APTA STANDARDS PROGRAM
WHITE PAPER

APTA SS-TCS-WP-001-26
First Published: May 13, 2026
Transit Cybersecurity Working Group

Cybersecurity Requirements for Operational Technology Procurement

Abstract: This white paper discusses the ways a mass transit and passenger rail operator and its vendors can collaborate to reduce cybersecurity risk when implementing new technology or augmenting existing systems. The approach was designed by the North American Transportation Cybersecurity Consortium.

Keywords: industrial control systems, NATCA, operational technology, procurement, risk management, system life cycle, system under consideration, wayside

Summary: The North American Transit Cybersecurity Consortium has designed an approach to meet the cybersecurity requirements and level the playing field for agencies by holding vendors responsible for the products and services they provide. The consortium's procurement standard, known as the North American Transit Cybersecurity Agreement (NATCA), outlines cybersecurity requirements that will define cybersecurity operational technology (OT) procurement requirements and serve as a guideline for members of the consortium.

This white paper is an overview and endorsement of the NATCA document as it attempts to support many of the previous APTA OT recommended practices and standards. The NATCA standard addresses requirements and expectations for vendors and service providers and outlines the steps agencies must take to ensure that the recommended steps to support resilience are addressed with consistent expectations across the transit sector.

The requirement for this guidance is predicated on a growing threat to transit. As mass transit and passenger railroad operators find themselves dependent on OT that are more open to cybersecurity threats, and as cybersecurity regulations are imposed by U.S. government agencies like the TSA, transportation agencies must enhance their ability to reduce cybersecurity risk and long-term security costs associated with technology integration. Currently, unsecured OT systems support the critical operations of transportation agencies, especially in railway and building management environments. Many of the legacy OT systems lack cybersecurity functionality and design consistent with meeting the current cyber threat environment. The addition of new unsecured and unmanaged technology exacerbates this issue and ensures that systems will eventually be more vulnerable to cyberattacks. This ultimately creates increased incident response costs when an agency is eventually breached.

Foreword

The American Public Transportation Association is a standards development organization in North America. The process of developing standards is managed by the APTA Standards Program's Standards Development Oversight Council (SDOC). These activities are carried out through several standards policy and planning committees that have been established to address specific transportation modes, safety and security requirements, interoperability, and other topics.

APTA used a consensus-based process to develop this document and its continued maintenance, which is detailed in the manual for the APTA Standards Program. This document was drafted in accordance with the approval criteria and editorial policy as described. Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

This document was prepared by the APTA Transit Cybersecurity Working Group as directed by the Security and Emergency Management Standards Policy and Planning Committee.

This document represents a common viewpoint of those parties concerned with its provisions, namely transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any recommended practices or guidelines contained herein is voluntary. APTA standards are mandatory to the extent incorporated by an applicable statute or regulation. In some cases, federal and/or state regulations govern portions of a transportation agency's operations. In cases where there is a conflict or contradiction between an applicable law or regulation and this document, consult with a legal adviser to determine which document takes precedence.

A shared understanding of the threat landscape among all stakeholders is vital for developing a centralized cybersecurity strategy. Such a strategy must address the detection, identification, prevention, mitigation, recovery, and management of cybersecurity threats that can jeopardize transit operations. NATCA facilitates this alignment by encouraging stakeholders to adopt a consensus-based approach, grounded in recognized and validated threat libraries and reports. This shared perspective fosters collaboration and streamlines the implementation of protective measures.

The NACTA document was developed by the North American Transportation Cybersecurity Consortium. While APTA Recommended Practices are formally reviewed and reaffirmed on a five-year cycle, this endorsement pertains specifically to the attached NACTA procurement guidance. At this time, APTA has not received confirmation that the North American Transportation Cybersecurity Consortium maintains a scheduled update process for this document.

This is a new document.

Table of Contents

Foreword ... ii
Participants ... iv
Introduction ... iv
Scope and purpose ... v

1. Overview ... 1
1.1 Who should use this paper and why? ... 2
1.2 How should the different stakeholders in procurement use this paper? ... 2

2. Why endorse NACTA ... 3
2.1 Cross-agency collaboration ... 4
2.2 Risk assessment ... 4
2.3 Physical and environmental impact ... 5
2.4 Risk assessment documentation ... 5
2.5 Zone and conduit requirements ... 6
2.6 Secure system development ... 6
2.7 Information sharing and vulnerability reporting ... 6
2.8 Vendor responsibility for patching ... 7
2.9 User awareness and training ... 7
2.10 Metrics and performance goals ... 7
2.11 Conclusion ... 8

References ... 8
Definitions ... 10
Abbreviations and acronyms ... 12
Document history ... 13

Appendix A: Text of North American Transit Cybersecurity Agreement ... 14

Appendix B: NATCA agreement Appendix 2 ... 42

Appendix C: Introduction to SBOM and resource materials ... 81

Participants

The American Public Transportation Association greatly appreciates the contributions of sub-committee chair **Michael Echols**; sub-committee members **Tariq Habib**, **Dr. Julius Smith**, **Tim Coogan, Ahmed Idrees**, **John Moore**, **Rafi Khan**, **David Moskowitz, Patrick Guest** and **Mark Johnston**.

Dr. Julius Smith, *DART,* TCSWG Chair
Tim Coogan, *RTD-Denver.* TCSWG Vice Chair
Ahmed Idrees, *Sound Transit*, CCSWG Sub-Chair
Mark Johnston, *TriMet USA*, ECSWG Sub-Chair

At the time this standard was completed, the Contributors to the Original NATCA document included the following consortium members:

AC Transit, Oakland, CA
Centro Syracuse, NY
Dallas Area Rapid Transit (DART), TX
Go Metro Cincinnati, OH
Golden Gate Bridge
Greyhound Lines North America
Hampton Roads Transit, VA
Long Beach Transit (LBT), CA
Massachusetts Bay Transportation Authority
Metra Commuter Rail (Metra) WI, IL
Metropolitan Atlanta Rapid Transit Authority, GA
Metropolitan Council Minneapolis, MN
Metropolitan Transit Authority, TX
New Jersey Transit
Nor. Indiana Commuter Transportation District
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 Trans Authority
Southern California Regional Rail Authority
Toronto Transit Commission, Canada
Transbay Joint Powers Authority, San Francisco
TransLink Vancouver, Canada
TriCounty Metropolitan Transportation District
Utah Transit Authority

Project team

Polly Hanson, *American Public Transportation Association*
Brian Heanue, *American Public Transportation Association*
Michael A. Echols, *Max Cybersecurity LLC*

Introduction

The cybersecurity threat posed to mass transit and passenger rail operators and authorities across the nation is an ever-evolving issue. This has been exacerbated by the increasingly complex and intertwined environment that operators find themselves in, relying increasingly upon unsecured operational technologies for their daily operations. This has left rail operators vulnerable to cyberattacks, with every new system being implemented as a potential new avenue for cyber threats to exploit. The goal of this white paper is to endorse the requirements put forward by the North American Transportation Cybersecurity Consortium to address this threat. Its agreement, called the NATCA, is a set of standards for OT technology procurement that both vendors and operators should follow. Because there are few procurement guidance documents for transportation that were written by transit practitioners, APTA considers this guidance an important set of

practices supporting agency resilience. This document supports risk practices supporting safety functions, customer service, cost/financial modeling, network availability, data integrity, and system assurance.

The North American Transportation Cybersecurity Consortium is a working group consisting of public transportation agencies, cybersecurity leaders, vendors and manufacturers. Therefore, the agreed-upon standards have been tacitly approved by the vendor, manufacturing and supplier industry supporting mass transit and railways. Vendors will also benefit from the standard because there will be a consistent approach to OT procurement, helping them to plan more effectively for common transit requirements when designing products and services.

There is a global consensus on the cybersecurity threat and the inability of current environments to meet the security requirements. This presents a challenge as well as an opportunity to create technology procurement security baselines. Products and services introduced into agencies that adopt the NATCA principles will begin a process of closing gaps currently made wider by factors exploited by the hacker community. This includes products and services that lack functionality to meet most cybersecurity standards like those developed by APTA and the National Institute of Standards and Technology.

APTA recommends the use of this white paper by:

- individuals or organizations that operate transit systems;
- individuals or organizations that contract with others for the operation of transit systems; and
- individuals or organizations that influence how transit systems are operated (including but not limited to consultants, designers and contractors).

Scope and purpose

The goal of the NATCA is to ensure a consistent approach to the implementation and integration of a system under consideration (SuC) into a transportation agency as to not introduce cybersecurity risk from the product or service. The SuC can be any system that contributes to the function of providing transportation. The SuC is a collection of integrated administration and control system assets, subsystems, and components, including network infrastructure, that provide complete automated solutions. These SuCs are not limited to a standalone system, as they can also be a system that is integrated within an existing system. Components may include but are not limited to signaling, communication, processing, OT, safety systems, SCADA and rolling stock.

The procurement guidelines are aligned with existing cybersecurity standards and support the network designer and the procurement official's ability to require vendor practices that are known to significantly reduce the cyber risk in critical infrastructure like transportation. The agreement aims to establish a unified management framework that leverages robust security protocols across railway infrastructures. It provides key guidance to help stakeholders address the dynamic and sophisticated threats facing the railway sector.

The NATCA applies to on-premises 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 the agreement is not on the cybersecurity implications associated with cloud infrastructure as a replacement for physical on-premises systems and networks. However, the NATCA does not restrict the use of cloud hosted services, provided that doing so does not adversely impact the target security level of the SuC as documented in the Detailed Cyber Risk Assessment. The main objectives of the agreement are the following:

- Minimize the future costs to public agencies by including cybersecurity requirements upfront.

- Make suppliers and manufacturers aware upfront of the baseline requirements of North American public transportation agencies.
- Protect against commonly exploitable components of the operational technologies by including prescriptive and specific requirements.
- Ensure that operators know how to run the system securely after it goes into production by including not only technical controls but also processes such as asset management, vulnerability (including patch management), incident response, incident detection and recovery.
- Be portable to a component of a system such as Active Directory, or a set of system components such as wireless, virtual servers, network security, rolling stock, etc.
- Ensure that production systems do not reach end of life or end of support before they are operational.
- Comply with Transportation Security Administration directives.

Cybersecurity Requirements for Operational Technology Procurement

1. Overview

New operational technology (OT) products, systems and services will continuously be implemented across transportation agencies. Cybersecurity experts agree that to meet the current and future requirements for cyber resilience there must be a transportation industry-wide set of practices that assist with standardizing the approach to assessing and managing the risk introduced by these new OT technologies. To meet this challenge, the North American Transportation Cybersecurity Consortium, consisting of transportation agency personnel, vendors and manufacturers, created an agreement called the North American Transit Cybersecurity Agreement (NATCA), which serves as a unifying commitment by those signing to adhere to a baseline for OT technology procurement. It holds vendors and suppliers responsible for identifying and mitigating cybersecurity risks from their products. It also serves as a set of guidelines for all transportation procurement teams.

The goal of the NATCA, and this white paper, is to address OT cybersecurity threats that are introduced at the procurement stage of engagements with vendors. These procurement vulnerabilities undermine global security standards and the ability to mature the OT cyber environment. The consortium has addressed the issue by developing an agreed-upon set of standards for OT procurement that both vendors and operators must follow to properly address a constantly changing and evolving threat.

The NATCA formalizes technology cybersecurity evaluation for systems under consideration (SuCs) to better ensure that they meet cybersecurity requirements aligned with national cybersecurity standards. All technology stakeholders agree that a collaborative and adaptive approach to transit agency cyber resilience is required to meet the skill and will of the hacker. The NATCA takes a step forward by requiring vendors to perform risk assessment and testing prior to bringing the product or service forward for offer into the transportation environment. Under this agreement, vendors are also responsible for performing failure analysis.

When a transportation agency implements the terms and conditions of the NATCA, a cybersecurity partnership is built between the vendor and the agency. Currently, many transportation agencies struggle to meet cybersecurity standards because of absent product functionality, lack of understanding of the impacts products have on existing systems, and the absence of a life cycle management system within the organization. The agreement defines practices and processes to make the vendors a partner in filling those gaps. Implementing processes and practices developed into standards by global cybersecurity leaders is critical to minimizing the risks of cybersecurity malfeasance. Each time an organization purchases a new service or product that does not support the cybersecurity maturity resilience roadmap, that agency undermines the ability to eventually reduce cybersecurity risk and potentially adds to its long-term cybersecurity costs.

APTA is endorsing NATCA because its guidelines and approach to OT cybersecurity risk management are consistent with APTA and NIST standards that recommend performing risk assessments to understand the

vulnerabilities, threats and consequences as preparedness measures to prevent and manage cyberattacks. The full text of the NATCA is in Appendix A, and its Appendix 2 is in Appendix B of this document.

1.1 Who should use this paper and why?

To establish a centralized consensus on minimizing cybersecurity risk, the NATCA recommendations and requirements can be utilized by all stakeholders in the procurement process. This includes railway operators, system integrators, product suppliers, risk managers and procurement teams. All stakeholders participating in the design, procurement, integration and management of OT systems will benefit and ensure stronger protection and prevention against increasing cybersecurity threats. The NATCA requirements and the approach to enhancing acquisitions and product management are applicable for all transportation agencies. When technical requirements are developed by engineers and system designers, they should consider the principles outlined by the NATCA. Most engineers are not cybersecurity experts. NATCA can support their efforts to develop the best requirements to support system resilience.

When procurement teams look to the market for vendors to address OT technology needs, they should ensure that the potential suppliers can deliver a product or service to the standard outlined in the requirements developed by the engineers. Later, as the agency matures in its cybersecurity journey, principles of the NATCA should be instantiated by policy by upper management. The NATCA creates an opportunity to build a procurement process that is collaborative and manageable. Vendors are made partners, and the resulting relationship creates an environment to focus on joint risk-reduction activities. Rail operators and transportation agencies can also use the NATCA document and its requirements to assist as an assurance of risk management in the acquisition process. By following the requirements and ensuring that vendors also follow them, operators greatly reduce the introduction of new risk to their existing networks.

Businesses and integrators who are on the supply side of procurement can use this document to help design functionality to better meet cybersecurity requirements. The adoption of the principles in the NATCA will provide the vendor with confidence that there is consistency in the procurement at transportation agencies. This will allow vendors to eventually put more focus on practices that highlight their offering as one that does not contribute to the tech debt suffered by most agencies. In turn, both vendors and suppliers can use the guidelines to better align themselves with the needs and expectations of a base level of cybersecurity for their transportation customers. They can use the commitment to a common set of standards to ensure that their systems meet the minimum safety requirements that rail operators expect.

1.2 How should the different stakeholders in procurement use this paper?

Rail operators and transportation agencies who procure systems can use this white paper and the NATCA document and its requirements to assist with risk management in the acquisition process. By following the requirements and ensuring that their vendors follow them, operators greatly reduce the potential risk introduced by new systems or augmentation of their existing networks.

APTA has produced recommended practices for cybersecurity that are based on global standards such as the NIST Cybersecurity Framework and IEC 62443. These guidelines for developing resilient cyber environments provide baseline approaches that cybersecurity and operations teams can use to minimize cybersecurity risk across the operational environments. Because new technology is constantly being introduced into those environments, failure to qualify risk strategy in the procurement process can undermine the cybersecurity impact from work performed by operational teams. Risks are constantly reintroduced because the new products or services were not properly assessed prior to their implementation and because there was no set of expectations provided to all suppliers prior to purchase. Further, the lack of life cycle management and ownership of how an SuC continues to support the agency’s cybersecurity requirement increases risk to the transportation agency over time. Procurement teams must partner with risk managers,

operators and system owners within their organizations to approach cybersecurity risk reduction in a holistic fashion. The NATCA document creates a shortcut to making this partnership possible.

Note: The IEC 63452 - Railway Cybersecurity standard is anticipated to be formally approved in spring of 2026. This forthcoming standard builds upon the IEC 62443 framework but is expected to supersede it for railway-specific applications. While IEC 63452 provides a sector-focused extension of cybersecurity principles, its procurement guidance remains limited and appears generally aligned with the NACTA document. Continued monitoring is recommended to ensure that the release of IEC 63452 does not necessitate substantive revisions to this endorsement and referenced NACTA guidance.

The guidelines contained in the NATCA assist the agency engineering design team to provide better cybersecurity requirements to the procurement team. The procurement team can then instantiate the requirements in requests for services or products, qualifications of potential vendors, and assurance activities following the purchase. The assurance is supported by the terms and conditions that can be put into contractual language.

The NATCA approach overcomes a longtime issue that hackers have exploited. Agencies have suffered successful cyberattacks because they lacked processes and personnel to meet the threat, had vulnerabilities introduced by technologies that could not meet basic cybersecurity standards, or lacked capabilities to support cross-sector cybersecurity goals. The NATCA creates a force multiplier by enhancing the knowledge of procurement personnel. They do not have to be cybersecurity experts or keep up with the latest cybersecurity threats to ensure that their purchases are aligned with OT cybersecurity risk reduction practices. The NATCA creates a platform to manage the cybersecurity relationship that puts some of the cybersecurity responsibility currently held by the agency onto the supplier.

The NATCA can be used in addition to or in combination with railway operators' and transportation agencies' preexisting cybersecurity practices to close the vulnerabilities present in the procurement process. For the rail transportation sector to eventually reduce sector risk, there must be a set of requirements accepted by the agency, the end user and the supplier.

2. Why endorse NACTA

The APTA TCSWG endorses the NATCA framework because it delivers a long-overdue, structured approach to securing OT systems in transportation environments. These systems increasingly serve as the backbone of safety, mobility, and efficiency and must be managed appropriately to reduce agency risk. NATCA goes beyond technical checklists by formalizing shared cybersecurity responsibilities between agencies and vendors, ensuring that cybersecurity is not an afterthought, but a foundational design principle. As cyber threats become more sophisticated and transportation agencies face growing regulatory pressure from entities such as TSA, the NATCA framework provides actionable standards that agencies of all sizes can adopt, regardless of their internal cybersecurity maturity. From pre-deployment risk assessments and secure-by-design mandates to detailed documentation and supply chain visibility, NATCA creates a level of discipline and transparency that aligns with APTA's mission to safeguard public transportation systems. APTA supports NATCA because it empowers agencies to demand better security from the products and services they procure, enables safer system integration, and creates the conditions for long-term resilience in the face of escalating cyber threats.

The NATCA framework prescribes specific actions that vendors must complete before deploying new OT products or services into transportation environments. These actions establish clear risk management expectations and require that the system under consideration (SuC) meets predefined standards before integration into the operational environment. This approach ensures a mutual understanding of the cybersecurity responsibilities held by transportation agencies and their suppliers. By subscribing to the

NATCA principles, both parties commit to managing risks collaboratively, maintaining acceptable risk levels and laying the groundwork for long-term cyber resilience.

The TCSWG wholly agrees with the principles and structure outlined in the NATCA framework. The TCSWG recognizes NATCA as a critical step forward in formalizing cybersecurity accountability within the OT procurement process and ensuring that vendors align with the unique safety, availability, and integration requirements of transportation systems. The framework's emphasis on clear documentation, collaborative risk assessments, system definition, and secure development practices directly supports the operational realities faced by transportation agencies. Below are key highlights from the NATCA document that the TCSWG believes will immediately strengthen OT procurement practices and help agencies implement secure, resilient technologies from the outset of vendor engagement. The following sections highlight some of the many NATCA requirements that will strengthen OT procurement across transportation agencies of all sizes. The full NATCA is located in Appendix A.

2.1 Cross-agency collaboration

The TCSWG supports the NATCA identification of the cross-agency review of the OT product or services. A key requirement of the NATCA standards is clear communication and definition of the SuC. This includes conducting risk assessments, analyses and vulnerability discovery to align the efforts of cybersecurity teams with the operational and business objectives of the agency. Such alignment enables agencies to meet their OT cybersecurity goals effectively while supporting operational continuity and safety.

The NATCA discusses cybersecurity availability. The reference is to the ability of the SuC to continue to operate reliably and to "fight through" cyberattacks and general component failures. This can be achieved by the vendor through redundancies and built-in work arounds to compensate for potential component and cybersecurity failures.

TCSWG believes that by integrating the NATCA standards into their practices, transportation agencies can foster a culture of shared responsibility with vendors and proactive risk management. This should ensure an increase in the probability that the evolving cyber threat landscape does not compromise the safety, efficiency or trustworthiness of operations.

2.2 Risk assessment

The NATCA calls for a comprehensive risk assessment of the SuC. This risk assessment is completed by the vendor in collaboration with an operator/agency and its cybersecurity, safety and operational staff. A vendor must deliver assessments on several areas of interest listed in the NATCA document. This includes areas such as defining the threat landscape, listing unmitigated risks, countermeasures to address identified threats, and several other specific requirements such as the following:

- The vendor will provide evidence-based assurance that cybersecurity functions do not negatively impact safety or essential operations. It will define threat landscapes, use cases and potential cybersecurity threats based on the MITRE ATT&CK framework and the MITRE ATT&CK for ICS for different zones and outline applicable security controls, both digital and physical, to mitigate identified threats.
- Documentation will cover how IT component failures affect operations and safety, as well as how security incidents can propagate to other components and connected systems, detailing potential cascading impacts from both physical and logical dependencies. The vendor will demonstrate that implementing the ISA/IEC 62443-3-3 standard security level target measures will effectively reduce risks to the agency's target risk level, with all components defaulting to Security Level 3 (unless otherwise specified).

- The vendor may request risk acceptance for specific risks, subject to the agency's approval, and will update the Detailed Cyber Risk Assessment (DCRA) annually following deployment. If the SuC processes or stores data with potential privacy implications, the vendor will document and manage privacy risks according to the NIST Privacy Risk Assessment Methodology (PRAM).

2.2.1 The cybersecurity plan

At a minimum, NATCA calls for the plan to cover cybersecurity risks and establish the programs described in the agreement. Upon completion of the risk assessment process, the vendor is required to submit a cybersecurity plan for the review and approval of the agency. This requirement alone changes the current relationship between agencies and their vendors or suppliers. The shared responsibility for cybersecurity allows the agency more time to do the work before it and reduces the burden of managing the technology life cycle by the agency alone.

2.2.2 SuC documentation and definition

As many of the cyber breaches experienced by critical infrastructure are due to poor configuration and error in design, understanding the impact of the SuC implementation is critical to ensuring that the proper controls are in place. The NATCA documentation requirement advantages the agency by addressing the SuC integration with other railway systems, specifying whether it incorporates or is part of a larger system, supported by dependency diagrams from the agency.

NATCA requires vendors to provide comprehensive documentation for the SuC and its components, including a definition document that outlines the overall scope, functionality, features and boundaries of the SuC. The documentation encompasses the SuC's objectives and mission profile, detailing its functions, boundaries and interfaces, as well as descriptions of each essential function. The requirements of the document will ultimately be defined by the transportation agency.

2.3 Physical and environmental impact

As part of the risk assessment, the vendor will analyze and document the potential physical and environmental impacts of cybersecurity risks associated with the SuC, including safety risks arising from a cybersecurity compromise. The vendor will evaluate the broader context of the SuC's operational environment within the agency's railway system, specifically addressing how a cybersecurity incident could lead to physical impacts on operations. This analysis will include the following:

- Defining how a cybersecurity incident could manipulate the physical environment and other railway operations, such as operational downtime caused by denial-of-service attacks.
- Documenting how a cybersecurity event on the SuC could trigger cascading physical impacts on other OT systems and railway operations.
- Designing features of the SuC aimed at mitigating or preventing the identified physical risks.

2.4 Risk assessment documentation

The vendor will conduct an initial risk assessment (IRA) to document the cybersecurity threat risk assessment, treatment and protection strategies. This assessment will evaluate the potential impact of cyberattacks on safety functions and forecast worst-case scenarios for railway operations, considering factors such as human health and safety, operational availability, and financial impact. The IRA will include the following:

- A cybersecurity impact assessment based on the agency's risk matrix.
- A likelihood assessment for cybersecurity risks, along with an evaluation of protection requirements.

The agency will review and approve the IRA documents. This IRA will help define and agree upon the security level targets for the SuC, subsystems and components according to the prevailing IEC standard for each zone and conduit, as outlined by the zone and conduit requirement (ZCR).

2.4.1 Cybersecurity initial risk assessment (IRA)

This risk assessment, to be completed independently by the vendor, will document the cybersecurity threat risk and associated treatments. This assessment shall be based upon an agency's risk matrix and must include the likelihood of cybersecurity risks. The agency will review and approve the IRA documents.

2.5 Zone and conduit requirements

NACTA calls out the ISA-62443-3-2-2020 standard, a structured approach to assessing zones and conduits within an industrial automation and control system (IACS). APTA also has a zones approach and encourages readers to review the APTA zones charts.

Product certification under the IEC 62443 series is administered through the ISA Secure program, which provides formal assurance that products and systems meet recognized cybersecurity requirements. This certification initiative should be considered as part of ongoing procurement and assurance discussions.

Consistent with most current APTA standards, the NACTA document aligns with the Cybersecurity and Infrastructure Security Agency (CISA) Secure by Design strategy, emphasizing proactive risk reduction, embedded security controls, and accountability throughout the system development lifecycle.

2.6 Secure system development

Like most current APTA standards, NATCA is aligned with the principles of the Cybersecurity and Infrastructure Security Agency Secure by Design strategy. Products designed with Secure by Design principles prioritize the security of customers as a core business requirement, rather than merely treating it as a technical feature. CISA advises that during the design phase of a product's development life cycle, companies should implement Secure by Design principles to significantly decrease the number of exploitable flaws before introducing them to the market for widespread use or consumption. Out of the box, products should be secure with additional security features such as multifactor authentication (MFA), logging and single sign-on (SSO) available at no extra cost.

2.7 Information sharing and vulnerability reporting

When vendors fail to share vulnerability information about their products with transportation agency customers, it creates challenges for cybersecurity and operational resilience. Without access to this critical information, transportation agencies cannot effectively assess risks, develop comprehensive threat models or implement timely mitigations. This lack of visibility delays responses to vulnerabilities, increasing the likelihood of cyber incidents that could disrupt operations, compromise safety, or result in noncompliance with regulatory standards such as those outlined by NIST or TSA. Furthermore, undisclosed vulnerabilities in third-party products expose agencies to supply chain risks, erode trust in vendor relationships and limit an agency's ability to act, making it "overly" reliant on the vendor.

NATCA requires that vendors establish and maintain a mandatory vulnerability reporting process for all identified or suspected security weaknesses within supplied systems. Vendors must implement a detection and remediation program that encompasses the entire System under Consideration (SuC), including all subsystems, components, and third-party dependencies. Additionally, NATCA requires that when vulnerabilities are discovered, there is a mandatory vulnerability reporting process by the vendor. The guidance calls on vendors to implement a detection and remediation program covering the SuC as well as all its subsystems and components via software bill of materials (SBOM) tracking. An SBOM is a

comprehensive inventory of a software system's components and their dependencies (see Appendix C for more information).

2.8 Vendor responsibility for patching

Under the NATCA, a vendor must establish a patch deployment program for its SuC and any associated subsystems and components among a list of several vendor requirements for providing and maintaining inventory. They must also establish a program and process to manage and report on the current inventory of systems. These reports must detail all the hardware and software components present, including their subsystems. They include but are not limited to maintaining a detailed asset inventory of all components; tracking of hardware, software and firmware; lists of hard-coded accounts; and several other requirements.

2.8.1 Hardware configuration

The NATCA hardware requirements emphasize stringent measures to protect both the physical security and cybersecurity of SuC components. The vendor must meet several requirements as it pertains to hardware configuration. These include the following system hardening processes that are in accordance with the latest Security Technical Implementation Guides (STIGs) and Center for Internet Security (CIS) benchmarks. STIGs provide a methodology for standardized secure installation and maintenance of Department of Defense devices and systems.

2.8.2 Software configuration

NATCA's software implementation requirements establish a comprehensive framework to ensure the security, reliability and functionality of software incorporated into an SuC. Vendors must use the latest supported versions of software, with original equipment manufacturer (OEM) support extending at least three years beyond the SuC's acceptance by the agency. Software installation must adhere to a strict "allowlist," permitting only preapproved software necessary to support SuC functionality, consistent with the principles of least functionality and least privilege. This means software must disable unnecessary services and communications by default and should not introduce undocumented ports or security bypasses. Additionally, SuC components must not rely on outdated, unsupported or end-of-life third-party software unless explicitly approved by the agency. Lastly, secure communication protocols and encryption are mandated to protect network interactions, ensuring data integrity and confidentiality.

2.9 User awareness and training

The NATCA guidelines require vendors to establish comprehensive training programs to ensure that personnel are well-prepared to support SuC deployment securely and reliably. Robust training and awareness are critical to maintaining the security and resilience of transportation systems, equipping employees and contractors with the knowledge necessary to uphold security practices and comply with the NATCA standards. These programs should include clear instruction on security and safety policies, annual training plans to maintain essential skills, and controlled lab environments for risk-free practice on SuC functions. Comprehensive user awareness programs must also cover topics such as security reporting, data security and secure web use, enabling personnel to proactively address security challenges and safeguard the operational integrity of the SuC.

2.10 Metrics and performance goals

TCSWG fully agrees with the push by CISA and standards organizations to monitor and measure performance. NATCA demands that vendors design the SuC to meet or exceed the agency's reliability and performance goals, ensuring safe and continuous operation even during failures. This includes implementing a program to minimize the impact of system failures and meeting the agency's recovery objectives. Vendors, in collaboration with the agency, must define and agree upon target values for mean time between failure and

mean time to recovery, documenting all assumptions in this process. Additionally, vendors must demonstrate competence in managing processes and tools to maintain adequate uptime levels and implement backup and restoration processes in accordance with NATCA requirements.

2.11 Conclusion

The NATCA framework marks a pivotal advancement in securing OT across transit environments. By embedding cybersecurity expectations directly into procurement, integration, and lifecycle management processes, NATCA offers a practical, standards-aligned roadmap for agencies and vendors alike. It addresses long-standing gaps that have enabled vulnerabilities to persist. They range from poor documentation to limited accountability for risk ownership. Transportation agencies no longer need to navigate procurement decisions in the dark or rely solely on internal resources to define cybersecurity requirements. Instead, NATCA provides a common language and set expectations that bridge engineering, procurement, operations, and vendor responsibilities. With clear guidance on system definition, secure development, vulnerability management, and performance metrics, agencies can reduce the risk of introducing new threats while strengthening resilience across their OT ecosystem. The APTA TCSWG strongly encourages widespread adoption of NATCA, as it empowers all stakeholders, whether buyers, integrators, or suppliers, to participate meaningfully in the shared goal of cyber-secure, reliable transportation operations.

References

Cybersecurity and Infrastructure Security Agency, Secure by Design series, November 2023. https://www.cisa.gov/securebydesign

Cybersecurity and Infrastructure Security Agency, “Recommended Cybersecurity Practices for Industrial Control Systems,” June 2021. https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf

Cybersecurity and Instructure Security Agency, “2025 Minimum Elements for a Software Bill of Materials (SBOM)” August 22, 2025. https://www.cisa.gov/resources-tools/resources/2025-minimum-elements-software-bill-materials-sbom

ISA Global Security Alliance, “Security Lifecycles in the ISA/IEC 62443 Series: Security of Industrial Automation and Control Systems,” October 2020. https://gca.isa.org/blog/download-the-new-guide-to-security-lifecycles-in-the-isa/iec-62443-series-of-standards

MITRE Corporation, “Finding Cyber Threats with ATT&CK-Based Analytics,” June 2017. https://www.mitre.org/publications/technical-papers/finding-cyber-threats-with-attck-based-analytics

National Institute of Standards and Technology (NIST), “Approaches for Federal Agencies to Use the Cybersecurity Framework,” NISTIR 8170, March 2020. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8170-upd.pdf

National Institute of Standards and Technology (NIST), “Assessing Security and Privacy Controls in Information Systems and Organizations,” NIST Special Publication 800-53A Rev. 5, January 2020. https://doi.org/10.6028/NIST.SP.800-53Ar5

National Institute of Standards and Technology (NIST), “Automation Support for Security Control Assessments,” NISTIR 8011, June 2017. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8011-1.pdf

National Institute of Standards and Technology (NIST), "Cybersecurity Framework Version 1.1 Manufacturing Profile," NISTIR 8183, October 2020. https://doi.org/10.6028/NIST.IR.8183r1

National Institute of Standards and Technology (NIST), "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach Publication," NIST SP 800-160, December 2021. https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final

National Institute of Standards and Technology (NIST), 2017. "Framework for Improving Critical Infrastructure Cybersecurity," Draft Version 1.1, April 2017. https://www.nist.gov/document/2017-04-11-ernstyoungpdf

National Institute of Standards and Technology (NIST), "Guide to Cyber Threat Information Sharing," NIST Special Publication 800-150, October 2016. http://dx.doi.org/10.6028/NIST.SP.800-150

National Institute of Standards and Technology (NIST), "Guide to Operational Technology (OT) Security," SP 800-82 Rev. 3, September 2023. https://csrc.nist.gov/pubs/sp/800/82/r3/final

National Institute of Standards and Technology (NIST), "NIST Risk Management Framework Overview." https://www.nist.gov/system/files/documents/2018/03/28/vickie_nist_risk_management_framework_overview-hpc.pdf

National Institute of Standards and Technology (NIST), "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," NIST Special Publication 800-171r3, May 2024.

Santos, O., "Cisco Cybersecurity Operations Fundamentals," December 2020. https://www.ciscopress.com/store/cisco-cyberops-associate-cbrops-200-201-official-cert-9780136807834

U.S. Department of Energy, Cybersecurity Capability Maturity Model (C2M2), June 2022. https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0

U.S. Department of Homeland Security CISA, "Cybersecurity Practices for Industrial Control Systems," December 2020. https://www.cisa.gov/publication/Cybersecurity-Best-Practices-for-Industrial-Control-Systems

U.S. Department of Homeland Security CISA, "Transportation Systems Sector Cybersecurity Framework Implementation Guidance," June 2015. https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf

U.S. Department of Homeland Security CISA, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," September 2016. https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

U.S. Department of Homeland Security, National Cyber Security Division, "Public Safety Communications Resiliency," July 2017. https://www.cisa.gov/sites/default/files/publications/07202017_10_Keys_to_Public_Safety_Network_Resiliency_010418_FINAL508C.pdf

Definitions

Cybersecurity and Infrastructure Security Agency (CISA): Operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.

Detailed Cyber Risk Assessment: A comprehensive evaluation process used to identify, evaluate and prioritize potential risks and vulnerabilities within an organization's systems and digital infrastructure.

encryption: The cryptographic transformation of data to produce ciphertext.

endpoint detection and response: Centrally manages threats across endpoint, network and web traffic.

Federal Information Processing Standards (FIPS): A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability. FIPS 201-3 is titled "Personal Identity Verification (PIV) of Federal Employees and Contractors."

hazard analysis: The process of identifying hazards that have the potential to arise from a system or environment, documenting their unwanted consequences.

initial risk assessment (IRA): Starting point for risk analysis activities. Defines the scope of future assessments, establishes the zone and conduit diagram, sets initial target security level for devices, and identifies high-risk areas for further analysis.

industrial automation and control system (IACS): Control system and any complementary hardware and software components installed and configured to operate in an industrial setting. Includes distributed control systems, programmable logic controllers, remote terminal units, and supervisory control and data acquisition (SCADA) systems.

ISA 62334: A series of standards that defines requirements and processes for implementing and maintaining electronically secure industrial automation and control systems. These standards set best practices for security and provide a way to assess the level of security performance.

log collection: The process of gathering data across computer networks, systems and applications.

mean time between failure: The average amount of time between repairable failures of a technology product.

mean time to recovery: A metric that tracks the average amount of time that it takes to recover from a product or system failure.

multifactor authentication (MFA): Authentication using two or more factors to achieve authentication. Factors include something one knows (e.g., password/PIN); something one has (e.g., cryptographic identification device, token); or something one is (e.g., biometrics).

National Institute of Standards and Technology (NIST): An agency of the United States Department of Commerce.

North American Transit Cybersecurity Agreement (NATCA): A collaborative effort aimed at enhancing cybersecurity protections for transit systems across North America.

North America Transit Cybersecurity Consortium: Association aimed at strengthening the cybersecurity of public transit systems across North America.

operational technology: Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes and events.

Privacy Risk Assessment Methodology (PRAM): A tool that applies the risk model from NISTIR 8062 and helps organizations analyze, assess and prioritize privacy risks to determine how to respond and select appropriate solutions. The PRAM can help drive collaboration and communication between various components of an organization, including privacy, cybersecurity, business and IT personnel.

public key infrastructure (PKI): The architecture, organization, techniques, practices and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. The framework was established to issue, maintain and revoke public key certificates.

Residency Plan: A structured approach for embedding cybersecurity expertise and resources directly within an organization over an extended period.

risk assessment: The process of identifying risks to organizational operations (including mission, functions, image and reputation), organizational assets, individuals, other organizations, and the nation, resulting from the operation of an information system.

risk management framework: A disciplined and structured process that integrates information security and risk management activities into the system development life cycle.

rolling stock: Locomotives, carriages, wagons or other vehicles.

remote access: Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the internet).

supply chain security: Aspect of supply chain management focusing on identifying and managing security risks associated with external vendors, suppliers, transportation and logistics.

system life cycle: Period that begins when a system is conceived and ends when the system is no longer available for use.

system under consideration (SuC): A specific system selected for evaluation of cybersecurity risks and vulnerabilities during a security assessment.

tabletop exercise: A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

target security level: An implementation-dependent statement of security needs for a specific identified target of evaluation.

third-party audit: Independent evaluations conducted by external organizations or certification bodies.

user account management system: Allows administrators to manage users' access to devices, software and services. This includes managing permissions, monitoring usage and providing authenticated access.

virtual private network: Protected information system link utilizing tunneling, security controls and endpoint address translation, giving the impression of a dedicated line.

Abbreviations and acronyms

API	Application Programming Interface
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CA	certificate authority
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CMDB	configuration management database
CVSS	Common Vulnerability Scoring System
DCRA	Detailed Cyber Risk Assessment
DMZ	demilitarized zone
DoS	denial of service
EDR	endpoint detection and response
FIDO	Fast IDentity Online
FIPS	Federal Information Processing Standards
GPS	Global Positioning System
HVAC	heating, ventilation and air conditioning
IACS	industrial automation and control system
ICS	industrial control systems
IEC	International Electrotechnical Commission
IP	Internet Protocol
IRA	initial risk assessment
ISO	International Organization for Standardization
IT	information technology
LSASS	Local Security Authority Subsystem Service
MFA	multifactor authentication
MTBF	mean time between failures
MTTR	mean time to recovery
NAC	network access control
NATCA	North American Transportation Cybersecurity Agreement
NDA	nondisclosure agreement
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Reports
NTP	Network Time Protocol
NVD	National Vulnerability Database
OEM	original equipment manufacturer
OT	operational technologies
PERA	Purdue Enterprise Reference Architecture
PKI	public key infrastructure
PRAM	Privacy Risk Assessment Methodology
RDP	Remote Desktop Protocol
RPO	recovery point objective
RTO	recovery time objective
SAT	system acceptance testing

SBOM software bill of materials
SCADA supervisory control and data acquisition
SL-T target security level
SMB Server Message Block
SSID service set identifier
SSO single sign-on
STIG Security Technical Implementation Guide
SuC system under consideration
TPM Trusted Platform Module
TSA Transportation Security Administration
UEFI Unified Extensible Firmware Interface
VEX Vulnerability Exploitability eXchange
ZCR zone and conduit requirement

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	CEO Approval	Policy & Planning Approval	Publish Date
First published	Oct. 31, 2025	Jan. 30, 2026	Feb. 28, 2026	April 10, 2026	May 13, 2026

Appendix A: Text of North American Transit Cybersecurity Agreement

1. Overview and scope

The North American Transit Cybersecurity Agreement (NATCA) specifies cybersecurity operational technologies procurement requirements as a guideline for members of the North American Transit Cybersecurity Consortium.

The NATCA 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 systems to form a system of systems. In others, the SuC may interface with other systems and processes only within the existing environment. In most cases, the SuC will need to perform both functions.

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

The North American Transit Cybersecurity Consortium comprises the following organizational entities:

- AC Transit, Oakland, California
- Central Ohio Transit Authority
- Centro, Syracuse, New York
- Chicago Transit Authority
- Dallas Area Rapid Transit, Texas
- Golden Gate Transit, California
- Greyhound Lines North America
- Hampton Roads Transit, Virginia
- Highway and Transportation District, California
- Long Beach Transit, California
- Massachusetts Bay Transportation Authority
- Massachusetts Department of Transportation
- Metra, Wisconsin/Illinois
- Metro, Cincinnati, Ohio
- Metro Transit, Minneapolis, Minnesota

- Metropolitan Atlanta Rapid Transit Authority, Georgia
- Metropolitan Transit Authority of Harris County, Texas
- New Jersey Department of Transportation's Office of Fixed Guideway
- New Jersey Transit
- Northern Indiana Commuter Transportation District
- Orange County Transportation Authority, California
- Pace Suburban Bus, Chicago
- Port Authority, Pittsburgh
- Port Authority of New York and New Jersey
- Regional Transportation Authority, Chicago
- Regional Transportation Authority, Denver
- Regional Transportation Commission of Southern Nevada
- Sacramento Regional Transit District
- San Diego Metropolitan Transit System
- San Francisco Municipal Transportation Agency
- Santa Clara Valley Transportation Authority, California
- Société de transport de Montréal, Canada
- Sound Transit, Seattle
- Southeastern Pennsylvania Transportation Authority, Philadelphia
- Southern California Regional Rail Authority
- Southwest Ohio Regional Transit Authority
- Toronto Transit Commission, Canada
- Transbay Joint Powers Authority, San Francisco
- TransLink, Vancouver, Canada
- Transportation District Commission of Hampton Roads
- Tri-County Metropolitan Transportation District of Oregon, Portland
- Utah Transit Authority

2. Cybersecurity SuC agreement requirements

This agreement stipulates security contract terms and conditions for SuCs. The cybersecurity requirements stated herein are to be implemented by the vendor responsible for providing SuCs that will be operated by the authority or by the vendor.

An 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. An SuC can be deployed into one or more zones and related conduits. All assets within an 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 and 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, composed 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 with affiliated/integrated systems.
5. The boundaries and interfaces of the systems, 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 life cycle 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 19 of this agreement.

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 of 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 and 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 target security levels for the SuC, subsystems and components based on the ANSI/ISA-62443-3-2-2020 standard for each zone and conduit as determined by the zone and conduit requirement (ZCR).

3.3.2 Zone and conduit design

As part of the risk assessment process, the vendor shall complete the initial design of the zone and conduit documents for the SuC. The design shall ensure that operational technologies systems can continue to function safely if a related information technology system has been compromised. The vendor shall submit for approval the zone 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.

Zones and conduits must be categorized in hierarchical groups wherein the highest security requirement is enforced as the security requirement for all components in the zone.

The design shall follow the Purdue Enterprise Reference Architecture (PERA) 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 zone 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. Provide 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. List the applicable security controls and countermeasures to address identified threats. Based on the nature of vulnerability and threat, security controls may be digital or physical.
4. List all unmitigated cybersecurity risks categorized by potential impact.
5. Validate target security level.
6. Document how the failure of IT components supporting the SuC impacts 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 the authority's OT environment. Document how cascading impacts could occur as the result of both physical and logical dependencies.
8. Provide proof that implementation of the suggested ISA-62443-3-3 target security level 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 target security levels 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 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 should 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 target security levels (SL-Ts) 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 target security levels based on the requirements of ANSI/ISA-62443-4-1-2018, "Security for Industrial Automation and Control Systems," Part 4-1: Product Security Development Life-Cycle Requirements, and 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 and 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 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 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 time frame to the authority in compliance with requirements stated in Section 6 of this agreement, “Security patching and mitigation governance.”
5. The vendor shall disclose vulnerabilities that may impact the safety of critical systems to the authority within one 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 patches or countermeasures for the vulnerability available 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 shall 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 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 the requirements stated in Section 6.

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 its 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 non-production environments. 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 to 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. The 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. The vendor shall supply the rollback step-by-step process. The 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 19 of this agreement, “System life cycle management.”
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 time frame, the vendor shall provide mitigations and/or workarounds within the period defined in Section 5 of this agreement, “Vulnerability discovery, reporting and assessment.”
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 time frame, 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 vulnerabilities has been achieved. The application of the patch or mitigation shall reduce the risk to a tolerable 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 of this agreement, “Operational governance.”
18. The authority shall dictate the manner and date that the patches or compensating controls will be deployed.

19. Patches and mitigation time frame shall adhere to the schedule tabulated below.

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. This includes 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 of this agreement, "SuC risk assessment." 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 hard-coded accounts in the SuC, including hard-coded 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 of this agreement, “Vulnerability discovery, reporting and assessment.”
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 its 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 cybersecurity 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 cybersecurity features and provide the methodologies 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. The 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 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 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 three years past the authority's acceptance of the SuC.
2. The SuC shall enforce a software installation "allowlist" and permit the installation of only approved software.
3. The vendor shall adhere to the principle of least functionality and install only software that is necessary to support the function of the SuC.
4. Software shall conform to the least privilege configuration principle and be granted only 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 that 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 (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 be installed only 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 section 21.1 of this agreement, "Log collection."
13. Vendor-produced or OEM-acquired software shall be cryptographically signed before installation on the SuC.
14. The vendor shall perform 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 processes and procedures to monitor information sources for the public disclosure of vulnerabilities.
16. The vendor shall provide full configuration backup of the 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 system choice for the SuC components, the vendor shall follow the CIS Security Technical Implementation Guides (STIGs) to securely configure operating systems for all operating system installations.
2. The vendor shall be responsible for maintaining operating system 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 clearlisting 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 agreement 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 Section 14.1 of this agreement, "Access control."
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 run only hypervisor vendor–approved software packages.
7. All components of virtualization environments 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 (RPOs and RTOs)
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 actions in sections 9.5.1 and 9.5.2 of this agreement 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 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 cache 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 be permitted only 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 clearlisting 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 target security level of the SuC as documented in Section 3.4 of this agreement, "Detailed cyber risk assessment."

11. Availability

Availability in the context of cybersecurity is the ability of the SuC to operate reliably while containing and "fighting through" cyberattacks and general OT and IT component failures. Resilient system architecture that

incorporates redundant systems and other workarounds to compensate for failed components helps to ensure 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 failure.
2. The vendor shall maintain a critical spare inventory.
3. The vendor shall design highly resilient information systems as described in Section 23 of this agreement.
4. The vendor shall design and implement a fault-tolerant system with redundant communication pathways to ensure that 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 23.1 of this agreement.
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 be used only 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, Part 1, 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 elements in sections 14.1 and 14.2.

14.1 Access control

The vendor shall establish and maintain an access control program to ensure that only authorized access is allowed to the SuC, its subsystems and its 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.

1. The SuC, its subsystems and its components shall require authentication and authorization prior to allowing access.
2. The vendor shall configure the SuC, its subsystems and applicable components with options for integration with the authority's single sign-on system.
3. 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.
4. The vendor shall configure the SuC, its subsystems and applicable components with support for FIDO2 U2F-based authentication.
5. 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.
6. If the SuC is not connected to the authority's 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.
7. The vendor shall establish identity management that uniquely identifies authorized people, processes and devices.
8. Field I/O level (Purdue Level 0) devices incapable of authentication require mitigating security controls to detect incorrect or malicious data.
9. The concept of least privilege shall be employed with a user account hierarchy in place.
10. The vendor shall provide documentation for the user, groups and role management and define security privileges and permissions.
11. The vendor shall perform account recertification and access reviews at least once every 30 days.
12. When feasible, access revocation and account deprovisioning shall be automated based on rules approved by the authority.
13. The vendor shall revoke access to accounts immediately upon termination of employees or change of roles.
14. All access from a less secure zone or network shall be challenged according to the FIDO2-based authentication specification.
15. Access for processes from a lower security zone to a higher security zone shall be logged and controlled.
16. Where feasible, the vendor shall 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.

17. The vendor shall ensure that access enforcement shall not adversely impact the operational performance of the SuC.
18. The vendor shall configure the SuC to log account usage to support monitoring of atypical account activity.
19. 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 principle of least privilege when granting privileged access.
2. All privileged access shall follow the request/evaluation/approval/denial process.
3. All privileged access authorizations 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 six 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 function 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 hard-coded 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. Service accounts shall be restricted to access only the systems the accounts are intended for.
16. Service accounts shall be denied interactive access to systems.
17. Service accounts where passwords have not changed for six 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 log-ins using the same authentication credentials, allow applications to retain log-in information between sessions, provide any autofill functionality during log-in, or allow anonymous log-ins.

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 that 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 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 support an ability to securely monitor 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 access control lists, 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 the 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., every 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 have operational impacts (e.g., reboots). The device shall receive accurate time as defined in the Section 12 of this agreement, "Time synchronization."

19. The vendor and authority shall agree on acceptable encryption protocols and secure communication processes appropriate for each target security level. 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 its 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 configurations shall be treated as privileged access.

16.1 Wireless network 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 preconfigured 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 "allowlist" authorized devices to prevent connection by rogue devices.
7. Wireless controllers shall be configured to detect rogue access points and rogue deployment locations, and shall 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, be 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.
13. The vendor shall provide a security plan to the target security level according to the zone 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 for 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 provide 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 traverses 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 that 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 log-ins and log-outs shall be logged in the authority's centralized logging system, including all metadata associated with the access transaction.
5. Remote log-ins shall require the use of strong multifactor authentication.
6. Remote access shall be possible only from a predefined clearlisted set of IPs.
7. Default remote log-in 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 five 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 programs to protect all onboard SuCs 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 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 gray-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 passenger information system controllers (with external access)—shall be monitored by a host-based intrusion detection system.
7. Onboard 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:
    a. train control and safety-critical systems;
    b. operational systems; and
    c. passenger-facing systems (such as Wi-Fi 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; and
    c. the authority's staff (whether train crew or maintenance staff).

11. Patching 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 operating 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 life cycle management

The vendor shall create a program to manage the life cycle of the SuC, its subsystems and its components. The program shall ensure that all components of the SuC remain under the available support of the OEM. Throughout the design life of the SuC, the vendor shall be responsible for maintaining all components, including those provided by third-party providers. Planned obsolescence found in IT components may not extend to SuC components.

1. The SuC, its subsystems and its components shall not reside on end-of-life operating systems or 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 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 of the SuC.
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 thorough regression testing to ensure that updated components work as expected when introduced to the operating environment.
8. The vendor shall perform security testing and validation after components have been replaced, including 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 life cycle, 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 the following:
    a. Processes for local and remote repairs, in accordance with existing authority policies and other sections of this agreement.
    b. Identification of maintenance tracking tools that facilitate scheduling, authorizing, monitoring and auditing repair activities for the SuC.
    c. Use of 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:
    a. Enumeration of all potential performance issues related to transitioning from old software to supported software, and plans to mitigate all identified performance issues.
    b. Description of when and how the old software will be decommissioned.
    c. Description of which, if any, software components, including library files and/or data, will be preserved.
    d. Description of which, if any, documentation related to the old software will be preserved.
    e. Description of disposal processes for old software documentation.
    f. Identification of vendor primary and backup points of contact for all service and support during the disposition timeline.
14. The vendor shall ensure the following:
    a. Security functionality shall be updateable without negatively affecting safety functions.
    b. The lifetime of the safety system shall be 25 years minimum.
    c. The security-relevant functionality shall be replaceable without replacing the full safety system.
    d. 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.

19.1 Supply chain security

The vendor shall institute a program to ensure that supply chain risks are managed in a manner that guarantees the integrity and 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 its 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 preconfigured, the cabinet is to be delivered to the authority and installed sealed.
4. Tampering shall be recognizable on all seals.
5. The information-processing devices must provide a secure boot including field-programmable gate array (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.

19.2 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 does not infringe on Section 7613 or future provisions, limiting the use of FTA funds or local funds to procure rolling stock.
3. The vendor shall not source any material, components or subcomponents from a supplier that is "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. The U.S. International Trade Administration's list of designated non–market economy countries is 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.

19.3 Software origins

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

19.4 Software bill of materials (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 is 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 emergency patching or bug fixes require the vendor to deploy software different from the SBOM, the vendor shall supply the authority with a revised SBOM within seven days of the deployment of the emergency patch.
3. The vendor shall provide an 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.

19.5 Hardware bill of materials (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.

20. Non-production 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 non-production 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 in this section.

21. 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 after a cybersecurity incident.
8. The vendor shall incorporate lessons learned from incidents to strengthen the SuC's security posture.

21.1 Auditing

The SuC, its subsystems and its 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 the 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 that enables detailed troubleshooting and diagnostics.
4. The vendor shall provide the authority and update as needed 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.

21.2 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 shall be synchronized across logging systems to ensure that 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 the log desk/quota nears its limit by two 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.

21.3 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 for 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 one 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 its components to enable threat and anomaly detections that perform the following functions:
    a. Detect and prevent unauthorized system intrusion.
    b. Detect and prevent unauthorized system modification.
    c. Detect denial-of-service attacks.
    d. Detect unplanned shutdowns.
    e. Detect unexpected remote log-ins.
    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.

21.4 Tabletop exercises

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

22. 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.
3. A yearly plan to train and maintain personnel necessary to fulfill SuC implementation and operational duties in a structured, secure and measurable manner.
4. Labs and methods to train personnel on SuC functions and services in a controlled and supervised manner before deployment to the authority's service.
5. 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. Security and safety 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. Rollout of 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, and address and monitor the progression of laggers (i.e., users who show weak/poor understanding of their security responsibilities) over time.
p. Reiteration of users' responsibility to abide by the NDAs signed by them, necessitating the protection of the vendor, authority and vendor-associated client information disclosed to them before, during and after onboarding.

23. 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 system 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 failures (MTBF) 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 the processes, tools and personnel needed to meet the uptime and performance goals set forth by the authority for the SuC.

23.1 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 recovery point objective (RPO) 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 that it has personnel with the expertise 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 in accordance with NIST SP 800-34 Rev. 1 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.

24. 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 the following:

1. System documentation detailing:
    a. detailed, as-built system documentation;
    b. operational and functional requirements of the system;
    c. performance and capacity requirements; and
    d. standard and safe operating thresholds.
2. Evidence of compliance with defined target security levels.
3. Test results of a full scope penetration test of the fully built SuC.
4. Current results of DCRA, including:
    a. assumptions;
    b. threat intelligence sources;
    c. threat scenarios;
    d. risks mitigated;
    e. results of independent penetration or controls testing to demonstrate the effectiveness of current security countermeasures;
    f. results of testing the resiliency of countermeasures;
    g. training of authority personnel and knowledge transfer;
    h. standard operating policies, procedures and playbooks;
    i. status of residual risks; and
    j. enumeration of accepted risks and associated justifications.

25. System retirement

25.1 Migration of system functionality

1. At the end of the SuC life cycle, all in-service system functionality shall be documented, or existing documentation shall be reviewed. This shall be 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 shall be tested, in a non-production environment, to the extent practicable.

25.2 Hardware disposal

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

25.3 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.

26. 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 that changes did not 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.

27. 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 B: NATCA agreement Appendix 2

List of tables

Appendix 2 Table 1, List of Abbreviations 42
Appendix 2 Table 2, List of Assumptions 44
Appendix 2 Table 3, SuC Components 46
Appendix 2 Table 4, SuC Overview 47
Appendix 2 Table 5, Protection Class Definitions 48
Appendix 2 Table 6, Predefinitions for the Application Protection Requirements Assessment 50
Appendix 2 Table 7, Application Protection Requirement Result 50
Appendix 2 Table 8, Definition of Exposure and Vulnerability 51
Appendix 2 Table 9, Definition of Impact 52
Appendix 2 Table 10, Risk Matrix 52
Appendix 2 Table 11, Initial Risk Assessment Result 52
Appendix 2 Table 12, APR and IRA Combined Results 53
Appendix 2 Table 13, Zones 54
Appendix 2 Table 14, Zone Communication Matrix 57
Appendix 2 Table 15, Conduits 57
Appendix 2 Table 16, Attacker Knowledge and Resources 58
Appendix 2 Table 17, Threat-FR Mapping 62
Appendix 2 Table 18, Component SL-T Ratings 63
Appendix 2 Table 19, Actual Risk 65
Appendix 2 Table 20, SR application 65
Appendix 2 Table 21, Additional countermeasures 65
Appendix 2 Table 22, DRA Results from Z01_HVAC_HMI 66
Appendix 2 Table 23, Public Vulnerability Databases 68
Appendix 2 Table 24, Vulnerability Database 68
Appendix 2 Table 25, Countermeasure Deployment Requirements 70

List of figures

Appendix 2 Figure 1, System Under Consideration 46
Appendix 2 Figure 2, Security Process for an Initial Zoning Concept 54
Appendix 2 Figure 3, Initial Zone Concept 55
Appendix 2 Figure 4, Climatic Zone 55
Appendix 2 Figure 5, Attacker Definition Process 58
Appendix 2 Figure 6, Zoning Concept with Security Gateway 67

List of abbreviations

Abbreviation	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

Abbreviation	Description
CENELEC	European Committee for Electrotechnical Standardization
CISA	Cyber Security and Infrastructure Agency
CMDB	configuration management database
CP	Control Panel
CS	control system
CVE	Common Vulnerabilities and Exposures
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 conditioning
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 target security level
LDAP	Lightweight Directory Access Protocol
LRA	local root account
NDA	nondisclosure agreement
NIST	National Institute of Science and Technology
NTP	Network Time Protocol
OC	Operations Center
OT	operational technology
PKI	public key infrastructure
POA&M	Plan of Action and Milestones
PTC	positive train control
RA	resource availability
RAMS	reliability, availability, maintainability and safety
RDF	restricted data flow

Abbreviation	Description
RDP	Remote Desktop Protocol
SI	system integrity
SIEM	security information and event management
SL	security level
SL-T	target security level
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
WI-FI	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 (including driver car/cab) to measure the actual temperatures
A_04	HVAC thermostats are in each wagon of a train (including 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 operations center have control over each individual wagon of a train
A_07	A fleet is remotely controlled by the HVAC operations center
A_08	The driver has permanent monitoring possibilities for all individual zones from the train they are 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 3 through 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 demonstrate the compliance process via hypothetical examples. An actual implementation will 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 cyberattacks. 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 section, 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.

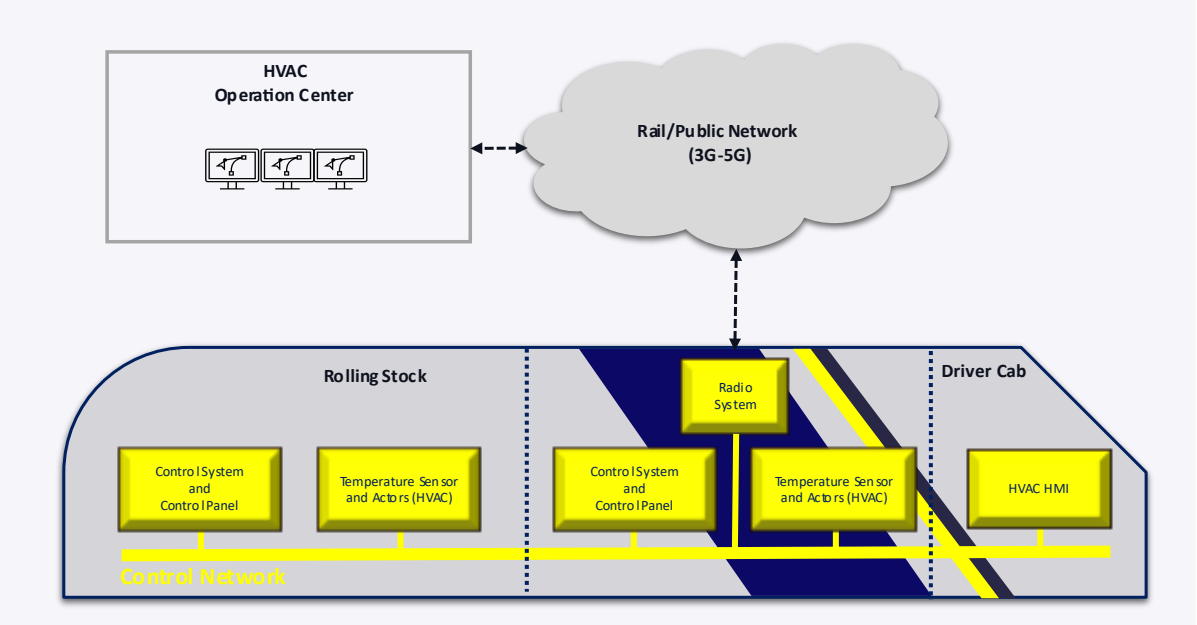
The following process steps based on IEC 62443, TS 50701 and best practices are used:

- 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, ventilation 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 operations 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 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 operations 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 Wi-Fi 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 operations 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

U.S. security legislation is used.

2.7 List of assumptions and justifications for the SuC

For the full list of assumptions, please refer to Table 2.

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:** See Table 5.
- **Predefinitions to cover relations between the security targets and safety:** See Table 6.

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 or 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 aspects may be relevant in the assessment end customer service provision and 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, loss of political trust.	Individuals may suffer minor injuries if the system fails.

Category/ Protection Class	Financial Impact	Privacy Violations	Violation of Laws, Regulations, and Rules	Disruption of Business Activity	Loss of Reputation	Health Damage
Middle	Tolerable financial damage. The financial thresholds are defined by the CISO or 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 aspects may be relevant in the assessment: end customer service provision and 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, loss of 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 or 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 aspects may be relevant in the assessment: end-user service delivery and 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, loss of 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.

Category/ Protection Class	Financial Impact	Privacy Violations	Violation of Laws, Regulations, and Rules	Disruption of Business Activity	Loss of Reputation	Health Damage
Very High	Existence-threatening damage. The financial threshold values are defined by the CISO or the CEO, taking into account 1:4 and external turnover.	There is a high need for protection, and 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 and 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, loss of political trust.	If the system fails, many people can be killed.

Appendix 2 Table 5, Protection Class Definitions

The following pre-definitions were used for the assessment of the protection requirements.

ID	Pre-Definitions
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 brake.
PD_05	Availability is set to high if a non-availability in one train is linked to a fleet fail.

Appendix 2 Table 6, Pre-Definitions 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

ID	Component Name	Confidentiality	Integrity	Availability
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 1, 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 possible only for a small group of attackers with high hacking skills (high capabilities needed). • Vulnerability is exploitable only 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 (low 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 operations disturbed for more than one week.	Could lead to the organization's bankruptcy
B	Several severe or critical injuries	Most operations are disturbed between one day and one week. Important operation disturbed for more than one week.	Impact in a significant way the organization's annual budget (>10% of revenue)
C	One severe injury or several injuries requiring hospitalization	Most operations disturbed between one hour and one day. Important operation disturbed between one day and one 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 one 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:

	Impact			
Likelihood	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 zone and conduit 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:

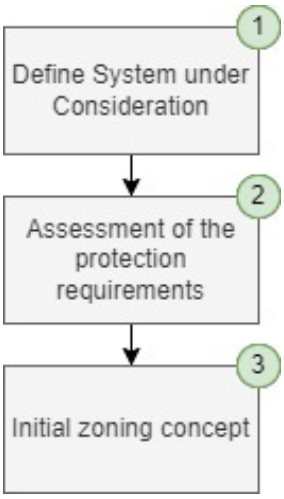
- components and systems with the same or similar protection requirements
- components and systems with similar operational and functional aspects at one location

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 Section 6.1 the following zones are defined.

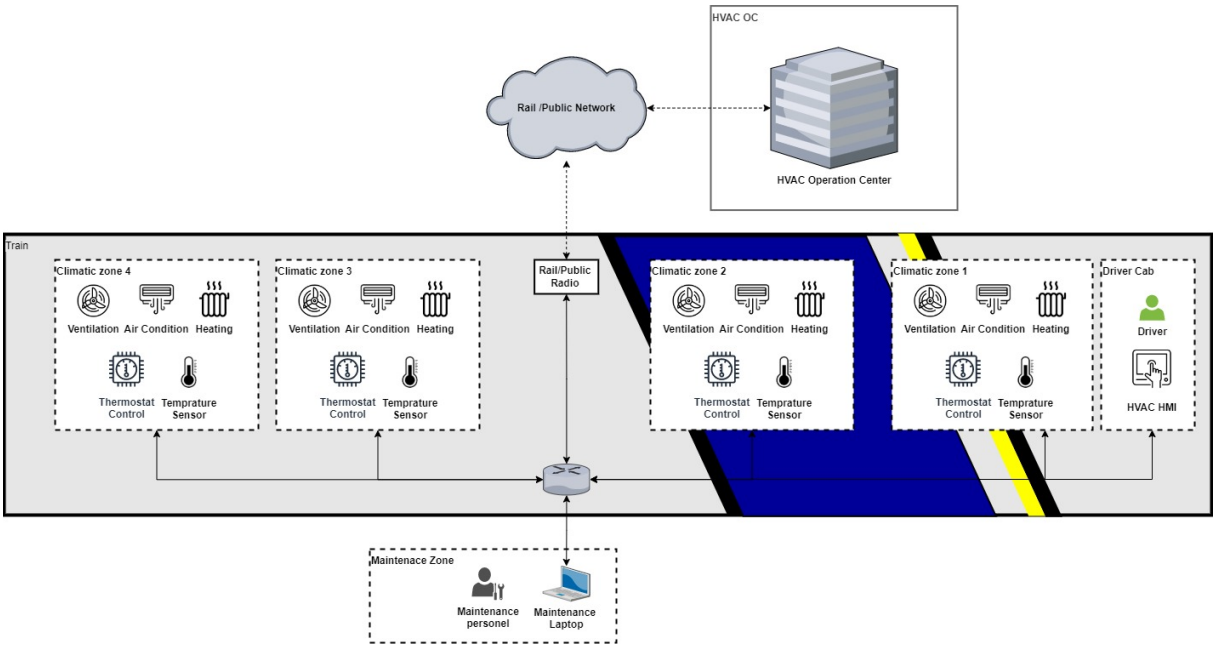
ID	Zone	Component/Subsystem	Reason
Z_01	HVAC HMI	HVAC HMI	Location, APR/IRA, Function
Z_02	Climatic Zone 1	SS, HS, AVS, AC, CS, CP	Location, APR/IRA, Function
Z_03	Climatic Zone 1+n	SS, HS, AVS, AC, CS, CP	Location, APR/IRA, Function
Z_04	Radio	RS	Location and Function
Z_05	Maintenance Zone	Maintenance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

Appendix 2 Table 13, Zones

In sections 6.3.1 to 6.3.6, a short zone description is provided.

6.3.1 Initial zone concept

The following figure shows the initial zone concept.



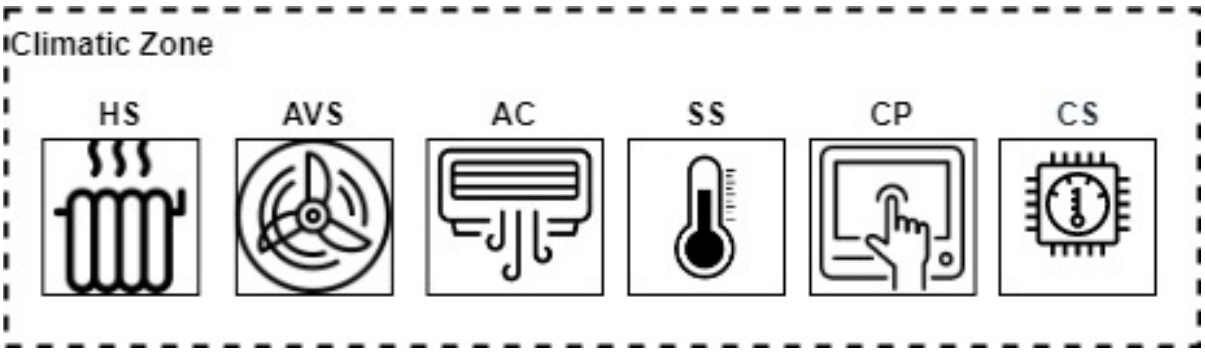
Appendix 2 Figure 3, Initial Zone Concept

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 4, Climatic Zone

6.3.3.1 Sensor system (SS)

The main function is to measure the actual parameters (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. 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.

6.3.3.3 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. 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 or a 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. 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.

6.3.3.5 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. 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.

6.3.3.6 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. 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.

6.3.4 Radio zone

The main function is to provide the interface to the HVAC operations 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. 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.

6.3.5 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.

6.3.6 HVAC OC

The main function of the HVAC operations 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.

Misadjustment may cause medium financial damage due to the ability to control multiple wagons or multiple trains. Misadjustment may cause high reputational loss nationwide or even worldwide if news of the cyberattack is published publicly.

Individuals may suffer in each train, and the interruption of operation of an entire fleet is very likely.

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 Maintnance Zone	X	X	X	X	-	-
Z_06 HVAC OC	X	-	-	X	-	-

Appendix 2 Table 14, Zone Communication Matrix

The resulting conduits are presented in the table below:

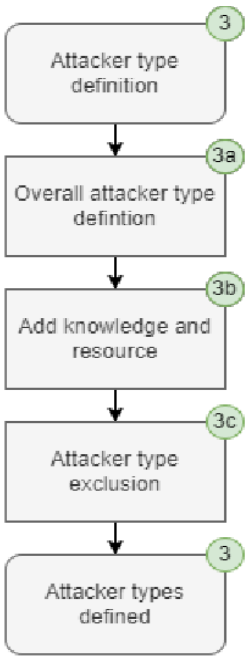
ID	Conduit	Zone 1	Zone 2
C_01	HMI -CZ 1	Z_01 HVAC HMI	Z_02 Climatic Zone 1
C_02	HMI -CZ 2	Z_01 HVAC HMI	Z_02 Climatic Zone 2
C_03	HMI -Radio	Z_01 HVAC HMI	Z_04 Radio
C_04	HMI -MZ	Z_01 HVAC HMI	Z_05 Maintenance Zone
C_06	CZ 1 -MZ	Z_02 Climatic Zone 1	Z_05 Maintenance Zone
C_07	CZ 2 -MZ	Z_02 Climatic Zone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

Appendix 2 Table 15, 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 that could cause certain threats.



Appendix 2 Figure 5, 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 that 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 recheck 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 16, 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 SL-Ts, 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 (target security level) 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 subsections:

- Establishment of the threat catalog
- 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 whether 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 that 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), 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.

8.2 Threat mapping to the foundational requirements

In this step, each threat (based on the catalog) must be mapped to the foundational requirements (FRs) from IEC 62443. This is to ensure that 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 17, 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 zone 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 threat catalog, an assessment of relevance and impact, and consideration of 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_Maintenance_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 18, 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 19, 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 20, 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 21, Additional Countermeasures

The whole process is described below.

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						System Requirements - 7c	Risk Assessment - 7d						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
0.0.8 Failure or Disruption of the Power Supply	TRE; RA	Yes	2	2	3	C	Medium	1	SR 6.1; SR 6.1 RE1; 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
0.0.9 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 RE1	2	1	2	C	Low	0		1	1	1	C	Low	0
0.0.14 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
0.0.15 Eavesdropping	IAC; UC; DC; RDF;	Yes	2	2	3	D	Low	0		1	1	1	D	Low	0		1	1	1	D	Low	0
0.0.16 Theft of Devices, Storage Media and Documents	DC; TRE; RA	Yes	2	2	3	C	Medium	1	SR 1.1; SR 1.1 RE1; SR 1.3; SR 1.7; SR 4.1; SR 4.1 RE1; SR 4.3; SR 6.2	2	1	2	C	Low	0		1	1	1	C	Low	0
0.0.17 Loss of Devices, Storage Media and Documents	DC; TRE; RA	Yes	2	2	3	C	Medium	1	SR 1.1; SR 1.1 RE1; SR 1.3; SR 1.7; SR 4.1; SR 4.1 RE1; SR 6.2	2	1	2	C	Low	0		1	1	1	C	Low	0
0.0.18 Poor Planning or Lack of Adaptation	SI; DC; TRE; RA	Yes	2	2	3	C	Medium	1	SR 1.1; SR 1.1 RE1; SR 2.1 RE 2; SR 5.1; SR 5.1 RE1; SR 5.2; SR 5.2 RE1; SR 6.1 RE 1; SR 6.2	2	1	2	C	Low	0		1	1	1	C	Low	0
0.0.19 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
0.0.20 Information or Products from an Unreliable Source	SI;	Yes	2	2	3	B	Significant		SR 3.1; SR 3.1 RE1 ; SR 3.2; SR 3.2 RE1; SR 3.2 RE2; SR 6.2	2	1	2	B	Medium	1	ORG 1.6; ORG 2.3	1	1	1	B	Low	0
0.0.21 Manipulation of Hardware or Software	IAC; UC; SI; DC; RDF; TRE; RA	Yes	2	2	3	B	Significant		SR 1.1; SR 1.1 RE1; 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 RE1; SR 2.3; SR 2.4; SR 2.5 ; SR 2.8; SR 2.9; SR 2.11; SR 3.2; SR 3.2 RE1; SR 3.2 RE2; SR 3.3; SR 3.3 RE1; SR 3.4 ; SR 3.4 RE1; SR 3.5 ; SR 3.6 ; SR 3.7; SR 3.9; SR 5.1; SR 5.1 RE1; SR 5.2; SR 5.2 RE1; SR 6.2; SR 7.3; SR 7.3 RE1; SR 7.3 RE2; SR 7.4	1	1	1	B	Low	0					B		0
0.0.22 Manipulation of Information	IAC; UC; SI; RDF; TRE; RA	Yes	2	2	3	B	Significant		SR 1.1; SR 1.1 RE1; SR 3.1; SR 3.1 RE1 ; SR 3.2; SR 3.2 RE1; SR 3.2 RE2; SR 3.9 ; SR 5.1; SR 5.1 RE1; SR 7.3 ; SR 7.3 RE1; SR 7.3 RE2; SR 7.4	1	1	1	B	Low	0					B		0
0.0.23 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 RE1; 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 RE1; SR 2.1; SR 2.1 RE1; SR 2.1 RE2; 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

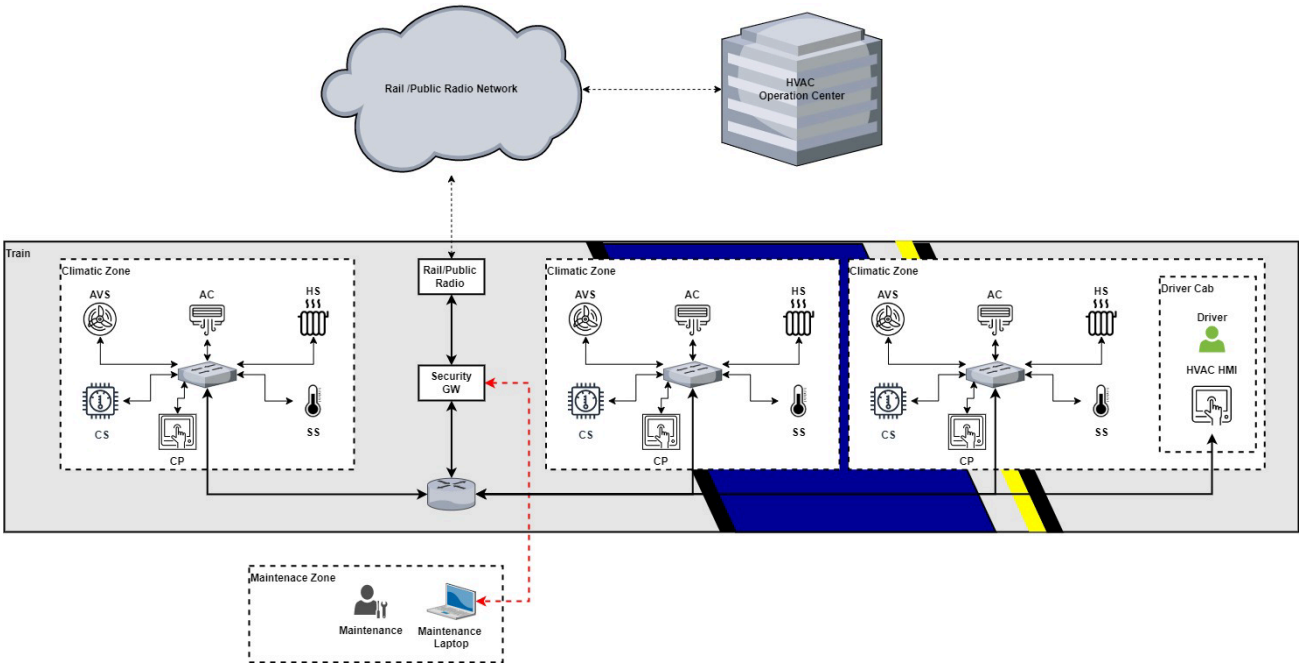
Appendix 2 Table 22, DRA Results from Z01_HVAC_HMI

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 (boundary protection, IAM, etc.) must be implemented.



Appendix 2 Figure 6, Zoning Concept with Security Gateway

11. Vulnerability discovery, reporting and assessment overview

This section describes the 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 life cycle. The vendor tailors the vulnerability management program to integrate into the authority's existing security and safety technology infrastructure. If such integration is not feasible, the vendor works with the authority to provide an independent solution that is compatible with the authority's existing security program. The 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. The 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. The 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. The vendor regularly consults publicly available vulnerability databases such as those listed in Table 23 below 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 23, Public Vulnerability Databases

Furthermore, the 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 24 below is a sample of the data contained in the vulnerability management database. The vulnerability management database supports monitoring and scanning tools to ensure that 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 24, Vulnerability Database

The 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, the vendor routinely conducts risk assessments as described in Section 9. Through its risk assessment process, the vendor previously identified the SuC operations center software and radio components as high-risk components due to their larger threat exposure. As such, the vendor targeted these systems for in-depth, independent analysis by an industry-leading OT 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 operations center through denial-of-service (DoS) attacks. The 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 operations center. Wagon components can operate indefinitely with the most recent instructions and schedules received from the operations center, and therefore a DoS attack on either the operations 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 members 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 onboard 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 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 in the operations 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 that the overall functioning of the SuC is not impacted. Considering the thorough testing and ability of both the operations 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 operations 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 the 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 operations 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. The

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 that 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

The 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 time frame 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.

The vendor prioritizes the development of patching or other mitigating controls according to the vulnerabilities risk score and the timelines listed in Table 25. All recommended patches and other mitigations come with instructions to assist the authority with automated deployment and monitoring.

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 25, Countermeasure Deployment Requirements

11.5.1 Vulnerability report

A vulnerability report is the primary communication vehicle and formal record of the 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 to the likely threat, the steps required to exploit it and the general sophistication required. 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.

This section of the vulnerability report also includes these subsections:

1. **Mitigation testing results:** All testing procedures performed to validate the effectiveness of the mitigation/security control and document its own implementation risk.
2. **Remediation steps:** A step-by-step guide to direct the 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. The 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. The vendor reports safety-impacting vulnerabilities to the authority within one day of becoming aware of them. While the 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 the vendor and authority-appointed stakeholders, the vendor creates an email distribution group specific to safety vulnerabilities. The vendor assists the authority with technical expertise and experience controlling the response life cycle from start to finish, guided by the NIST SP 800-40r4 standard.

The 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, the 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, the 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 that no new vulnerabilities are introduced and that 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 that risk is effectively reduced to acceptable levels going forward.

11.7 Vulnerabilities impacting safety disclosure

The vendor releases safety-impacting vulnerability information publicly only after a patch or other mitigation is provided to the authority. The vendor requires a nondisclosure agreement with the authority intended to ensure that the vendor maintains purview over public disclosure. Additionally, the vendor requests written acknowledgment that information on both the vulnerability and appropriate mitigations are received by the authority once provided. The 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 the vendor's vulnerability testing team. Once an NDA is completed, the vendor will work with the authority on the timing of public disclosure to limit the authority's threat exposure of operational systems.

However, if an SuC vulnerability that impacts safety is disclosed publicly by some other source outside of the 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 the vendor as described in Section 11.6.

In most cases, vulnerabilities are first detected by the vendor or an SuC third-party manufacturer, and the vendor has full control or influence on the timing of public disclosure. The vendor maintains agreements with all major SuC subcomponent 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 the vendor is contracted to manage vulnerability enumeration, the vendor will collaborate with the authority to develop a vulnerability scanning schedule. Credentialed vulnerability scanning of the operations 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 operations 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, the 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, the 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.

The 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, the 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 the vendor according to the process described in Section 11.5.

11.9 Authority or appointed third-party vulnerability scan

If the authority contracts the vendor to manage SuC security services, then the 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. The 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. The vendor maintains all required licenses to scan and analyze subcomponents 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 the vendor no closer than 30 days before the intended test date to ensure that 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 agreement 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
SuCs 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 × 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 operations center. In addition, physical enclosures should be inspected for signs of tampering. Any unlocked enclosures should be re-secured to prevent access to the thermostat's USB port.

12. Security patching and mitigation governance

The vendor provides SuC patch deployment and security mitigation support to the authority to include support for all third-party manufactured subcomponents. If the authority patch deployment tooling is available for use, the vendor will provide support for its configuration and integration with the SuC. In addition, the vendor provides training and reference documentation for the operation of the provided tool with the SuC and documents any SuC configuration changes required for compatibility. If existing tooling is not available, the 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. The 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, the vendor recommends the VulPatch system described in Section 12.5.

The SuC is designed with a centralized operations 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 operations center maintain continuous communication through the cellular radio. The SuC's operations 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 operations 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 operations 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 reestablished 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 be performed only while the train is in the depot. The patching is coordinated by the OT security team and planned through the TMS.

The vendor recommends the automated patch management system operate at level 3 of the Purdue model, as does the SuC operations center. While the operations 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 operations center and system patching/updating. For increased security, the 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. The 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 the authority's broader patch management program. The 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, the 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 roll back 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 take approximately two minutes to complete, before putting the system into service.

The operations 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 check the operations center.

12.3 Patch testing (Requirement 6C)

The vendor thoroughly tests all patches and updates in an 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 composed of physical SuC components, including the operations 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.

The 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, the 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)

The 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. The vendor provides detailed instructions and checklists to guide manual installation. For automated patching, the vendor provides all necessary technical configuration guidance and best-practice suggestions to enable efficient and comprehensive patching.

In addition, the vendor supports the development of standard operating procedures to assist the authority with the patch deployment process specific to its chosen patch deployment system. The 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, the vendor creates 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, the 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 that 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 the 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 multifaceted system assembled of a diverse composite of hardware and software products. The 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. The 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, but it is also 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 nonstandard 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 12.6, the vendor maintains detailed records and closely manages configuration and version dependencies. This allows the vendor to forecast obsolescence and prepare for it through system engineering and testing of updated software versions, software replacements or other workarounds. For example, the operations center relies on the Microsoft Net framework, currently at version 7.0. Microsoft will stop supporting version 7.0 in May of 2024, and the 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.

The 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 the 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 recordkeeping 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 11.10.
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, the vendor will provide third parties with patches and mitigation methodologies for the SuC. The vendor closely manages the public release of patches to ensure authority, and that 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 the vendor restricting the release of patch and vulnerability information will be asked to sign an NDA. Additionally, the vendor is restricted by similar

agreements with some SuC component manufacturers, and the vendor will seek approval from these manufacturers to release their patches to the authority's requested third party. Subcomponent 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. The 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 that all complications are detected at the earliest possibility. The 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)

The vendor supports and maintains the SuC through its entire life cycle. The vendor's SuC maintenance program includes updating and patching software to offer new features or remediate vulnerabilities. The 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, the 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 time frame as listed in Table 25, "Countermeasure Deployment Requirements." The vendor develops mitigations within the time frame required. This may require the vendor to develop an immediate stopgap 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. The 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 the vendor does not receive a third-party patch within the time frames required, the 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, the vendor could release a temporary software update that forces users to reauthenticate on each operations center log-in attempt, thereby preventing the use of the hijacked session credentials.

3. Methods to monitor the effectiveness of patching are developed and implemented during the 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 test 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 that some impact is expected, the vendor provides either an additional patch or a 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 that no new vulnerabilities or security weaknesses are introduced. The testing process includes static code analysis and active red team testing. As a result, the 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 the vendor for release, it is submitted to the authority's Change Management Board for review. If the vendor is contracted to manage the authority's patch deployment process, the 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 Table 25.

Appendix C: Introduction to SBOM and resource materials

A *software bill of materials* (SBOM) has emerged as a key building block in software security and software supply chain risk management. An SBOM is a nested inventory, a list of ingredients that make up software components. While not a brand-new concept, the ideas and implementation have advanced since 2018 through a number of collaborative community effort, including the National Telecommunications and Information Administration's (NTIA) multistakeholder process.

CISA is advancing the SBOM adoption and practices by facilitating community-led work, with a focus on scaling and operationalization, as well as tools, new technologies, and new use cases. This website will also be a nexus for the broader set of SBOM resources across the digital ecosystem and around the world.

An SBOM-related concept is the Vulnerability Exploitability eXchange (VEX). A VEX document is an attestation, a form of security advisory that indicates whether a product or products are affected by a known vulnerability or vulnerabilities.

CISA also advances the SBOM work by facilitating community engagement to advance and refine SBOM, coordinating with international, industry and interagency partners on SBOM implementation, and promoting SBOM as a transparency tool across the broader software ecosystem, the U.S. government, and the world. Agencies can reach out to CISA with any questions at SBOM@cisa.dhs.gov.

As the idea of an SBOM has grown and matured, guidance has emerged to help clarify concepts, guide implementation, share insights and address related issues. This CISA site aims to collect guidance documents from a number of sources, including the CISA community-led work publications, the earlier National Telecommunications and NTIA multistakeholder process, guidance from CISA and other federal agencies, and other relevant policy documents from governments around the world.

