprises a situation/series of situations that have contractual, legal, or political consequences for parts of the company branch. Note: The following aspects may be relevant for the assessment: contractual agreements, federal organizations for security, rail authority, network, right to personal self-determination and integrity.	Extensive constraints in operations with high impact on capabilities/ processes or critical infrastructure facilities. Note: The following aspect may be relevant in the assessment: - End-user service delivery - public supply	National/international critical reporting. The reputation of the operator is at risk, and market share and new business are at risk. Note: The following aspects may be relevant when assessing reputation: Employee reputation, employer reputation, strategic goal achievement at risk, customer, or market share loss / political trust.	If the system fails, many people can suffer serious injuries. As a rule, inpatient hospitalization is required. Individuals may also be killed by the failure of the system.
Very High	Existence-threatening damage. The financial threshold values are defined by the CISO of the CEO, taking into account 1:4 and external turnover.	There is a high need for protection and, moreover, the processing of personal data is an existential business purpose of the company. An impairment of the right to informational self-determination can threaten the existence of the company. For example, personal data that is subject to professional secrecy or bank or credit card accounts at the call center.	The occurrence of risk comprises a series of circumstances that lead to critical contractual, legal, and political consequences for the entire company. Note: The following aspects may be relevant for the assessment: contractual agreements, federal organizations for security, rail authority, network, and right to personal self-determination and integrity.	Large-scale cessation of operations. Capabilities/processes have been interrupted or are operating below the legal thresholds for critical infrastructure facilities. Note: The following aspect may be relevant in the assessment: - End customer service provision - Public supply	International negative reporting, image of the company damaged for the long term with all stakeholders. Note: The following aspects may be relevant when assessing reputation: Employee reputation, employer reputation, strategic goal achievement at risk, loss of customers or market share / political trust.	If the system fails, many people can be killed.

Appendix 2 Table- 5 Protection Class Definition

The following predefinitions were used for the assessment of the protection requirements.

ID	Predefinitions
PD_01	Availability is always connected to the evaluation of the assessed interface.
PD_02	Availability is set to high or very high, if a non-availability is linked to a safety critical reaction
PD_03	Availability is always connected to the evaluation of the assessed interface.
PD_04	Availability is set to high or very high, if a non-availability is linked to a safety critical reaction, e.g., the emergency break.
PD_05	Availability is set to high, if a non-availability of one in one train is linked to a fleet fail.

Appendix 2 Table- 6 Predefinitions for the Application Protection Requirements Assessment

3.2 APR Results

The classification results are presented in the following table:

ID	Component Name	Confidentiality	Integrity	Availability
1	HVAC HMI	Low	High	High
2	SS	Low	Middle	High
3	HS	Low	Middle	High
4	AVS	Low	Middle	High
5	AC	Low	Middle	High
6	CS	Low	Middle	High
7	CP	Low	Middle	High
8	RS	Low	High	High
9	CN	Low	High	High
10	OC	Low	High	High

Appendix 2 Table- 7 Application Protection Requirement Result

The assessment of the protection requirements and initial risk assessment are documented in a separate file. The complete results are shown in Section 5 *Table 12 APR and IRA Combined Results* .

4 Initial Risk Assessment

The initial risk assessment (IRA) documents high-level cybersecurity risks via the worst-case scenario considerations for the SuC.

4.1 IRA Definitions

The following definitions for exposure and vulnerability are used for the initial risk assessment:

Rating	Exposure	Vulnerability
1	Highly restricted logical or physical access for attackers, e.g. - highly restricted network and physical access, or - product or components cannot be acquired by attackers or only with high effort	- Successful attack is only possible for a small group of attackers with high hacking skills (high capabilities needed) - Vulnerability is only exploitable with high effort, and if strong technical difficulties can be solved, non-public information about inner workings of system is required - State of the art security measures to counter the threat - High chance for attacker to be traced and prosecuted

2	Restricted logical or physical access for attackers, e.g. - internal network access required, or - restricted physical access, or - product or components can be acquired by attacker with medium effort	- Successful attack is feasible for an attacker with average hacking skills (medium capabilities needed) - Vulnerability is exploitable with medium effort, requiring special technology, domain, or tool knowledge - Some security measures to counter the threat - Medium chance for attacker to be traced and prosecuted
3	Easy logical or physical access for attackers, e.g. - Internet access sufficient, or - public physical access, or - attacker has access as part of daily work, operation, or maintenance activities, or - product or components can be acquired by attacker with low effort	- Successful attack is easy to perform, even for an unskilled attacker (little capabilities needed) - Vulnerability can be exploited easily with low effort, since no tools are required, or suitable attack tools freely exist. - No or only weak security measures to counter the attack caused by the threat - Low chance for attacker to be traced and prosecuted

Appendix 2 Table- 8 Definition of Exposure and Vulnerability

The following definition of impact is used for the initial risk assessment (TS 50701):

Impact	Human health and safety	Operational availability	Financial impact
A	One or several fatalities	Most of operations disturbed for more than 1 week	Could lead to the organization's bankruptcy
B	Several severe or critical injuries	Most of the operations are disturbed between 1 day and 1 week. Important operation disturbed for more than 1 week	Impact in a significant way the organization annual budget (> 10% of revenue)
C	One severe injury or several injuries requiring hospitalization	Most of the operations disturbed between 1 hour and 1 day. Important operation disturbed between 1 day and 1 week	Significant impact to the organization's annual benefits.
D	One injury requiring hospitalization or several light injuries (not requiring any hospitalization)	Important operation disturbed less than 1 day.	Impact not visible on annual basis

Appendix 2 Table- 9 Definition of Impact

The following risk matrix from TS 50701 is used for the initial risk assessment:

Likelihood	Impact			
	D	C	B	A
1	Low	Low	Low	Medium
2	Low	Low	Medium	Significant
3	Low	Medium	Significant	High
4	Medium	Significant	High	High
5	Significant	High	High	Very high

Appendix 2 Table- 10 Risk Matrix

4.2 IRA Results

The result of the IRA is presented in the following table:

ID	Component	CIA	Exposure	Vulnerability	Likelihood	Impact	Risk
1	HVAC HMI	High	2	2	3	B	High
2	SS	High	2	2	3	C	Medium
3	HS	High	2	2	3	C	Medium
4	AVS	High	2	2	3	C	Medium
5	AC	High	2	2	3	C	Medium
6	CS	High	2	2	3	C	Medium
7	CP	High	2	2	3	C	Medium
8	RS	High	2	2	3	B	High
9	CN	High	2	2	3	B	High
10	OC	High	2	2	3	B	High

Appendix 2 Table- 11 Initial Risk Assessment Result

5 APR AND IRA COMBINED RESULTS

ID	Subsystem	Confidentiality	Integrity	Availability	Exposure	Vulnerability	Likelihood	Impact	Risk	Explanations
1	HVAC HMI	Low	High	High	2	2	3	B	High	C: Financial Impact: No or only minor financial damage I: Health damage - people in a single train (all wagons) may suffer from heat or cold with the possibility of loss of consciousness, Disruption of business activity, loss of reputation nation wide or bigger, scaling effect A: Health damage, Loss of reputation, Disruption of business activity
2	SS	Low	Middle	High	2	2	3	C	Medium	C: Financial Impact: No or only minor financial damage I: Health damage - some people in an individual wagon may suffer from heat or cold with the possibility of loss of consciousness, Disruption of business activity, loss of reputation locally or bigger A: Health damage, Disruption of business activity
3	HS	Low	Middle	High	2	2	3	C	Medium	C: Financial Impact: No or only minor financial damage I: Health damage - some people in an individual wagon may suffer from heat or cold with the possibility of loss of consciousness, Disruption of business activity, loss of reputation locally or bigger A: Health damage, Disruption of business activity
4	AVS	Low	Middle	High	2	2	3	C	Medium	C: Financial Impact: No or only minor financial damage I: Health damage - some people in an individual wagon may suffer from heat or cold with the possibility of loss of consciousness, Disruption of business activity, loss of reputation locally or bigger A: Health damage, Disruption of business activity
5	AC	Low	Middle	High	2	2	3	C	Medium	C: Financial Impact: No or only minor financial damage I: Health damage - some people in an individual wagon may suffer from heat or cold with the possibility of loss of consciousness, Disruption of business activity, loss of reputation locally or bigger A: Health damage, Disruption of business activity
6	CS	Low	Middle	High	2	2	3	C	Medium	C: Financial Impact: No or only minor financial damage I: Health damage - some people in an individual wagon may suffer from heat or cold with the possibility of loss of consciousness, Disruption of business activity, loss of reputation locally or bigger A: Health damage, Disruption of business activity
7	CP	Low	Middle	High	2	2	3	C	Medium	C: Financial Impact: No or only minor financial damage I: Health damage - some people in an individual wagon may suffer from heat or cold with the possibility of loss of consciousness, Disruption of business activity, loss of reputation locally or bigger A: Health damage, Disruption of business activity
8	RS	Low	High	High	2	2	3	B	High	C: Financial Impact: No or only minor financial damage I: Health damage - people in a single train (all wagons) may suffer from heat or cold with the possibility of loss of consciousness, Disruption of business activity, loss of reputation nation wide or bigger, scaling effect A: Health damage
9	CN	Low	High	High	2	2	3	B	High	C: Financial Impact: No or only minor financial damage I: Health damage - people in a single train (all wagons) may suffer from heat or cold with the possibility of loss of consciousness, Disruption of business activity, loss of reputation nation wide or bigger, scaling effect A: Health damage, Disruption of business activity
10	OC	Low	High	High	2	2	3	B	High	C: Financial Impact: No or only minor financial damage I: Health damage - people in several trains may suffer from heat or cold with the possibility of loss of consciousness, Disruption of business activity, loss of reputation nation wide or bigger, scaling effect A: Health damage, Disruption of business activity

Appendix 2 Table- 12 APR and IRA Combined Results

6 ZONES AND CONDUITS

The documented System Definition according to EN 50126, created in the first two phases of the development of the project is used to define the SuC. Together with the results from the APR/IRA it provides the basis for defining zones and conduits.

Zones defined in this process are explicitly not equal to physical network zones. The development of the networking design comes at a later stage of the process, but the network design and architecture need to follow the segregation defined in the Zones and Conduits design.

6.1 DEFINITION OF ZONES AND CONDUITS

The purpose of defining zones and conduits is to group functions (performed by systems, subsystems, or components) that have the same cybersecurity requirements, considering similar threats and potential impacts. Therefore, an initial risk assessment is needed. As an alternative, the zones can be analyzed based on the protection requirements. If both approaches (IRA and APR) are combined, they deliver a thorough first security analysis of the SuC.

The final zone model may be modified based on the Authority's risk tolerance, integration requirement, and legacy systems considerations. For this example, minimal considerations of such constraints were assumed. CBTC and PTC systems run on decisively separate networks and have their own zones and conduits models.

The following definitions are applied to form zones and conduits for the SuC:

Zones are groupings of:

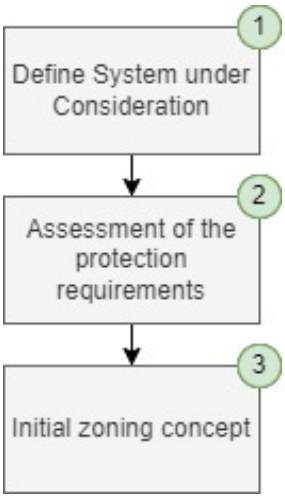
- components and systems with the same or similar protection requirements
- components and systems with similar operational and functional aspects at one location

Conduits connect:

- zones with different protection requirements
- zones with the same protection requirements in different locations

6.2 ZONING PROCESS

The process is represented in the following figure.



Appendix 2 Figure- 2 Security Process for an Initial Zoning Concept

6.3 ZONES

Following the results from the APR/IRA and the definition provided in Chapter 6.1 the following zones are defined.

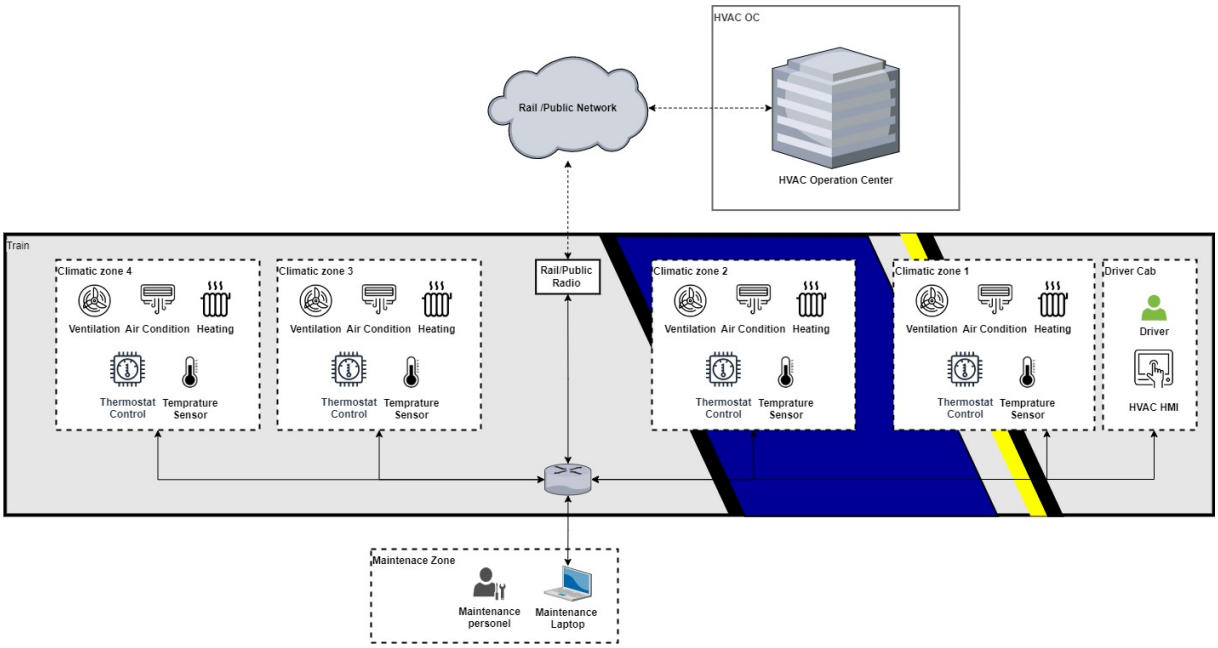
ID	Zone	Component/Subsystem	Reason
Z_01	HVAC HMI	HVAC HMI	Location, APR/IRA, Function
Z_02	Climatic Zone 1	SS, HS, AVS, AC, CS, CP	Location, APR/IRA, Function
Z_03	Climatic Zone 1+n	SS, HS, AVS, AC, CS, CP	Location, APR/IRA, Function
Z_04	Radio	RS	Location and Function
Z_05	Maintenance Zone	Maintenance Laptop	Function
Z_06	HVAC OC	HVAC Operation Center	Location, APR/IRA, Function

Appendix 2 Table- 13 Zones

In the subchapters 6.3.1 to 6.3.5 a short zone description is provided.

6.3.1 Initial Zone Concept

The following figure shows the initial Zone Concept.



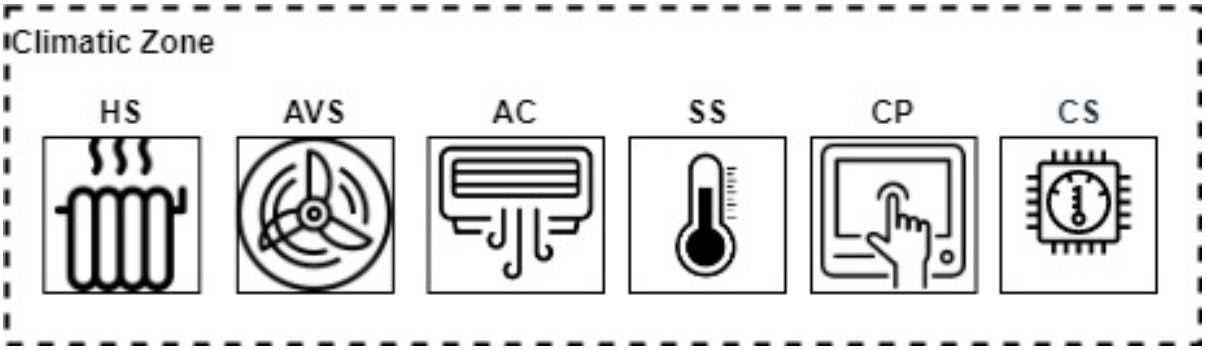
Appendix 2 Table- 14 Initial Zoning Concept

6.3.2 HVAC HMI Zone

The HMI forms its own zone due to its location and unique functionality. The driver has control over each individual wagon (climatic zone 1-n) via the HMI across the entire train. It is assumed that the driver only powers the systems on. All parameters (e.g., temperature and ventilation strengths) are controlled based on information system input. Only one HMI per train is installed and used to control the HVAC systems. The impact of an attack is localized to one zone. The impact can spread if the attack is based on an intentionally malicious component through a supply chain attack.

6.3.3 Climatic Zone

A climatic zone is a combination of all subsystems needed to enable a stable climatic environment in one wagon of rolling stock. The following drawing shows all the subsystems to form a climatic zone:



Appendix 2 Figure- 3 Climatic Zone

6.3.3.1 Sensor System (SS):

The main function is to measure the actual parameters (e.g., temperature, ventilation speed etc.) in each wagon. False information reported by sensors will cause errant operation of the control system and can cause health damage to the passengers. It is assumed that only one system per wagon is installed.

No scalability in terms of an attack is to be expected during operation. A fleet can be compromised only via a supply-chain attack. The worst-case scenario is a stop of the train due to unbearable temperatures.

6.3.3.2 Heating System (HS):

The main function is to raise the temperature in one climatic zone.
It is assumed that only one system per wagon is installed.
No scalability in terms of an attack is to be expected during operation. Only via a supply-chain attack, a fleet can be compromised. The worst-case scenario is a stop the train due to unbearable temperatures.

6.3.3.3 Air and Ventilation System (AVS):

The main function is to circulate air in one climatic zone.
It is assumed that only one system per wagon is installed. No scalability in terms of an attack is to be expected during operation. Only via a supply-chain attack, a fleet can be compromised. The worst-case scenario is a stop of the train due to unbearable temperatures. The worst-case scenario is a stop of the train due to lack of oxygen.

6.3.3.4 Air Condition (AC):

The main function is to lower the temperature in one climatic zone.
It is assumed that only one system per wagon is installed.
No scalability in terms of an attack is to be expected during operation. Only via a supply-chain attack, a fleet can be compromised. The worst-case scenario is a stop of the train due to unbearable temperatures. The worst-case scenario is a stop of the train due to unbearable temperatures.

6.3.3.5 Control System (CS):

The main function is to adjust and control HS, AVS, and AC in each wagon while considering the measured data from SS.
It is assumed that only one system per wagon is installed.
No scalability in terms of an attack is to be expected during operation. Only via a supply-chain attack, a fleet can be compromised. The worst-case scenario is a stop of the train due to unbearable temperatures. The worst-case scenario is a stop of the train due to unbearable temperatures.

6.3.3.6 Control Panel (CP):

The main function is to control and monitor locally in a wagon.
It is assumed that only one system per wagon is installed.
No scalability in terms of an attack is to be expected during operation. Only via a supply-chain attack, a fleet can be compromised. The worst-case scenario is a stop of the train due to unbearable temperatures.

6.3.4 Radio Zone

The main function is to provide the interface to the HVAC operation center.
It is assumed that only one system per train is installed. No scalability in terms of an attack is to be expected during operation. Only via a supply-chain attack, a fleet can be compromised. The worst-case scenario is a stop of the train due to unbearable temperatures.

6.3.5 HVAC OC

The main function of the HVAC Operation Center is to control and monitor all HVAC-related onboard systems remotely. It is assumed that one system is used to control and monitor a train

fleet. It is possible to remotely modify the target temperature or air ventilation criteria. Mis-adjustment may cause medium financial damage due to the ability to control multiple wagons or multiple trains. Mis-adjustment may cause high reputational loss nationwide or even worldwide if news of the cybersecurity attack is published publicly.
Individuals may suffer in each train, and interruption the of operation of an entire fleet is very likely.

6.3.6 Maintenance Zone

The main function is to provide an interface for the maintenance of all HVAC subsystems in terms of local diagnostics, software, and configuration updates. It is assumed that the maintenance for all HVAC subsystems is done via a central component. A maintenance zone can contain functions such as jump servers to be used to perform system updates or a physical computer that will be used to perform various maintenance functions such as firmware updates. Such a computer, even if not always connected, needs to be secured to the SL-T of the zone.

6.4 CONDUITS

In this scenario, a communication matrix is used to identify all conduits. An example of such a matrix is shown below:

	Z_01 HVAC HMI	Z_02 Climatic Zone 1	Z_03 Climatic Zone 2	Z_04 Radio	Z_05 Maintenance Zone	Z_06 HVAC OC
Z_01 HVAC HMI	-	X	X	-	X	X
Z_02 Climatic Zone 1	X	-	-	-	X	-
Z_03 Climatic Zone 2	X	-	-	-	X	-
Z_04 Radio	-	-	-	-	X	X
Z_05 Maintenance Zone	X	X	X	X	-	-
Z_06 HVAC OC	X	-	-	X	-	-

Appendix 2 Table- 15 Zone Communication Matrix

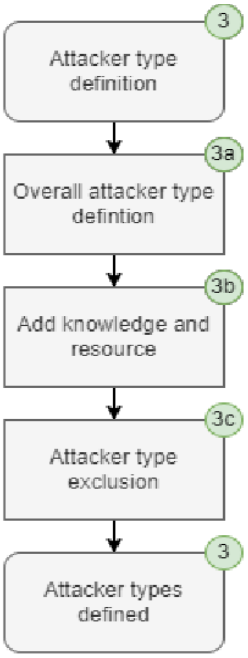
The resulting conduits are presented in the table below:

ID	Conduit	Zone 1	Zone 2
C_01	HMI - CZ 1	Z_01 HVAC HMI	Z_02 Climatic Zone 1
C_02	HMI - CZ 2	Z_01 HVAC HMI	Z_02 Climatic Zone 2
C_03	HMI - Radio	Z_01 HVAC HMI	Z_04 Radio
C_04	HMI - MZ	Z_01 HVAC HMI	Z_05 Maintenance Zone
C_06	CZ 1 - MZ	Z_02 Climatic Zone 1	Z_05 Maintenance Zone
C_07	CZ 2 - MZ	Z_02 Climatic Zone 2	Z_05 Maintenance Zone
C_08	RZ - MZ	Z_04 Radio	Z_05 Maintenance Zone

Appendix 2 Table- 16 Conduits

7 Define Attacker Types and determine the preliminary Security Level

In this step, from whom or from what the threat emanates is considered. The IEC 62443-3-3 definition of the term “attack” is an assault on a system that derives from an intelligent threat. The attacker can be a person or a group/organization. The determination of the severity of a threat event follows the system of the IEC 62443, referenced in TS 50701, after which the type of attacker and its possibilities are defined. In this step, attacker types are identified which could cause certain threats.



Appendix 2 Figure- 4 Attacker Definition Process

Some attackers might be excluded as they are not expected to target the SuC. For example, nation-state attackers might not be considered a threat to the operator of a local railway line which is not categorized as critical infrastructure. As the reason for excluding some attacker types may change over time or due to a change in the threat landscape, it is mandatory to periodically re-check the exclusion list or be prepared to mitigate the attacker type within reasonable timing and effort. The set of all attacker types without excluded attackers results in the maximum requirement for resources and knowledge.

7.1 Overall Attacker Type Definition

The attacker definition is the basis for defining the classification of the threats and defining the likelihood of attack. Intentional, targeted attackers can be split into several categories. These threat actors intend to damage the SuC. Targeted attacks are the focus of the analysis.

7.2 Add Knowledge and Resources

In this step, the knowledge required, and resources required ratings are added to the attacker type. The range of values for both categories is defined in the following table from IEC 62443-3-3.

SL-T_Max		Resources		
		2 Low	3 Moderate	4 Extended
Know-ledge	2 General	2	3	4
	3 Specific	3	3	4
	4 Extended	3	4	4

Appendix 2 Table- 17 Attacker Knowledge and Resources

For this SuC the following values are set:
Knowledge = Extended (4)
Resources = Extended (4)
The ratings above are not the proposed SLTs, but rather the maximum possible value.

7.3 Attacker Type Exclusion

The maximum values of the attacker type taken into consideration in the assessment are used to define the maximum SL-T (SL-T_Max). The SL-T_Max represents the upper bound of the SL-T (Security Level Target) which is used to derive Systems Requirements (SR).
SL-T_Max = 4
Therefore, no attackers are excluded and no upper restriction in terms of mapping IEC 62443 system requirements to any potential threat is applied in the next steps of the detailed risk assessment.

8 Threat Definition

The threat definition is separated into two major steps, which are described in the following two subchapters:

- Establishment of the threat catalog and
- The threat mapping to the foundational requirements according to IEC 62443-3-3

8.1 Threat Catalog

The risk assessment as well as the definition of the SL-T is based on the threats defined in the risk assessment tool. Different threat catalogs can be used. The threat catalog needs to cover all relevant aspects of the domain. It is necessary to define if environmental threats and physical attacks should be considered as well. If these aspects are excluded, it must be documented.

The detailed definition of different threats needs to be sufficient to perform a detailed analysis of them. However, the number of threats must be limited to a realistic minimum which is feasible to address in the analysis phase.

Each threat must be described in sufficient detail to be distinguished from other threats. As existing threat catalogs might not take all relevant aspects into account, (e.g., railway-specific threats). Hence additional threats can be defined and added to the risk assessment tool. Furthermore, threats of an existing catalog can be split up or aggregated according to the requirements of the assessment.

Due to the absence of a North American government developed threat catalog this risk assessment leverages the threat catalog “Elementare Gefährdungen” from the German Bundesamt für Sicherheit in der Informationstechnik (BSI):

G 0.1 Fire
G 0.2 Unfavorable Climatic Conditions
G 0.3 Water
G 0.4 Pollution, Dust, Corrosion
G 0.5 Natural Disasters
G 0.6 Catastrophes in the Vicinity
G 0.7 Major Events in the Vicinity
G 0.8 Failure or Disruption of the Power Supply
G 0.9 Failure or Disruption of Communication Networks
G 0.10 Failure or Disruption of Supply Networks
G 0.11 Failure or Disruption of Service Providers
G 0.12 Electromagnetic Interference
G 0.13 Interception of Compromising Interference Signals
G 0.14 Interception of Information / Espionage
G 0.15 Eavesdropping
G 0.16 Theft of Devices, Storage Media, and Documents
G 0.17 Loss of Devices, Storage Media, and Documents
G 0.18 Poor Planning or Lack of Adaptation
G 0.19 Disclosure of Sensitive Information
G 0.20 Information or Products from an Unreliable Source
G 0.21 Manipulation of Hardware or Software
G 0.22 Manipulation of Information
G 0.23 Unauthorized Access to IT Systems
G 0.24 Destruction of Devices or Storage Media
G 0.25 Failure of Devices or Systems
G 0.26 Malfunction of Devices or Systems
G 0.27 Lack of Resources
G 0.28 Software Vulnerabilities or Errors
G 0.29 Violation of Laws or Regulations
G 0.30 Unauthorized Use or Administration of Devices and Systems
G 0.31 Incorrect Use or Administration of Devices and Systems
G 0.32 Misuse of Authorization
G 0.33 Shortage of Personnel
G 0.34 Assault
G 0.35 Coercion, Blackmail or Corruption
G 0.36 Identity Theft
G 0.37 Repudiation of Actions
G 0.38 Misuse of Personal Information
G 0.39 Malware
G 0.40 Denial of Service
G 0.41 Sabotage
G 0.42 Social Engineering
G 0.43 Attack with Specially Crafted Messages
G 0.44 Unauthorized Entry to Premises
G 0.45 Data Loss
G 0.46 Loss of Integrity of Sensitive Information
G 0.47 Harmful Side Effects of IT-Supported Attacks
For the detailed threat description please follow this link:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Elementare_Gefaehrdungen.pdf?__blob=publicationFile&v=4

8.2 Threat Mapping to the Foundational Requirements

In this step, each threat (based on the catalog) must be mapped to the foundational requirements (FR) from IEC 62443. This is to ensure the actual security measures conform with TS 50701 which itself refers to IEC 62443. Based on this mapping, the SL-T is defined, and relevant SRs from IEC 62243-3-3 are selected. There are seven FRs in place, and the identified threats need to be sorted into these FRs as described below.

8.2.1 Identification and authentication (IAC - Identification and authentication control)

In this FR, threats are assigned that lead to unauthorized access and/or access to the system or system components.

8.2.2 Usage control and monitoring, authorization (UC - Use control)

In this FR, threats that lead to an unauthorized use of the system due to missing or dysfunctional use control are classified.

8.2.3 System integrity (SI - System integrity)

In this FR, threats that are related to the manipulation of data or components are assigned.

8.2.4 Confidentiality (DC - Data confidentiality)

In this FR, threats are assigned that are related to unauthorized access to, or disclosure of sensitive data or information.

8.2.5 Restricted data flow (RDF - Restricted data flow)

In this FR, threats are assigned that lead to inadmissible managed data flows.

8.2.6 Reacting to events in good time (TRE - Timely response to events)

Threats that delay or prevent the response to security-relevant events are assigned to this FR.

8.2.7 Availability of resources (RA - Resource availability)

In this FR, threats that interrupt resource supply, which is required for continuous operation, e.g., energy supply are assigned.

In the following table the FR mapping to the threats is presented:

Threat Name	IAC	UC	SI	DC	RDF	TRE	RA
G 0.1 Fire	-	-	-	-	-	X	X
G 0.2 Unfavorable Climatic Conditions	-	-	-	-	-	X	X
G 0.3 Water	-	-	-	-	-	X	X
G 0.4 Pollution, Dust, Corrosion	-	-	-	-	-	X	X
G 0.5 Natural Disasters	-	-	-	-	-	X	X
G 0.6 Catastrophes in the Vicinity	-	-	-	-	-	X	X
G 0.7 Major Events in the Vicinity	-	-	-	-	-	X	X
G 0.8 Failure or Disruption of the Power Supply	-	-	-	-	-	X	X
G 0.9 Failure or Disruption of Communication Networks	-	-	-	-	-	X	X
G 0.10 Failure or Disruption of Supply Networks	-	-	-	-	-	X	X
G 0.11 Failure or Disruption of Service Providers	-	-	-	-	-	X	X
G 0.12 Electromagnetic Interference	-	-	X	-	-	X	X
G 0.13 Interception of Compromising Interference Signals	-	-	-	X	-	-	-
G 0.14 Interception of Information / Espionage	X	X	-	X	X	-	-
G 0.15 Eavesdropping	X	X	-	X	X	-	-
G 0.16 Theft of Devices, Storage Media and Documents	-	-	-	X	-	X	X
G 0.17 Loss of Devices, Storage Media and Documents	-	-	-	X	-	X	X
G 0.18 Poor Planning or Lack of Adaptation	-	-	X	X	-	X	X
G 0.19 Disclosure of Sensitive Information	X	X	-	X	X	-	-
G 0.20 Information or Products from an Unreliable Source	-	-	X	-	-	-	-
G 0.21 Manipulation of Hardware or Software	X	X	X	X	X	X	X
G 0.22 Manipulation of Information	X	X	X	-	X	X	X
G 0.23 Unauthorized Access to IT Systems	X	X	X	X	X	X	X
G 0.24 Destruction of Devices or Storage Media	-	-	-	-	-	X	X
G 0.25 Failure of Devices or Systems	-	-	X	-	-	X	X
G 0.26 Malfunction of Devices or Systems	-	-	X	-	X	X	X
G 0.27 Lack of Resources	-	-	-	-	-	X	X
G 0.28 Software Vulnerabilities or Errors	-	-	X	X	X	-	X
G 0.29 Violation of Laws or Regulations	X	X	-	-	-	-	-
G 0.30 Unauthorized Use or Administration of Devices and Systems	X	X	X	X	X	X	X
G 0.31 Incorrect Use or Administration of Devices and Systems	X	X	X	X	X	X	X
G 0.32 Misuse of Authorization	X	X	X	X	X	X	X
G 0.33 Shortage of Personnel	-	-	-	-	-	-	-
G 0.34 Assault	-	-	-	-	-	X	X
G 0.35 Coercion, Blackmail or Corruption	-	X	-	-	-	X	-
G 0.36 Identity Theft	X	X	-	-	-	X	-
G 0.37 Repudiation of Actions	-	X	-	-	-	X	-
G 0.38 Misuse of Personal Information	X	X	-	-	-	-	-
G 0.39 Malware	-	X	X	X	X	X	X
G 0.40 Denial of Service	-	-	-	-	X	X	X
G 0.41 Sabotage	-	X	X	-	-	X	X
G 0.42 Social Engineering	X	X	-	X	-	-	-
G 0.43 Attack with Specially Crafted Messages	-	-	X	-	X	X	-
G 0.44 Unauthorized Entry to Premises	X	X	-	X	-	X	-
G 0.45 Data Loss	-	-	-	-	-	-	X
G 0.46 Loss of Integrity of Sensitive Information	X	X	X	-	X	X	X
G 0.47 Harmful Side Effects of IT-Supported Attacks	-	-	X	-	-	X	X

Appendix 2 Table- 18 Threat-FR Mapping

9 Detailed Risk Assessment

In this step, the Detailed Risk Assessment (DRA) is performed in collaboration with the Authority's cybersecurity, safety, and operational staff according to the Authority's risk matrix.

The DRA takes the zones and conduit design, essential and nonessential functions, and operational requirements of the SuC into consideration.

9.1 Security Level Target (SL-T)

In the first phase of the DRA, the SL-T vector is determined for each zone.
by using the following,

- The threat catalog,
- Assessment of relevance and impact, and
- Considering the reducing factor (if applicable)

This results in the following vectors:

Z_01_ HVAC_HMI:

IAC	2
UC	2
SI	3
DC	2
RDF	2
TRE	3
RA	3
Vector - 6c	{2,2,3,2,2,3,3}
SL-T	**3**

Z_02_Climatic_Zone_1:

IAC	3
UC	3
SI	3
DC	3
RDF	3
TRE	3
RA	3
Vector - 6c	{3,3,3,3,3,3,3}
SL-T	**3**

Z_03_Climatic_Zone_2:

IAC	3
UC	3
SI	3
DC	3
RDF	3
TRE	3
RA	3
Vector - 6c	{3,3,3,3,3,3,3}
SL-T	**3**

Z_04_Radio:

IAC	3
UC	3
SI	3
DC	3
RDF	3
TRE	3
RA	3
Vector - 6c	{3,3,3,3,3,3,3}
SL-T	**3**

Z_05_Maintance_Zone:

IAC	3
UC	3
SI	3
DC	3
RDF	3
TRE	3
RA	3
Vector - 6c	{3,3,3,3,3,3,3}
SL-T	**3**

Z_06_HVAC_OC:

IAC	3
UC	3
SI	3
DC	3
RDF	3
TRE	3
RA	3
Vector - 6c	{3,3,3,3,3,3,3}
SL-T	**3**

Appendix 2 Table- 19 Component SL-T Ratings

9.2 Risk Assessment and Mitigation

The actual risk is calculated by determining the likelihood (exposure and vulnerability) for each relevant threat from the threat catalog:

Threat Catalog	FR	Relevance	Exposure - 7b	Vulnerability - 7b	Likelihood - 7b	Impact - 7b	Actual Risk - 7b
G 0.8 Failure or Disruption of the Power Supply	TRE; RA	Yes	2	2	3	C	Medium

Appendix 2 Table- 20 Actual Risk

The next step mitigates the existing risk and reduces the risk by applying system requirements from IEC 62443-3-3:

Measure (SR) from 62443-3-3	Exposure - 7d	Vulnerability - 7d	Likelihood - 7d	Impact - 7d	Actual Risk 2 - 7d
SR 6.1; SR 6.1 RE 1; SR 6.2; SR 7.3; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4; SR 7.5; SR 7.6 RE 1	2	1	2	C	Low

Appendix 2 Table- 21 SR application

After all applicable system requirements from IEC 62443-3-3 are chosen, a reassessment of the exposure and vulnerability must be performed.

If the risk is acceptable the risk assessment process ends, if not, an additional possibility to reduce the risk is to apply countermeasures (e.g.: measures from IEC 62443-2-1):

Measures from 62443-2-1	Exposure - 7f	Vulnerability - 7f	Likelihood - 7f	Impact - 7f	Residual Risk - 7f
ORG 2.2 ORG 2.3	1	1	1	C	Low

Appendix 2 Table- 22 Additional countermeasures

The whole process is described below in *Table 23 DRA Results from Z01_HVAC_HMI*

9.3 DRA RESULTS FROM Z01_HVAC_HMI

Please read the Security Guideline which explains the usage of this tool. The guideline is available at https://ertms.be/activities/ertms-security-core-group

Target Risk:	Low																										
Threats			Risk Assessment - unmitigated Risk Assessment (without implemented measures) - 7b						Risk Delta	System Requirements - 7c	Risk Assessment - 7d						Risk Delta	Compensation Measures - 7e	Final Risk Assessment - 7f							
Threat Catalogue	FR	Relevance	Exposure - 7b	Vulnerability - 7b	Likelihood - 7b	Impact - 7b	Actual Risk - 7b	Risk Delta - 7b	Measure (SR) from 62443-3-3	Exposure - 7d	Vulnerability - 7d	Likelihood - 7d	Impact - 7d	Actual Risk - 7d	Risk Delta - 7d	Measures from 62443-2-1	Exposure - 7f	Vulnerability - 7f	Likelihood - 7f	Impact - 7f	Residual Risk - 7f	Final Risk Delta
G 0.8 Failure or Disruption of the Power Supply	TRE; RA	Yes	2	2	3	C	Medium	1	SR 6.1; SR 6.1 RE 1; SR 6.2; SR 7.3; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4; SR 7.5; SR 7.6 RE 1	2	1	2	C	Low	0		1	1	1	C	Low	0
G 0.9 Failure or Disruption of Communication Networks	TRE; RA	Yes	2	2	3	C	Medium	1	SR 2.8; SR 2.11; SR 3.7; SR 6.2; SR 7.6 RE 1	2	1	2	C	Low	0		1	1	1	C	Low	0
G 0.14 Interception of Information / Espionage	IAC; UC; DC; RDF;	Yes	2	2	3	D	Low	0		2	1	2	D	Low	0		1	1	1	D	Low	0
G 0.15 Eavesdropping	IAC; UC; DC; RDF;	Yes	2	2	3	D	Low	0		1	1	1	D	Low	0		1	1	1	D	Low	0
G 0.16 Theft of Devices, Storage Media and Documents	DC; TRE; RA	Yes	2	2	3	C	Medium	1	SR 1.1; SR 1.1 RE 1; SR 1.3; SR 1.7; SR 4.1; SR 4.1 RE 1; SR 4.3; SR 6.2	2	1	2	C	Low	0		1	1	1	C	Low	0
G 0.17 Loss of Devices, Storage Media and Documents	DC; TRE; RA	Yes	2	2	3	C	Medium	1	SR 1.1; SR 1.1 RE 1; SR 1.3; SR 1.7; SR 4.1; SR 4.1 RE 1; SR 6.2	2	1	2	C	Low	0		1	1	1	C	Low	0
G 0.18 Poor Planning or Lack of Adaptation	SI; DC; TRE; RA	Yes	2	2	3	C	Medium	1	SR 1.1; SR 1.1 RE 1; SR 2.1 RE 2; SR 5.1; SR 5.1 RE 1; SR 5.2; SR 5.2 RE 1; SR 6.1 RE 1; SR 6.2	2	1	2	C	Low	0		1	1	1	C	Low	0
G 0.19 Disclosure of Sensitive Information	IAC; UC; DC; RDF;	Yes	2	2	3	D	Low	0		2	1	2	D	Low	0		1	1	1	D	Low	0
G 0.20 Information or Products from an Unreliable Source	SI;	Yes	2	2	3	B	Significant	2	SR 3.1; SR 3.1 RE 1 ; SR 3.2; SR 3.2 RE 1; SR 3.2 RE 2; SR 6.2	2	1	2	B	Medium	1	ORG 1.6; ORG 2.3	1	1	1	B	Low	0
G 0.21 Manipulation of Hardware or Software	IAC; UC; SI; DC; RDF; TRE; RA	Yes	2	2	3	B	Significant	2	SR 1.1; SR 1.1 RE 1; SR 1.2,; SR 1.3; SR 1.4; SR 1.5; SR 1.7; SR 1.10; SR 1.11; SR 1.12; SR 2.1; SR 2.1 RE 1; SR 2.3; SR 2.4; SR 2.5; SR 2.8; SR 2.9; SR 2.11; SR 3.2; SR 3.2 RE 1; SR 3.2 RE 2; SR 3.3; SR 3.3 RE 1; SR 3.4; SR 3.4 RE 1; SR 3.5; SR 3.6; SR 3.7; SR 3.9; SR 5.1; SR 5.1 RE 1; SR 5.2; SR 5.2 RE 1; SR 6.2; SR 7.3; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4	1	1	1	B	Low	0					B		0
G 0.22 Manipulation of Information	IAC; UC; SI; RDF; TRE; RA	Yes	2	2	3	B	Significant	2	SR 1.1; SR 1.1 RE 1; SR 3.1; SR 3.1 RE 1 ; SR 3.2; SR 3.2 RE 1; SR 3.2 RE 2; SR 3.9; SR 5.1; SR 5.1 RE 1; SR 7.3; SR 7.3 RE 1; SR 7.3 RE 2; SR 7.4	1	1	1	B	Low	0					B		0
G 0.23 Unauthorised Access to IT Systems	IAC; UC; SI; DC; RDF; TRE; RA	Yes	2	2	3	C	Medium	1	SR 1.1; SR 1.1 RE 1; SR 1.2,; SR 1.3; SR 1.4; SR 1.5; SR 1.7; SR 1.10; SR 1.11; SR 1.12; SR 1.13; SR 1.13 RE 1; SR 2.1; SR 2.1 RE 1; SR 2.1 RE 2; SR 2.3; SR 2.5; SR 2.6; SR 2.8; SR 2.11; SR 3.9	2	1	2	C	Low	0					C		0

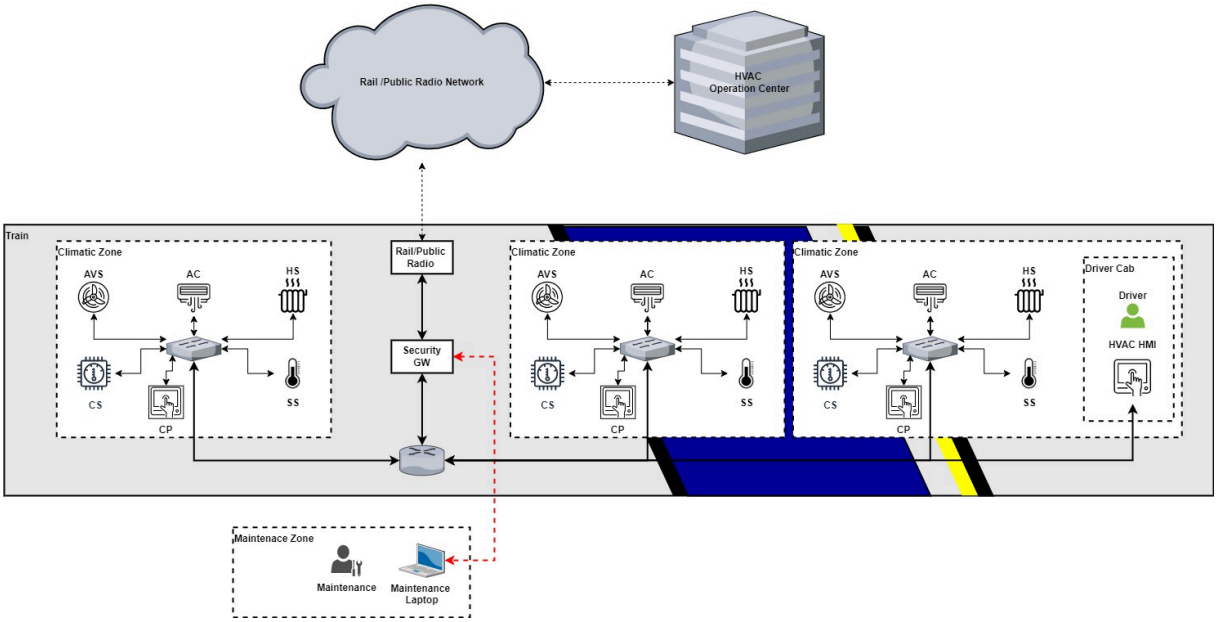
Appendix 2 Table- 23 DRA Results from Z01_HVAC_HMI

10 CONCLUSION OF THE DRA PROCESS

An availability target for the SuC (especially for the HVAC OC) is set by the Authority. At the request of the Authority, the vendor will be required to establish a secondary (geo-redundant) operations center to reach the requested availability target.

According to the results from the detailed risk assessment and based on the SL-T from all assessed zones, certain security services (PKI, Time, NTP, IAM, Backup) must be implemented in the system to realize necessary cybersecurity requirements (SR from IEC 62443-3-3). A decentralized solution is recommended (shared security services).

Furthermore, a component (Security Gateway) that handles these security services within the SuC (provides these functionalities to all zones/components/subsystems) and realizes other obvious necessary cybersecurity requirements e.g.: boundary protection, IAM, etc., must be implemented. *Figure 6 Zoning Concept with Security Gateway* .



Appendix 2 Figure- 5 Zoning Concept with Security Gateway

11 VULNERABILITY DISCOVERY, REPORTING, AND ASSESSMENT OVERVIEW

This section describes Vendor's SuC vulnerability management program. It includes details on the detection, remediation, and reporting of vulnerabilities to ensure system security for the SuC's individual components over the entirety of their useful lifecycle. Vendor tailors the vulnerability management program to integrate into the Authority's existing security and safety technology infrastructure. If such integration is not feasible, Vendor works with the Authority to provide an independent solution that is compatible with the Authority's existing security program. Vendor tracks all assets including hardware serial numbers and software/firmware versions and utilizes automated asset tracking and configuration management software to maintain detailed records on the SuC. Vendor's inventory records enable risk quantification and the prioritization of vulnerability mitigation efforts. In this example, the vendor leverages the Authority's existing asset management, configuration management database (CMDB), and change management system. Vendor also relies on the Authority's Train Maintenance System (TMS)

11.1 Public Vulnerability Sources

The SuC is delivered with updated firmware and software versions already installed and configured. All known existing vulnerabilities are either patched or remediated through appropriate security controls upon delivery. Vendor regularly consults publicly available vulnerability databases such as those listed in Table 24 Public Vulnerability Databases and maintains agreements with third-party suppliers to disclose vulnerabilities before they are released publicly.

Vulnerability Sources		
Organization	**Source**	**Link**
Cybersecurity & Infrastructure Agency (CISA)	Cyber Alerts & Advisories	https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A93&page=1
National Institute of Science and Technology (NIST)	National Vulnerability Database	https://nvd.nist.gov/
Thermostat Vendor	Thermostat Vendor Database	https://ven1.org/vulndb
HVAC HMI Vendor	HVAC HMI Vendor Database	https://ven2.org/vulndb
AVS Vendor	AVS Vendor Database	https://ven3.org/vulndb

Appendix 2 Table- 24 Public Vulnerability Databases

Furthermore, Vendor creates a comprehensive list of all known SuC vulnerabilities broken out by component. These are tracked in the Authority's existing vulnerability management system. For the purpose of this example, *Table 25 Vulnerability Database* is a sample of the data contained in the vulnerability management database. The vulnerability management database supports monitoring and scanning tools to ensure previously mitigated vulnerabilities do not recur.

Vulnerability Management Database									
Vuln	**Date Disc.**	**Comp.**	**Description**	**Source**	**CVSS**	**SuC Impact**	**Operational Impact**	**Status**	**Control**
CVE-2123-5391	3/2015	Thermostat	Physical access required, Authentication bypassed when utilizing USB service port	CISA	5	Denial of Service/ Single unit	Single SuC fails to cool/heat	Hot Fix TE0123 Deployed	HotFix TE0123 & locked enclosure
CVE-2123-5432	1/2016	Thermostat	Authentication bypased through exploiting buffer overflow vulnerability Permits privilage escalation and remote code execution	Third party Vendor	8.7	Potential widespread loss of temp monitoring, uncontrolled heateing/cooling operation	Safety hazard extreme temps	SYSTEMP Patch ST1234 tested, ready for deployment	Patch & Disable Feature

Appendix 2 Table- 25 Vulnerability Database

Vendor mitigates vulnerability risk through patching and other security mitigating controls. For a fictious example, CVE-2123-5432 details a vulnerability in the web UI for the onboard thermostat which permits arbitrary code execution and privilege escalation by an attacker with remote access. There is a patch available. Also, the web UI is not a necessary feature in the proposed SuC design and therefore it is both patched and disabled through configuration controls. The thermostat's physical access port is secured through a lockable enclosure providing additional assurance that the web UI vulnerability cannot be exploited.

In conjunction with its public research, Vendor routinely conducts risk assessments as described in section 9. Through its risk assessment process, Vendor previously identified the SuC operation center software and radio components as high-risk components due to their larger threat exposure. As such, Vendor targeted these systems for in-depth, independent analysis by an industry-leading Operational Technology red team. The red team was not able to compromise either system without utilizing social engineering techniques but was able to overwhelm both the radio and the operation center through Denial-of-Service (DoS) attacks. Vendor employs a defense-in-depth approach to mitigate the insider

threat. For example, the SuC is configured according to the concept of “least privilege” with strict user role management. Additionally, access control and privileged account use are monitored by the Security Information and Event Management (SIEM) system. Anomalies are detected and reported for further investigation in real-time. While it is difficult to counter a DoS attack in nearly any environment, the SuC has an advantage in that it can operate independently without requiring continuous system-wide communication between wagon components and the operation center. Wagon components can operate indefinitely with the most recent instructions and schedules received from the operation center and therefore a DoS attack on either the operation center or radio has a very limited impact on the immediate function of the SuC. Additionally, the train operator can adjust the temperature in each car manually via the HMI or thermostat located in a locked cabinet in each wagon.

11.2 Vulnerability Reporting

Combined with section 5.5, the process is the same for new “zero-day” and existing vulnerabilities.

11.3 Safety Considerations

The SuC has passenger and crew safety implications since it is responsible for maintaining safe temperatures in occupied wagons. Comfort is not the only consideration given that without effective climate control, wagons can quickly reach temperatures that promote heat stress or drop to temperatures that increase hypothermia risk. Additionally, the air circulation and filtration components are essential to limiting the spread of airborne pathogens and ensuring the respiratory health and safety of crew and passengers. The air conditioning unit, the heating unit, and the air circulation unit have very little direct cyber risk exposure in terms of remote threat. These units are mostly mechanical with on-board microcontrollers that cannot be reprogrammed or even accessed without specialized tools and knowledge. Aside from physical damage, these units are highly reliable and resilient. However, an attacker with access to the operations center or the driver’s HMI could manipulate these components or disable them altogether. The attacker would require valid credentials and have authenticated access to the Authority’s OT network.

The air circulation and filtration unit is expected to cycle on and off frequently and does not report status changes to the HMI but it does report error conditions. If the unit is turned off through an authenticated command, it will not report this status to the HMI. However, if a major component was to be maliciously disabled, the SuC would not be able to maintain a stable temperature. In this case, a corresponding visual and audible alert is generated on the driver’s HMI along with standard problem reporting and visual alerting on the operation center. Additionally, the passengers will report uncomfortable temperatures to the train staff.

Given the SuC’s safety considerations, software patches are thoroughly tested prior to deployment to ensure the overall functioning of the SuC is not impacted. Considering the thorough testing and ability of both the operation center and HMI to monitor system functions, the Authority’s OT safety case is not materially impacted by the SuC’s vulnerability management program.

11.4 Methods for Bypassing System Authentication

The driver’s HMI is a component of the SuC. It monitors and controls local conditions through its execution of the heating/cooling schedule received from either the operation center or entered manually by the driver. Given competing instructions, the driver’s HMI commands take precedence. In addition to the operations center, the HMI is responsible for the overall health monitoring of the SuC as well as processing and reporting error messages from each major component. The HMI’s firmware and software are installed, configured, and thoroughly tested by Vendor. Aside from occasional patching and software updates, the HMI does not require configuration adjustment or any other routine maintenance. In the unlikely event that the HMI’s configuration becomes corrupted or is unable to authenticate to the operation center, a Local Root Account (LRA) exists to enable local software installation and reconstitution of the HMI’s configuration manually. The LRA account name is

HMIAdmin across all deployed systems. Vendor creates a unique password for each SuC installation and provides those passwords to the Authority separately. Each system password can be changed manually, but it is important to ensure they are retained and not used except in the circumstance that the HMIAdmin account is the only option. Additionally, the thermostat incorporates a default admin account. This account is intended for use via the web UI that has been disabled. Log monitoring rules for the use of the HMIAdmin, and the thermostat's default admin account are provided for integration into the Authority's existing or Vendor recommended log aggregation and monitoring tools.

11.5 Newly Discovered Vulnerabilities

Vendor reports the existence of any newly discovered vulnerability to the Authority as soon as a vulnerability report with a risk analysis has been completed or within a maximum timeframe of 14 days. The vulnerability report includes technical details along with an impact analysis as demonstrated in section 11.5.1. The report additionally describes any residual risk remaining once all mitigations have been completed and all security controls have been established.
Vendor prioritizes the development of patching or other mitigating controls according to the vulnerabilities risk score and the timelines listed in *Table 26 Countermeasure Deployment Requirements*. All recommended patches and other mitigations come with instructions to assist the Authority with automated deployment and monitoring.

11.5.1 Vulnerability Report

A vulnerability report is the primary communication vehicle and formal record of Vendor's compliance with the Authority's vulnerability reporting requirements. It includes the following sections.

11.5.1.1 Executive Summary

High-level description of the vulnerability and its current, or potential impact on the operation of the SuC. It details a potential exploit's resulting impact on the operational environment. In plain terms, this summary provides executive leadership with all the facts necessary to inform risk decisions.

11.5.1.2 Overview

General context describing the vulnerability, the steps required to exploit it, and the general sophistication required of the likely threat. Includes background information helpful to understanding the real-world impact of the successfully exploited vulnerability.

11.5.1.3 Risk Analysis

Describes the applicable threat exposure (likelihood), and impact of a successful threat event. The risk analysis is guided by the CVSS model.

11.5.1.4 Technical Analysis

Detailed and low-level description of the vulnerability and threat. The technical analysis includes evidence-driven root cause analysis. It details the attack path an attacker must traverse to successfully exploit the vulnerability.

11.5.1.5 Technical Mitigation and Security Controls

Describes all relevant patching and security controls designed to reduce the risk to a tolerable level. Additionally, if the vulnerability did not originate in software (configuration, credential, etc...) this section describes methods to correct the error across the operational network as well as monitoring techniques to decrease the likelihood of a vulnerability reoccurrence going unnoticed.

a. Mitigation testing results: Sub-section to include all testing procedures performed to validate the effectiveness of the mitigation/security control and document its own implementation risk.

b. Remediation Steps: A step-by-step guide to direct Vendor and/or the Authority in the implantation of the countermeasure whether in the form of security controls or software patch installation

11.5.1.6 Procedures, Processes, Policies, and Training

Changes designed to harden the deployed SuC. For many vulnerabilities, technical security controls are either not appropriate, or not the only corrective action. This is especially true for security mishaps in which legitimate credentialed maintainers or system users simply make errors in their normal day-to-day duty performance. Vendor will recommend policies and procedures to limit the reoccurrence of these types of threat events as well as methods to monitor for any deviations and report them to the SIEM for logging and alerting. Finally, lessons learned are compiled and reflected in SuC training manuals and made available to the Authority electronically.

11.5.1.7 Key Success/Failure Indicators

This brief section answers the question "How do we know if the security control or patch worked?" This section includes monitoring signatures, log analysis filters, and vulnerability scanner rules to continuously monitor effectiveness.

11.5.1.8 References

List of outside resources used in the analysis of the risk.

11.6 Vulnerabilities Impacting Safety

Safety and security are closely coupled concepts and all security concerns with potential safety implications are considered critical priorities. Safety-critical priorities are declared by authoritative third parties, government agencies such as ICS CERT, the Authority, or the Vendor's vulnerability testing team. Vendor reports safety-impacting vulnerabilities to the Authority within one day of becoming aware of them. While Vendor practices responsible disclosure of vulnerabilities, no public disclosure occurs until after the Authority is provided the opportunity to patch all systems or otherwise mitigate the security concern. To organize communication, and reporting, and to assist with coordination between Vendor and Authority-appointed stakeholders, Vendor created an email distribution group specific to safety vulnerabilities. Vendor assists the Authority with technical expertise and experience controlling the response lifecycle from start to finish guided by the NIST SP 800-40r4 standard.

Vendor provides an initial discovery report no later than five days following the safety vulnerability detection. The discovery report is an abridged version of the vulnerability final report described in section 11.5.1. containing information needed in the near term to categorize the vulnerability's risk and impact.

Following the initial report or within 14 days at a maximum, Vendor delivers a full report as described in section 11.5.1. The report recommends immediate mitigation actions to reduce or eliminate the Authority's safety risk exposure. If necessary, Vendor further develops stronger, more permanent mitigations and security controls following the urgent deployment of the initial controls. For example, an initial urgent control could be to disable the HMI's remote configuration service until a more permanent patch can be created, tested, and installed. All mitigations are tested in the Vendor's testing environment ensuring no new vulnerabilities are introduced and patches have the desired

impact of reducing risk. All relevant technical details and implementation instructions are provided as well as a monitoring plan to ensure risk is effectively reduced to acceptable levels going forward.

11.7 Vulnerabilities Impacting Safety Disclosure

Vendor releases safety-impacting vulnerability information publicly only after a patch or other mitigation is provided to the Authority. Vendor requires a Non-Disclosure Agreement (NDA) with the Authority intended to ensure Vendor maintains purview over public disclosure. Additionally, Vendor requests written acknowledgment that information on both the vulnerability and appropriate mitigations are received by the Authority once provided. Vendor's legal counsel can assist with questions concerning the NDA, while any technical questions concerning the vulnerability or corresponding mitigations can be directed to Vendor's vulnerability testing team. Once an NDA is completed, Vendor will work with the Authority on the timing of public disclosure to limit the Authority's threat exposure of operational systems.

However, if a SuC vulnerability that impacts safety is disclosed publicly by some other source outside of Vendor's control, the threat exposure of the SuC could be negatively affected depending on the impact and likelihood of the risk associated with the vulnerability. This scenario could drive an urgent, prioritized mitigation response by Vendor as described in section 11.6.

In most cases, vulnerabilities are first detected by Vendor or s SuC third-party manufacturer and Vendor has full control or influence on the timing of public disclosure. Vendor maintains agreements with all major SuC sub-component providers and therefore offers the Authority a high level of confidence that the SuC will be appropriately hardened before public disclosures of vulnerabilities with a material safety impact.

11.8 Vulnerability Enumeration

If Vendor is contracted to manage vulnerability enumeration, Vendor will collaborate with the Authority to develop a vulnerability scanning schedule. Credentialed vulnerability scanning of the operation center and at least 4% of all wagons is conducted every 14 days. This schedule ensures the completion of all wagons within one year and promotes a high degree of security and confidence in the operation center. Scanning of wagon components is completed while the train is in the depot. The date and time of each scan are coordinated with the Vehicle OT Security team and managed through the Train Management System. To limit downtime, Vendor assists the Authority in integrating SuC scanning with the Authority's existing vulnerability scanning technology, or other vulnerability scans scheduled by other vendors or the Authority. When SuC scanning cannot be combined with other OT scans, Vendor works with the Authority to develop a plan that schedules each wagon for a scan on a specific date while out of revenue service.

Vendor recommends the VulICS scanning system to perform the vulnerability scans. VulICS is an industry-leading ICS vulnerability scanner that is capable of detecting vulnerabilities of all types. VulICS will report scan results in a variety of standardized machine-readable, and human-readable formats that can be ingested into the Authority's automated monitoring and configuration management tools. Following a Vendor scan, Vendor interprets the reported results detailing all discovered vulnerabilities and submits a report to the Authority within one week of the scan's completion. Any newly identified vulnerability will be prioritized and remediated by Vendor according to the process described in section 11.5.

11.9 Authority or Appointed Third-Party Vulnerability Scan

If the Authority contracts Vendor to manage SuC security services, Vendor will support the Authority, or third parties appointed by the Authority to scan the system as desired. Credentials with the appropriate permissions are provided along with technical diagrams and other assistance as needed. Vendor requests an NDA with the Authority's appointed third party to maintain control over the public disclosure of discovered vulnerabilities impacting SuC components, including all components produced by other manufacturers. Vendor maintains all required licenses to scan and analyze sub-

components acquired from third-party manufacturers. Licenses extend to the Authority as the system owner, or the Authority's appointed security scanning delegate upon acceptance of the SuC as part of the acceptance agreement.

The Authority is provided the option to test vulnerability scanners in the Vendor's SuC testing environment before scanning the production OT network. If desired, the authority should coordinate with Vendor no closer than 30 days before the intended test date to ensure the testing lab can be made available in time.

11.10 Vulnerability Risk Assessment

This section focuses on the risk specifically associated with technical system vulnerabilities, see section 9 of this document for the detailed SuC risk assessment. Risk is evaluated and reported through a standardized process. The following report demonstrates a risk analysis completed for the fictitious vulnerability CVE-2123-5432, thermostat Web UI remote code execution.

Vulnerably Risk Analysis for CVE-2123-5432

Date: 3-Nov-2023

Prepared By: Vendor Vulnerability Testing Team, vvtt@fake_vendor.com

1. Description

SuC's with a manufacture date of October 2016 or later contain the Systemp brand thermostat that features a browser user interface (UI). Web UI versions of 4.6 or newer contain a buffer overflow vulnerability that if successfully exploited could allow an attacker to escalate privileges and execute arbitrary code remotely. The vulnerability can also be exploited locally by an attacker accessing the thermostat's USB access port. With control of a thermostat, an attacker could control wagon temperature and could prevent the HMI from accurately monitoring and overriding temperature settings. This would allow an attacker to disrupt the operation of the SuC and create an unsafe condition by raising or lowering the temperature on a single or multiple wagons.

2. Assets Impacted:

There are 77 thermostats in the Authority's enterprise that are impacted, their serial numbers are listed in Attachment A. The thermostats are installed in the wagons identified in Attachment B *(not provided in this example).*

3. Threat assessment: 5 (high)

The attack could be executed by threat actors with low skill and physical access to the thermostat's USB port. The vulnerability is publicly disclosed, and malicious code targeting the vulnerability already exists. More advanced adversaries could use social engineering or other techniques to gain access to the SuC OT network and gain remote control of all vulnerable thermostats without a privileged account.

4. Vulnerability Severity Assessment: HIGH 8.7 (Base CVSS)

   Exploit Metrics

   a. Attack Vector: (Network) Vulnerable thermostats are accessible from remote network.
   b. Attack Complexity: (Low) Thermostat's simple software has few safeguards preventing code execution on the stack and exploit code is freely available.
   c. Attack Requirements: (Present) No special condition must exist to permit exploitation.
   d. Privileges required: (Low) Attacker must be authenticated to SuC network for remote attack, None for physical attack.
   e. User Interaction: (None)
   f. Vulnerability System Confidentiality: (High)

   Vulnerability System Impact Metrics

   a. Confidentiality: (High) Attacker can escalate privileges to root on thermostat

b. Integrity: (High) Attacker can modify or delete thermostat control data
c. Availability: (High) Attacker gains full control to disable system

Vulnerability Subsequent System Impact Metrics

a. Confidentiality: (None) does not gain privileged access to other components
b. Integrity: (None) does not gain privileges to compromise data on other components
c. Availability: (High): The attacker could create a denial of service condition on HMI

5. Impact Analysis: 5 (safety)
   By controlling the temperature of individual or multiple wagons across the Authority's fleet, an attacker would be able to create unsafe conditions that promote either heat stress or hypothermia. Because of the potential to cause a widespread impact on passenger and crew safety, the impact is considered severe.

6. Likelihood Assessment: 2
   There is a low likelihood that passengers will attempt to physically bypass the thermostat's locked enclosure and connect to a thermostat's USB port to exploit the vulnerability. However, if the security enclosure is bypassed, an attacker could impact the temperature in one wagon at a time and move to other wagons in the train to conduct the same attack. There is a low likelihood that an attacker would gain remote access to the SuC network through the defense-in-depth security controls currently in place on the Authority's OT network, therefore there is a low likelihood of a widespread attack that impacts many wagons simultaneously.

7. Risk Calculation**:** 10 **(**High)
   Risk = **(**Likelihood) x (Impact). While there are security controls in place that reduce the likelihood of an attack the impact of a successful attack impacts safety and is therefore considered severe.

8. Mitigation Recommendations
   Immediate countermeasures are available to eliminate the risk associated with this vulnerability. The Web UI is not a feature required for SuC operation and should be immediately disabled on all thermostats across the Authority's fleet. This can be accomplished by adjusting the SuC's configuration through the operation center. In addition, physical enclosures should be inspected for signs of tampering. Any unlocked enclosures should be resecured to prevent access to the thermostat's USB port.

12 Security Patching and Mitigation Governance

Vendor provides SuC patch deployment and security mitigation support to the Authority to include support for all third-party manufactured subcomponents. If Authority patch deployment tooling is available for use, Vendor will provide support for its configuration and integration with the SuC. In addition, Vendor provides training and reference documentation for the operation of the provided tool with the SuC and will document any SuC configuration changes required for compatibility. If existing tooling is not available, Vendor proposes the implementation of the VulPatch system to handle automated patch deployment for all components of the SuC. Regardless of the automated patch deployment system utilized, Vendor performs the patch management program described in this section. Vendor's patch management program is a comprehensive risk-control strategy that minimizes the operational impact of patching and other mitigation efforts.

12.1 Patching Distributed HVAC Components (Requirement 6a)

SuC software patching is automated and managed remotely, but on-site monitoring is recommended for immediate response in the rare event of a critical failure. The SuC is

configured for compatibility with the Authority's preferred patch management software. Otherwise, Vendor recommends the VulPatch system described in section 12.5.
The SuC is designed with a centralized operation center and dispersed heating/cooling components across the Authority's fleet of wagons. It is a mobile, distributed network and wagon components can operate independently. However, by design wagon components and the operation center maintain continuous communication through the cellular radio. The SuC's operation center exists at layer 3 of the Purdue model while the driver HMI exists at level 2 and the radio and thermostat components operate at level 1. The operation center remotely manages wagon component configuration and monitors the operation of the HMI's underlying operating system as well as the HMI's control interface. Following patching and updating, the operation center validates the HMI's functionality. Firmware for wagon components including the HMI, radio, and thermostat is also updated remotely. In addition, the HMI has a "fail-safe" mechanism that enables network communication and file transfer capability intended to restart a firmware update after a failure. However, if network connectivity is interrupted and cannot be re-established for whatever reason, HMI patching is restarted locally with physical boot media.
For remote patching of wagon components, software updates are delivered across the existing secure connectivity. Therefore, remote patching of the wagons has no additional impact on the SuC's existing zone and conduit segmentation. Remote patching will only be performed while the train is in the depot. The patching is coordinated by the OT security team and planned through the TMS.

Vendor recommends the automated patch management system operate at level 3 of the Purdue model as does the SuC operation center. While the operation center is hosted on a standard Windows system, patching it from a higher level, or the Authority's enterprise IT network could significantly increase the SuC's threat exposure. Authentication and authorization are handled by the Authority's existing OT IAM system which should also reside at level 3. The SuC is compatible with LDAP-based directory services including Windows Active Directory for the detailed management of all roles and privileges associated with the operation center and system patching/updating. For increased security, Vendor recommends the SuC occupy its own security zone in the Authority's OT environment.

While the Authority could establish independent patch management systems within each security zone or Purdue model level of its OT network, it is likely more manageable to establish a centralized system that controls all patching and updating for several systems across many zones at level 3 and below. Vendor assists the Authority by providing firewall rules and a network segmentation design to isolate the SuC's security zones while still permitting automated remote patch management and proper authentication and authorization from centralized systems. With this design, SuC scanning, and patch management can securely participate in Authority's broader patch management program. Vendor recommends that the SuC security zones occupy a VLAN with a unique IP space and that the SuC's network be physically segregated as much as possible. Through logical and physical segmentation and close firewall management, remote patching is secure and does not introduce unacceptable security weaknesses into existing zone and conduit segmentation.

12.2 Patch Deployment Plans (Requirement 6b)

To ensure the safety of crew and passengers, Vendor does not recommend patching wagon components while in operation. Despite extensive testing as described in section 12.3, some

risk remains due to the impossibility of modeling every dynamic real-world complexity within the lab environment. Wagon components can be patched through either a local manual process or automatically through the patch deployment system described in section 12.4. If widespread urgent patching is required, the automated system can push the patch to predefined control groups at regular intervals. For example, the initial push could include a test group consisting of 1% of all operational systems. After a live test period, the patch can then be pushed to a larger observation group, then a validation group, and finally scheduled for a controlled release across the entire fleet. An observation period between each patching group will provide the opportunity to detect and remediate any problems earlier in the patch deployment cycle. Under normal conditions, with the use of an automated patch management system, the general process is as follows,

1. Load approved patches into patch management software.
2. Establish rules for patch deployment, rules are simple per system or per group schedules, or logical conditions such as the train is out of revenue service or in a maintenance depot.
3. Deploy patches, and automatically rollback if necessary.
4. Automated success/failure reporting
5. Automated configuration management update
6. Manual driver confirmation
7. Security team testing and verification through vulnerability scanning and other techniques.

After patching a wagon component, the associated HMI will indicate any errors, once completed the HMI will prompt the driver to perform a series of simple confirmation checks which takes approximately two minutes to complete before putting the system into service.

The operation center is installed in a high-availability cluster with automated fault failover. This design prevents loss of service if an updated operations center malfunctions for any reason and allows the system to be recovered immediately if a patch fails. Both the operations center software and the underlying host Windows operating system are patched by the same patch deployment system. Once patching is complete, the system will visually cue technicians to review the patch report and ops check the operations center.

12.3 Patch Testing (Requirement 6c)

Vendor thoroughly tests all patches and updates in a SuC testing environment before recommending installation on operational systems. The testing environment consists of a software-focused virtual test environment and a physical SuC “simulator”. The simulator is comprised of physical SuC components including the operation center, radio/cellular wireless network, driver HMI, and wagon components in common configurations. The simulator is adjusted to test unique configurations existing in the Authority’s operational environment.

All patches are developed in accordance with the secure coding process as guided by IEC 62443. Finished patches are subjected to a manual code security review and an automated static code security scan by industry-leading static code analysis tools. Once installed in the virtual environment and simulator, the patched software is actively probed through dynamic analysis for vulnerabilities and other unintended secondary effects. Any problems detected during testing are corrected before the patch is again processed through the same test procedure.

Vendor’s testing process is designed to detect and ultimately reduce or eliminate the risk of patches introducing new vulnerabilities or causing malfunctions with the operation of the SuC. The final phase of testing is designed to exercise the patch uninstall capability. In most cases, automated patch

management software successfully performs patch rollback procedures without unintended consequences. However, Vendor documents required steps to complete rollbacks manually if required due to a system malfunction, or other complication. Upon completion of formal testing, a test report documenting all tests completed with corresponding results is drafted. The test report includes a risk analysis developed in accordance with IEC 62443 and is submitted to the Authority's Change Management Board for consideration with its patch approval decision.

12.4 Authority Orchestrated Patching (Requirement 6d)

Vendor supports the Authority's planning and execution of patching with relevant technical details and tooling as required. The SuC is designed and configured for compatibility with automated remote patching as described in section 12.5. However, in some cases a manual process may be required, this scenario is typically the result of a failed automated patch attempt on a particular SuC component. Vendor provides detailed instructions and checklists to guide manual installation. For automated patching, Vendor provides all necessary technical configuration guidance and best practice suggestions to enable efficient and comprehensive patching.

In addition, Vendor supports the development of Standard Operating Procedures (SOP) to assist the Authority with the patch deployment process specific to its chosen patch deployment system. Vendor provides additional technical support to the Authority to cover edge cases as well as immediate response support if security complications arise during or immediately following patch deployment. As described in section 12.6, Vendor created extensive SuC design documentation with details on software and firmware versions for all components including third-party components. These configuration details are documented and maintained in the CMDB as part of the configuration management program. Some nuances exist concerning compatibility between the various software component versions within the SuC and these version control requirements are factored into the patch-testing process described in the previous section. The CMDB serves as the official document repository for all version control-related instructions providing an authoritative reference to the Authority in informing the patch planning process.

12.5 Patch Automation (Requirement 6e)

If the Authority does not have, or cannot authorize the use of an existing patch management tool, Vendor recommends the implementation of the VulPatch patch management system. VulPatch is specifically designed to work efficiently in a geographically dispersed and mobile transportation OT environment. It is highly resilient to the increased network latency and restricted bandwidth that is common to transportation OT networks. VulPatch is compatible with major automated configuration management and security monitoring tools to enable a comprehensive "hands-off" automated patching program. Additionally, it works seamlessly with the SuC's patch rollback capability.

Regardless of which system is chosen by the Authority, the SuC is configured for compatible integration with it provided the system conforms to common protocols and standards. Once operational, the patching system enables automated patching that is accurately logged and highly resilient to many of the common errors encountered with a more inconsistent and labor-intensive manual process. Automated patch deployment is tested as part of the patch-testing process and Vendor provides relevant technical details concerning any recommended configuration changes required to ensure smooth patch deployments.

12.6 SuC Documentation (Requirement 6f)

The SuC is a multi-faceted system assembled of a diverse composite of hardware and software products. Vendor directly manufactures many of the SuC's components but others are acquired from third-party manufacturers and then configured and assembled into the final design. Vendor maintains highly detailed, precise, and accurate records of each component incorporated into the SuC including serial numbers, firmware versions, and software versions if applicable. Not only is this information provided to the Authority as part of the initial purchase documentation, it is maintained electronically

in the CMDB. The CMDB is the authoritative reference for patch and maintenance planning of the SuC.

Several individual third-party components require modification or non-standard configurations to integrate successfully with the SuC's design. All required integration modifications are tested and accurately documented in the CMDB. Additionally, these modifications are officially licensed and supported by each component's respective manufacturer to ensure the future availability of compatible patches and a valid warranty. The initial inventory records for each SuC are provided to the Authority after acceptance testing is completed and the SuC's ownership formally transfers.

12.7 Component End-of-Life (Requirement 6g)

Upon delivery of the SuC, all software components are fully updated and supported by their respective vendors. As third-party components reach end-of-life, they are removed from the SuC's design, and updates are issued for existing systems where feasible. As described in section 12.8, Vendor maintains detailed records and closely manages configuration and version dependencies. This allows Vendor to forecast obsolesces and prepare for it through system engineering and testing of updated software versions, software replacements, or other workarounds. For example, the operation center relies on the Microsoft .Net framework currently at version 7.0. Microsoft will stop supporting version 7.0 in May of 2024 and Vendor is actively testing version 8.0 for compatibility. Any inconsistencies between versions that create complications in the operation of the SuC will be remediated before an update is issued. Once testing is complete, the .Net update, as well as any requisite supporting update will be submitted for Authority approval to cover existing systems.

Vendor creates a Plan of Action and Milestones (POAM) for the Authority's review if a software component becomes unsupported by its manufacturer and cannot be updated in the SuC in a timely manner. The POAM describes compensating controls to manage vulnerabilities as they arise from the unsupported software as well as a timeline for removing it from the system. POAMs have an expiration date upon which Vendor must either have removed the vulnerable software or must submit another POAM for the Authority's review. All submitted POAMs will be standardized to include the following sections.

1. Control Number: Uniquely identifies a POAM for tracking and record keeping in the format SUCYYYYMMDD-#
2. Description of unsupported system and any resulting vulnerability or security weakness: Technical overview of the issue, including applicable context
3. Detection Date: Date Vendor became aware of the vulnerability.
4. Reason for Deviation: Why the unsupported and vulnerable system cannot be removed or mitigated in a timely manner.
5. Asset Identifier: Identifies component and version numbers impacted by vulnerability or security weakness.
6. Risk Rating(s): The CVSS score, computed for any active vulnerability according to the process detailed in section 5.10.
7. Corrective Action Plan (CAP)
    a. Countermeasure Description: Details how additional security controls will limit the risk presented by the vulnerable component in lieu of updating or removing it.
    b. Timeline for remediation including milestones.
    c. Action items – steps required to remediate the vulnerability.
    d. Completion Metrics: measures the progress and eventual completion of the CAP's implementation.
    e. Dependencies – list of outside requirements needed to ensure CAP success.

8. Roles and responsibilities: All stakeholders in the approval and implementation of the CAP
9. Expiration Date: Date when either the vulnerability must be mitigated or removed, or when a new POAM must be submitted.

12.8 Third-Party Cooperation (Requirement 6h)

Upon receiving a request from the Authority, Vendor will provide third parties with patches and mitigation methodologies for the SuC. Vendor closely manages the public release of patches to ensure Authority and other SuC owners have an opportunity to update all systems before vulnerabilities become widely known. Third parties that do not have a direct contractual agreement with Vendor restricting the release of patch and vulnerability information will be asked to sign a NDA Additionally, Vendor is restricted by similar agreements with some SuC component manufacturers and Vendor will seek approval from these manufacturers to release their patches to the Authority's requested third party. Sub-component manufacturers may also require an NDA or other agreement directly with the Authority's appointed third party.

12.9 SuC Documentation (Requirement 6i)

Most SuC software patches are designed for simple and safe removal after installation if required. Patch rollback capability is developed and tested as described in section 12.3 and is engineered for compatibility with automated patch deployment systems. Patch rollback is initiated automatically in response to critical error conditions. The firmware patching process in wagon components works by overwriting existing firmware and therefore a previous firmware version is simply reinstalled over the active version when rollback is required. Vendor maintains a library of all firmware and software versions previously deployed into the production environment.

In some cases, patch rollback is prohibitively impractical or too technically complex to complete without unacceptable risk. This can occur when multiple core components are updated together to maintain intra-component compatibility. Additionally, this can occur when subsequent patches and updates have dependencies on prior patches and updates. In this scenario, the patch rollback process must be conducted in a specific sequence. As a result, complex patching with many dependencies that cannot be easily reversed should be deployed into production in small increments with significant observation and testing periods in between. This strategy will help ensure all complications are detected at the earliest possibility. Vendor assists the Authority with developing and configuring complex patch removal scripts utilizing the automated patch management system when necessary. In some cases, the straightforward process of reimagining the operations center and/or HMI component may offer less risk of complication.

12.10 Patch Management Guidance (Requirement 6j)

Vendor supports and maintains the SUC through its entire lifecycle. Vendor's SuC maintenance program includes updating and patching software to offer new features or remediate vulnerabilities. Vendor closely tracks the development of third-party components and updates the SuC's configuration and design to maintain backward compatibility. If a software or firmware update cannot be obtained from the original third-party provider, Vendor develops other mitigations to reduce the SuC's risk exposure. These mitigations include steps that range from adding additional security controls, up to a design change that removes a vulnerable or obsolete component altogether.

1. As described in section 11.10, a vulnerability risk assessment is completed to establish the countermeasure development urgency. Risk level is formulated from threat, impact, and likelihood measures and defines the countermeasure development timeframe as listed in *Table 26 Countermeasure Deployment Requirements*. Vendor develops mitigations within the timeframe required. This may require Vendor to develop an immediate stop-gap mitigation to meet the timeline requirement while a more permanent mitigation is developed and tested.

2. The SuC contains third-party hardware, software, and firmware. Vendor relies on third-party manufacturers to provide patches and updates specific to their products. Once received, an update is tested for compatibility with the SuC. In the event Vendor does not receive a third-party patch within the timeframes required, Vendor will develop alternate countermeasures to control risk. For example, a hypothetical critical vulnerability in Windows' Remote Desktop Protocol (RDP) allows attackers to hijack previously closed RDP sessions and masquerade as a real user able to authenticate to the operations center. If a Microsoft patch cannot be acquired and tested within 30 days, Vendor could release a temporary software update that forces users to re-authenticate on each operation center login attempt thereby preventing the use of the hijacked session credentials.
3. Methods to monitor the effectiveness of patching is developed and implemented during Vendor's testing process. Specific log analysis rules and vulnerability scanning tests are created to validate the effectiveness of patching and other mitigations. The monitoring and scanning rules/tests are provided to the Authority for incorporation into production monitoring and scanning systems. They enable confirmation that implemented patches and security mitigations effectively meet risk-level goals.
4. Beyond validation of the efficacy of the patch or mitigating control to address the original cybersecurity control, vendors also tests that the patch does not impact Reliability, Availability, Maintainability and Safety (RAMS). The testing report provided with each security change request characterizes test coverage and identifies any potential impact on the safety case and/or RAMS. In the event some impact is expected, Vendor either provides an additional patch or mitigating control.
5. Patch development is guided by *ANSI/ISA-62443-4-1-2018*, Security for industrial automation and control systems, Part 4-1. Additionally, as described in section 12.3, patches undergo a formal testing process to ensure no new vulnerabilities or security weaknesses are introduced. The testing process includes static code analysis and active red team testing. As a result, Vendor has high confidence in the security of all patches submitted to the Authority for consideration. Weaknesses are identified, corrected, and retested. Testing and reporting provide the Authority with authoritative and objective data when considering patch deployment approval.
6. After a patch is tested and authorized by Vendor for release, it is submitted to the Authority's Change Management Board for review. If Vendor is contracted to manage Authority's patch deployment process, Vendor will deploy the patch in accordance with the Authority's operational processes.
7. Risk mitigation urgency is defined by a vulnerability's risk rating. Section 11.10 describes the process for calculating risk. Once the risk rating is calculated, mitigations are made available within a timeline that does not exceed the requirements in the table below.

Risk Rating Deadline Patching Schedule	
Risk Rating	**Patching/Mitigation (Compensating Controls) Availability Deadline**
Low	180 Days
Medium	60 Days
High	45 Days
Critical	30 Days

Appendix 2 Table- 26 Countermeasure Deployment Requirements