INTELLIGENT TRANSPORTATION SYSTEMS (ITS) SECURITY CONTROL SET FOR TRAFFIC SIGNAL CONTROLLERS

www.its.dot.gov/index.htm

Final Report – July 31, 2023

FHWA-JPO-23-121

U.S. Department of Transportation

Produced by (Name of Contract)
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
(List all USDOT agencies sponsoring this report; only list one agency on the report cover)

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Technical Report Documentation Page

1. Report No.

FHWA-JPO-23-121

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle

Intelligent Transportation Systems (ITS) Security Control Set for Traffic Signal Controllers

5. Report Date

July 31, 2023

6. Performing Organization Code

V-337

7. Author(s)

Randy Gabel, Christina Sames, Hector Martinez, Pam Miller, Dr. Michaela Vanderveen

8. Performing Organization Report No.

9. Performing Organization Name and Address

U.S. DOT Volpe National Transportation Systems Center
220 Binney Street
Cambridge MA 02142

10. Work Unit No. (TRAIS)

11. Contract or Grant No.

IAA 693JJ320N300058

12. Sponsoring Agency Name and Address

ITS-Joint Program Office
1200 New Jersey Avenue, S.E.
Washington, DC 20590

13. Type of Report and Period Covered

Final Report August 28, 2020 – August 27, 2023

14. Sponsoring Agency Code

HOIT-1

15. Supplementary Notes

This work was performed in collaboration with the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) and the MITRE Corporation.

16. Abstract

This control set document identifies security controls typically needed to mitigate security risks to traffic signal controllers operating in the role of ITS Roadway Equipment (ITSRE) described by the Connected Vehicle Traffic Signal System service package in the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) TM04. The objective of this control set is to provide a means to better protect the traffic signal controller and the information flows supported by its interfaces as more advanced features are added.

The controls (primarily technical controls) relevant to traffic signal controllers are specified in this control set document. Security controls are safeguards or countermeasures prescribed for a system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

17. Keywords

Intelligent Transportation Systems, Cybersecurity, Control Sets, NIST SP 800-53

18. Distribution Statement

19. Security Classif. (of this report)

unclassified

20. Security Classif. (of this page)

unclassified

21. No. of Pages

154

22. Price

Table of Contents

List of Tables

List of Figures

Chapter 1. Identification

1.1 Purpose, Scope, and Applicability

This control set document identifies security controls typically needed to mitigate security risks to traffic signal controllers operating in the role of ITS Roadway Equipment (ITSRE) described by the Connected Vehicle Traffic Signal System service package in the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) TM04.[1] The objective of this control set is to provide a means to better protect the traffic signal controller and the information flows supported by its interfaces as more advanced features are added.

The controls (primarily technical controls[2]) relevant to traffic signal controllers are specified in this control set document. Security controls are safeguards or countermeasures prescribed for a system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

This control set is intended to be used by system and service managers/owners, system integrators, system engineers, and system component manufacturers to derive security requirements for the traffic signal controller. Therefore, the focus of this control set is on the advanced transportation controller (ATC)[3] implementations, as there is an opportunity for the controls identified in the control set to influence security requirements in standards relevant to the ATC, to drive requirements specifications by system owners/engineers, and to improve security in future ATC implementations. The control set may also be used to identify requirements needed to improve the security of existing or legacy implementations of traffic signal controllers. However, considerable resources would be required to make changes to improve security and organizations (i.e., infrastructure owner/operator’s [IOO’s][4]) typically are not inclined or resourced to make investments in older technology. It may be more efficient to replace older, less secure systems or components.

The scope of this control set is focused primarily on how a typical ATC would be implemented by the ITS community for common use cases using today’s technology. The effort is to identify and select controls that would be applicable to most ATC implementations. Nuances of other implementations (i.e., legacy,

[1] https://www.arc-it.net/html/servicepackages/sp43.html#tab-3.

[2] The technical controls are typically implemented by systems rather than by people.

[3] This control set focuses on devices described in the Institute of Transportation Engineers (ITE) / American Association of State Highway and Transportation Officials (AASHTO) / National Electrical Manufactures Association (NEMA), Advanced Transportation Controller (ATC) Standard 5201 Version 06 or later.

[4] NIST refers generically to “the organization.” This document refers specifically to the IOO, which includes public agencies.

future) may be discussed in the Guidance element of an individual control in **Chapter 4, Detailed Control Specifications**, of this control set.

The risk mitigation and protection provided by other controls[5] implemented in larger systems, operations, or data centers, or by the IOOs operating ITS provide benefit to physical objects that are part of these larger systems, centers, or IOOs. Owners, operators, and users of ATCs may examine the security assessment[6] of the larger system to determine which risks might not be mitigated and/or might be passed on to an ATC itself and then select controls that mitigate that risk. Some controls tagged in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*, as organizational controls are included in this control set because there are aspects of the control that need to be conveyed to the manufacturer/vendor for design and implementation. In some cases, the organizational control is purely non-technical but is so important to successfully securing ATCs that the control cannot be ignored and must be addressed by the IOO before, during, or after an ATC is delivered and installed.

Figure 1 depicts the entirety of the Connected Vehicle Traffic Signal System service package, but the scope of this control set is narrowed to only the ITSRE physical object and its information flows in the red box. More specifically the scope is narrowed to the three functions in the included light brown ITS Roadway Equipment box: Roadway Field Management Station Operation, Roadway Signal Control, and Roadway Basic Surveillance. These may apply to the capabilities or services provided by an ATC.

[5] Examples of these control are policies and procedures; awareness and training; assessments, authorizations, and monitoring; contingency planning, incident response, maintenance, planning, personnel security, privacy, risk assessments.

[6] The assessment reports may be incorporated into the larger system’s risk management process and documentation. Risk management processes are identified in NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, and NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

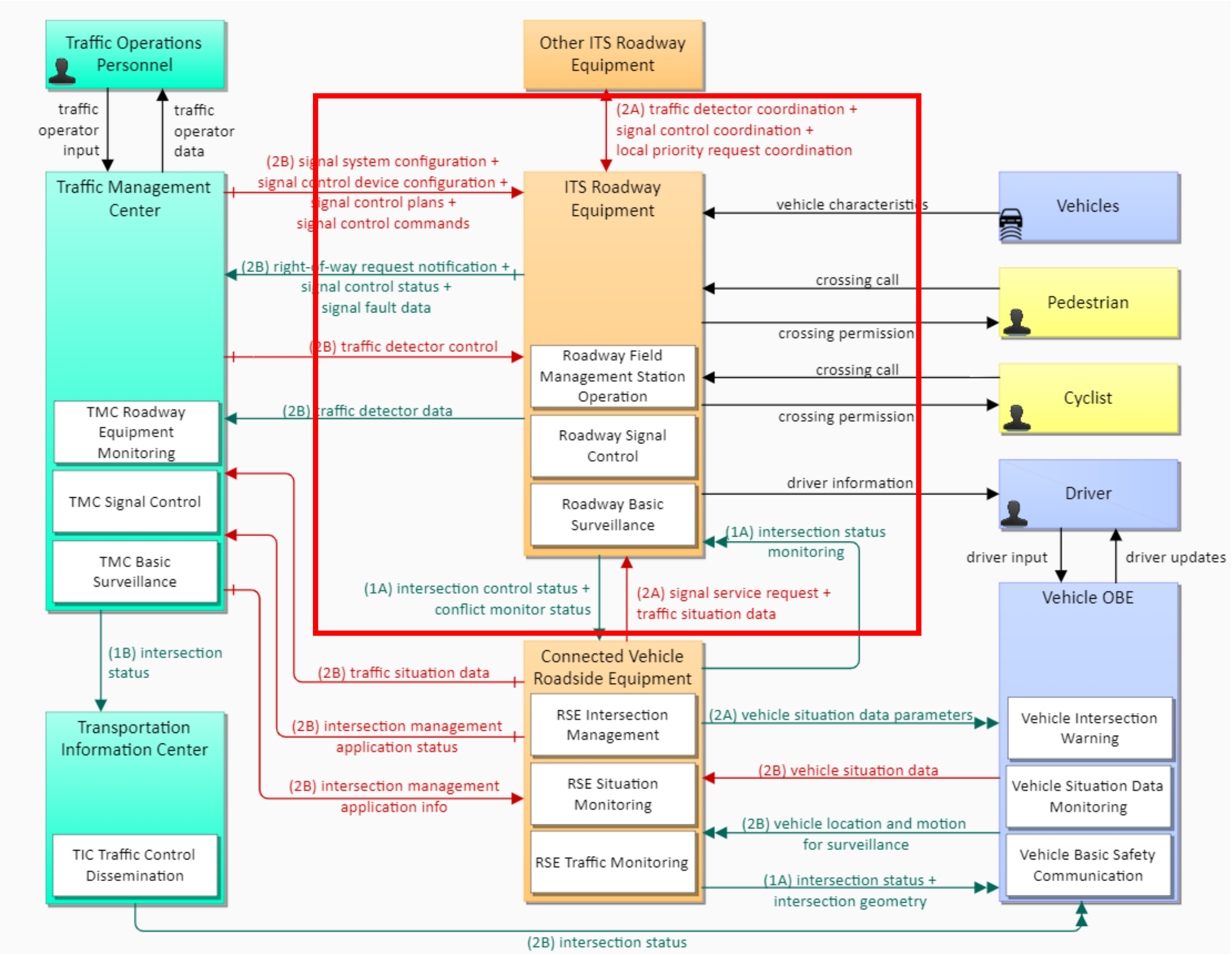
Traffic Operations Personnel
Other ITS Roadway Equipment
traffic operator input
traffic operator data
(2A) traffic detector coordination + signal control coordination + local priority request coordination
(2B) signal system configuration + signal control device configuration + signal control plans + signal control commands
Traffic Management Center
ITS Roadway Equipment
vehicle characteristics
Vehicles
(2B) right-of-way request notification + signal control status + signal fault data
crossing call
Pedestrian
crossing permission
(2B) traffic detector control
Roadway Field Management Station Operation
crossing call
Cyclist
crossing permission
TMC Roadway Equipment Monitoring
(2B) traffic detector data
Roadway Signal Control
TMC Signal Control
driver information
Driver
Roadway Basic Surveillance
(1A) intersection status monitoring
TMC Basic Surveillance
driver input
driver updates
(1A) intersection control status + conflict monitor status
(2A) signal service request + traffic situation data
Vehicle OBE
(1B) intersection status
(2B) traffic situation data
Connected Vehicle Roadside Equipment
Transportation Information Center
(2B) intersection management application status
RSE Intersection Management
(2A) vehicle situation data parameters
Vehicle Intersection Warning
(2B) vehicle situation data
(2B) intersection management application info
RSE Situation Monitoring
Vehicle Situation Data Monitoring
(2B) vehicle location and motion for surveillance
TIC Traffic Control Dissemination
RSE Traffic Monitoring
(1A) intersection status + intersection geometry
Vehicle Basic Safety Communication
(2B) intersection status

Figure 1: Connected Vehicle Traffic Signal System Physical Architecture Diagram

This scope was chosen because of the ubiquitous nature of ATCs, the ITS community's familiarity with ATCs, the constant pace of evolution of the ATC to keep up with traffic modernization goals, and the acknowledged need to identify and codify cybersecurity requirements in standards relevant to the ATC.

This control set is only a starting point for controls selection that informs derivation of security requirements; final control selections and tailoring are guided by the IOO's risk tolerances and may be justified after cost/benefit analyses, as it may not be feasible or affordable to mitigate all risks.

1.2 Revisions

This control set document should be evaluated for revision, when necessary, including when:

- NIST issues new revisions of NIST SP 800-30, *Guide for Conducting Risk Assessments*.

- NIST issues new revisions of NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*.
- NIST issues new revisions of NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*.
- ARC-IT is significantly revised in areas that impact traffic signal controllers.
- Relevant standards are developed or updated.
- Significant changes to technologies are made.
- New threats and/or vulnerabilities are discovered that impact the subject of this document.
- New methodologies for assessing threats and/or vulnerabilities are developed.

1.3 Sources

The following are key resources used to create this document and inform the identification of controls needed to mitigate risk to ATCs. Each listed resource includes a brief context for how it influenced or informed the controls selection.

- ARC-IT version 9.1, for Device Security Classes based on the potential impact to the confidentiality, integrity, and availability of information flows between physical objects and their associated functional objects. (NOTE: the current version 9.1 of controls for Class 3 devices are sometimes cited verbatim, but for some controls this control set contains updates to reflect current recommendations for cybersecurity.)
- NIST SP 800-30, Revision 1, for typical threat sources and vulnerabilities that may be relevant or tailored to apply to ITS.
- Draft NIST SP 800-82, Guide to Operational Technology (OT) Security, for operational technology (was industrial control system) threats and vulnerabilities that may be relevant or tailored to apply to ITS.
- MITRE ATT&CK® version 12, Adversarial Tactics, Techniques, and Common Knowledge, for Industrial Control Systems (ICS) for threat sources’ tactics, techniques, and procedures (TTPs), mitigations, and control mappings that may also be relevant or tailored to apply to ITS.[7]

[7] After this control set was drafted, ATT&CK version 13 was released. Users of this control set should periodically check ATT&CK for updates and identify differences that may affect their control selection or tailoring decisions. ATT&CK is updated twice a year and roughly 6 months apart. Reference the ATT&CK page (https://attack.mitre.org/resources/updates/) for versions to determine the timeframe and a changelog link for each new version, to include minor and major versions for each ATT&CK object type.

1.4 Relationship Between ARC-IT, the Cybersecurity Framework, and Control Sets

Cybersecurity in ARC-IT[8] is addressed through the analysis of the confidentiality, integrity, and availability (C-I-A) required for information flows within each service package. Each information flow need was scored using a Low-Moderate-High (L-M-H) rating. These ratings are then applied to the physical object where the information flow originates or ends, and a device security class is assigned to those objects. Because there could be 27 possible (and potentially untenable) combinations of L-M-H ratings over the C-I-A dimensions, ARC-IT groups the ratings into more manageable five device security classes.[9] Within the ITS Architecture, devices are the building blocks for physical objects; therefore, if the devices that implement a physical object collectively meet a given device class, that physical object does as well. ARC-IT provides a mapping of security controls to each device security class.

The NIST Cybersecurity Framework (CSF)[10] is comprised of cybersecurity outcomes and activities, and mappings of those to cybersecurity best practices. The NIST CSF aligns goals, called Mission Objectives in the Profile, to priority NIST CSF cybersecurity outcomes, activities, and groups of cybersecurity best practices. These cybersecurity best practices, called Informative References by the NIST CSF, are a mapping of existing standards, guidelines, and practices (e.g., security controls) to cybersecurity activities or Subcategories.[11] Prioritized Subcategories communicate which cybersecurity activities and outcomes are most important to leadership and reflect an organization’s business/mission requirements, risk tolerance, and resources. Those priorities can be used to guide efforts to select, tailor, implement, and manage controls over time at the system/program level, especially given limited resources.

The ITS CSF Profile (ITS Profile) provides a risk-based approach for managing cybersecurity activities and reducing cyber risk to and protect the ITS ecosystem. The ITS Profile uses the NIST CSF to align ITS goals (i.e., Mission Objectives) to NIST CSF cybersecurity outcomes and activities. The ITS Profile contains 14 ITS-specific Mission Objectives. For each Mission Objective, the ITS Profile includes the prioritized the CSF Subcategories (i.e., cybersecurity activities) most supportive of that Mission Objective. These Mission Objectives and the prioritized Subcategories reflect input from the ITS community. State and local transportation organizations can use the ITS Profile as a strategic planning tool to communicate priority cybersecurity outcomes within their organization and to other organizations within the ITS community. The ITS Profile’s overall purpose is focused on the high-level strategic and broad actions versus specific requirements implementations and precise actions typically conducted at the system level.

[8] https://www.arc-it.net/html/security/security.html

[9] https://www.arc-it.net/html/security/deviceclasses.html

[10] https://www.nist.gov/cyberframework/framework

[11] While CSF v1.1 Informative References are mapped to NIST SP 800-53 Revision 4 controls, NIST provides a mapping of Subcategories to NIST SP 800-53 Revision 4 and Revision 5 controls in its Cybersecurity and Privacy Reference Tool available at: https://csrc.nist.gov/projects/cprt/catalog#/cprt/home.

In comparison to the ITS Profile’s applicability, ITS control sets are applied at the system/physical object level to provide detailed controls and implementation specifics. ITS control sets are specifications of controls needed to mitigate the risk of operating ITS physical objects. ITS control sets are comprised of selected controls from the NIST Special Publication (SP) 800-53 controls catalog and include specifications based on the risk (i.e., a combination of threats, vulnerabilities, likelihood, and impact) associated with the physical objects.

Chapter 2. Physical Object Characteristics

2.1 Definition/Description

The ATC operates in the Field environment,[12] as described in ARC-IT typically as part of the implementation of roadway signal control systems. The general elements of a Transportation Field Cabinet System using an ATC are described below and illustrated in **Figure 2**. If other components are included in an instantiation of a cabinet, it may be necessary to address any increased security risks to or from these components by tailoring the control selections.

[12] ARC-IT defines the Field as: Infrastructure proximate to the transportation network which performs surveillance (e.g., traffic detectors, cameras), traffic control (e.g., signal controllers), information provision (e.g., Dynamic Message Signs (DMS)), connected vehicle processing and communications (e.g., roadside units), and local transaction (e.g., tolling, parking) functions and are typically governed by IOO centralized or cloud-based transportation management systems.

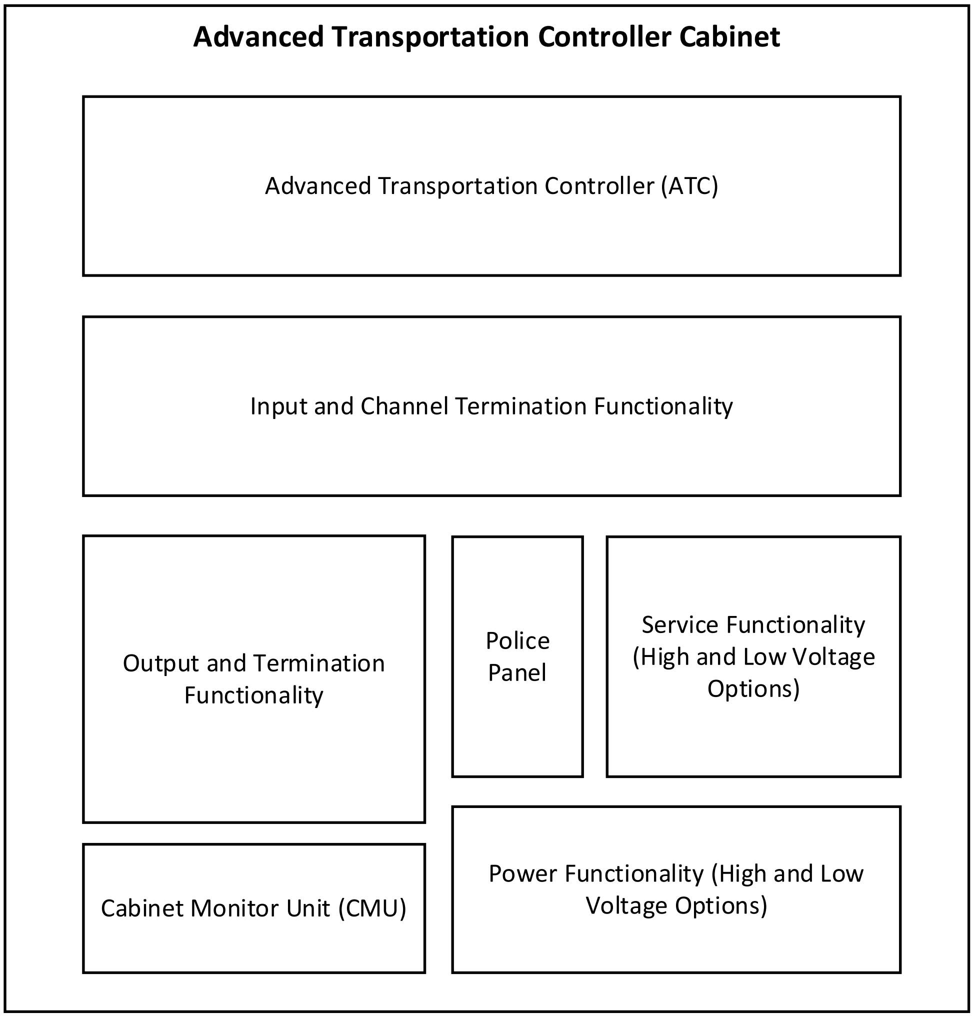
Advanced Transportation Controller Cabinet
Advanced Transportation Controller (ATC)
Input and Channel Termination Functionality
Output and Termination Functionality
Police Panel
Service Functionality (High and Low Voltage Options)
Cabinet Monitor Unit (CMU)
Power Functionality (High and Low Voltage Options)

Figure 22: High Level Functional Diagram of a Transportation Field Cabinet System (TFCS)[13]

The ATC is an environmentally ruggedized computational device used for on-street field applications. The controller not only supports simple intersection signal control but also sophisticated ITS applications such as adaptive signal control, active traffic management and real-time vehicle-infrastructure systems. The controller can perform a diversity of tasks, running concurrent application programs, and operating in high-speed communication networks. The architecture of the controller may follow two approaches: 1) "open architecture" where third parties can develop application software for the device and 2) "closed

[13] Source: Derived from Institute of Transportation Engineers (ITE) / American Association of State Highway and Transportation Officials (AASHTO) / National Electrical Manufactures Association (NEMA), Advanced Transportation Controller (ATC) Cabinet Standard 5301 Version 02 and ITE/AASHTO/NEMA, Advanced Transportation Controller (ATC) Standard 5201 Version 06.

architecture" where the hardware and application software are manufactured and sold as a package. The computational components of the controller reside on a single small, printed circuit board called the "Engine Board" with standardized connectors and pinout. It is made up of a central processing unit, Linux operating system, memory, external and internal interfaces (e.g., application programming interface [API], universal serial bus [USB], ethernet ports, and serial ports), and other hardware necessary to create an embedded transportation computing platform.

The Input and Channel Termination Functionality is the part of the system that gathers the input from various on-street sensor devices. There are numerous sensor technologies used for detection such as inductive loops, video image processing, microwave radar, magnetometers, and others. Depending on the communications standard used by the sensors, they may be connected to the input functionality via Serial Interface Unit (SIU) or directly to the traffic signal controller.

The Output and Termination Functionality contains the high-density switch pack and flasher unit in the form of a modular printed circuit board providing solid-state switches to drive field signal loads. It operates in two modes: switch pack mode or flasher mode. It monitors the voltage and current outputs and has the function to diagnose internal malfunction to go into an OFF state. The output terminations provide the interface between the signal head field wires and the output functionalities' connectors enabling or disabling the flow of electricity to the signal heads accordingly.

The Cabinet Monitor Unit (CMU) is the principal part of the cabinet monitoring system, and it queries various cabinet conditions to determine if the applications require actions such as transferring control from the traffic signal controller to the flashing control mode. The components of the CMU may include a microprocessor, non-volatile memory, communications circuitry to interface with the serial buses, front panel indicators, front panel communication connectors and serial memory key device. The operating program in the non-volatile memory is user upgradable via the front panel communication port. The serial memory key contains all the conditions and function selections of the CMU.

Service Functionality (high and low voltage configuration options) provides the entry points for the utilities' terminals, main breakers panel and transient voltage suppressor that feed the power needs of the cabinet components.

Power Functionality (high and low voltage configuration options) allows for multiple configurations of power supply input and converts and distributes the power needs to the electrical and mechanical components within the cabinet as well as the traffic signals. It provides flexibility for multiple form factors and ratings. The standard functionality supports voltages between 48 volts direct current (VDC) at 1 amp and 12 VDC at 5 amps and a modular rack mounted power supply.

The Police Panel provides switch access to the police during event response situations for manual control of the traffic signals.

2.2 Assumptions and Characteristics

This control set document is necessary because ITS have a set of characteristics and assumptions that often differentiate them from other types of technologies (e.g., general enterprise information technology). The assumptions and characteristics are necessary to fully explain how the ATCs are different from devices based on other technologies and, most importantly, to establish the essential foundation for selection of controls. The justification for selecting a control can and should trace back to this list of assumptions and characteristics. The assumptions relevant to the ATC are listed here.

Assumption #1: ATCs are implemented using current components and technologies that are compliant with current available recommended standards.

> As expressed in **Chapter 1.1, Purpose, Scope, and Applicability**, the primary scope is implementations of an ATC. Legacy controllers (i.e., those without ethernet communications and without an operating system) may not include all the features or capabilities of ATCs; therefore, not all the controls specified in this document can or need to be implemented by a legacy controller. Future ATC implementations may include innovative or complex features that are not typically implemented today. As such, the controls specified within this control set will have limitations to address risks associated with those features or capabilities and system owners must tailor in additional controls to mitigate those risks.

Assumption #2: ATCs are typically located in the Field environment, not in a building.

> ATC are deployed in exposed environments rather than located in buildings. This presents a set of risks not experienced by information technology (IT) systems in traditional facilities (e.g., Traffic Management Centers (TMCs)). From a risk management perspective, ATCs are more akin to operational technology (OT) than to IT. For example, Physical and Environmental (PE) controls (e.g., gates, guards, fire detection and suppression, lighting) associated with a fixed facility may not be implemented for ATCs. However, other PE controls that address physical access (e.g., PE-3(4), Physical Access Control | Lockable Casings) or monitoring the environment (e.g., PE-14, Environmental Controls) are needed.

Assumption #3: ATCs support both persistent and non-persistent data.

> Some data created or processed by ATC may be more perishable than persistent in nature. As such, not all the data may require the same protections. For example, non-perishable data is stored and, therefore, may require integrity protection to prevent unauthorized changes. In contrast, perishable data is processed and discarded so quickly that it may not require similar protections. ATC data may be used by physical objects or vehicles and may also be collected, correlated, analyzed, or otherwise processed for human consumption and decisions. Each “phase” of the data’s lifecycle may have unique protection requirements. Also, it is possible the data is collected and used in a way not originally intended or for which ATCs were designed; therefore, additional security protections may be necessary.

Assumption #4: The concept of “users” of the ATC is different than for typical IT.

> Most ATC "users" are not typical computer users with user accounts. The ATC includes some user accounts for person or non-person entities access (i.e., log into) to the ATC. Non-person entities include other devices or applications that use the data from the ATC and from the TMC. Person entities include administrators and technicians who access the ATC as per normal functionality. Each type of user may have different access control, identification, and authentication requirements.

Assumption #5: ATCs exist in networked environments.

ATCs employ many of the same functions and communications paradigms as traditional IT systems. ATC subcomponents may use different communications protocols at the higher layers of the protocol stack (e.g., NTCIP). Secure communications are required to and from the equipment, especially in cases where the medium is wireless. The authentication and access control are required to ensure the integrity and availability of the software that implements the signal management logic. The semi-autonomous operations of the ATCs may require increased levels of assurance of functionality. ATCs must also function if connections are lost.

Assumption #6: ATCs are highly specialized equipment that perform a limited set of functions.

ATCs are not general purpose in nature and, therefore, may have limited capacity to implement some controls that require considerable processing, storage, or communications resources. To support advanced functionality as it becomes available and the requisite security functionality, the ATCs are expected to have sufficient computing power to last an average of 10 years in the field.

2.3 Resources for Identifying Threats, Vulnerabilities, and Predisposing Conditions

To identify and manage ITS risk, the relevant threats, vulnerabilities, and predisposing conditions must be identified, typically through a risk assessment. Key resources[14] used to help understand and to identify potential threats, vulnerabilities, and predisposing conditions, include:

- NIST SP 800-30 – provides a generic set of adversarial and non-adversarial threat events.
- NIST SP 800-82 – provides a more specific set of threats and vulnerabilities applicable to OT. ITS are much like OT with respect to the operational environment and the risk profile.
- ATT&CK for ICS – provides a mapping of controls to mitigations for adversarial tactics, techniques, and procedures.
- ARC-IT –identifies the computing environment ITS operate in, the interfaces, and often the protocols used on those interfaces, which are relevant for identifying threats; maps security controls to Device Security Classes and lists “Mechanisms” that are requirements-like statements.

Each of these key resources is discussed in the following paragraphs.

The general threat events from NIST SP 800-30 that are applicable to ATC are provided in **Table 2** and **Table 3**. The threat events from NIST SP 800-82 applicable to ATC are provided in Appendix D **Table 4**.

[14] CAPEC™ (Common Attack Pattern Enumeration and Classification) provides a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities. While CAPEC™ may be useful key resource for other types of technology, it is not relevant to ITS and was not used in this document. For more information, see https://capec.mitre.org/.

The vulnerabilities and predisposing conditions from NIST SP 800-82 applicable to ATC are provided in Appendix D **Table 5**, with vulnerabilities and predisposing conditions grouped according to where they exist, such as in an IOO's policy and procedures, or the inadequacy of security mechanisms implemented in hardware, firmware, and software. Policies and procedures are typically implemented by the ITS IOO while security mechanisms are implemented in the system. Understanding the source of vulnerabilities and predisposing conditions can assist in determining optimal mitigation strategies.

ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, the government, and the cybersecurity product and service community. Of the three ATT&CK matrices (i.e., typical Enterprise systems, Mobile devices, and ICS, the one used to inform this control set is ATT&CK for ICS.

ATT&CK contains adversarial techniques and mitigations for those techniques. Mitigations are mapped to security controls. Techniques represent "how" an adversary achieves a tactical goal by performing an action. For example, adversaries with privileged network access may seek to modify network traffic in real time using adversary-in-the-middle (AiTM) attacks. Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

ARC-IT Device Security Class 3 is applicable to ITSRE, Connected Vehicle Roadside Equipment (CVRSE), and On-board Equipment (OBE), as described in ARC-IT. ATCs are an instantiation of ITSRE; therefore, those controls mapped to Class 3 were considered for relevance to the ATC. Not all the assumptions about and the characteristics of ITRSE, CVRSE, and OBE apply to ATC; therefore, not every control selected in Device Security Class 3 was selected in this control set. For those controls that were selected, the ARC-IT Mechanisms were adopted/adapted. The Mechanisms are requirements-like statements that can be conveyed to manufacturers/vendors for design and implementation of ATC.

Chapter 3. Summary of Control Specifications

This control set specifies the controls and control enhancements for ATCs with consideration for the impact a compromise of security objectives (i.e., confidentiality, integrity, and availability) would have on these physical objects. Controls selected for this control set are primarily technical in nature. These controls can be implemented by the physical object manufacturers/vendors to mitigate risk specific to the physical object. The presumption is that the IOO that owns the larger system, of which the physical object is a part, will implement the non-technical controls to further protect the physical objects. However, some of the non-technical controls (i.e., organizational controls) are included in this control set if they are considered critical to the success and security of the ATC in the Field. The IOO should convey some of those non-technical controls (e.g., the System and Services Acquisition [SA] family of controls) to the manufacturer/vendor to ensure the physical objects are designed and built correctly and can be integrated into the larger system and mitigate risk. For other non-technical controls, the IOO must implement them.

Table 1 below contains a summary of the control specifications as they apply in this control set document. The symbols used in the table are as follows:

- "G" indicates there is guidance for the control, including specific applicability guidance or implementation tailoring guidance.
- "V" indicates this control set document defines a value for an ITS-specific parameter for the control, but only to address unique physical object risks and to direct the manufacturers/vendors to comply; other parameter values are left to the discretion of the ITS program that is deploying the physical objects to define based on industry best practices.
- "R" indicates there is at least one risk reference or resource that affects a control selection and prescribes or recommends a security capability provided by a control.
- "S" indicates there is at least one reference (e.g., standard, best practice) that affects a control selection or that a control helps to meet.
- "M" indicates the control is implemented by the developer (typically the manufacturer/vendor) of the physical object.
- "I" indicates the control is implemented by the IOO.
- "M/I" indicates the control is implemented by the developer manufacturer/vendor and the IOO.

Due to the nature of the ATC and the operational environment, unique implementations are described in the guidance provided in **Chapter 4, Detailed Control Specifications**, of this control set document. The fourth column of **Table 1** below indicates if the control should be implemented by the developer manufacturer/vendor within or for the ATC, by the IOO, or by both. Allocation of responsibility for the controls may be different than what is implied in the control text in NIST SP 800-53, in that controls may need to be applied to the ATC itself that are typically implemented by the IOO, or vice versa. Otherwise, it may be prudent for the IOO to convey certain organizational controls (e.g., the SA family) to the developer manufacturer/vendor for implementation as the physical object is designed, built, and tested.

Table 1: Control Specifications for ATCs

ID	TITLE	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
AC-1	(Access Control) Policy and Procedures	GVR	I
AC-2	Account Management	GVR	I
AC-2(3)	Account Management | Disable Accounts	GV	M/I
AC-2(4)	Account Management | Automated Audit Actions	G	M
AC-2(5)	Account Management | Inactivity Logout	GVR	M/I
AC-2(12)	Account Management | Account Monitoring for Atypical Usage	GR	M/I
AC-3	Access Enforcement	GR	M/I
AC-3(4)	Access Enforcement | Discretionary Access Control	G	M/I
AC-3(5)	Access Enforcement | Security-Relevant Information	G	M/I
AC-3(7)	Access Enforcement | Role-Based Access Control	G	M/I
AC-3(8)	Access Enforcement | Revocation of Access Authorizations	G	M/I
AC-3(11)	Access Enforcement | Restrict Access to Specific Information Types	GR	M/I
AC-3(12)	Access Enforcement | Assert and Enforce Application Access	G	M/I
AC-4	Information Flow Enforcement	GR	M/I
AC-6	Least Privilege	R	I
AC-6(1)	Least Privilege | Authorize Access to Security Functions	GR	M/I
AC-6(3)	Least Privilege | Network Access to Privileged Commands	GR	I

ID	TITLE	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
AC-6(8)	Least Privilege | Privilege Levels for Code Execution	G	M/I
AC-6(9)	Least Privilege | Log Use of Privileged Functions	GR	M/I
AC-6(10)	Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions	GR	M/I
AC-7	Unsuccessful Logon Attempts	GVR	M/I
AC-9	Previous Logon Notification	G	M/I
AC-11	Device Lock	GVR	M/I
AC-11(1)	Device Lock | Pattern-Hiding Displays	R	M
AC-12	Session Termination	GR	M/I
AC-12(1)	Session Termination | User-Initiated Logouts	GR	M/I
AC-12(2)	Session Termination | Termination Message		M
AC-17	Remote Access	GR	I
AC-17(1)	Remote Access | Monitoring and Control	GR	M/I
AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	GRS	M
AC-17(10)	Remote Access | Authenticate Remote Commands	GR	M/I
AC-18	Wireless Access	GR	I
AC-18(1)	Wireless Access | Authentication and Encryption	R	M
AC-18(3)	Wireless Access | Disable Wireless Networking		M/I
AC-20	User of External Systems	GR	M/I
AC-20(1)	Use of External Systems | Limits on Authorized Use		I
AC-20(2)	Use of External Systems | Portable Storage Devices – Restricted Use		I

ID	TITLE	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
AC-24	Access Control Decisions	G	M/I
AC-24(1)	Access Control Decisions | Transmit Access Authorization Information	G	M/I
AT-3	Role-Based Training	GVR	M/I
AT-3(2)	Role-Based Training | Physical Security Controls	GV	I
AU-2	Event Logging	GVRS	I
AU-3	Content of Audit Records	GR	M/I
AU-4	Audit Log Storage Capacity	GR	M/I
AU-4(1)	Audit Log Storage Capacity | Transfer to Alternate Storage	GR	M/I
AU-5	Response to Audit Logging Process Failures	GVR	M/I
AU-5(1)	Response to Audit Logging Process Failures | Storage Capacity Warning	GVR	M/I
AU-5(2)	Response to Audit Logging Process Failures | Real-Time Alerts	GVR	M/I
AU-7	Audit Record Reduction and Report Generation		M
AU-8	Time Stamps	GR	M
AU-9	Protection of Audit Information	GR	M/I
AU-9(2)	Protection of Audit Information | Store on Separate Physical Systems or Components	GVR	M
AU-9(3)	Protection of Audit Information | Cryptographic Protection	GR	M
AU-9(6)	Protection of Audit Information | Read-Only Access	G	M/I
AU-10	Non-Repudiation	GR	M
AU-12	Audit Record Generation	GVR	M

ID	TITLE	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
AU-12(1)	Audit Record Generation | System-Wide and Time-Correlated Audit Trail	GVR	M
AU-12(2)	Audit Record Generation | Standardized Formats	G	M
AU-12(3)	Audit Record Generation | Changes by Authorized Individuals	GVR	M
CA-5	Plan of Actions and Milestones	GVR	I
CA-6	Authorization	GV	I
CA-7	Continuous Monitoring	GR	I
CA-7(6)	Continuous Monitoring | Automation Support for Monitoring	G	M/I
CA-8	Penetration Tests	GVR	I
CA-9	Internal System Connections	GVR	I
CM-2	Baseline Configuration	GV	M/I
CM-3	Configuration Change Control	GR	M/I
CM-3(5)	Configuration Change Control | Automated Security Response	GV	M
CM-3(8)	Configuration Change Control | Prevent or Restrict Configuration Changes	GVR	M
CM-5	Access Restrictions for Change	GR	M/I
CM-5(1)	Access Restrictions for Change | Automated Access Enforcement and Audit Records	G	M
CM-5(6)	Access Restrictions for Change | Limit Library Privileges	G	M/I
CM-6	Configuration Settings	G	M/I
CM-7	Least Functionality	GR	M/I
CM-7(1)	Least Functionality | Periodic Review	GV	M/I

ID	TITLE	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
CM-7(2)	Least Functionality | Prevent Program Execution	GR	M/I
CM-7(5)	Least Functionality | Authorized Software – Allow-by-Exception	GVR	M/I
CM-7(8)	Least Functionality | Binary or Machine Executable Code	G	M/I
CM-7(9)	Least Functionality | Prohibiting the Use of Unauthorized Hardware	GV	M/I
CM-11	User-Installed Software	GVR	M/I
CM-11(2)	User-Installed Software | Software Installation with Privileged Status	G	M/I
CM-11(3)	User-Installed Software | Automated Enforcement and Monitoring	G	M
CM-14	Signed Components	GV	M/I
CP-9	System Backup	GVR	M/I
CP-9(1)	System Backup | Testing for Reliability and Integrity	GVR	M/I
CP-9(2)	System Backup | Test Restoration Using Sampling	GR	M/I
CP-9(8)	System Backup | Cryptographic Protection	G	M/I
CP-12	Safe Mode	GR	M/I
IA-2	Identification and Authentication (Organizational Users)	GR	M/I
IA-2(1)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts	GR	M
IA-2(2)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts	GR	M
IA-2(5)	Identification and Authentication (Organizational Users) | Individual Authentication with Group Authentication	GR	M/I

ID	TITLE	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
IA-2(8)	Identification and Authentication (Organizational Users) | Access to Accounts — Replay Resistant	GVR	M
IA-3	Device Identification and Authentication	GVR	M/I
IA-3(1)	Device Identification and Authentication | Cryptographic Bidirectional Authentication	GVR	M
IA-5	Authenticator Management	GVRS	M/I
IA-5(1)	Authenticator Management | Password-Based Authentication	GVRS	M/I
IA-5(2)	Authenticator Management | Public Key-Based Authentication	GR	M/I
IA-5(5)	Authenticator Management | Change Authenticators Prior to Delivery	G	M/I
IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators	G	M/I
IA-5(13)	Authenticator Management | Expiration of Cached Authenticators	G	M/I
IA-6	Authenticator Feedback	GR	M
IA-7	Cryptographic Module Authentication	GR	M/I
IA-8	Identification and Authentication (Non-Organizational Users)	GR	M
IA-9	Service Identification and Authentication	GR	M/I
IA-11	Re-Authentication	GR	M/I
MA-4	Nonlocal Maintenance	G	M/I
MA-4(1)	Nonlocal Maintenance | Logging and Review	G	M/I
MA-4(4)	Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions	G	M/I

ID	TITLE	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
MA-4(6)	Nonlocal Maintenance | Cryptographic Protection		M/I
MP-3	Media Marking	GR	I
MP-4	Media Storage	GR	I
MP-7	Media Use	GR	I
PE-2	Physical Access Authorizations	GV	I
PE-2(1)	Physical Access Authorizations | Access by Position or Role	GV	I
PE-3	Physical Access Control	GVR	M/I
PE-3(4)	Physical Access Control | Lockable Casings	GV	M/I
PE-3(5)	Physical Access Control | Tamper Protection	GV	M/I
PE-4	Access Control for Transmission	R	I
PE-6	Monitoring Physical Access	G	M/I
PE-9	Power Equipment and Cabling	G	M/I
PE-11	Emergency Power	G	M/I
PE-11(1)	Emergency Power | Alternate Power Supply – Minimal Operational Power		I
PE-14	Environmental Controls	GVR	M/I
PE-20	Asset Monitoring and Tracking	GV	M/I
PL-2	System Security and Privacy Plans	GVR	I
RA-3	Risk Assessment	GV	M/I
RA-3(1)	Risk Assessment | Supply Chain Risk Assessment	GV	M/I
RA-5	Vulnerability Monitoring and Scanning	GVR	M/I
RA-7	Risk Response	G	M/I

ID	TITLE	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
SA-4	Acquisition Process	GR	M/I
SA-4(2)	Acquisition Process | Design and Implementation Information for Controls	R	M/I
SA-4(5)	Acquisition Process | System, Component, and Service Configurations	G	M/I
SA-4(9)	Acquisition Process | Functions, Ports, Protocols, and Services in Use	GR	M/I
SA-5	System Documentation	G	M/I
SA-8	Security and Privacy Engineering Principles	G	M/I
SA-9	External System Services	G	I
SA-10	Developer Configuration Management	GVR	M/I
SA-10(1)	Developer Configuration Management | Software and Firmware Integrity Verification	GR	M/I
SA-10(6)	Developer Configuration Management | Trusted Distribution		M/I
SA-11	Developer Testing and Evaluation	R	M/I
SA-11(1)	Developer Testing and Evaluation | Static Code Analysis		M/I
SA-11(2)	Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses	G	M/I
SA-11(6)	Developer Testing and Evaluation | Attack Surface Reviews	G	M/I
SA-11(8)	Developer Testing and Evaluation | Dynamic Code Analysis		M/I
SA-15	Development Process, Standards, and Tools		I
SA-15(5)	Development Process, Standards, and Tools | Attack Surface Reduction		M/I

ID	TITLE	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
SA-17	Developer Security and Privacy Architecture and Design		M/I
SA-17(5)	Developer Security and Privacy Architecture and Design | Conceptually Simple Design		M/I
SA-17(7)	Developer Security and Privacy Architecture and Design | Structure for Least Privilege	G	M/I
SA-20	Customized Development of Critical Components	G	M/I
SC-2	Separation of System and User Functionality	GR	M
SC-2(1)	Separation of System and User Functionality | Interfaces for Non-Privileged Users	G	M
SC-3	Security Function Isolation	GR	M
SC-3(2)	Security Function Isolation | Access and Flow Control Functions	G	M
SC-3(3)	Security Function Isolation | Minimize Non-Security Functionality		M
SC-3(4)	Security Function Isolation | Module Coupling and Cohesiveness	G	M
SC-3(5)	Security Function Isolation | Layered Structures	G	M
SC-5	Denial-of-Service Protection	GR	M/I
SC-5(1)	Denial-of-Service Protection | Restrict Ability to Attack Other Systems	G	M
SC-5(2)	Denial of Service Protection | Capacity, Bandwidth, and Redundancy	G	M
SC-5(3)	Denial of Service Protection | Detection and Monitoring	G	M/I
SC-7	Boundary Protection	GR	M
SC-7(3)	Boundary Protection | Access Points	GR	M/I

ID	TITLE	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
SC-7(4)	Boundary Protection | External Telecommunications Services	GVR	M/I
SC-7(5)	Boundary Protection | Deny by Default — Allow by Exception	GR	M
SC-7(7)	Boundary Protection | Split Tunneling for Remote Devices	GR	M
SC-7(16)	Boundary Protection | Prevent Discovery of System Components	G	M
SC-7(18)	Boundary Protection | Fail Secure	GR	M
SC-7(19)	Boundary Protection | Block Communication from Non-Organizationally Configured Hosts	G	M/I
SC-7(21)	Boundary Protection | Isolation of System Components	GR	M
SC-7(23)	Boundary Protection | Disable Sender Feedback on Protocol Validation Failure	G	M
SC-7(28)	Boundary Protection | Connections to Public Networks	GVR	I
SC-8	Transmission Confidentiality and Integrity	GVRS	M
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic Protection	GVR	M
SC-10	Network Disconnect	GVR	M
SC-13	Cryptographic Protection	GRS	M
SC-17	Public Key Infrastructure Certificates	G	M/I
SC-18	Mobile Code	GR	I
SC-18(3)	Mobile Code | Prevent Downloading and Execution	GV	M
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	GR	M
SC-23	Session Authenticity	GRS	M

ID	TITLE	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
SC-23(1)	Session Authenticity | Invalidate Session Identifiers at Logout	G	M
SC-23(3)	Session Authenticity | Unique System-Generated Session Identifiers	G	M
SC-23(5)	Session Authenticity | Allowed Certificate Authorities	G	M
SC-24	Fail In Known State	GVR	M
SC-27	Platform-Independent Applications	G	M
SC-28	Protection of Information at Rest	GR	M
SC-28(1)	Protection of Information at Rest | Cryptographic Protection	GVR	M
SC-28(3)	Protection of Information at Rest | Cryptographic Keys	G	M
SC-35	External Malicious Code Identification	G	M
SC-39	Process Isolation	GR	M
SC-40	Wireless Link Protection	G	M
SC-41	Port and I/O Device Access	GR	M/I
SC-45	System Time Synchronization	GR	M/I
SC-45(1)	System Time Synchronization | Synchronization with Authoritative Time Source	GR	M
SI-2	Flaw Remediation	GVR	M/I
SI-2(4)	Flaw Remediation | Automated Patch Management Tools	G	M/I
SI-3	Malicious Code Protection	VR	M/I
SI-3(4)	Malicious Code Protection | Updates Only by Privileged Users		M/I
SI-4	System Monitoring	GR	M/I

ID	TITLE	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
SI-4(2)	System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis	R	M
SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic	GR	M/I
SI-4(5)	System Monitoring | System-Generated Alerts	GR	M/I
SI-4(7)	System Monitoring | Automated Response to Suspicious Events	G	M/I
SI-4(14)	System Monitoring | Wireless Intrusion Detection	G	M/I
SI-4(23)	System Monitoring | Host-Based Devices	G	M/I
SI-7	Software, Firmware, and Information Integrity	R	M/I
SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks	GR	M/I
SI-7(2)	Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations	GR	M/I
SI-7(6)	Software, Firmware, and Information Integrity | Cryptographic Protection		M
SI-7(9)	Software, Firmware, and Information Integrity | Verify Boot Process	R	M
SI-7(10)	Software, Firmware, and Information Integrity | Protection of Boot Firmware	GR	M/I
SI-7(12)	Software, Firmware, and Information Integrity | Integrity Verification		M/I
SI-10	Information Input Validation	GVR	M/I
SI-10(5)	Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats	G	M/I
SI-11	Error Handling	GR	M/I
SI-16	Memory Protection	GR	M/I

ID	TITLE	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
SI-17	Fail-Safe Procedures	GR	M/I
SR-2	Supply Chain Risk Management Plan	GV	M/I
SR-3	Supply Chain Controls and Processes	GV	M/I
SR-4	Provenance	GV	M/I
SR-4(2)	Provenance | Track and Trace	G	M/I
SR-4(3)	Provenance | Validate as Genuine and Not Altered	G	M/I
SR-5	Acquisition Strategies, Tools, and Methods	G	M/I
SR-6	Supplier Assessments and Reviews	GV	M/I

Chapter 4. Detailed Control Specifications

This chapter provides details on the controls specified in **Chapter 3, Summary of Control Specifications**. For each control, one or more elements may be provided. The elements are discussed in the following paragraphs. The element or sub-element will be included for a control only if there are values or information relevant to that element or sub-element.

Responsible Party (M/I): Indications for which entity implements a control include Manufacturer (M), IOO (I), or both the Manufacturer and the IOO (D/O).

Various aspects of a control may be implemented by different roles, depending on whether the control content is technical, non-technical, or a combination of both. Non-technical controls (e.g., policies, procedures, desired security functionality, leadership/management decisions) are most often implemented by the IOO. Within the IOO there may be ITS engineers/ integrators (organic or contracted) who manage some of the non-technical security decisions but more likely manage the bulk of the technical security decisions on behalf of the IOO leadership/management. Technical controls are typically implemented by the system and, therefore, would be levied against a developer (organic or contracted) or a manufacturer/vendor. However, the IOO must often make decisions on the technical aspects of the system and convey those to the manufacturer/vendor for design and implementation. Therefore, some controls are tagged herein as D/O regardless of whether they are tagged in NIST SP 800-53 as system or organizational. In this chapter, there are references to the above roles, primarily the manufacturer/vendor and the IOO. Distinctions may be made when it is important to understand if the IOO has primary responsibility.

Justification to Select: A risk-based justification is provided to indicate why the control is selected for this control set. That justification is relevant to a typical instantiation of an ATC (not every possible instantiation) consistent with the assumptions for this control set in **Chapter 2.2, Assumptions and Characteristics**. Where appropriate, the threat sources, vulnerabilities, and/or predisposing conditions in Appendix D Tables 2 through 5 are referenced (i.e., the selected control/enhancement helps mitigate the threat, vulnerability, and/or predisposing condition).

Guidance: The guidance indicates how a control may be applied to the ATC. In some cases, the guidance for the selected controls and control enhancements must be modified from NIST SP 800-53 to address the characteristics of the topic of the control set and the environments in which the system or components operate.

Parameter Value(s): The control text in NIST SP 800-53 may include a parameter (e.g., password length and complexity) that needs to be defined before the control can be implemented. If it is appropriate to define a parameter value (PV) in this control set to support consistency across the ITS community, a recommended value is provided. However, state and local transportation agencies may tailor that value based on system-specific risk or other considerations (e.g., technology capabilities, cost to implement). If it is not appropriate to define a parameter value for all ATC within the scope of this control set, no parameter value entry is included. Organizations within the ITS community must define all remaining parameter values for controls selected for systems within their organization.

The parameter values are defined to flow within the control text, and their placement/position within the control is noted since the entirety of the control text is not included.

For example, “2nd PV” indicates the value being provided is for the second parameter value within the control text. Where controls contain multiple paragraphs (e.g., a., b., c.) and subparagraphs within those paragraphs (e.g., a.1., a.2, a.3), then the paragraph/subparagraph to which the value applies is provided.

If a control has a parameter value in paragraph a. and paragraph c. for which values are being provided, but no parameter value to define for paragraph b., then the notation will identify only paragraph a. and c. and will not contain a reference to paragraph b.

Where multiple values may be defined within a paragraph or subparagraph, their position will be noted using 1st PV or 2nd PV as appropriate. If the parameter value contains no annotation regarding its placement, then this indicates there is only one value to define for the control and annotation of its placement within the control is not needed. It should be noted that sometimes a parameter value begins with the word “a” which should not be confused with a paragraph annotation of “a.”

Parameter values are contextual, and many are typically a suggested minimum, such as “at least annually.” The parameter value should be read in the context of the full control text in NIST SP 800-53 to fully understand the meaning.

Risk References and Resources: If there is an authoritative source (e.g., ATT&CK for ICS, NIST SP 800-82, or ARC-IT) that prescribes or recommends a security capability provided by the control, that authoritative source is included in this element.

For controls selected below for which there is an ATT&CK for ICS mapping, the relevant mitigations and techniques will be listed. Where there is an ATT&CK mapping, only those techniques deemed relevant to the typical ATC implementation are listed, as not every technique is feasible or possible against a typical ATC. However, system owners may consider the relevance of other techniques based on their specific system architecture, design, or use. This control set and the related mitigations and techniques are only a starting point from which system owners must tailor controls in or out based on a risk assessment.

NIST SP 800-82 includes an “OT Discussion” for some controls in its overlay for OT. Those discussions are included if relevant to the ATC, but wording may be adapted to the unique features or functions of the ATC.

The ARC-IT Mechanisms are requirements-like statements that could be conveyed to a manufacturer/vendor for ATC design and implementation.

Standards: This element lists standards relevant to the ATC that prescribe capabilities or cybersecurity requirements.

AC FAMILY – ACCESS CONTROL

AC-1, (Access Control) Policy and Procedures

Responsible Party (M/I): I

Justification to Select: Vulnerability "Inadequate security policy for ITS" in **Table 5**, Section *Policy and Procedure Vulnerabilities and Predisposing Conditions.* The establishment, maintenance, and dissemination of access control policies and procedures is part of the governance required to manage the cybersecurity risks of an IOO. It is a pre-requisite to the implementation and lifecycle management of cybersecurity protections and safeguards for ITS.

Guidance: This is an organizational control, as the IOO (not the manufacturer), would create the policies and procedures. If the IOO does not have access control policies and procedures, the integrator, engineers, or developers may have no direction or guidance to design, develop, and manage access control capabilities in the ATC. This control is not implemented on or by the ATC itself, but the IOO develops, publishes, and conveys to the manufacturer/vendor key access control policies and procedures to guide implementation of other access controls from this family on the ATC.

Parameter Value(s):

paragraph c.1. "at least annually"

paragraph c.2. "first PV: at least annually"

Risk References and Resources:

NSIT SP 800-82: The policy specifically addresses the unique properties and requirements of ITS and the relationship to non-ITS systems. ITS access by vendors and maintenance staff can occur over a large facility footprint or geographic area and into unobserved spaces such as mechanical/electrical rooms and field substations.

AC-2, Account Management

Responsible Party (M/I): I

Justification to Select: Vulnerability "Inadequate access controls applied" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, as the IOO (not the manufacturer/vendor) would create and manage accounts. However, this control is selected because account management is so fundamental to protecting access to the ATC. Improperly managed accounts have a direct impact on the cybersecurity posture of all ITS systems/components to which users have access. Given the only users of the ATCs are operational users (e.g., maintainers, installers, administrators) with several types of elevated privileges, it is even more important to properly and timely manage their accounts.

Parameter Value(s):

paragraph h.1. "24 hours"

paragraph h.2. "24 hours"

paragraph h.3. "24 hours"

paragraph j. "at least quarterly"

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0918 / T0822, T0838, T0886, T0881, T0859
- M0926 / T0809, T0811, T0866, T0842, T0859
- Comments: T0838 is relevant but only to advanced/multi-function ATCs. T0886 is relevant because the ATC may have "remote services" installed, but there is also concern about remote access from other devices to compromise the ATC and/or other connected devices. T0809 will become relevant as ATC data typically stored at the TMC is pushed out to the cloud or stored locally on the ATC. For T0842 there is concern about unencrypted credentials.

NIST SP 800-82: In ITS systems, physical security, personnel security, intrusion detection, or auditing measures may assist in supporting this control objective.

ARC-IT Mechanisms:

- Often attackers will leverage compromised user accounts when they know they will not be authenticated. Consider restricting access to some aspects of corporate accounts or prevent users from logging in while they are on vacation, in off hours or over holidays.
- Having the capability to restrict user access to various systems when they are being serviced or updated can also be a handy feature to ensure information system data integrity is preserved during system maintenance.
- The organization will employ a wide range of heuristics to monitor and report on user activity. Common heuristics to look for include source location, source device identifiers, time of day heuristics, typical usage behaviors, and abnormalities in file access or a-typical download sizes.

AC-2(3), Account Management | Disable Accounts

Responsible Party (M/I): M/I

Justification to Select: This control is important to the security of the ATC as inappropriate or unauthorized access to the ATC could be possible after accounts have expired, are no longer associated with a user or individual, are in violation of organizational policy, or have been inactive.

Guidance: This control requires the IOO to manage accounts which includes disabling them after a defined time period under the conditions discussed in the control text. Also, the functionality that allows the IOO to disable accounts needs to be implemented at the ATC (by the manufacturer/vendor), and at the TMC. This functionality should support the scenario of disconnected operations of the ATC.

Parameter Value(s):

1st PV: “Not to exceed 72 hours”

paragraph (d) “90 days”

AC-2(4), Account Management | Automated Audit Actions

Responsible Party (M/I): I

Justification to Select: Threat event “Incorrect privilege settings” in **Table 3**.

Guidance: This is a technical control implemented by a system, but it is not implemented on the ATC. Rather, account management is performed primarily at the TMC. The ATC would simply authenticate local or remote access requests based on information recorded in account management records at the TMC. Most operating systems support the capability to audit accounts that are created within the operating system; however, the IOO ensures appropriate account management actions are audited through control AU-2.

AC-2(5), Account Management | Inactivity Logout

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate access controls applied” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should define the time period of expected inactivity or description of when to log out of the ATC and develop training and procedures for the users to proceed as required by policy. The manufacturer/vendor should develop the functionality on the ATC for the user to voluntarily log out as required by policy.

Parameter Value(s):

“expecting 5-15 minutes of inactivity or as soon as activities are completed.”

Risk References and Resources:

NIST SP 800-82: This control enhancement defines situations or timeframes in which users log out of accounts in policy; automatic enforcement is not addressed by this control enhancement (see AC-11). Organizations determine if this control enhancement is appropriate for the mission and/or functions of the ITS system and define the timeframe or scenarios. If no timeframe or scenario(s) apply, the organization-defined parameter reflects as such.

ARC-IT Mechanisms: See AC-2

AC-2(12), Account Management | Account Monitoring for Atypical Usage

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate access controls applied” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational and technical control. The logging capability (see AU-2) supports monitoring for atypical usage, and that logging can be performed on the ATC. The IOO then examines the usage logs (and other artifacts) to determine and respond to any atypical usage. The IOO ensures usage events are correctly identified for control AU-2 and may need to convey some requirements to the manufacturer/vendor to ensure the logging capabilities are designed and implemented in the ATC.

Risk References and Resources:

ARC-IT Mechanisms: See AC-2.

AC-3, Access Enforcement

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate access controls applied" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The ATC contains assets that need to be accessed for operational use; therefore, access control is enforced at the ATC to ensure only authorized parties obtain access as appropriate for their role. If access control cannot be enforced at the ATC, it should be enforced upstream at the first router or other component capable of enforcing access control.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0800 / T0800, T0858, T0868, T0816, T0871, T0838, T0836, T0843, T0845, T0886
- M0801 / T0800, T0858, T0812, T0868, T0816, T0871, T0891, T0838, T0839, T0843, T0845, T0886, T0857, T0859
- M0807 / T0800, T0878, T0802, T0803, T0804, T0805, T0806, T0858, T0879, T0868, T0816, T0838, T0839, T0861, T0843, T0845, T0886, T0848, T0856, T0869, T0857, T0855
- M0930 / T0800, T0830, T0878, T0802, T0805, T0806, T0858, T0885, T0868, T0816, T0819, T0866, T0822, T0838, T0839, T0842, T0861, T0843, T0845, T0886, T0848, T0881, T0856, T0869, T0857, T0864, T0855
- M0935 / T0822
- M0937 / T0800, T0806, T0884, T0868, T0816, T0839, T0861, T0843, T0845, T0886, T0848, T0856, T0857, T0855, T0859

NIST SP 800-82: The organization ensures access enforcement mechanisms do not adversely impact the operational performance of the ITS. Example compensating controls include encapsulation. Policy for logical access control to non-addressable and non-routable system resources and the associated information is made explicit. Access control mechanisms include hardware, firmware, and software that control the device or have device access, such as device drivers and communications controllers. Physical access control (see the PE family of controls) may serve as a compensating control for logical access control; however, it may not provide sufficient granularity in situations where users require access to different functions.

ARC-IT Mechanisms:

- The device shall support a role-based access mechanism in which:
  - There is an access control policy that defines protected resources and functions to which access control is applied; users and processes must demonstrate that they are authorized to access those resources per the policy.
  - The device shall be able to grant at least one of ongoing privileged access or periodic privileged access as defined in Notes on Access Control[15].

[15] https://www.arc-it.net/html/security/controlsclarification.html

- The device may support an installer that can grant ongoing privileged access to installed processes.
- The access control policy may only be edited by privileged users.

AC-3(4), Access Enforcement | Discretionary Access Control

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate access controls applied" in **Table 5**, Section Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO should define the discretionary access control policies, develop training for the users to follow the policy, and update the training and policy, as necessary. The manufacturer/vendor should develop the functionality at the ATC to support access control policies and the flexibility to modify such system controls as required by the IOO and managed centrally at the TMC.

AC-3(5), Access Enforcement | Security-Relevant Information

Responsible Party (M/I): M/I

Justification to Select: Threat event "Theft of Operational Information" in **Table 4**, Physical Object Threat Events*.*

Guidance: The IOOs define the security relevant information that should not be accessed during ATC operations. This information should be provided to the manufacturer/vendor for implementation of functionality at the ATC that prevents the access of this information during ATC operations. It should be a standard practice to prevent access to security-relevant information while the ATC is in an operational state.

AC-3(7), Access Enforcement | Role-Based Access Control

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate access controls applied" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.* The types of operations that can be performed on the ATC vary in terms of risk and so call for controlling access based on the job function of personnel. Within a class of users for a given role, access need not differ with the individual user.

Guidance: The ATC should allow operations to be performed based on the role of the user currently logged in, for example: Operational users (technicians) are only shown the signal timing application (e.g., front- panel controls), while other Operational users (administrators) or User Developers are able to make other authorized system-level configuration changes or make changes to the actual applications.

AC-3(8), Access Enforcement | Revocation of Access Authorizations

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate security policy for ITS” in **Table 5**, Section *Policy and Procedure Vulnerabilities and Predisposing Conditions.* This control is an integral part of the access enforcement at the ATC; even though it may be the TMC that actually revokes access authorization for individuals, this information should be conveyed to the ATC, so it no longer allows access to revoked accounts.

Guidance: The IOO should define the rules governing the timing of revocations of access authorities. The attributes are the characteristics (e.g., privilege level) of subjects (e.g., users) with respect to access to objects (e.g., systems settings and applications).

AC-3(11), Access Enforcement | Restrict Access to Specific Information Types

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate access controls applied” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is a more detailed control in line with AC-3 (7) role-based access control (RBAC). The IOO should define information types that should be restricted via access control mechanisms. The manufacturer/vendor should implement the functionalities to restrict such defined information types at the ATC such that in the case the ATC is disconnected from its TMC where access control is centrally managed, the ATC can still perform the access control required at its remote location and report back once connectivity to the TMC is restored. See Guidance of AC-3(7).

Risk References and Resources:

> NIST SP 800-82: The organization identifies and restricts access to information that could impact the ITS environment, accounting for information types that are sensitive, proprietary, contain trade secrets, or support safety functions. The loss of availability, integrity, and confidentiality of certain types of information residing on a high impact ITS may result in severe or catastrophic adverse effects on operations, assets, or individuals that include severe degradation or loss of mission capability, major damage to organizational assets, or result in harm to individuals involving loss of life or life-threatening injuries.

AC-3(12), Access Enforcement | Assert and Enforce Application Access

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate testing of security changes” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should define ATC applications and functions that require assertion and enforcement of access during the installation process of new applications. The manufacturer/vendor should implement the functionalities to assert and enforce access to the list of ATC applications and functions that require access enforcement.

AC-4, Information Flow Enforcement

Responsible Party (M/I): M/I

Justification to Select: This control helps protect against multiple threats (e.g., many of the threats in **Table 2**, Adversarial Threat Events require adequate information flow enforcement as a preventative measure).

Guidance: The IOO should define information flow control policies required to ensure the flow of information between systems is securely controlled. The manufacturers/vendors should implement the ATC functions required to enforce the flow of information between systems connected to the ATC according to developed policies.

Risk References and Resources:

NIST SP 800-82: Information flow policy may be achieved using a combination of logical and physical flow restriction techniques. Inspection of message content may enforce information flow policy. For example, ITS protocols may be restricted using inbound and outbound traffic rules on a network control device between ITS and TMC networks. For non-routable communication such as serial connections, devices may be configured to limit commands to and from specific tags within the ITS device. Information flow policy may be supported by labeling or coloring physical connectors to aid in connecting networks. Devices that do not have a business need to communicate should not be connected (i.e., air gapped).

ARC-IT Mechanisms: The device shall support defining information flow control policies which identify constraints on the flow of information in and out of the device, including in particular Identification and Authentication (IA) and System and Communication (SC) protection mechanisms that must be applied to information flows in order for them to be permissible. See Notes on Access Control for a discussion and examples of information flow control. The ability to define an information flow control policy shall be restricted to privileged users.

AC-6, Least Privilege

Responsible Party (M/I): I

Justification to Select: The Principle of Least Privilege (POLP) is a fundamental security concept of giving a user account or process only those privileges which are essential to perform its intended function. Applying POLP reduces the risk of attackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M092/T0809, T0811, T0872, T0849, T0873, T0881, T0882

NIST SP 800-82: Example compensating controls include providing increased personnel security and auditing. The organization carefully considers the appropriateness of a single individual having multiple critical privileges. System privilege models may be tailored to enforce integrity and availability (e.g., lower privileges include read access and higher privileges include write access).

ARC-IT Mechanisms: See AC-3. A user shall not be given more permission to resources via network access than if they were physically present at the device. Where possible, additional controls should be in place to only allow limited network functionality for a remote user. This way, if the account is compromised, the amount of damage caused by an attacker with network access is reduced.

AC-6 (1), Least Privilege | Authorize Access to Security Functions

Responsible Party (M/I): M/I

Justification to Select: Security functions consist of sensitive functionality whose trustworthiness underpins the security of the entire system. Therefore, it is necessary to properly authorize access to these functions by individuals and by services.

Guidance: The IOO should define the list of individuals and roles that require access to security functions. The IOO should also define which security functions will be deployed in hardware, software, and firmware. The IOO should also define the security relevant information that will require authorization for access. The IOO should convey this information to the manufacturer/vendor so they can implement the authorization mechanisms in the hardware, software, and firmware.

Risk References and Resources:

> NIST SP 800-82: In situations where the ITS components (e.g., programmable logic controllers [PLC]) cannot support logging of privileged functions, other system components within the authorization boundary may be used (e.g., engineering workstations or physical access monitoring).

AC-6 (3), Least Privilege | Network Access to Privileged Commands

Responsible Party (M/I): I

Justification to Select: Vulnerability “Inadequate access controls applied” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.* Some commands/actions on the ATC can have a drastic impact on its operation and so allowing these to be enacted remotely (over the network) comes with an increased risk.

Guidance: The IOO should define the privileged commands relevant to the services offered by the ATC for which there are compelling operational needs requiring authorized access to the ATC via network access (as opposed to local access). These should be documented in the security plan for the system."

Risk References and Resources:

> NIST SP 800-82: In situations where the ITS components (e.g., ATCs) cannot support logging of privileged functions, other system components within the authorization boundary may be used (e.g., engineering workstations or physical access monitoring).

AC-6 (8), Least Privilege | Privilege Levels for Code Execution

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate authentication, privileges, and access control in software” in **Table 5**, Section *Software Development Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should define the list of software that will require higher level of privileges to execute and assign an administrator with the proper privileges to execute that software. The manufacturer/vendor should implement the functionality on the ATC to prevent the execution of software that requires elevated privileges by a user (person or service) that does not have those privileges.

AC-6 (9), Least Privilege | Log Use of Privileged Functions

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate authentication, privileges, and access control in software” in **Table 5**, Section *Software Development Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should convey to the manufacturer/vendor that any execution of privileged functions or privileged commands should be logged.

Risk References and Resources:

NIST SP 800-82: In situations where the ITS components (e.g., ATCs) cannot support logging of privileged functions, other system components within the authorization boundary may be used (e.g., engineering workstations or physical access monitoring).

AC-6 (10), Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate authentication, privileges, and access control in software” in **Table 5**, Section *Software Development Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should create a list of “privileged functions” or may request such a list from the manufacturer/vendor. The manufacturer/vendor should implement the functionality to prevent non-privileged users from executing those functions as required by policy.

Risk References and Resources:

NIST SP 800-82: Example compensating controls include enhanced auditing.

ARC-IT Mechanisms: See AC-6.

AC-7, Unsuccessful Logon Attempts

Responsible Party (M/I): M/I

Justification to Select: Threat event, “Conduct brute force login attempts/password guessing attacks” in **Table 2**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).* This control helps mitigate fraudulent use of the ATC. An adversary can try multiple passwords to breach the ATC.

Guidance: The IOO should define the number of consecutive invalid logon attempts and the time period for which these attempts should be considered. The IOO should also define the set of automated actions that need to take place when unsuccessful attempts are exceeded. The manufacturer/vendor should implement on the ATC the unsuccessful logon attempts requirement as per policy. At minimum, the portion required to support disconnected operations for the scenario in which there is no connection to the centralized management system.

Parameter Value(s):

paragraph a. 1st PV: “5”; 2nd PV: “15 minutes”

paragraph b. “Delay next logon prompt for 3 minutes”

Risk References and Resources:

NIST SP 800-82: Many ITS remain in continuous operation and operators remain logged onto the system continuously. A “log-over” capability may be employed. Example compensating controls include logging or recording all unsuccessful login attempts and alerting ITS security personnel through alarms or other means when the number of organization-defined consecutive invalid access attempts is exceeded. Unsuccessful logon attempt limits are enforced for accounts (e.g., administrator) or systems (e.g., engineering workstations) not required for continuous operation.

ARC-IT Mechanisms:

- The device supports the functionality of defining what types of authentication attempts shall be counted for the purposes of further security action.
- The device shall support login as one of these types of authentication attempts and may support other types of authentication attempts, for example authentication attempts for specific types of access to specific resources.
- The device shall support counting unsuccessful authentication attempts for users and locking them out for a period of time.
- The device is configurable such that for accounts with identified privileged roles the threshold number of unsuccessful login attempts is three in five minutes and the lockout period is five minutes starting immediately after the third unsuccessful login attempt.
- The device may be configurable such that a user role exists that allows a user in that role to unlock other user accounts before the lockout period expires.
- This feature should not reveal valid users of the system through the invalid login error messages it gives. Generic error messages should be provided that do not reveal valid user information.
- The authentication system response time should not be noticeably different for valid and invalid users.

AC-9, Previous Logon Notification

Responsible Party (M/I): M/I

Justification to Select: Threat event, “Conduct brute force login attempts/password guessing attacks” in **Table 2**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).*

Guidance: The IOO should incorporate in their technician’s cybersecurity training the process to inform the IT department of any suspicious logon attempts discovered from a previous logon notification from the ATC. The manufacturer/vendor should develop the capability for the ATC to display a previous logon notification to all users.

AC-11, Device Lock

Responsible Party (M/I): M/I

Justification to Select: Threat event, “Theft of Operational Information” in **Table 4**, Physical Object Threat Events. The ATC must be capable of automatically locking after a designated period of inactivity to protect against malicious activity. Without a device locking capability, an attacker could take control of the ATC when an operational user logs in but leaves the system accessible when no longer using the ATC.

Guidance: The IOO should determine the policy for device locking the ATC. The manufacturer/vendor should develop a capability to: 1) lock the device automatically after a period of user inactivity, based on the policies established by the IOO, and 2) allow for a user-initiated device lock. While the ATC may be locked by one user, the ATC should allow other users to log on without conflicts with existing users' logon (who previously locked the ATC) to allow the ATC to be accessed or to operate normally.

Parameter Value(s):

paragraph a. "initiating a device lock after no more than 5 minutes of inactivity, requiring the user to initiate a device lock before leaving the system unattended"

Risk References and Resources:

NIST SP 800-82: This control assumes a staffed environment where users interact with system displays. This control may be tailored appropriately where systems do not have displays configured, systems are placed in an access-controlled facility or locked enclosure, or immediate operator response is required in emergency situations. Example compensating controls include locating the display in an area with physical access controls that limit access to individuals with permission and need-to-know for the displayed information.

ARC-IT Mechanisms:

- The device supports the functionality of monitoring user activity for users in privileged roles and locking out the session after a certain period of inactivity, such that the user must re-authenticate to continue conducting privileged activities.
- The device is configurable such that the threshold inactivity length is 5 minutes.
- The device supports the functionality of an appropriately privileged user being able to explicitly lock an active session at any time.
- The device shall support the functionality of a user locking their own session.
- The device may support the functionality of an appropriately privileged administrator locking another user's session.

AC-11(1), Device Lock | Pattern-Hiding Displays

Responsible Party (M/I): M

Justification to Select: Threat event "Theft of Operational Information" in **Table 4**, Physical Object Threat Events. Requiring the system to conceal the information previously visible on the display after session lock helps to prevent unauthorized users from viewing an authorized user's display as a means to gain unauthorized access.

Risk References and Resources:

NIST SP 800-82: Physical protection may be employed to prevent access to a display or prevent attachment of a display. In situations where the system cannot conceal displayed information, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-12, Session Termination

Responsible Party (M/I): M/I

Justification to Select: Threat event, “Conduct externally based session hijacking” in **Table 2**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).*

Guidance: The IOO should define user session termination conditions and/or trigger events requiring session disconnect at the ATC. The manufacturer/vendor should develop the capabilities on the ATC to support the session termination policies provided by the IOO.

Risk References and Resources:

NIST SP 800-82: Example compensating controls include providing increased auditing measures or limiting remote access privileges to key personnel.

ARC-IT Mechanisms:

- The device supports the functionality of an appropriately privileged user being able to terminate an active session at any time.
- The device shall support the functionality of a user terminating their own session.
- The device may support the functionality of an appropriately privileged administrator terminating another user's session.
- The device shall display an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

AC-12(1), Session Termination | User-Initiated Logouts

Responsible Party (M/I): M/I

Justification to Select: Threat event, “Conduct externally based session hijacking” in **Table 2**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).*

Guidance: The IOO should define information resources that require logout capabilities at the ATC. The manufacturers/vendors should implement a logout capability at the ATC for information resources defined by the IOOs policies.

Risk References and Resources:

ARC-IT Mechanisms: See AC-12

AC-12(2), Session Termination | Termination Message

Responsible Party (M/I): M

Justification to Select: Threat event, “Conduct externally based session hijacking” in **Table 2**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).*

AC-17, Remote Access

Responsible Party (M/I): I

Justification to Select: Vulnerability, “Poor remote access controls” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, whereby the IOO establishes rules for what activities can be performed on the ATC remotely, and how to protect that link. The IOO should require the manufacturer/vendor to enable the ATC to set up secure tunnels (e.g., Transport Layer Security [TLS]-based virtual private networks [VPNs]), for every access path (wireless [wireless fidelity (WiFi) or cellular], or Ethernet).

Risk References and Resources:

NIST SP 800-82: In situations where the ITS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

ARC-IT Mechanisms: See SC-8, SC-12, SC-13

AC-17(1), Remote Access | Monitoring and Control

Responsible Party (M/I): M/I

Justification to Select: Vulnerability, “Poor remote access controls” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should establish how it is going to monitor all external access events. The manufacturer/vendor should enable the ATC to log all such TLS tunnel set up and tear-down events.

Risk References and Resources:

NIST SP 800-82: Example compensating controls include employing nonautomated mechanisms or procedures as compensating controls. Compensating controls could include limiting remote access to a specified period or placing a call from the ITS site to the authenticated remote entity.

AC-17(2), Remote Access | Protection of Confidentiality and Integrity Using Encryption

Responsible Party (M/I): M

Justification to Select: Vulnerability, “Poor remote access controls” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The ATC should support the setup of tunnels with TLS 1.2 (with approved cypher suites) or TLS 1.3, using certificate-based mutual authentication of both endpoints. The cypher suites for confidentiality and integrity used to protect the data should be NIST-approved.

Risk References and Resources:

NIST SP 800-82: Encryption-based technologies should be used to support the confidentiality and integrity of remote access sessions. While ITS devices often lack the ability to support modern encryption, additional devices (e.g., VPNs) can be added to support these features. This control should not be confused with SC-8 – Transmission Confidentiality and Integrity, which discusses confidentiality and integrity requirements for general communications, including between ITS devices.

ARC-IT Mechanisms: See SC-8, SC-12, SC-13

Standards: [ATC 5201v06], Section 2.5, RFC 8446[16]

AC-17(10), Remote Access | Authenticate Remote Commands

Responsible Party (M/I): M/I

Justification to Select: Vulnerability, “Poor remote access controls” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should define the mechanisms necessary to authenticate the defined remote commands at the ATC. The manufacturer/vendor should implement such mechanisms on the ATC. This authentication is beyond/separate from that offered by the secure tunnel setup between the ATC and the remote device. This may require a protocol level measure whereby some cryptographic protection is attached to the control protocol data sent to the ATC (e.g., Simple Network Management Protocol [SNMP]v3).

Risk References and Resources:

NIST SP 800-82: The ability to authenticate remote commands is important to prevent unauthorized commands that may have immediate or serious consequences such as injury, death, property damage, loss of high-value assets, failure of mission or business functions, or compromise of sensitive information.

AC-18, Wireless Access

Responsible Party (M/I): I

Justification to Select: Vulnerabilities, “Inadequate authentication between clients and servers over wireless connection” and “Inadequate data protection between clients and servers over wireless connection” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: Regardless of whether the IOO *intends* to use wireless access for the system of interest, this control is selected to ensure the IOO defines the limitations on wireless access. Many information technology products are developed to have wireless capabilities by default. If those wireless capabilities are enabled, either inadvertently or intentionally, there is a risk of unauthorized access to sensitive information. Selecting this control does not imply intent to allow wireless access, but instead

[16] Internet Engineering Task Force (IETF) Request for Comment 8446, The Transport Layer Security (TLS) Protocol Version 1.3, August 2018.

serves to ensure the IOO takes conscious actions to either allow and to establish appropriate restrictions on its use or disallow its use.

Risk References and Resources:

NIST SP 800-82: In situations where ITS cannot implement any or all the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

ARC-IT Mechanisms:

- See AC-1, AC-3, AC-6.
- Only high-privileged users explicitly identified will have permission to modify wireless configurations. See AC-3.
- Appropriately tune wireless antennas in an organization or make use of directional antennas to only propagate wireless signals within the physical confines of the organization.

AC-18(1), Wireless Access | Authentication and Encryption

Responsible Party (M/I): M

Justification to Select: Vulnerability, "Inadequate authentication between clients and servers over wireless connection" in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Risk References and Resources:

NIST SP 800-82: Implementation of authentication and encryption is driven by the ITS environment. There are some scenarios where devices and users cannot all be authenticated and encrypted due to operational or technology constraints. In such scenarios, compensating controls include providing increased auditing for wireless access, limiting wireless access privileges to key personnel, or using AC-18 (5) to reduce the boundary of wireless access.

ARC-IT Mechanisms: See AC-18

Standards: NTCIP 9014 v01.20, Annex B[17]

AC-18(3), Wireless Access | Disable Wireless Networking

Responsible Party (M/I): M/I

[17] National Transportation Communications for ITS Protocol (NTCIP) 9014 v01.20, Infrastructure Standards Security Assessment (ISSA), Aug 2021. This standard is referenced to highlight that there is an existing SNMPv3 standard that provides for the use of authentication and encryption, the subject of this control enhancement. Annex B calls for authentication and encryption for SNMPv3, the main protocol used by the ATC; therefore, by extension authentication and encryption should be used for wireless access.

Justification to Select: Wireless access increases the ATC attack surface. If the IOO does not *intend* to use wireless networking, this control should be applied to prevent its use.

AC-20, Use of External Systems

Responsible Party (M/I): M/I

Justification to Select: The IOO needs to establish procedures and controls to either allow or prevent use of external systems, which can present unique challenges for protecting sensitive information.

Guidance: External systems[18] may be used in an ATC deployment. For example, a map store, a cloud storage system, or a Certificate Authority may be used. The IOO can set up rules for use of these systems by operational users via or from the ATC device, and the manufacturer/vendor designs the ATC to accommodate these rules and/or allow the IOO to configure the ATC accordingly.

Risk References and Resources:

> NIST SP 800-82: Organizations refine the definition of "external" to reflect lines of authority and responsibility; granularity of organization entity; and their relationships. An organization may consider a system to be external if that system performs different functions, implements different policies, falls under different management authorities, or does not provide sufficient visibility into the implementation of controls to allow the establishment of a satisfactory trust relationship. For example, an ITS and a business data processing system may be considered external to each other depending on the organization's system boundaries. Access to an ITS for support by a business partner, such as a vendor or support contractor, is another common example. The definition and trustworthiness of external systems is re-examined with respect to ITS functions, purposes, technology, and limitations to establish a clearly documented technical or business case for use and an acceptance of the risk inherent in the use of an external system.

AC-20(1), Use of External Systems | Limits on Authorized Use

Responsible Party (M/I): I

Justification to Select: If external systems are authorized for use, the IOO needs to establish and document clear limits on their use as well as accepting the risk inherent in the use of external systems.

AC-20(2), Use of External Systems | Portable Storage Devices – Restricted Use

Responsible Party (M/I): I

[18] External systems are systems that are used by but not part of organizational systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness NIST SP 800-53.

Justification to Select: If external systems are authorized for use, the IOO needs to determine what restrictions should be applied to use of portable storage devices (e.g., thumb drives) with ATCs. Portable storage devices are a common way to compromise a system.

AC-24, Access Control Decisions

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate access controls applied” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should define access authorization information, controls, and systems that require enforcement of access control decisions. The manufacturer/vendor should implement functions on the ATC that enforce those decisions as required by policy.

AC-24(1), Access Control Decisions | Transmit Access Authorization Information

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate access controls applied” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should define access authorization information (e.g., which operational user can be allowed to perform what activity on the ATC), controls (e.g., rules that these users need to follow) and systems (e.g., ATC) that require enforcement of access control decisions. The manufacturer/vendor should implement functions on the ATC that enforce those decisions as required by policy. The access control management system at the TMC transmits the authorization information and controls to the ATC.

AT FAMILY – AWARENESS AND TRAINING

AT-3 Role-Based Training

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate ITS security training and awareness program” in **Table 5**, Section *Policy and Procedure Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, but it is also applicable for developer training as per ATT&CK mitigation M0913 and technique T0859. This control might also be applicable for operational user training to ensure they understand their cybersecurity responsibilities as they conduct their day-to-day roles.

Parameter Value(s):

paragraph a. “manufacturers/vendors and ATC operational users (administrators, maintainers, project managers and governance team)”

paragraph a.1. “annually”

paragraph b. 1st PV: “annually”

2nd PV: “after new threats and relevant adversary tactics, techniques and procedures have been identified.”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques: M0913 / T0859

NIST SP 800-82: Security training includes initial and periodic review of ITS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ITS security training program is consistent with the requirements of the security awareness and training policy established by the organization. The training may be customized for specific ITS roles, which could include operators, maintainers, engineers, supervisors, and administrators.

AT-3(2), Role-Based Training | Physical Security Controls

Responsible Party (M/I): I

Justification to Select: Vulnerability “Inadequate ITS security training and awareness program” in **Table 5**, Section *Policy and Procedure Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control that is important to implement since the ATC is heavily dependent on physical security controls. The IOO ensures the ATC operational users know and understand the physical security requirements. The IOO may require the manufacturer/vendor to provide training upon delivery of the ATC on certain physical security features offered by/for the ATC.

Parameter Value(s):

2nd PV: “At least annual (NOTE: Significant changes to physical security systems may drive more frequent training.)”

AU FAMILY – AUDIT AND ACCOUNTABILITY

AU-2, Event Logging

Responsible Party (M/I): I

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control but is likely performed by the IOO’s engineer/integrator who would select events to be logged. This control is essential, as it feeds into AU-12 which is the control specified for the ATC itself. That is, AU-2 determines what must be logged, and AU-12 implements those decisions on each system component.

See also AC-2(12) that determines if inappropriate actions are performed and whether the ATC would need the auditing function to capture those actions, such that the TMC personnel can monitor and respond accordingly.

Parameter Value(s):

paragraph a. “Logging for General and Security Purposes Design Details

- The ATC should be able to be configured to support at the minimum, the following events:
  - System startup and shutdown
  - Service and application startup and shutdown
  - Application failures/exceptions
  - Application configuration changes (e.g., application security profile)
  - Network connection and loss events (e.g., wireless or Ethernet connection)
  - Modifications to security-related settings
  - Successful and unsuccessful logon attempts
  - Software and firmware updates
  - Creation, modification and deletion of accounts and account privileges (users and apps)
  - Accesses to files/directories used by software/firmware updates
  - Unauthorized access attempts to corresponding private key operations (Optional)
  - Network and firewall configuration changes
  - Any changes to audit and audit reporting behavior
  - Modifications to certificate trust lists
  - Unauthorized attempts to modify log files

Otherwise, the design details for logging are vendor specific (e.g., the event messages).”

Risk References and Resources:

NIST SP 800-82: Organizations may want to include relevant ITS events (e.g., alerts, alarms, configuration and status changes, operator actions) in their event logging, which may be designated as audit events.

ARC-IT Mechanisms:

- Device provides a means to define a list of auditable activities. This shall be based on the list of resources for which privileged access is required as discussed in Notes on Access Control[19].
- Device provides a means to define and update a policy for auditing of auditable activities.
- Device provides access control mechanisms to restrict read or write access to the list of auditable activities and to the audit policy.

[19] https://www.arc-it.net/html/security/controlsclarification.html.

- Device shall support an audit policy in which a log is created that contains a list of all the distinct processes that have accessed or attempted to access each privileged function during one power-on time and may support additional audit policies.
- Device may provide a means for storing audit logs in an external location.

Standards: CTI 4001[20]

AU-3, Content of Audit Records

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Logs not maintained" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is primarily a technical control, but the IOO first determines what information should be collected about the events as they are logged in the audit trail and then convey the requirements to the manufacturer/vendor for design and implementation on the ATC.

Risk References and Resources:

ARC-IT Mechanisms: Any mechanism that meets the above requirements [specified by the controls] is acceptable.

AU-4, Audit Log Storage Capacity

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Logs not maintained" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is both an organizational and a technical control. The IOO defines the audit log retention requirements and conveys those to the manufacturer/vendor for design and implementation on the ATC.

Risk References and Resources:

ARC-IT Mechanisms: As specified in control.

ARC-IT PIC Statement: Provides 4 megabytes of audit storage.

AU-4 (1), Audit Log Storage Capacity | Transfer to Alternate Storage

Responsible Party (M/I): M/I

[20] Institute of Transportation Engineers (ITE) / American Association of State Highway and Transportation Officials (AASHTO) / National Electrical Manufactures Association (NEMA) NEMA, Connected Transportation Interoperability (CTI) 4001 v01.00, *Roadside Unit (RSU) Standard,* September 2021.

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: It may be necessary to transfer audit logs from the ATC to a centralized system at the TMC where the auditing function will ingest the logs.

Risk References and Resources:

NIST SP 800-82: Organizational requirements may require storage of exceptionally large amounts of data, which ITS components may not be able to support directly.

AU-5, Response to Audit Logging Process Failures

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is primarily a technical control, but the organization identifies who is to be alerted of audit logging process failures and what additional actions, if any, should be taken. If notifications are performed by the ATC, or if the ATC must implement the additional actions, the IOO conveys these requirements to the manufacturer/vendor for design and implementation on the ATC.

Parameter Value(s):

paragraph a. “2nd PV: Near real time”

Risk References and Resources:

ARC-IT Mechanisms:

- Device shall support the identification of a device management service to which audit processing failures shall be reported if connectivity is available.
- The ability to alter the device management service shall be restricted to privileged users per control AC-3.
- Device shall identify information flows to the device management service as a secured information flow per control AC-4 and shall protect those information flows with an approved mechanism per control SC-8.
- Device shall report any audit processing failure to the device management service if it has connectivity when the audit processing failure occurs.
- Device may maintain a backup logging service used to record failures in the audit processing service.
- Device shall reboot its audit processing service and thereafter attempt to start processing again on a failure. If no successful audit processing occurs over three reboot attempts, device shall log a report via a different mechanism and suspend auditing.

AU-5(1), Response to Audit Logging Process Failures | Storage Capacity Warning

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is primarily a technical control, but the IOO conveys to the manufacturer/vendor the time period within which a warning is to be provided and the maximum percentage of audit log storage, so the manufacturer/vendor can design and configure the ATC accordingly.

Parameter Value(s):

3rd PV: “Maximum of 90%, but ideally 75%”

Risk References and Resources:

ARC-IT Mechanisms: Provides a warning to the device administrator when audit record storage reaches 90% of maximum.

AU-5(2), Response to Audit Logging Process Failures | Real-Time Alerts

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is primarily a technical control, but the IOO may need to define and convey to the manufacturer/vendor the time period within which alerts are to be provided, unless the time period is configurable by the IOO once the manufacturer/vendor delivers the ATC.

Parameter Value(s):

1st PV: See ARC-IT Mechanisms below.

2nd PV: See ARC-IT Mechanisms below.

3rd PV: “Minimally but not limited to:

- auditing software/hardware errors
- failures in the audit capturing mechanisms, and
- audit storage capacity being reached or exceeded."

Risk References and Resources:

ARC-IT Mechanisms:

- Provides an alert within 5 seconds to the device operator for any audit failure.
- Provides an alert within 10 seconds to the device administrator for any audit failure; conditional on connectivity to administrator.

AU-7, Audit Record Reduction and Report Generation

Responsible Party (M/I): M

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

AU-8, Time Stamps

Responsible Party (M/I): M

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The ATC has at least one reliable time source (internal or external), and two are recommended. All audit logs should be time-stamped based on that time source (see parameter value).

Risk References and Resources:

NIST SP 800-82: Example compensating controls include using a separate system designated as an authoritative time source. See related control SC-45.

ARC-IT Mechanisms: The device shall support Network Time Protocol (NTP) and/or contain or have a means of synchronizing with a Global Positioning System (GPS) receiver.

AU-9, Protection of Audit Information

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is primarily a technical control implemented by the manufacturer/vendor, but the IOO identifies who is to be alerted upon detection. The IOO also controls access to audit logs, permitting access by only privileged users.

Risk References and Resources:

ARC-IT Mechanisms: Audit information is to be treated as information for which privileged access is required and protected per control AC-3.

AU-9(2), Protection of Audit Information | Store on Separate Physical Systems or Components

Responsible Party (M/I): M

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is primarily a technical control, but the IOO determines the frequency of storing audit records in a repository. The IOO may also need to convey to the manufacturer/vendor any ATC design requirements to enable storing audit records in a separate system identified by the IOO or recommended by the manufacturer/vendor, which may require ATC configuration and connectivity to “external systems” (e.g., cloud storage).

Parameter Value(s):

“at least weekly”

Risk References and Resources:

ARC-IT Mechanisms: See control AU-9.

AU-9(3), Protection of Audit Information | Cryptographic Protection

Responsible Party (M/I): M

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is primarily a technical control, but the IOO may recommend or require the manufacturer/vendor the type and strength of cryptographic mechanism (e.g., signed hash using asymmetric cryptography).

Risk References and Resources:

ARC-IT Mechanisms: See control AU-9.

AU-9(6), Protection of Audit Information | Read-Only Access

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is both an organizational and a technical control. This control would be necessary if the TMC operators, for example, are monitoring activities and, therefore, would need to read (but not modify) the audit logs. Only audit administrators would need full read/write access. The manufacturer/vendor would need to design the ATC to restrict access to read-only for authorized personnel.

AU-10, Non-Repudiation

Responsible Party (M/I): M

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is a technical control applicable only for device non-repudiation (see the ARC-IT Mechanisms discussion below). However, the IOO conveys to the manufacturer/vendor which actions are to be covered by non-repudiation.

Risk References and Resources:

NIST SP 800-82: Some ITS devices may not enforce non-repudiation of audit records and may require compensating controls. Examples of compensating controls include physical security systems, cameras to monitor user access, or a separate device for log collection.

ARC-IT Mechanisms:

- Device non-repudiation is limited to configuration changes and application installation. All such actions shall require the use of digital credentials associated with the user or process.
- Stores credentials associated with configuration changes for a minimum of one year.
- Stores credentials associated with application installation (including updates, patches) for a minimum of one year.

AU-12, Audit Record Generation

Responsible Party (M/I): M

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is a technical control implemented by the manufacturer/vendor. But the audit record generation capability is conveyed by the IOO to the manufacturer/vendor based on determinations made when implementing controls AU-2a, AU-2c, and AU-3.

Parameter Value(s):

paragraph a: “all information systems and network components”

Risk References and Resources:

ARC-IT Mechanisms: No specific mechanisms are mandated or prohibited.

AU-12(1), Audit Record Generation | System-Wide and Time-Correlated Audit Trail

Responsible Party (M/I): M

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is a technical control to be implemented by the manufacturer/vendor. A typical ATC by design should log all activities (e.g., those of connected sensors); therefore, compilation is not necessary, but time correlation is required.

Parameter Value(s):

2nd PV: “Organizational tolerance defined in AU-8”

Risk References and Resources:

NIST SP 800-82: Example compensating controls include providing time-correlated audit records on a separate system.

AU-12(2), Audit Record Generation | Standardized Formats

Responsible Party (M/I): M

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is a technical control, but the IOO should convey to the manufacturer/vendor what standard format is desired. The manufacturer/vendor’s concern is that standardized formats across diverse types of physical objects are required to enable audit analysis.

AU-12(3), Audit Record Generation | Changes by Authorized Individuals

Responsible Party (M/I): M

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is a technical control implemented by the manufacturer/vendor, but the IOO conveys to the manufacturer/vendor the ATC components on which logging can be changed by a given type of authorized user, and the selectable event criteria and time thresholds the IOO specifies for the parameter values.

Parameter Value(s):

1st PV: “audit administrator”

Risk References and Resources:

NIST SP 800-82: Example compensating controls include employing non-automated mechanisms or procedures.

CA FAMILY – ASSESSMENT, AUTHORIZATION, AND MONITORING

CA-5, Plan of Action and Milestones

Responsible Party (M/I): I

Justification to Select: Vulnerability “Lack of a vulnerability management program” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control implemented primarily by the IOO; however, the IOO may advise or require the manufacturer/vendor to initiate a plan of action and milestones (POA&M) as the ATC is being designed and built and then provide that POA&M upon delivery of the ATC. The IOO uses the PO&AM to better understand which security controls (and, therefore, requirements) were not implemented satisfactorily. The IOO needs to understand the risk the ATC brings to ITS operations before allowing the ATC to be installed and operated. If unacceptable risks are identified, the IOO may mitigate the risks or require the manufacturer/vendor to do so. Compensating controls may also be implemented to reduce the risk to an acceptable level.

Parameter Value(s):

“at least quarterly or as weaknesses (e.g., non-compliant controls) are corrected”

Risk References and Resources:

NIST SP 800-82: Corrective actions identified in assessments may not be immediately actionable in an ITS environment; therefore, short-term mitigations may be implemented to reduce risk as part of the gap closure plan or plan of action and milestones.

CA-6, Authorization

Responsible Party (M/I): I

Justification to Select: Threat “Exploit poorly configured or unauthorized systems exposed to the Internet.” in **Table 2**, Section *Exploit and compromise.*

Guidance: This is an organizational control implemented by the IOO, but not necessarily in the same sense as large organizations would implement it in accordance with NIST SP 800-37. The entire Risk

Management Framework with all its official roles and responsibilities need not be implemented, but to manage risk and incrementally improve the cybersecurity posture, at the very least there should be a senior official in the IOO who is apprised of the risk and explicitly accepts that risk of operating the ITS. This control, in fact this entire control set, is leading the ITS community to a more risk-based approach. As the ITS community begins to develop and use control sets, the need will likely arise for a more formal, holistic approach to managing risk. That approach should be based on NIST SP 800-39 that lays out a comprehensive process for IOOs to *frame* risk (i.e., establish the context for risk-based decisions), *assess* risk (i.e., consider threats, vulnerabilities, likelihood, and impact), *respond* to risk once determined (i.e., accept, avoid, mitigate, share, or transfer risk), and *monitor* risk on an ongoing basis.

Parameter Value(s):

> paragraph e. "If the organization and/or system is adequately covered by a continuous monitoring program, the Security Authorization may be continuously updated: If not; at least every three (3) years, when significant security breaches occur, whenever there is a significant change to the system, or to the environment in which the system operates."

CA-7, Continuous Monitoring

Responsible Party (M/I): I

Justification to Select: Vulnerability "Inadequate incident detection & response plan and procedures" in **Table 5**, Section *Policy and Procedure Vulnerabilities and Predisposing Conditions.*

Guidance: This control is entirely an organizational control. The IOO needs to determine what level of continuous monitoring is appropriate for their specific ITS implementation.

Risk References and Resources:

> [SP 800-82]: Continuous monitoring programs for ITS should be designed, documented, and implemented with input from ITS personnel. The organization ensures that continuous monitoring does not interfere with ITS functions. The individual/group designing and conducting the continuous monitoring for the ITS implements monitoring consistent with the organizational information security policies and procedures, the ITS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. Continuous monitoring can be automated or manual at a frequency sufficient to support risk-based decisions. For example, the organization may determine for lower-risk, isolated systems to monitor event logs manually on a specified frequency less often than for higher-risk, networked systems.

CA-7(6), Continuous Monitoring | Automation Support for Monitoring

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate incident detection & response plan and procedures" in **Table 5**, Section *Policy and Procedure Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should define the automated mechanisms required to ensure accuracy, currency, and availability of monitoring results for the ATC. The manufacturer/vendor should implement the required features to enable continuous monitoring at the ATC side, at the network connectivity side (e.g., router/firewall upstream from the ATC), and/or at the TMC side. The manufacturer/vendor may be able to recommend what those features may be.

CA-8, Penetration Tests

Responsible Party (M/I): I

Justification to Select: Vulnerability "Lack of a vulnerability management program" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.* Pen tests serve as a way to examine whether an IOO's security policies are genuinely effective. Pen-tests also identify vulnerabilities in a system and provide awareness of and enhance cybersecurity hygiene.

Guidance: This is entirely an organizational control, but it is selected due to the considerable benefits that can be realized by the IOO through regular penetration testing. Results of penetration tests are used to identify vulnerabilities and corrective actions required to reduce the risk of operating ATCs.

Parameter Value(s):

"at least annually"

Risk References and Resources:

NIST SP 800-82: Penetration testing is used with care on ITS networks to ensure ITS functions are not adversely impacted by the testing process. In general, ITS systems are highly sensitive to timing constraints and have limited resources. Example compensating controls include employing a replicated, virtualized, or simulated system to conduct penetration testing. Production ITS may need to be taken off-line before testing can be conducted. If ITS are taken off-line for testing, tests are scheduled to occur during planned ITS outages whenever possible. If penetration testing is performed on non-ITS networks, extra care is taken to ensure that tests do not propagate into the ITS network.

CA-9, Internal System Connections

Responsible Party (M/I): I

Justification to Select: Vulnerability "Inappropriate segmentation of asset management system" in **Table 5**, Section *Sensor, Final Element, and Asset Management Vulnerabilities and Predisposing Conditions.*

Guidance: This approach of pre-approving specific types of internal connections (e.g., connecting an operational user's laptop directly or wirelessly to the ATC) is essential to managing connection risks to the ATC. The IOO should not authorize each internal system connection individually, as that could be unmanageable. Rather, the IOO should authorize internal connections for a class of system components (e.g., operational user laptop, road crossing signs, cameras, railroad crossing gates) with common characteristics and/or configurations.

Parameter Value(s):

paragraph d. "at least annually"

Risk References and Resources:

NIST SP 800-82: Organizations perform risk-benefit analysis to determine whether ITS equipment should be connected to other internal system components, then document these connections. The authorizing official fully understands the potential risks associated with approving individual connections or approving a class of components to be connected. The authorizing official may broadly approve the connection of a certain type of sensors, while other connection types (e.g., serial or ethernet) require individual approval. Decisions to accept risk are documented.

CM FAMILY – CONFIGURATION MANAGEMENT

CM-2, Baseline Configuration

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is a technical control that needs to be primarily implemented by the IOO, but the manufacturer/vendor may be contracted to provide configuration management support.

Parameter Values: paragraph b.1. “at least annually”

CM-3, Configuration Change Control

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is a technical control that needs to be primarily implemented by the IOO, but the manufacturer/vendor may be contracted to provide configuration management support.

Risk References and Resources:

NIST SP 800-82: Configuration change control procedures should align with the organization’s management of change practices.

CM-3(5), Configuration Change Control | Automated Security Response

Responsible Party (M/I): M

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is a technical control that could be implemented on the ATC, but the configuration baselines that would need to be referenced are likely maintained at the TMC. The ATC would not likely halt functions or halt processing, but the ATC should alert the TMC when there is an unauthorized modification to a configuration item.

Parameter Value(s):

“ATC alerts the TMC”

CM-3(8), Configuration Change Control | Prevent or Restrict Configuration Changes

Responsible Party (M/I): M

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: If the ATC cabinet is broken into, there needs to be a means to restrict configuration changes. This refers to software and hardware that is not changed often; it does not refer to settings of traffic signal program.

Parameter Value(s):

“when the configuration change may adversely impact operations or mission (e.g., exercises, real world operations)”

Risk References and Resources:

NIST SP 800-82: The organization prevents or restricts configuration changes based on a risk determination that the system should not be modified without additional permission.

CM-5, Access Restrictions for Change

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: Only the "enforce" function can be performed at the ATC. All other functions (define, document, and approve) are performed by the IOO staff (e.g., at the TMC). The IOO may need to convey to the manufacturer/vendor any requirements for the physical or logical access restrictions to be implemented by the ATC.

Risk References and Resources:

NIST SP 800-82: Some ITS devices may allow for the configuration and use of mode change switches. Where available, these should be used to prevent unauthorized changes.

CM-5(1), Access Restrictions for Change | Automated Access Enforcement and Audit Records

Responsible Party (M/I): M

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is a technical control, but the IOO may need to advise on, or the manufacturer/vendor may recommend, the automated mechanisms used to enforce access restrictions for change. Ensure control AU-2 includes the requirement to log accesses associated with applying configuration changes.

CM-5(6), Access Restrictions for Change | Limit Library Privileges

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Hardware, firmware, and software not under configuration management" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is both an organizational and a technical control. More advanced ATCs may have software libraries, and if so, privileges to change software resident in those libraries are limited to authorized personnel. The manufacturer/vendor designs these features, but the IOO determines and limits privileges.

CM-6, Configuration Settings

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Hardware, firmware, and software not under configuration management" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is both an organizational and a technical control. The IOO may determine the appropriate configuration settings and then require the manufacturer/vendor to design and implement the ITS with those configuration settings. Alternatively, the manufacturer/vendor can convey recommended configuration settings to the IOO, and the configuration settings can be changeable by the IOO.

CM-7, Least Functionality

Responsible Party (M/I): M/I

Justification to Select: The principle of least functionality specifies that systems are configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, and/or services that are not integral to the operation of the system. Implementing Least Functionality is fundamental security best practice.

Guidance: This is primarily a technical control implemented by the manufacturer/vendor, but the IOO determines and conveys to the manufacturer/vendor the mission critical capabilities and which functions, ports, protocols, software, and or services are prohibited or restricted. To consistently manage risk across ITS systems, it may be helpful for the ITS community to develop a process for evaluating all functions, ports, protocols, software, and/or services the community may use and publish a matrix of allowed and disallowed functions, ports, protocols, software, and/or services. Mechanisms such as a host-based firewall may be used to restrict ITS ports and protocols. Additionally, the ITS should implement an internal monitoring capability to detect unauthorized services that may be running.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0814 / T0830, T0878, T0803, T0842, T0846, T0888
- M0928 / T0847

- M0942 / T0830, T0807, T0885, T0816, T0866, T0822, T0847
- M0954 / None[21]

NIST SP 800-82: The organization implements least functionality by allowing only specified functions, protocols, and/or services required for ITS operations. For non-routable protocols such as serial communications, interrupts could be disabled or set points could be made read-only except for privileged users to limit functionality. Ports are part of the address space in network protocols and are often associated with specific protocols or functions. For routable protocols, ports can be disabled on many networking devices to limit functionality to the minimum required for operation.

ARC-IT Mechanisms:

- Device shall expose only those services required to operate and currently deemed secure (e.g., secure shell [SSH] version 2.0, secure web interface).
- Device shall enable disabling all system services and applications that are not essential to operation.
- Device shall support data loss prevention policies.
- The device shall implement one or both of the following:
    - The device requires that all software installed is signed (corresponding to ongoing privileged access in the language of Notes on Access Control[22]).
        - If this approach is taken, the integrity of the verification key shall be protected by local hardware, either by directly storing the key in local hardware, or by creating a chain of trust from the key to a hardware-protected key. The hardware protection shall be equivalent to Federal Information Processing Standard FIPS 140-2[23] level 2, 3 or 4 as specified in Notes on Access Control[24].
    - The device allows unsigned software to be installed only by an authenticated user with periodic privileged access to the specific resources necessary for program installation, i.e., it does not automatically boot into a state where that access is permitted.
        - If this approach is taken, the device shall require that the authenticated user be authenticated using multi-factor authentication and that at least one of the factors is protected by cryptographic hardware on the device. See control IA-2 for further description.

[21] No specific technique is mapped to this mitigation. Rather, it is expected to implement configuration changes to software (other than the operating system) to mitigate security risks associated with *how the software operates*.

[22] https://www.arc-it.net/html/security/controlsclarification.html

[23] Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 25, 2001.

[24] https://www.arc-it.net/html/security/controlsclarification.html

CM-7(1), Least Functionality | Periodic Review

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Poor configurations are used” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This control is both organizational and technical. The IOO reviews the system to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services, and resolves any issues that can be resolved at that level. However, the manufacturer/vendor may also need to identify required changes and potentially implement those changes on configuration items they manage on behalf of the IOO.

Parameter Value(s):

paragraph a. “At least annually or as system changes or incidents occur.”

paragraph b. “All functions, ports, protocols, software, and services within the system identified per control CM-7 to be unnecessary and/or nonsecure.”

CM-7(2), Least Functionality | Prevent Program Execution

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Poor configurations are used” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is primarily a technical control, but the IOO should identify and then convey to the manufacturer/vendor any policies, rules of behavior, and/or access agreements regarding software program usage and restrictions as well as any rules authorizing the terms and conditions of software program usage. The concern is mostly about the danger of the auto-execute feature.

Risk References and Resources:

ARC-IT Mechanisms:

- Require that software be signed.
- Use hardware protection to secure a key used to verify software before installation.
- Only allow software to be installed by a particular user role which is not activated by default on startup.
- Support an approved user authentication mechanism for the user role of updating software.

CM-7(5), Least Functionality | Authorized Software – Allow-by-Exception

Responsible Party (M/I): M/I

Justification to Select: Using an allow-list provides a configuration management method to allow the execution of only authorized software which can decrease the likelihood of malicious software executing on the system.

Guidance: This is both an organizational and a technical control. The IOO identifies software programs authorized to execute on the system and conveys that to the manufacturer/vendor to design and implement, using a deny-all, permit-by-exception approach. The IOO reviews and updates the list of authorized software programs, and if needed, conveys any changes to the manufacturer/vendor for configuration items they manage on behalf of the IOO. The set of applications that run on the ATC should be relatively static, which makes it easy to list the applications. If the set of applications is not static, implement control CM-7(4) instead.

Parameter Value(s):

paragraph c. “at least annually”

Risk References and Resources:

NIST SP 800-82: The set of applications that run in ITS is relatively static, making allow listing practical; therefore, the organization may recommend using application allow listing for ITS equipment.

CM-7(8), Least Functionality | Binary or Machine Executable Code

Responsible Party (M/I): M/I

Justification to Select: Binaries, especially those from questionable sources or without source code, are difficult to verify and may be used by an adversary for attacks such as proxy execution, and thus pose a threat to proper ATC function if allowed to run on the ATC.

Guidance: This is both an organizational and a technical control. The IOO decides whether to prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code and then conveys those decisions to the manufacturer/vendor to design and build into the ATC.

CM-7(9), Least Functionality | Prohibiting the Use of Unauthorized Hardware

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is both an organizational and a technical control. The IOO identifies and conveys to the manufacturer/vendor any hardware components that are authorized for system use or are prohibited from use or connection. The IOO reviews and updates the list of authorized hardware components and, as needed, conveys changes to the manufacturer/vendor who may be managing the configuration on behalf of the IOO.

Parameter Value(s):

paragraph c. “at least annually”

CM-11, User-Installed Software

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is primarily an organizational control, as the IOO establishes policies governing the installation of software by users. However, the IOO should convey to the manufacturer/vendor those policies and the requirement for the ATC to enforce software installation policies through appropriate methods. Once the ATC is delivered and operational, the IOO monitors for policy compliance. The IOO is concerned mostly with the privileged operational users, as they are the only users who are allowed to install software.

Parameter Value(s):

paragraph c. “continuously”

Risk References and Resources:

ARC-IT Mechanisms: As specified in control CM-7.

CM-11(2), User-Installed Software | Software Installation with Privileged Status

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is primarily a technical control, and it applies to the privileged operational users, as they are the only users who can install software. However, the IOO conveys to the manufacturer/vendor the requirement for the ATC to be designed and built to allow installation of software only with explicit privileged status. Note the linkage to related controls AC-5 and AC-6.

CM-11(3), User-Installed Software | Automated Enforcement and Monitoring

Responsible Party (M/I): M

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is primarily a technical control. Enforcement and monitoring of compliance with software installation policies is typically implemented using automation on the system. As such, the IOO should convey such requirements to the manufacturer/vendor for design and implementation on the ATC in such a manner that it provides an indicator of attack.

CM-14, Signed Components

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This control is both an organizational and a technical control. The IOO identifies which software and firmware components require verification that the component has been digitally signed (typically any software and firmware components) and conveys that requirement to the manufacturer/vendor for design and implementation. The IOO may also specify which certificates are recognized and approved by the IOO.

Parameter Value(s):

“any software and firmware components”

CP FAMILY – CONTINGENCY PLANNING

CP-9, System Backup

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Critical configurations are not stored or backed up” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, but some aspects could be performed on the ATC. There is no user information to back up, so part a of the control text is not relevant. Also, it would not be feasible for the ATC to have a back-up ATC device or a hot standby ATC. Backups of system information could be automated on the ATC, but that might not always be feasible. It is more likely the TMC would perform the backups, but the ATC may need to be designed to allow such actions, which is a requirement the IOO would need to convey to the manufacturer/vendor.

Parameter Value(s):

paragraph b. “At least weekly or as defined in the contingency plan”

paragraph c. “When created, received, updated, or as defined in the contingency plan “

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0953 / T0809, T0813, T0826, T0827, T0831

CP-9(1), System Backup | Testing for Reliability and Integrity

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Critical configurations are not stored or backed up” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: Testing is typically performed by the IOO, not by the ATC. But, if automation is desired for testing, it may be necessary for the IOO to convey those requirements to the manufacturer/vendor to design and build in that capability.

Parameter Value(s):

“at least monthly or as defined in the contingency plan”

Risk References and Resources:

NIST SP 800-82: Testing for reliability and integrity increases confidence that the system can be restored after an incident, and minimizes the impact associated with downtime and outages. The ability to test backups is often dependent on resources, such as the availability of spare devices and testing equipment, needed to appropriately represent the environment. Testing backup and restoration on ITS is often limited to systems with redundancy or spare equipment; in certain cases, sampling will be limited to those redundant systems. Compensating controls may include alternative methods for testing backups such as hash or checksum validations.

CP-9(2), System Backup | Test Restoration Using Sampling

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Critical configurations are not stored or backed up” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: Testing the restoration capability is typically performed by the IOO and not by the ATC. However, if automation is desired to facilitate testing the restoration capability, it may be necessary for the IOO to convey those requirements to the manufacturer/vendor to design and build in that capability.

Risk References and Resources:

NIST SP 800-82: Testing for reliability and integrity increases confidence that the system can be restored after an incident, and minimizes the impact associated with downtime and outages. The ability to test backups is often dependent on resources, such as the availability of spare devices and testing equipment, needed to appropriately represent the environment. Testing backup and restoration on ITS is often limited to systems with redundancy or spare equipment; in certain cases, sampling will be limited to those redundant systems. Compensating controls may include alternative methods for testing backups such as hash or checksum validations.

CP-9(8), System Backup | Cryptographic Protection

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Use of unsecure ITS protocols” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: This is both an organizational and a technical control. The IOO may need to convey to the manufacturer/vendor which backup information requires protection and any protection requirements (e.g., cryptography for integrity) for backup information transmitted from the ATC to the backup location (e.g., the TMC) so those requirements can be designed and built into the ATC and its communications.

CP-12, Safe Mode

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: Safe mode is roughly equivalent to flash (i.e., all not-steady red) on the ATC. The IOO may need to define the conditions under which the ATC should go into safe mode (i.e., flash) and any restrictions of safe mode operation, but the IOO conveys those conditions and restrictions to the manufacturer/vendor so they can design and build those capabilities into the ATC.

Risk References and Resources:

NIST SP 800-82: This control provides a framework for the organization to plan its policy and procedures for dealing with ITS conditions beyond its control in the environment of operation to minimize potential safety and environmental impacts.

ARC-IT Mechanisms:

- Device shall support identification of conditions to trigger safe mode.
- The list of conditions that trigger safe mode shall require privileged access to modify.
- Device shall monitor its state to identify satisfactory conditions to trigger safe mode.
- Device shall apply safe mode operations as identified in Supplemental Guidance Table[25].
- Device shall stop sending messages for applications affected by related failure condition(s).

IA FAMILY – IDENTIFICATION AND AUTHENTICATION

IA-2, Identification and Authentication (Organizational Users)

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Authentication of users, data or devices is substandard or nonexistent" in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.* Whenever a user needs to make changes or perform operations to the ATC, user identification and authentication is required to prevent unauthorized access and other attacks to the ATC.

Guidance: This is both an organizational and a technical control. The IOO identifies the types of users and the identification and authentication needs, then conveys those requirements to the manufacturer/vendor who designs and builds in the capability to uniquely identify and authenticate users. The ATC supports both privileged and non-privileged users; both would need to be uniquely identified and authenticated when accessing the controller either locally or remotely. The types of authentication may vary from one type of user to another.

[25] https://www.arc-it.net/html/security/control21.htm.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0804 / T0800, T0858, T0885, T0816, T0871, T0838, T0839, T0861, T0843, T0845, T0886, T0857

NIST SP 800-82: In cases where shared accounts are required, compensating controls include providing increased physical security, personnel security, and auditing measures. For certain ITS, the capability for immediate operator interaction is critical. Local emergency actions for ITS are not hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical controls.

ARC-IT Mechanisms:

- Device shall require multi-factor authentication for the system management actions defined in Notes on Access Control[26]:
    - Install software other than signed software whose signature chains to a verification key whose integrity is protected by hardware on the device.
    - Modify the access control policy specified in control AC-3.
    - Modify the information flow control policy specified in control AC-4.
    - Define what types of failed authentication attempts are logged for future action as specified in control AC-7.
    - The list of auditable activities and the audit log specified in control AU-2.
    - Deletion of audit log data as specified in control AU-9, except in the case where the audit log has exceeded the allotted storage space.
    - Add or remove root certificates except when this is done via a signed instruction whose signature chains to a verification key whose integrity is protected by hardware on the device.
    - Device may require multi-factor authentication for other actions.
- Passwords used in multi-factor authentication shall meet the requirements specified in control IA-5(1).
- Device shall require multi-factor authentication for the system management actions defined in Notes on Access Control[27].
- Device may require multi-factor authentication for other locally accessed actions.
- Network access to privileged accounts shall be over SSH, which provides replay resistance. NOTE: SSH shall use Rivest, Shamir, and Adleman (RSA) keys of length 2048 bits or longer or elliptic-curve cryptography (ECC) keys of length 256 bits or longer.

[26] https://www.arc-it.net/html/security/controlsclarification.html.

[27] https://www.arc-it.net/html/security/controlsclarification.html.

- Device may accept personal identity verification (PIV) credentials as specified in FIPS 201-3[28] and supporting guidance documents.
- The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

IA-2(1), Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts

Responsible Party (M/I): M

Justification to Select: Vulnerability "Authentication of users, data or devices is substandard or nonexistent" in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: The ATC privileged users (privileged Operational Users and User Developers) perform privileged operations on the ATC, and these operations' security is paramount to the ATC functioning correctly (e.g., "load programs and maintain both application programs and the Linux environment itself" [ATC 5401[29]]). Therefore, such users would need to be uniquely identified and authenticated via more than one factor when accessing the ATC either locally or remotely.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques: M0932 (applicable to both connections from the TMC and local to the ATC) / T0822, T0842, T0859

NIST SP 800-82: As a compensating control, physical access restrictions may sufficiently represent one authentication factor, provided the system is not remotely accessible.

ARC-IT Mechanisms: Passwords used in multi-factor authentication meet the requirements specified in control IA-5(1).

ARC-IT Protocol Implementation Conformance Statements:

- Supports multi-factor authentication for network-accessed security management actions.
- Supports installation of non-signed software. Only if previously approved by the IOO and it is software required by policy of the IOO.
- Supports modification of the access control policy specified in AC-3.
- Supports modification of information flow control policy specified in AC-4.

[28] Federal Information Processing Standard (FIPS) 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors, January 2022.

[29] Institute of Transportation Engineers (ITE) / American Association of State Highway and Transportation Officials (AASHTO) / National Electrical Manufactures Association (NEMA), Application Programming Interface (API) Standard for the Advanced Transportation Controller (ATC) 5401 Version 02A, July 29, 2020.

- Supports definition of what types of failed authentication attempts are logged for future action as specified in AC-7.
- Supports the list of auditable activities and the audit log specified in AU-2.
- Allows deletion of audit log data as specified in AU-9, except in the case where the audit log has exceeded the allotted storage space.
- Supports add or remove root certificates.
- Requires multi-factor authentication for other network-accessed actions.

Passwords used in multi-factor authentication meet the requirements specified in IA-5(1).

IA-2(2), Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts

Responsible Party (M/I): M

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: This control is applicable if the ATC or more likely any associated applications require actions by non-privileged users (e.g., regular Operational Users). Multi-factor authentication should be used for all types of accounts, privileged or non-privileged.

Risk References and Resources:

NIST SP 800-82: As a compensating control, physical access restrictions may sufficiently represent one authentication factor, provided the system is not remotely accessible.

IA-2(5), Identification and Authentication (Organizational Users) | Individual Authentication with Group Authentication

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: This is both an organizational and a technical control. The IOO determines if group accounts will be allowed. Given many operational users may need to access an ATC, it could be prudent to establish a group account to which operational users can authenticate, but only after having authenticated to their individual account. Once that decision is made, the IOO conveys the requirements to the manufacturer/vendor to design and build the capability into the ATC.

Risk References and Resources:

NIST SP 800-82: For local access, physical access controls and logging may be used as an alternative to individual authentication on an ITS. For remote access, the remote access authentication mechanism will be used to identify, permit, and log individual access before permitting use of shared accounts.

IA-2(8), Identification and Authentication (Organizational Users) | Access to Accounts — Replay Resistant

Responsible Party (M/I): M

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Parameter Value(s):

“privileged accounts, at a minimum”

Risk References and Resources:

ARC-IT Mechanisms:

- Support SSH access to privileged accounts, requiring RSA keys of length 2048 bits or longer or ECC keys of length 256 bits or longer.

IA-3, Device Identification and Authentication

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should define devices and types of devices that must be uniquely identified and authenticated by the ATC before allowing access to ATC data and applications. The manufacturer/vendor implements the functionality on the ATC to identify and authenticate devices and types of devices as required by the IOO. For user-initiated actions via complex/powerful devices (e.g., operational user’s laptop –which are intermittently connected for diagnostics or maintenance), the ATC should be configured to authenticate the device (not just the user) that is trying to connect to it. This applies in cases where access is via the network (including short-range wireless). For device-initiated actions from permanently fixed, directly connected devices with limited functionality (e.g., cameras, signs, other sensors/actuators), the ATC would need to identify them, likely using a Media Access Control (MAC) address. But such devices may not need to be authenticated each time they perform some action, as they are permanently connected.

Parameter Value(s):

1st PV: “all devices”

2nd PV: “local, remote, and network”

Risk References and Resources:

NIST SP 800-82: ITS devices (e.g., cameras, signs) often may not inherently support device authentication. If devices are local to one another, physical security measures that prevent unauthorized communication between devices can be used as compensating controls. For remote communication, additional hardware may be required to meet authentication requirements.

Given the variety of ITS devices and physical locations of ITS devices, organizations may consider if types of ITS devices that may be vulnerable to tampering or spoofing require unique identification and authentication, and for what types of connections.

IA-3(1), Device Identification and Authentication | Cryptographic Bidirectional Authentication

Responsible Party (M/I): M

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: Cryptographic authentication of operational user’s laptops connecting to the ATC for diagnostics or maintenance is desirable so the controller may confirm the laptop is legitimate. It is also advisable for the laptop to require cryptographic authentication of the ATC or any of its components to which the laptop connects to ensure none of the components have been substituted, counterfeited, or compromised, which potentially compromises the laptop and anything it connects to in the future.

Parameter Value(s):

1st PV: “all devices”

2nd PV: “local, remote, or network”

Risk References and Resources:

NIST SP 800-82 For ITS that include industrial internet of things (IIoT) devices, this enhancement may be needed to protect device-to-device communication.

IA-5, Authenticator Management

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: This is both an organizational and a technical control. The IOO manages the authenticators, such as verifying identity for initial authenticator distribution, administrative procedures, or changing or refreshing authenticators. But the IOO also conveys requirements to the manufacturer/vendor for authenticators, such as authenticator content, authenticator strength of mechanism, changing default authenticators prior to use, or protecting authenticators.

Parameter Value(s):

paragraph f. 1st PV: (reference NIST SP 800-63B for the most current values for refreshing passwords.)

paragraph f. 2nd PV: “as a minimum, when compromise of the authenticator is suspected or confirmed.”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0927 / T0812, T0822, T0886, T0859
- M0936 / T0822, T0859

NIST SP 800-82: Example compensating controls include physical access control and encapsulating the ITS to provide authentication external to the ITS.

ARC-IT Mechanisms:

- Device shall store encrypted hashed passwords in a database (only accessible to privileged users) using a strong encryption algorithm.
- Device shall enforce password-related security policy (e.g., frequent change, difference between old and new passwords, length)
- Device shall provide a secure mechanism for users to update their password.
- Device shall only allow network login attempts over a secure channel.
- Device shall require the old password for password reset by a user.
- Device shall implement a secure mechanism for “forgot password.”
- Device shall be able to store public key infrastructure (PKI)-based credentials.
- Device shall support X.509 certificate chain construction.

Standards: [SP 800-63B]

IA-5(1), Authenticator Management | Password-Based Authentication

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Passwords generation, use, and protection not in accord with policy” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is both an organizational and a technical control. The IOO, for example, decides whether to allow password authentication (as opposed to other methods) and maintain and update a list of commonly used, expected, or compromised passwords such that when users create or update passwords they can be verified against the list. The IOO should convey to the manufacturer/vendor password-based authentication requirements, such as the need to transmit passwords only over cryptographically protected channels, storing passwords securely, employing automated tools to assist in password selection, and enforcing composition and complexity rules.

Parameter Value(s):

paragraph a. “at least quarterly”

paragraph h. “A case sensitive minimum of 8-character mix of uppercase letters, lower case letters, numbers, and special characters in including at least one of each; modify at least 50% of the characters when new passwords are created.”

Risk References and Resources:

ARC-IT Mechanisms: See control IA-5.

- Stores encrypted hashed password in a database (only accessible to privileged users)
- Enforces password-related security policy.
- Provides a secure mechanism for users to update their password.
- Allows network login attempts over a secure channel.
- Requires old password for password reset by a user.
- Implement a secure mechanism for “forgot password.”

Standards: [SP 800-63B]

IA-5(2), Authenticator Management | Public Key-Based Authentication

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: Where the IOO has decided to use public key-based authentication for individuals (e.g., operational users), machines, and/or devices, the IOO conveys to the manufacturer/vendor the requirements associated with this control for design and implementation on the ATC. This control is likely more relevant to the machines and devices than to the operational users, but those users are not necessarily out of scope.

Risk References and Resources:

ARC-IT Mechanisms: See control IA-5

ARC-IT Protocol Implementation Statements:

- Stores PKI-based credentials
- Supports X.509 certificate chain construction.

IA-5(5), Authenticator Management | Change Authenticators Prior to Delivery

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, but the IOO requires the manufacturer/vendor to provide unique authenticators or change default authenticators before delivery and/or installation.

IA-5(7), Authenticator Management | No Embedded Unencrypted Static Authenticators

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, but the IOO requires the manufacturer/vendor to not use embedded unencrypted static authenticators.

IA-5(13), Authenticator Management | Expiration of Cached Authenticators

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: This is a technical control implemented by the manufacturer/vendor on the ATC, but the IOO decides if cached authenticators may be used to authenticate to the local machine when the network is not available. The IOO defines the time period after which the cached authenticator is no longer valid. The concern is that if cached authentication information is out of date, the validity of the authentication information may be questionable. Therefore, care must be taken in selection of the parameter value.

IA-6, Authenticator Feedback

Responsible Party (M/I): M

Justification to Select: Threat “Theft of Operational Information” in **Table 4**, Physical Object Threat Events.

Guidance: It is standard practice to obscure the authentication information (e.g., password, personal identification number [PIN]) as it is being entered, so casual observers cannot glean that information and use it to compromise the system. Given operational users may connect with a laptop in an open, public environment, there is a greater need to obscure the authenticator. Where that is not possible, care must be taken to conceal the screen as the authenticator is being entered.

Risk References and Resources:

NIST SP 800-82: This control assumes a visual interface that provides feedback of authentication information during the authentication process. When ITS authentication uses an interface that does not support visual feedback (e.g., protocol-based authentication), this control may be tailored out.

ARC-IT Mechanisms: system shall not leak information about valid vs invalid usernames by errors or login processing time.

IA-7, Cryptographic Module Authentication

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Use of unsecure ITS protocols” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: This control is applicable, but only if the crypto module is supported at the ATC; for example, a Hardware Security Module (HSM) for TLS support. Additionally, IOOs determines and provide as a requirement to the manufacturers/vendors the policies and standards that apply to embedded systems such as the ATC. This allows the manufacturer/vendor to implement the capabilities on the hardware.

Risk References and Resources:

ARC-IT Mechanisms:

- The device shall distinguish between different keys stored by the cryptographic module and shall ensure that different processes on the device have only the appropriate access to only the appropriate keys. See control SC-39 for more discussion.

- A cryptographic module in the device shall require that operators accessing the module in a privileged role authenticate to the cryptographic module using an approved mechanism. Approved mechanisms are any approved for use with FIPS 140-2[30] level 2.

IA-8, Identification and Authentication (Non-Organizational Users)

Responsible Party (M/I): M

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: Maintenance contractors are considered non-organizational users and would need to be authenticated when connecting to the ATC to perform diagnostics, maintenance, software/firmware updates, patches, etc.

Risk References and Resources:

NIST SP 800-82: The ITS Discussion for control IA-2, Identification and Authentication (Organizational Users) is applicable for non-organizational users. That is, in cases where shared accounts are required, compensating controls include providing increased physical security, personnel security, and auditing measures. For certain ITS, the capability for immediate operator interaction is critical. Local emergency actions for ITS are not hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical controls.

IA-9, Service Identification and Authentication

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: This is both an organizational and a technical control. The IOO decides which services, if any, require identification and authentication based on their criticality to ITS operations. The IOO also decides which methods of identification and authentication are appropriate and then conveys those requirements to the manufacturer/vendor for design and implementation on the ATC.

The ATC may run web services for example, to offer a better graphical user interface (GUI) to the operational user to interact with the traffic signal program (main application). As such the ATC needs to validate that the software is authorized; and for this, the software needs to be identified and authenticated (e.g., its hash of the image compared to a list of trusted applications).

[30] Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0813 / T0800, T0830, T0858, T0868, T0838, T0839, T0861, T0843, T0845, T0886, T0856, T0857, T0855, T0860 (when wireless is supported)

IA-11, Re-Authentication

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: This is both an organizational and a technical control. The ATC can, for example, force reauthentication locally when an operational user’s device connection times out or after a fixed time period. However, the ATC would not be able to discern when an operational user’s role changes or if the system categorization changes; the IOO discerns this and responds accordingly. Additionally, the IOO shall define the circumstances or situations requiring re-authentication of users and providing that requirement to the manufacturer/vendor to implement the system checks required to support such functions.

Risk References and Resources:

ARC-IT Mechanisms:

- Device shall provide the ability to force re-authentication when any of the conditions identified in “control” above holds.

ARC-IT Protocol Implementation Conformance Statements:

- Device requires user to re-authenticate when authenticator changes.
- Device requires user to re-authenticate when service provider changes.
- Device requires user to re-authenticate when security categories changes.
- Device requires user to re-authenticate when privileged functions execute.
- Device requires user to re-authenticate after a fixed period of time.
- Device requires user to re-authenticate periodically.
- Device requires process to re-authenticate when authenticator changes.
- Device requires process to re-authenticate when service provider changes.
- Device requires process to re-authenticate when security categories changes.
- Device requires process to re-authenticate when privileged functions execute.
- Device requires a process to re-authenticate after a fixed period of time.
- Device requires process to re-authenticate periodically.

MA FAMILY – MAINTENANCE

MA-4, Nonlocal Maintenance

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Poor remote access controls” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control for the most part, but per part c., the IOO should convey to the manufacturer/vendor that the ATC needs to employ strong authentication in the establishment of nonlocal (e.g., remotely from the TMC) maintenance and diagnostic sessions.

MA-4(1), Nonlocal Maintenance | Logging and Review

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, but the IOO should convey to the manufacturer/vendor that the ATC must be able to log the defined audit events for nonlocal maintenance and diagnostic sessions, such that the IOO may review the audit records to detect anomalous or suspicious activities.

MA-4(4), Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Poor remote access controls” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, but the IOO should convey to the manufacturer/vendor that the ATC must be capable of employing the defined authenticators that are replay resistant and be able to authenticate and separate the maintenance sessions from other network sessions.

MA-4(6), Nonlocal Maintenance | Cryptographic Protection

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Poor remote access controls” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

MP FAMILY – MEDIA PROTECTION

MP-3, Media Marking

Responsible Party (M/I): I

Justification to Select: Vulnerability "Unauthorized personnel have physical access to equipment" in **Table 5**, Section *Physical Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control. The ATC has a port for media, namely a USB flash drive or stick. Such media is sometimes used to load and store firmware/software updates (at the TMC) and then install them into the ATC by an operational user. Thus, the technician is expected to transport the USB flash drives, and labeling is important in order to avoid human error. It is possible for the ATC to inform the user about the contents of the USB flash drive upon insertion.

Risk References and Resources:

ARC-IT Mechanisms:

- All data deemed sensitive in nature as classified by the organization will have its intended reader/distribution clearly marked on it.
- Information such as document creator, owner, data, sensitivity rating, and distribution level should all be visible electronically and physically on any sensitive media.
- Watermarks, digital signatures, and tamper resistant seals are common methods that can be used to mark media.

MP-4, Media Storage

Responsible Party (M/I): I

Justification to Select: Vulnerability "Unauthorized personnel have physical access to equipment" in **Table 5**, Section *Physical Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control. The ATC has a port for media, namely a USB flash drive or stick. Such media is sometimes used to load and store firmware/software updates (at the TMC) and then install them into the ATC by an operational user. This type of software should be stored securely within the IOO domain, and staff should be trained to safeguard it.

Risk References and Resources:

ARC-IT Mechanisms:

- Any media storing sensitive information (either physical or digital) shall be stored and disposed of securely.
- All physical media storing sensitive information will be securely locked away when it is not in use.
- The organization will make use of proper document shredding practices including having secure receptacles for disposing of sensitive documents.
- All digital media storing sensitive information will be sufficiently encrypted at rest.
- All digital media including hard drives, portable drives, and RAM will be properly wiped and destroyed (all bits set to 0) following industry best practices when it is no longer needed.

MP-7, Media Use

Responsible Party (M/I): I

Justification to Select: Vulnerability “Unauthorized personnel have physical access to equipment” in **Table 5**, Section *Physical Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, but the IOO should require the ATC manufacturer/vendor to design/build the ATC such that it can be configured to block users or groups from installing or using unapproved hardware on systems, including USB devices. Locking the ATC cabinets helps, but if that security layer is breached, the ATC configuration must prevent this attack. The ATC must enforce system policies or physical restrictions to limit hardware such as USB devices on critical assets to prevent malware spread through removable media.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques: M0934 / T0847

PE FAMILY – PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-2, Physical Access Authorizations

Responsible Party (M/I): I

Justification to Select: Vulnerability “Unauthorized personnel have physical access to equipment” in **Table 5**, Section *Physical Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, but it is implemented differently for the ATC. There is no facility (i.e., a building); rather, the ATC is housed in a cabinet that provides physical access control. The access authorizations (i.e., who is authorized to have keys to the cabinet) are managed by the IOO.

Parameter Value(s):

paragraph c. “at least annually”

PE-2(1), Physical Access Authorizations | Access by Position or Role

Responsible Party (M/I): I

Justification to Select: Vulnerability “Unauthorized personnel have physical access to equipment” in **Table 5**, Section *Physical Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, but it is implemented differently for the ATC. There is no facility (i.e., a building); rather, the ATC is housed in a cabinet that provides physical access control. The ATC cabinet should be accessed only by authorized operational users in specialized positions or roles (e.g., installers, maintainers, administrators) who have privileged access to the logical components via physical access to the cabinet. Police also need to obtain control of an intersection in emergencies.

Parameter Value(s):

paragraph c. “at least annually”

PE-3, Physical Access Control

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Unauthorized personnel have physical access to equipment" in **Table 5**, Section *Physical Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, but it is implemented differently for the ATC. There is no facility (i.e., a building); rather, the ATC is housed in a cabinet that provides physical access control. The IOO may need to convey to the manufacturer/vendor the physical security protection requirements for the cabinet if the cabinet is delivered with the ATC. For example, part e of the control (secure keys, combinations, and other physical access devices) may be required of the manufacturer/vendor, whereas the IOO may need to implement parts a, f, and g.

Parameter Value(s):

paragraph a. "the cabinet door"

paragraph a.2. "integrated keyed lock or external padlock"

paragraph f. 2nd PV: "at least annually, or when personnel with access to keys are transferred or terminated"

Risk References and Resources:

NIST SP 800-82: The organization considers ITS safety and security interdependencies. The organization considers access requirements in emergency situations. During an emergency-related event (e.g., police need to control an intersection), the organization may restrict access to authorized individuals only. Physical access controls and defense-in-depth measures are used by the organization when necessary and possible to supplement ITS security when electronic mechanisms (e.g., cabinet alarm when opened) are unable to fulfill the security requirements of the organization's security plan.

PE-3(4), Physical Access Control | Lockable Casings

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Unauthorized personnel have physical access to equipment" in **Table 5**, Section *Physical Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should require the manufacturer/vendor to design/build the ATC components with the cabinet as a lockable casing for the equipment within.

Parameter Value(s):

"TMS components within the cabinet."

PE-3(5), Physical Access Control | Tamper Protection

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Unauthorized personnel have physical access to equipment" in **Table 5**, Section *Physical Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, but the IOO should require the manufacturer/vendor to design/build the ATC components with tamper protection/detection for key/critical components within the cabinet. The cabinet itself may also need tamper protection, as a sort of defense in depth.

Parameter Value(s):

2nd PV: “prevent and detect”

3rd PV: “key/critical components”

PE-4, Access Control for Transmission

Responsible Party (M/I): I

Justification to Select: Threat “Compromise critical systems via physical access” in **Table 2**, Section *Exploit and Compromise.*

Risk References and Resources:

ARC-IT Mechanisms:

- The organization shall restrict physical access to all servers and network infrastructure.
- The organization shall implement a Network Access Control system to prevent unauthorized access to corporate networks.

PE-6, Monitoring Physical Access

Responsible Party (M/I): M/I

Justification to Select: Threat “Compromise critical systems via physical access” in **Table 2**, Section *Exploit and compromise.*

Guidance: This is an organizational control, but it is implemented differently for the ATC. While the ATC is not installed in a facility (i.e., a building), it is almost always housed in a cabinet in a publicly accessible area. There may not be any access logs to review. The IOO should require the manufacturer/vendor to design/build the cabinet to provide monitoring of key components/functions, such that the IOO can perform physical access monitoring and be notified of unauthorized access.

PE-9, Power Equipment and Cabling

Responsible Party (M/I): M/I

Justification to Select: Threat “Conduct physical attacks on infrastructures supporting organizational facilities” in **Table 2**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).*

Guidance: This is an organizational control, but the IOO may need to require the manufacturer/vendor to design/build the ATC cabinet to protect internal cabling and uninterruptable power sources. The IOO should also determine and implement the protection needs for external power equipment and cabling not installed by the manufacturer/vendor as part of the system or component delivery.

PE-11, Emergency Power

Responsible Party (M/I): M/I

Justification to Select: Threat "Conduct physical attacks on infrastructures supporting organizational facilities" in **Table 2**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).*

Guidance: This is an organizational control, but the IOO may need to require the manufacturer/vendor to design/build the ATC to connect to emergency power sources.

PE-11(1), Emergency Power | Alternate Power Supply – Minimal Operational Capability

Responsible Party (M/I): I

Justification to Select: Threat "Conduct physical attacks on infrastructures supporting organizational facilities" in **Table 2**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).*

PE-14, Environmental Controls

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Loss of environmental control" in **Table 5**, Section *Physical Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, and it is not implemented in the same manner as for typical information technology systems (e.g., air conditioning, humidifiers). Rather, the system components are hardened to withstand environmental extremes (e.g., extreme heat or sub-zero temperatures). As such, the IOO should require the manufacturer/vendor of the ATC cabinet to design it and the components to be tolerant to relevant environmental conditions (e.g., temperature, humidity, barometric pressure, and UV index). These conditions should be well defined in the standards for the ATC.

Parameter Value(s):

paragraph b. "continuously"

Risk References and Resources:

NIST SP 800-82: ITS can operate in extreme environments and both interior and exterior locations. For a specific ITS, the temperature and humidity design and operational parameters dictate the performance specifications. As ITS and IT become interconnected and the network provides connectivity across the hybrid domain, power circuits, distribution closets, routers, and switches that support fire protection and life safety systems must be maintained at the proper temperature and humidity. When environmental controls cannot be implemented, use hardware that is engineered to withstand the unique environmental hazards.

PE-20, Asset Monitoring and Tracking

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Hardware, firmware, and software not under asset management" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, and it is not implemented in the same manner as for typical information technology systems. It may be advisable to track high value ITS assets. For a connected intersection (where ATCs are connected to roadside equipment), there is a requirement to "be connected to the correct intersection," so asset monitoring and tracking is a means to satisfy that requirement. ATCs may use the global positioning system (GPS) to monitor where they are located and will stop functioning if they are uprooted and placed somewhere else. It may also be advisable to monitor and track message signs if they are portable.

Parameter Value(s):

1st PV: "GPS"

2nd PV: "ATCs and portable message signs"

PL FAMILY – PLANNING

PL-2, System Security and Privacy Plans

Responsible Party (M/I): I

Justification to Select: Vulnerability "Inadequate security policy for ITS" in **Table 5**, Section *Policy and Procedure Vulnerabilities and Predisposing Conditions.*

Guidance: A system security plan is necessary at the very minimum in terms of security that an infrastructure owner/operator should implement. Reference PL-2 a. 14, "Include security-related activities affecting the system that require planning and coordination." The system security plan should include, for example, how ATCs use external systems (i.e., Certificate Authorities, directly or via the TMC) to periodically obtain new digital certificates for TLS support. Such external communication should be planned out.

Parameter Value(s):

paragraph c. "at least annually"

Risk References and Resources:

NIST SP 800-82: When systems are highly interconnected, coordinated planning is essential. A low-impact system could adversely affect a higher-impact system.

RA FAMILY – RISK ASSESSMENT

RA-3, Risk Assessment

Responsible Party (M/I): M/I

Justification to Select: Vulnerability, "Inadequate organizational ownership of risk assessments" in **Table 5**, Section *Policy and Procedure Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, but the IOO should require the manufacturer/vendor to perform risk assessments to identify relevant threats, vulnerabilities, and potential impacts to the ATCs and then design/build in mitigations to reduce the risk during design and development. Once the ATC is delivered, the IOO takes over risk assessments and risk mitigation but may consult the manufacturer/vendor for appropriate risk mitigations. A quantitative risk assessment approach is desirable, but resource constraints and expertise may lead to more qualitative approaches[31].

Parameter Value(s):

paragraph d "at least annually"

paragraph f. "at least annually"

RA-3(1), Risk Assessment | Supply Chain Risk Assessment

Responsible Party (M/I): M/I

Justification to Select: Threat "Inadequate organizational ownership of risk assessments" in **Table 2**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).*

Guidance: This is an organizational control, but the IOO should require the manufacturer/vendor to perform supply chain risk assessments to identify potential risks to system components, then select suppliers accordingly and/or design/build in mitigations to reduce the risk in development.

Parameter Value(s):

paragraph a. "system components determined to be key or critical to ATC functions and/or security features"

paragraph b. "at least annually"

RA-5, Vulnerability Monitoring and Scanning

Responsible Party (M/I): M/I

Justification to Select: Vulnerability, "Lack of a vulnerability management program" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This is an organizational control, but the IOO should require the manufacturer/vendor to perform vulnerability scans while the ATC is in development. Once the controller is delivered, the IOO takes over the vulnerability monitoring and scanning, possibly with the assistance of the manufacturer/vendor.

Parameter Value(s):

paragraph a. "at least every 30 days"

[31] Reference NIST SP 800-30.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques: M0916 / T0819

NIST SP 800-82: The organization makes a risk-based determination of how to monitor or scan for vulnerabilities on their systems. This may include active scanning, passive monitoring, or compensating controls, depending on the system being scanned. For example, vulnerability examination may be performed using passive monitoring and manual visual inspection to maintain an up-to-date inventory of assets. That inventory can be cross-referenced against a list of known vulnerabilities (e.g., Cybersecurity and Infrastructure Security Agency [CISA] advisories and NIST National Vulnerability Database [NVD]). Production may need to be taken offline before active scans can be conducted. Scans are scheduled to occur during planned ITS outages whenever possible. If vulnerability scanning tools are used on adjacent non-ITS networks, extra care is taken to ensure they do not mistakenly scan the ITS network. Automated network scanning is not applicable to non-routable communications such as serial networks. Compensating controls include providing a replicated or simulated system for conducting scans or host-based vulnerability applications.

ARC-IT Mechanisms:

- Device scanning to investigate application patch levels, device configuration, exposed services and known vulnerabilities shall occur at regular intervals (daily, weekly)
- The device scanning tool will maintain regular security signature updates of its own.
- The device will report on security weaknesses so vulnerabilities can be tracked and remediated centrally.
- Regular network scanning of all connected hosts shall occur.
- This could be periodic (monthly) or with any major changes to the network configuration (say the addition of new services or servers).
- Regular network scanning shall look for the following:
    - Hosts and services that are exposed but should not be.
    - Known vulnerabilities in exposed services based on public vulnerability databases.
    - Unpatched services that need updating.
    - Weak security configurations (default passwords, lack of authorization controls)
- All exposed Web Applications/Services will undergo regular web application scanning to look for common vulnerabilities affecting web applications (including OWASP-Top 10 vulnerabilities).
- Any Web applications (inaccessible from the public Internet) shall undergo a privileged access scan per [Control Enhancement 5] to identify issues affecting authenticated users.
- Application source code shall undergo regular audits, either periodically or before any major release. This can involve static analysis code audit tools, peer code review, and/or external auditors.
- Regular external audits or penetration tests on the network infrastructure, exposed services, and web applications shall be conducted.
- Application binaries shall be scanned using a binary analyzer or input fuzzer.

- The organization must have a defined process for tracking all security-related issues and remediation status identified by any scanning or auditing activities.
- The organization shall react to all legitimate vulnerabilities.

RA-7, Risk Response

Responsible Party (M/I): M/I

Justification to Select: Threat "Inadequate organizational ownership of risk assessments" in **Table 5**, Section *Policy and Procedure Vulnerabilities and Predisposing Conditions.*

Guidance: Risk cannot be mitigated until an appropriate risk response is selected and implemented. This is an organizational control, but after having identified risk through other controls in this and other families (e.g., risk assessments, vulnerability monitoring and scanning) and decided on and appropriate risk response, the IOO may need to direct the manufacturer/vendor to perform certain actions such as updating or patching hardware, software, or firmware the manufacturer/vendor is developing or is maintaining on behalf of the IOO.

SA FAMILY – SYSTEM AND SERVICES ACQUISITION

SA-4, Acquisition Process

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate incorporation of security into architecture and design" in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: This is primarily an organizational control for the IOO to implement, as it is important for the IOO to understand and document their cybersecurity requirements. More importantly, the IOO conveys those requirements to the manufacturer/vendor for implementation throughout all acquisition phases. The IOO's emphasis on certain aspects of this control will likely vary depending on their risk tolerance. For example, security assurance requirements may not be as important as acceptance criteria. Based on the cybersecurity acquisition rigor the IOO desires of the manufacturer/vendor, the IOO may want to select additional enhancements to this control, such as SA-4(1), Functional Properties of Controls. Note: The ITS community does not presently perform security categorization to select controls, so guidance and discussions on security categorization in NIST SP 800-53 can be ignored.

Risk References and Resources:

> NIST SP 800-82: Organizations engage with ITS suppliers to raise awareness of cybersecurity needs. The Supervisory Control and Data Acquisition (SCADA)/Control Systems Procurement Project provides example cybersecurity procurement language for ITS.

SA-4(2), Acquisition Process | Design and Implementation Information for Controls

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Risk References and Resources:

> NIST SP 800-82: When acquiring ITS products, consideration for security requirements may not have been incorporated into the design. Procurement may need to consider alternative products or complementary hardware, or plan for compensating controls.

SA-4(5), Acquisition Process | System, Component, and Service Configurations

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Poor configurations are used” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: Per IOO request, the manufacturer/vendor can provide the security controls of the ATC by default, and optionally described in a Security Technical Implementation Guides (STIG). For example, all unused ports will be closed by default, all passwords require reset upon first use, TLS (v1.2 or 1.3) is enabled for all communications, wireless interfaces are set to a secure setting, only required services are enabled at the ATC.

SA-4(9), Acquisition Process | Functions, Ports, Protocols, and Services in Use

Responsible Party (M/I): M/I

Justification to Select: Threat “Conduct attacks using unauthorized ports, protocols, and services” in **Table 2**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities.*

Guidance: The IOO should convey to the manufacturer/vendor the appropriate requirements in terms of what functions, ports/protocols (including version numbers) and services are to be enabled or supported by the ATC.

Risk References and Resources:

> NIST SP 800-82: When acquiring ITS products, consideration for security requirements may not have been incorporated into the design. Procurement may need to consider alternative products or complementary hardware, or plan for compensating controls.

SA-5, System Documentation

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: Documentation should be provided for both the controller and the applications running on the controller.

SA-8, Security and Privacy Engineering Principles

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO can require the manufacturer/vendor to apply the following security engineering principles: layered protections; establishing security architecture, incorporating security requirements into the system development life cycle.

SA-9, External System Services

Responsible Party (M/I): I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: Applicable to the ATC only if external systems are leveraged by the ATC; for example, there is a need to externally obtain TLS certificates or to subscribe to a weather or map service or cloud storage system.

SA-10, Developer Configuration Management

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO may convey to the manufacturer/vendor what configuration data the IOO needs to be able to adjust and by what means. For example, the IOO may need some service running at the ATC to be using a port number chosen by the IOO and not a well-known port. The manufacturer/vendor may also be expected to provide means for the IOO to track all configuration changes, and track security related updates to ATC software.

Parameter Value(s):

paragraph a. “design; development; implementation; operation; disposal”

paragraph b. “all configuration items under configuration management”

Risk References and Resources:

NIST SP 800-82: Personnel knowledgeable in security and privacy requirements are included in the change management process for the developer.

ARC-IT Mechanisms:

- Configuration management changes shall be logged and auditable.
- Application developers will use a change management / version control system to ensure that bugs and vulnerabilities do not get reintroduced to the device once they have already been patched.

SA-10(1), Developer Configuration Management | Software and Firmware Integrity Verification

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should require that all software and firmware be checked against known good values to ensure it has not been modified from the state it was when the manufacturer/vendor delivered it. In addition, all software updates from the manufacturer/vendor should be signed by the manufacturer/vendor and verified by the IOO before updating the ATCs.

Risk References and Resources:

NIST SP 800-82: Personnel knowledgeable in security and privacy requirements are included in the change management process for the developer.

ARC-IT Mechanisms:

- Configuration management changes shall be logged and auditable.
- Application developers will use a change management / version control system to ensure that bugs and vulnerabilities do not get reintroduced to the device once they have already been patched.

SA-10(6), Developer Configuration Management | Trusted Distribution

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

SA-11, Developer Testing and Evaluation

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate testing of security changes” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Risk References and Resources:

ARC-IT Mechanisms:

- Developers shall conduct application security penetration testing before any major release.
- Testers shall develop a test plan, execute it, and report on findings.
- All flaws identified must be properly documented and either remediated or accepted.

SA-11(1), Developer Testing and Evaluation | Static Code Analysis

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate testing of security changes” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

SA-11(2), Developer Testing and Evaluation | Threat Modeling and Vulnerability Analyses

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate testing of security changes” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO system engineer or integrator should ensure they convey to the manufacturer/vendor the appropriate requirements. However, this control may be tailored out due to the expense associated with the modeling and analyses.

SA-11(6), Developer Testing and Evaluation | Attack Surface Reviews

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate testing of security changes” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: Attack surfaces relevant to the ATCs include all its communication interfaces.

SA-11(8), Developer Testing and Evaluation | Dynamic Code Analysis

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate testing of security changes” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

SA-15, Development Process, Standards, and Tools

Responsible Party (M/I): I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

SA-15(5), Development Process, Standards, and Tools | Attack Surface Reduction

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

SA-17, Developer Security and Privacy Architecture and Design

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

SA-17(5), Developer Security and Privacy Architecture and Design | Conceptually Simple Design

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

SA-17(7), Developer Security and Privacy Architecture and Design | Structure for Least Privilege

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: The manufacturer/vendor could consider whether the ATC design can support preventing the instantiation of a root-level process with elevated privileges. All applications running on the ATC should be limited (sandboxed) in their computing and memory resources.

SA-20 Customized Development of Critical Components

Responsible Party (M/I): M/I

Justification to Select: Threat “Compromise software of organizational critical information systems” in **Table 2**, Section *Deliver/insert/install malicious capabilities.*

Guidance: A critical system component is the CMU. If it is done in hardware, there can be more assurance that it can be trusted (since it is more difficult to make unauthorized changes to it). However, if the CMU is a software component, then it should be considered as a candidate for this control.

SC FAMILY – SYSTEM AND COMMUNICATIONS PROTECTION

SC-2, Separation of System and User Functionality

Responsible Party (M/I): M

Justification to Select: Allowing non-privileged users to access operating system management functionality capabilities increases the risk that non-privileged users may obtain elevated privileges.

Guidance: The system management functionality should only be accessed by the Administrator/Privileged User. The user functionality (e.g., interface to the traffic signal applications) should only be accessed by the Non-Privileged User. The User Developer should only have access to application development functionality.

Risk References and Resources:

> NIST SP 800-82: Physical separation includes using separate systems for managing the ITS than for operating ITS components. Logical separation includes the use of different user accounts for administrative and operator privileges. Example compensating controls include providing increased auditing measures.

ARC-IT Mechanisms:

- The device shall separate system management functionality from user application functionality by implementing all the following:
  - The device requires an authentication mechanism for system management that is not used for any other function.
  - The device requires system management functions use memory that is either:
    - Dedicated exclusively to system management functions, or
    - Allocated dynamically to system management functions and not shared with non-management functions once allocated.
- See also SC-39 in this document.

SC-2 (1), Separation of System and User Functionality | Interfaces for Non-Privileged Users

Responsible Party (M/I): M

Justification to Select: Allowing non-privileged users to access operating system management functionality capabilities increases the risk that non-privileged users may obtain elevated privileges.

Guidance: A regular Operational User, without administrator privileges, should not have access to the ATC administration/system environment.

SC-3, Security Function Isolation

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: Security function isolation is built into most modern operating systems, to include those operating systems, (e.g., Linux) used by ATCs. Security functions for the ATC relate to establishments of secure tunnels for communication with the TMC or the roadside unit (RSU). Such authentication procedures may be done by a separate, “sandboxed” process.

Risk References and Resources:

NIST SP 800-82: Organizations consider implementing this control when designing new architectures or updating existing components. An example compensating control includes access controls.

ARC-IT Mechanisms: The device shall separate security functionality from user application functionality by implementing all the following:

- The device requires an authentication mechanism for security functions that is not used for any other function.
- The device requires security functions to use memory that is dedicated exclusively to security functions.
- See also SC-39 in this document.

SC-3(2), Security Function Isolation | Access and Flow Control Functions

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: Access and flow control functions (e.g., auditing, intrusion detection, and malicious code protection functions) could easily be implemented in software (e.g., TLS module), but using hardware could be difficult.

SC-3(3), Security Function Isolation | Minimize Non-Security Functionality

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

SC-3(4), Security Function Isolation | Module Coupling and Cohesiveness

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: Application modules should be separate from modules that manage communications security or user access control.

SC-3(5), Security Function Isolation | Layered Structures

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: Applications (e.g., traffic signal application, ramp meter application) are layered on top of the operating system functions. The manufacturer/vendor should consider that cybersecurity functions can be separated via layers from other functions of the ATC. Isolation of these functions prevents adversaries from easily accessing them with non-privileged access.

SC-5, Denial-of-Service Protection

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Denial of Service (DoS)” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.* There is limited traffic supported between the ATC and the TMC. However, DoS attacks on the ATC (by sending many legitimate-looking messages to the ATC from inside the IOO network) have been observed and caused the ATC to transition into cabinet flash.

Guidance: The IOO should define the types of DoS events that need to be limited. Additionally, the IOO should define the controls required to limit DoS events. The manufacturer/vendor should implement the controls required by the IOO. There is some rudimentary flow control protection that comes with embedded Linux; however, the ATCs are envisioned to be protected by firewall routers operating in the network hop next to them. Furthermore, some ATCs come with a firewall in the same cabinet, even though it is not required by the ATC standard.

Risk References and Resources:

NIST SP 800-82: Some ITS equipment may be more susceptible to DoS attacks due to the criticality of some ITS applications. Risk-based analysis informs prioritization of DoS protection and establishment of policy and procedure.

ARC-IT Mechanisms: See also CP-12 in this document for safe mode.

- The application shall take the current environment into consideration when determining whether to verify, forward, or react to an incoming application datagram and shall not verify, forward, or react to a datagram if it seems likely that this would lead to resource exhaustion.
- The application shall take the current environment into consideration when determining whether to cryptographically verify incoming application datagrams.
- The device shall discard internet protocol (IP) packets whose source address is unknown to the device.
- The device shall discard IP packets whose source address is known to the device if the device does not have either:
    - A request pending to the source or
    - The source is on an allow list of sources that may send the device unsolicited IP traffic.
- If the ATC is connected to an RSU, the device shall enforce limit on transmission of data to and from the RSU.
    - This limit shall be configurable through a system management function.

SC-5(1), Denial-of-Service Protection | Restrict Ability to Attack Other Systems

Responsible Party (M/I): M

Justification to Select: Vulnerability “Denial of Service (DoS)” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

It is possible that vulnerabilities in the ATC can be leveraged to exploit other connected devices such as the RSU and the TMC.

Guidance: The IOO should convey to the manufacturer/vendor the desired functionality to restrict the ability of individuals to launch DoS attacks from the ATC, but one possible solution is that the ATC may be placed on a separate virtual local area network (VLAN) from other more vulnerable devices (e.g., surveillance cameras) for security reasons and to support different bandwidth needs. This separation of ATCs may help protect them from being used to attack other connected devices. Transmission of data to the RSU or the TMC should be limited (e.g., via firewalls).

SC-5(2), Denial of Service Protection | Capacity, Bandwidth, and Redundancy

Responsible Party (M/I): M

Justification to Select: Vulnerability “Denial of Service (DoS)” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: This control can be implemented by sizing the network interface cards (e.g., wireless network interfaces) to manage a large number of ingress packets. This functionality can also be implemented (instead of or in addition to the above) at the router upstream from the ATC.

SC-5(3), Denial of Service Protection | Detection and Monitoring

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Denial of Service (DoS)” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should define monitoring tools to detect indicators of DoS attacks and they should also define the system resources that require DoS monitoring. The manufacturer/vendor should implement the monitoring tools required by the IOO. For example, the manufacturer/vendor could employ a SIEM (security information and event management) tool at the ATC.

SC-7, Boundary Protection

Responsible Party (M/I): M

Justification to Select: Vulnerability “Firewalls nonexistent or improperly configured” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

ATCs are becoming more advanced and, therefore, often provide connectivity beyond that to/from the TMC. As such, it is necessary to provide boundary protection to ensure only authorized communications are used to perform approved functions. It is not advisable to rely solely on routers external to the ATC, such as at the TMC, regional network boundaries, or other ITS shelter locations, as there may be other connections to the ATC that need to be managed.

Guidance: The manufacturer/vendor should consider implementing functionality such as advanced filtering or firewall capabilities such as packet or state inspection. ATCs should not be placed in subnetworks that are publicly accessible.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0935 / T0822
- M0937 / T0806, T0868, T0816, T0839, T0861, T0843, T0845, T0886, T0856, T0857, T0855, T0859

ARC-IT Mechanisms:

- The device shall maintain a mechanism for monitoring all communications that cross its boundary, such that:
    - All communications can be scanned and optionally logged irrespective of the function those communications are associated with:

    - Communications monitoring diagnostics and settings are restricted from general application use.
    - Communications monitoring diagnostics and settings may be modified through an administrative interface.

- The device shall discard IP packets whose source address is known to the device if the device does not have either:
  - A request pending to the source.
  - The source is on an allow list of sources that may send the device unsolicited IP traffic.
- The device shall discard IP packets whose source address is unknown to the device.
- The device shall monitor the status of its inbound firewall. If its firewall is not operating, the device:
  - Shall not accept any data from external sources targeting management, security, or application update functions (Fail Secure).
- The device shall provide support for assigning applications to categories such that two applications may only exchange data if they are classified in the same category. The device may support assigning one application to more than one category. The device shall support at least four application categories and may support more.

SC-7(3), Boundary Protection | Access Points

Responsible Party (M/I): M/I

Justification to Select: Vulnerability, "No security perimeter defined" in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions*

Guidance: The access points refer to major entry points from outside entities into an organization's internal network; this control does not refer to local connections or WiFi access points. External access is not often needed or allowed for ITS networks, but the decision on whether access is allowed or how many access points to establish and where in the infrastructure is an IOO's decision. That decision may be based on the need to allow, for example, contracted maintenance of ITS components from external sources to the internal ITS network.

Risk References and Resources:

ARC-IT Mechanisms: See SC-7

SC-7(4), Boundary Protection | External Telecommunications Services

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Firewalls nonexistent or improperly configured" in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: If implemented at the ATC, the connection to the cellular network should use the security afforded to the regular cellular devices to protect that external interface to an acceptable level. The IOO can request over-the-air security (ideally this should be the default) via the service level agreement with a mobile network operator.

Parameter Value(s):

paragraph e. “At least every 180 days”

Risk References and Resources:

ARC-IT Mechanisms: See SC-7

SC-7(5), Boundary Protection | Deny by Default — Allow by Exception

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate security policy for ITS” in **Table 5**, Section *Policy and Procedure Vulnerabilities and Predisposing Conditions.*

Guidance: Since the ATC communication peers are well known in advance and extremely limited in number, it is both feasible and advisable to enforce allowing/disallowing communication at the ATC via allow-list only.

Risk References and Resources:

ARC-IT Mechanisms: See SC-7

SC-7(7), Boundary Protection | Split Tunneling for Remote Devices

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate security policy for ITS” in **Table 5**, Section *Policy and Procedure Vulnerabilities and Predisposing Conditions.*

Guidance: Employ mechanisms to detect split tunneling in remote devices connecting to the ATC.

Risk References and Resources:

ARC-IT Mechanisms: See SC-7

SC-7(16), Boundary Protection | Prevent Discovery of System Components

Responsible Party (M/I): M

Justification to Select: Vulnerability “Perform perimeter network reconnaissance/scanning.” In **Table 5**, Section *Perform reconnaissance and gather information.*

Guidance: There should be a mechanism employed at the ATC that does not allow the discovery of the IP address of the TMC.

SC-7(18), Boundary Protection | Fail Secure

Responsible Party (M/I): M

Justification to Select: Threat event, “Loss of Safety” in **Table 4** and the vulnerability “Firewalls nonexistent or improperly configured” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: In case of failure, the secure way is to block all incoming/outgoing communications and continue to operate the traffic signal application. However, the settings for that application may have been compromised themselves. If it is desired to guard against this additional risk, the ATC could have default settings that are set in memory that is more protected.

Risk References and Resources:

NIST SP 800-82: The organization selects an appropriate failure mode (e.g., permit or block all communications). Rationale: The ability to choose the failure mode for the physical part of the ITS differentiates the ITS from other IT systems. This choice may be a significant influence in mitigating the impact of a failure.

ARC-IT Mechanisms: See SC-7

SC-7(19), Boundary Protection | Block Communication from Non-Organizationally Configured Hosts

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Firewalls nonexistent or improperly configured” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: The manufacturer/vendor should implement the functionality to block the traffic between non-organizationally configured clients that the IOO defines. It should be possible for the ATC to block communication unless that communication is from hosts in a securely configured “allow list.” If device authentication is necessary before user-level authentication is performed, then the list of approved/trusted devices that can connect to the ATC should be configured in advance in the ATC.

SC-7(21), Boundary Protection | Isolation of System Components

Responsible Party (M/I): M

Justification to Select: Vulnerability “Firewalls nonexistent or improperly configured” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: It should be possible for the ATCs to be isolated in their own VLAN separate from other field devices that may be more vulnerable (e.g., surveillance cameras).

Risk References and Resources:

ARC-IT Mechanisms: See SC-7

SC-7(23), Boundary Protection | Disable Sender Feedback on Protocol Validation Failure

Responsible Party (M/I): M

Justification to Select: Vulnerability “Firewalls nonexistent or improperly configured” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: ATCs typically do not provide error feedback. If packets are received for a protocol that is not supported (e.g., not SNMP), the packets are simply discarded by design. If the ATC is running applications other than the traffic signal itself, then those applications, when receiving packets from the network, should not return an error that reveals to an adversary probing the field device network that such application is running at that ATC.

SC-7(28), Boundary Protection | Connections to Public Networks

Responsible Party (M/I): I

Justification to Select: Vulnerability "Firewalls nonexistent or improperly configured" in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: The only authorized connections are to the TMC via managed interfaces. There may be a need to allow vendors to connect to the ATCs, but that connection should not be direct. Rather, the vendor should enter one of the approved external access points to the managed ITS network.

Parameter Value(s):

"all systems"

Risk References and Resources:

NIST SP 800-82: Organizations consider the need for a direct connection to a public network for each ITS system, including potential benefits, additional threat vectors, and potential adverse impact specifically relevant to what type of public access that connection introduces. Rationale: Access to ITS should be restricted to individuals required for operation. A connection made from the ITS directly to a public network has limited applicability in ITS environments, but significant potential risk.

SC-8, Transmission Confidentiality and Integrity

Responsible Party (M/I): M

Justification to Select: Threat event, "Perform network sniffing of exposed networks" in **Table 2**, Section *Perform reconnaissance and gather information.*

The control applies to components that transmit or receive information, as communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. S.

Guidance: The ATC transmits and receives information to/from TMC and RSU. The ATC should implement the control either in a typical manner if resources permit or in a customized manner to provide equivalent protections. Integrity protection is more important than confidentiality since the impact of information disclosure is low compared to the impact of data spoofing.

Parameter Value(s):

"confidentiality and integrity" (Note: using NIST-approved algorithms and protocols).

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0802 / T0830, T0858, T0868, T0816, T0831, T0832, T0839, T0861, T0843, T0845, T0848, T0856, T0857, T0855, T0860
- M0808 / T0839, T0842, T0857, T0860, T0887

ARC-IT Mechanisms:

- Role-based access control as specified in the Access Control family with cryptographically enforced integrity checking:
    - VPN using TLS 1.2 or 1.3 with a minimum of 128-bit (256 bit recommended) security symmetric cryptography for two-way information flows using strong password or preferably X.509 certificates for integrity protection.
    - VPN using TLS 1.2 and 1.3 with a minimum of 128-bit (256 bit recommended) security symmetric cryptography for two-way information flows using strong password or preferably X.509 certificates for confidentiality protection.

Standards: RFC 8446[32], NTCIP 9014 v01.20, section B.2[33]

SC-8(1), Transmission Confidentiality and Integrity | Cryptographic Protection

Responsible Party (M/I): M

Justification to Select: Threat events, “Perform network sniffing of exposed networks” in **Table 2**, Section *Perform reconnaissance and gather information,* and “Obtain sensitive information through network sniffing of external networks” in **Table 2**, Section Achieve results (i.e., cause adverse impacts, obtain information).

Guidance: Cryptographic protection is the only feasible means to protect the information in transit, as physical protection is not possible in most ITS environments. Ensure the strength of the confidentiality or the integrity mechanism is sufficient to protect the sensitivity of the information.

Parameter Value(s):

“prevent unauthorized disclosure of information and detect changes to information”

Risk References and Resources:

NIST SP 800-82: When transmitting across untrusted network segments, the organization explores all possible cryptographic integrity mechanisms (e.g., digital signature, hash function) to protect confidentiality and integrity of the information. Example compensating controls include physical protections such as a secure conduit (e.g., point-to-point link) between two system components.

ARC-IT Mechanisms: See SC-8

[32] Internet Engineering Task Force (IETF) Request for Comment 8446, The Transport Layer Security (TLS) Protocol Version 1.3, August 2018.

[33] National Transportation Communications for ITS Protocol (NTCIP) 9014 v01.20, Infrastructure Standards Security Assessment (ISSA), Aug 2021.

SC-10, Network Disconnect

Responsible Party (M/I): M

Justification to Select: The control applies to typical and atypical information technology that transmits or receives information. Communication paths that remain established beyond their usefulness unnecessarily expose transmitted information to the possibility of interception. Physical objects within the scope of this control set transmit or receive information; therefore, the control applies and is implemented on the physical object or possibly the distant end, either in a typical manner if resources permit or in an atypical manner to provide equivalent protections.

Guidance: Applicable for local connections by an operational user who accesses the signal program, or a User Developer who makes changes to the API. Not applicable for connections to the TMC, to allow for TLS, heartbeat, etc. Ensure the time period for disconnect is sufficiently short given the sensitivity of the information (e.g., shorter timeout periods for communications paths where information with higher sensitivity is exchanged).

Parameter Value(s):

"no more than 15 minutes"

Risk References and Resources:

NIST SP 800-82: NOTE: The intent of this control is effectively covered by AC-17 (9) for ITS systems.

ARC-IT Mechanisms:

- For Transmission Control Protocol/Internet Protocol (TCP/IP) ports in any state other than 'LISTENING,' the device shall de-allocate that TCP/IP port once 15 minutes have passed with no activity on that port.
- For UDP/IP ports in any state other than 'LISTENING,' the device shall de-allocate that User Datagram Protocol/Internet Protocol (UDP/IP) port once 15 minutes have passed with no activity on that port.

SC-13, Cryptographic Protection

Responsible Party (M/I): M

Justification to Select: Threat events, "Perform network sniffing of exposed networks" in **Table 2**, Section *Perform reconnaissance and gather information,* and "Obtain sensitive information through network sniffing of external networks" in **Table 2**, Section Achieve results (i.e., cause adverse impacts, obtain information).

Guidance: The ATC device should support the cryptographic algorithms necessary to set up TLS tunnels with device certificates. This includes a secure random number generator (see ARC-IT guidance below). This also includes securely procuring, storing, updating, and using its own certificate for TLS use, and being able to verify the TLS certificate of the communication endpoint (e.g., TMC).

Risk References and Resources:

ARC-IT Mechanisms:

- Devices may support additional cryptographic algorithms.

- Devices shall provide a FIPS 140-2[34] compliant random number generator, i.e., compliant to NIST SP 800-90A Revision 1[35].

Standards: FIPS 140-3[36], NIST SP 800-90A Rev. 1[37]

SC-17, Public Key Infrastructure Certificates

Responsible Party (M/I): M/I

Justification to Select: Threat event, "Craft counterfeit certificates" in **Table 2**, Section *Craft or create attack tools.*

Guidance: The IOO should provide means for the ATC to be securely provisioned with digital certificates, and periodically renew those certificates (e.g., annually). To this end, access to a (usually) external certificate authority is required. The provisioning could also be done by the TMC. The IOO does not need to employ its own certificate authority in their enterprise for this purpose of managing certificates for their ATC devices. The ATC should be able to generate a certificate and request a certificate to be signed by a certificate authority. Requirements for secure storage and use of the certificates are in SC-13.

SC-18, Mobile Code

Responsible Party (M/I): I

Justification to Select: Multiple threat events in **Table 2**, Section *Deliver/insert/install malicious capabilities.* Vulnerability "Inadequate authentication, privileges, and access control in software" in **Table 5**, Section *Software Development Vulnerabilities and Predisposing Conditions*.

Guidance: Mobile code in the ATC may mean binary executable data that travels on communication links. The ATC may support a web-like interface to the signal program application which may require the use of JavaScript. For security reasons, JavaScript and other such mobile code can only be run locally; running JavaScript from an external (to the ATC) source should be prohibited in the ATC by design.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0921 / T0817, T0863

[34] Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 25, 2001.

[35] National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015.

[36] Federal Information Processing Standard (FIPS) 140-3, Security Requirements for Cryptographic Modules, March 22, 2019

[37] National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015.

ARC-IT Mechanisms: The device shall only permit any code to run, whether it is "mobile code" as identified above or not, if it is installed using a mechanism permitted under CM-7.

SC-18 (3), Mobile Code | Prevent Downloading and Execution

Responsible Party (M/I): M

Justification to Select: Multiple threat events in **Table 2**, Section *Deliver/insert/install malicious capabilities.* Vulnerability "Inadequate authentication, privileges, and access control in software" in **Table 5**, Section *Software Development Vulnerabilities and Predisposing Conditions*.

Guidance: Mobile code in the ATC may mean binary executable data that travels on communication links. The ATC may support a web-like interface to the signal program application, which may require use of JavaScript. For security reasons, JavaScript and other such mobile code can only be run locally; running JavaScript from an external (to the ATC) source should be prohibited in the ATC by design.

Parameter Value(s):

"All unacceptable mobile code, such as:

- Emerging mobile code technologies that have not undergone a risk assessment nor been assigned to a risk category.
- Mobile code technologies and implementations that cannot differentiate between signed and unsigned mobile code.
- risk Unsigned mobile code deemed higher risk.
- Mobile code not obtained from a trusted source over an assured channel (e.g., TLS connection, S/MIME, code is signed with an approved code signing certificate)."

SC-21, Secure Name/Address Resolution Service (Recursive or Caching Resolver)

Responsible Party (M/I): M

Justification to Select: Vulnerability "Control network services dependent on a non-control network" in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: The ATC may need to make use of Domain Name Service (DNS) services, and so the response from the DNS server should be checked for correctness.

Risk References and Resources:

NIST SP 800-82: The use of secure name/address resolution services should be determined only after careful consideration and after verification that it does not adversely impact the operational performance of the ITS.

ARC-IT Mechanisms: The device shall require the use of Domain Name Service Security Extensions (DNSSec).

SC-23, Session Authenticity

Responsible Party (M/I): M

Justification to Select: Multiple vulnerabilities in **Table 5**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).*

Guidance: The ATC sets up TLS sessions with the TMC and the RSU if connected. As such, these are protected with standard TLS security. Any other session level protocols running should also make use of the latest security controls for that protocol (e.g., SSH equivalents).

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0802 / T0830, T0858, T0868, T0816, T0831, T0832, T0839, T0843, T0845, T0856, T0857, T0855

NIST SP 800-82: Example compensating controls include auditing measures.

ARC-IT Mechanisms:

- Approved mechanisms for session authenticity are TLS and Internet Protocol Security (IPSec) with the following parameters, which must be periodically reviewed as algorithms “age” over time and key size recommendations are updated:
    - TLS 1.2 or preferably 1.3 using algorithms currently approved by NIST, with key sizes appropriate for this use.
    - IPSec using AES (Advanced Encryption Standard) based algorithms currently approved by NIST.
- The device shall support at least one of these mechanisms.

Standards: [RFC 8446]

SC-23(1), Session Authenticity | Invalidate Session Identifiers at Logout

Responsible Party (M/I): M

Justification to Select: Multiple vulnerabilities in **Table 5**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).*

Guidance: Upon user logout, all session material should be deleted at the ATC, including session identifiers and any derived cryptographic material.

SC-23(3), Session Authenticity | Unique System-Generated Session Identifiers

Responsible Party (M/I): M

Justification to Select: Multiple vulnerabilities in **Table 5**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).*

Guidance: This control is applicable to the TLS sessions that the ATC sets up. The ATC should generate unique identifiers for any new session the ATC sets up with a communication endpoint.

SC-23(5), Session Authenticity | Allowed Certificate Authorities

Responsible Party (M/I): M

Justification to Select: Threat event, “Craft counterfeit certificates” in **Table 5**, Section *Craft or create attack tools.*

Guidance: Since the ATC has an extremely limited set of possible communication peers, it should be possible to restrict the list of trusted Certificate Authorities to a very small set. Trust in the security posture of a set of one or more certificate authorities is important for validation of peer certificates during TLS tunnel/session setup at the ATC. The list of allowed Certificate Authorities should be updated securely and in a timely fashion.

SC-24, Fail in Known State

Responsible Party (M/I): M

Justification to Select: Failing to a known state helps prevent access by unauthorized persons and ensure integrity of the information is maintained.

Guidance: Since the ATC operation affects traffic (including pedestrian) safety, the failed state should be a known *secure* state. For example, the ATC continues operating a traffic signal program though it may not be optimized. In worst cases, the ATC transitions into flash mode.

Parameter Value(s):

1st PV: “Known secure state”

Risk References and Resources:

NIST SP 800-82: The organization selects an appropriate failure state. Preserving ITS state information includes consistency among ITS state variables and the physical state which the ITS represents (communication permitted or blocked, continue operations).

Rationale: As part of the architecture and design of the ITS, the organization selects an appropriate failure state of an ITS in accordance with the function performed by the ITS and the operational environment. The ability to choose the failure mode for the physical part of ITS differentiates ITS systems from other IT systems. This choice may be a significant influence in mitigating the impact of a failure since it may be disruptive to ongoing physical processes.

ARC-IT Mechanisms: Upon detection of a device failure, the device shall cease Dedicated Short-Range Communications (DSRC)-based transmissions.

SC-27, Platform-Independent Applications

Responsible Party (M/I): M

Justification to Select: This control decreases vendor lock, increases the pool of available applications that can run on a given ATC, and requires less planning and translation across an enterprise.

Guidance: The ATC by design employs applications that are written in high-level languages (e.g., C) and so are able to run on more than one platform. Application portability and independence from underlying hardware/firmware are the tenets of modern ATC designs.

SC-28, Protection of Information at Rest

Responsible Party (M/I): M

Justification to Select: Encryption of information in storage (i.e., data-at-rest) protects the confidentiality and integrity of the information.

Guidance: The signal program data (e.g., setting of length of green light) should be afforded integrity protection. Other configuration parameters and settings (e.g., clock source, signal pre-emption data) should also be integrity protected. If desired, such data may also be confidentiality protected (e.g., encrypted with a key that is determined and stored locally), but that is not deemed strictly necessary for safe operation of the ATC. ARC-IT mechanisms can be used.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0941 / T0839, T0857

NIST SP 800-82: The use of cryptographic mechanisms is implemented only after careful consideration and after verification that it does not adversely impact the operational performance of the ITS. Cryptographic mechanisms may not be feasible on certain ITS devices. In these cases, compensating controls may be relocating the data to a location that does support cryptographic mechanisms.

ARC-IT Mechanisms:

- The device shall encrypt data on disk if that data is accessed only by entities with periodic privileged access as defined in Notes on Access Control[38].
- The device may encrypt data on disk if that data is accessed by entities with ongoing privileged access or with no privileges.
- Keys used to encrypt data on disk shall be protected by hardware of at least FIPS 140-2[39] level 2 equivalent security, such that they cannot be used other than by booting the device.

SC-28(1), Protection of Information at Rest | Cryptographic Protection

Responsible Party (M/I): M

Justification to Select: Encryption of information in storage (i.e., data-at-rest) protects the confidentiality and integrity of the information.

Guidance: Cryptographic protection is the most widely used method for protection of information at rest. For example, ATC data can be integrity protected (e.g., with a signature or a Message Integrity Check value computed with a key at the ATC).

Parameter Value(s):

1st PV: “all system components and media”

[38] https://www.arc-it.net/html/security/controlsclarification.html

[39] Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 25, 2001.

2nd PV: “all information”

Risk References and Resources:

ARC-IT Mechanisms: See SC-28.

SC-28(3), Protection of Information at Rest | Cryptographic Keys

Responsible Party (M/I): M

Justification to Select: Encryption of information in storage (i.e., data-at-rest) protects the confidentiality and integrity of the information.

Guidance: The ATC should come with protected storage such as a trusted platform module (TPM[40]) to protect the private key of the TLS certificates, and all symmetric and asymmetric keys needed to set up secure connections to external services (e.g., cloud storage).

SC-35, External Malicious Code Identification

Responsible Party (M/I): M

Justification to Select: Multiple threat events in **Table 2**, Section *Deliver/insert/install malicious capabilities.*

Guidance: The manufacturer/vendor should implement functionality that identifies external malicious code such as malware that is downloaded by mistake or intentionally by a technician connected directly to the ATC. The ATC can employ mechanisms to detect network-based malicious code. This code can be hidden in legitimate signaling packets sent towards the ATC, or it may be running on devices that the ATC communicates with (e.g., network firewalls, or the TMC or the RSU).

SC-39, Process Isolation

Responsible Party (M/I): M

Justification to Select: Vulnerability “Control network services dependent on a non-control network” in **Table 5**, Section *Architecture and Design Vulnerabilities and Predisposing Conditions.*

Guidance: Each application running on the ATC should have its own separate code execution and memory. Security functionality should also be separated. See also ARC-IT guidance as it is applicable to the ATC.

Risk References and Resources:

NIST SP 800-82: Example compensating controls include partition processes to separate platforms.

[40] TPM Version 2.0 is currently recommended.

ARC-IT Mechanisms:

- Devices shall provide a separate address space for each executing process.
- Devices shall ensure that access to protected resources, including signing keys, is only granted to processes that have the appropriate permissions per AC-3.
- Devices shall provide Address Space Layout Randomization, Data Execution Prevention, and application sandboxing.

SC-40, Wireless Link Protection

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate data protection between clients and servers over wireless connection” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: ATCs are being developed/delivered with wireless capability; both WiFi and cellular are possible. Appropriate security protection for the WiFi link is advised (e.g., Wi-Fi Protected Access [WPA] based). The cellular link should come protected by default. The goal is to reduce the risk of intrusion via these interfaces. The capturing of data sent over these interfaces may also be a concern.

SC-41, Port and I/O Device Access

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate data protection between clients and servers over wireless connection” in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: In many cases the ATC is delivered with ports that are not used, and so these ports should be closed prior to operation, to reduce the risk that an adversary may get unauthorized access to the ATC via these ports

Risk References and Resources:

NIST SP 800-82: ITS functionality is generally defined in advance and does not change often.

SC-45, System Time Synchronization

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The ATC should have a reliable internal or external source of accurate timing. Accurate timing is necessary for constructing Signal Phase and Timing (SPaT) messages to be sent to the RSU, and for other traffic signal processes. This way, there will be time synchronization within the ATC and with its communication peers.

Risk References and Resources:

NIST SP 800-82: Organizations coordinate time synchronization on ITS to allow for accurate troubleshooting and forensics. Rationale: Organizations may find relative system time beneficial for many ITS systems to ensure safe, reliable delivery of essential functions. Time synchronization can also make root cause analysis more efficient by ensuring audit logs from different systems are aligned so that, when the logs are aggregated, organizations have an accurate view of events across multiple systems.

SC-45(1), System Time Synchronization | Synchronization with Authoritative Time Source

Responsible Party (M/I): M

Justification to Select: Vulnerability "Logs not maintained" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The possible values for the time source are listed in the ATC standards. At least one of them should be external to the ATC and should be checked with a given periodicity (determined by the IOO), and the internal clock should be suitably adjusted. Second-level accuracy is advised.

Risk References and Resources:

NIST SP 800-82: Syncing with an authoritative time source may be selected as a control when data is being correlated across organizational boundaries. ITS employ suitable mechanisms (e.g., GPS, Institute of Electrical and Electronics Engineers 1588[41] for time stamps.

SI FAMILY – SYSTEM AND INFORMATION INTEGRITY

SI-2, Flaw Remediation

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Lack of a vulnerability management program" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: System flaws should be remediated as soon as feasible. Once an update is released from the manufacturer/vendor due to a discovered flaw, the IOO should define the time period required to perform software and/or firmware updates. The manufacturer/vendor should also be responsible for flaw remediation (identify, correct, report, test, install, incorporate) and provide timely reports and updates for the products (controller and applications). If the manufacturer cannot immediately provide

[41] Institute of Electrical and Electronics Engineers (IEEE) 15888-2019, Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, 2016.

a software and/or firmware update for a newly discovered flaw, the manufacturer should recommend or provide other mitigations to be employed while the update is being developed.

Parameter Value(s):

paragraph c. “less than 30 days (NOTE: less than 30 days is ideal but may not be feasible for all IOOs due to resource limitations and the limited impact to ATCs if flaws are not remediated immediately.)”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques: M0951 / T0820, T0890, T0866, T0862, T0857, T864

NIST SP 800-82: Flaw remediation, or patching, is a complex process since an IOO may employ operating systems and software maintained by various vendors. ITS operators may also not have the resources or capability to test patches and are dependent on vendors to validate the operability of a patch. Sometimes the organization has no choice but to accept additional risk if no vendor patch is available, patching requires additional time to complete validation/testing, or deployment requires an unacceptable operations shutdown. In these situations, compensating controls should be implemented (e.g., limiting the exposure of the vulnerable system, restricting vulnerable services, implementing virtual patching). Other compensating controls that do not decrease the residual risk but increase the ability to respond may be desirable (e.g., provide a timely response in case of an incident; devise a plan to ensure the ITS can identify the exploitation of the flaw). Testing flaw remediation in an ITS may exceed the organization’s available resources.

SI-2(4), Flaw Remediation | Automated Patch Management Tools

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Lack of a vulnerability management program” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: There is a desire to have patches to the ATC not downloaded automatically (e.g., from the manufacturer/vendor pushing updates), but rather, first tested by the IOO. Therefore, such a tool could be used under the control of a privileged user, to push updates in a controlled fashion to a set of the ATCs in the network.

SI-3, Malicious Code Protection

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Malware protection not installed or up to date” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Parameter Value(s):

paragraph c.1 1st PV: “At least weekly.”

paragraph c.1 2nd PV: “Endpoints and network entry/exit points”.

paragraph c.2 1st PV: “Block and quarantine malicious code”

paragraph c.2 3rd PV: “system administrator at a minimum”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0938 / T0807, T0871, T0849, T0834, T0853
- M0949 / T0864

NIST SP 800-82: The use and deployment of malicious code protection is determined after careful consideration and after verification that it does not adversely impact the operation of the ITS. Malicious code protection tools should be configured to minimize their potential impact on the ITS (e.g., employ notification rather than quarantine). Example compensating controls include increased traffic monitoring and auditing.

ARC-IT Mechanisms:

- The device shall be configured to only permit installation and execution of signed code by trusted approved sources. See also, CM-7 in this document.
- The device shall detect, prevent, and report download and attempted execution of potentially malicious code.
- The device detection technology implemented will maintain frequent updates of malicious code signatures.

SI-3(4), Malicious Code Protection | Updates Only by Privileged Users

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Malware protection implemented without sufficient testing” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

SI-4, System Monitoring

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Intrusion detection/prevention software not installed” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: ATCs may have limited resources, so this control may not be implementable on all ATCs. Even so, vendors should strive to increase resources to enable the use of commonly accepted security solutions. For example, some ATCs come with their own firewall hardware, which can be used to perform system monitoring.

Only paragraphs a-c of this control are technical in nature and could be implemented on the ATC, but even these are more likely implemented at the TMC. Paragraphs d-g are management/operational controls implemented by people outside the ATC; the controller inherits the protections.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques: M0931 / T0830, T0885, T0884, T0867, T0869

NIST SP 800-82: The organization ensures that use of monitoring tools and techniques do not adversely impact the operational performance of the ITS. Example compensating controls include deploying sufficient network, process, and physical monitoring.

ARC-IT Mechanisms:

- Each device shall have adequate endpoint malware detection and reporting system deployed. In most cases a software suite of end point protections will include firewalls, anti-virus and malware detection, endpoint protection, reporting and logging capabilities (among other features). Consider the capabilities when choosing a software suite and take care in ensuring they are all configured securely.
- Data from each device will be sent to a central collection and monitoring system for threat analysis and auditing.
- Associated malware detection systems will maintain regular updates.
- A network intrusion detection system/intrusion prevention system (IDS/IPS) shall be configured to monitor data and detect malicious code signature in transit from all network infrastructure devices including routers, gateways, firewalls, load balancers and switches.
- The IDS/IPS shall be configured to detect abnormalities in network activity compared to normal operation.
- The network will support centralized monitoring of all relevant security data.
- The IDS/IPS shall be updated regularly and tuned to properly report security incidents.
- A defined notification and response policy and procedure shall be in place for relevant personnel to be informed and act on security incidents.
- A system may be in place to automatically notify relevant personnel per defined policy and further escalate notifications if action is not taken within a defined time period.

SI-4(2), System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis

Responsible Party (M/I): M

Justification to Select: Vulnerability "Intrusion detection/prevention software not installed" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Risk References and Resources:

NIST SP 800-82: In situations where the ITS cannot support the use of automated tools to support near-real-time analysis of events, the organization employs compensating controls (e.g., providing an auditing capability on a separate system, nonautomated mechanisms or procedures) in accordance with the general tailoring guidance.

ARC-IT Mechanisms: See SI-4

SI-4(4), System Monitoring | Inbound and Outbound Communications Traffic

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Lack of integrity checking for communications" in **Table 5**, Section *Communication and Network Configuration Vulnerabilities and Predisposing Conditions.*

Guidance: The IOOs should be responsible for defining the frequency of monitoring of inbound and outbound traffic as well as unusual or unauthorized activities and conditions. The manufacturer/vendor should implement logging and reporting mechanisms at the ATC that support the monitoring required by the IOO.

Risk References and Resources:

ARC-IT Mechanisms: See SI-4.

SI-4(5), System Monitoring | System-Generated Alerts

Responsible Party (M/I): M/I

Justification to Select: Threat "Spoofed Reporting Message" in **Table 4**, Physical Object Threat Events.

Guidance: The IOO should define the personnel or roles that need to be alerted by the ATC when a potential compromise indicator is detected, and it should also define the compromise indicators that require monitoring by the ATC. The manufacturer/vendor should implement the alerting functions at the ATC to enable the proper response to the compromise.

Risk References and Resources:

NIST SP 800-82: Example compensating controls include manual methods of generating alerts.

ARC-IT Mechanisms: See SI-4.

SI-4(7), System Monitoring | Automated Response to Suspicious Events

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Intrusion detection/prevention software not installed" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should define incident response personnel by name and/or role that will be notified automatically of any suspicious events and shall define the least disruptive actions to terminate suspicious events. The manufacturer/vendor should implement on the ATC the required automated event notification capability to the centralized event management system that supports automated personnel notifications.

SI-4 (14), System Monitoring | Wireless Intrusion Detection

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Unauthorized wireless access to sensors or final elements" in **Table 5**, Section *Sensor, Final Element, and Asset Management Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should implement procedures to proactively search for unauthorized wireless connections and scan the wireless spectrum around the ATC facilities for unauthorized endpoints that may connect to the ATC wireless network. The manufacturer/vendor should implement wireless intrusion detection mechanisms on the ATC wireless capabilities.

SI-4 (23), System Monitoring | Host-Based Devices

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Intrusion detection/prevention software not installed" in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should define the host-based monitoring mechanism that the manufacturer/vendor should implement on the ATC.

SI-7, Software, Firmware, and Information Integrity

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0945/T0849, T0821, T0889, T0839, T0843, T0851, T0862, T0857
- M0946/T0839, T0857
- M0947/T0830, T0811, T0874, T0821, T0836, T0889, T0839, T0843, T0851, T0862, T0857, T0864, T0859

NIST SP 800-82: The organization determines whether the use of integrity verification applications would adversely impact the operation of the ITS and employs compensating controls (e.g., manual integrity verifications that do not affect performance).

ARC-IT Mechanisms:

- The device shall support integrity checks on software, hardware, and information under certain conditions.
- The device shall protect the list of what is checked and under what circumstances from unauthorized modification per IA-2.
- The device shall support the integrity checks specified in NIST SP 800-147 section 3.1.2 if the device supports a basic input/output system (BIOS).
- The integrity checks supported by the device shall be hardware-based, i.e., they shall use cryptographic information stored in hardware such as a cryptographically secure hash value or a public key to be used for verification.
- Approved mechanisms for satisfying secure boot process in enhancements SI-7(9) and SI-7(10).
- Approved mechanisms specific to dealing with integration of detection and response are specified in IR-4, IR-5.
- The device shall either shut down or restart on detection of an integrity violation. Different violations may result in different responses (i.e., a device may support restart and shut down and use them in different circumstances)
- The device shall notify the device operator of integrity violations.

SI-7 (1), Software, Firmware, and Information Integrity | Integrity Checks

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should define software, firmware, and information that requires integrity checks and the time/lifecycle instances when this check is to be performed. The IOO should also define the transitional states or security relevant events that require integrity checks and the frequency of these checks. The manufacturer/vendor should implement the functionality of integrity checking on the ATC based on the IOOs requirements.

Risk References and Resources:

NIST SP 800-82: The organization ensures that the use of integrity verification applications does not adversely impact the operational performance of the ITS.

ARC-IT Mechanisms: See SI-7.

SI-7 (2), Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

Guidance: The IOO should define the personnel or roles that should receive a notification when an integrity violation occurs at an ATC. The manufacturer/vendor should implement the functionality on the ATC to support integrity violation and log sharing to the centralized system (e.g., TMC) that supports automated personnel/role notifications.

Risk References and Resources:

NIST SP 800-82: In situations where the organization cannot employ automated tools that provide notification of integrity discrepancies, the organization employs nonautomated mechanisms or procedures. Example compensating controls include performing scheduled manual inspections for integrity violations.

ARC-IT Mechanisms: See SI-7.

SI-7 (6), Software, Firmware, and Information Integrity | Cryptographic Protection

Responsible Party (M/I): M

Justification to Select: Threat “Compromise mission-critical information” in **Table 2**, Section *Exploit and compromise.*

SI-7 (9), Software, Firmware, and Information Integrity | Verify Boot Process

Responsible Party (M/I): M

Justification to Select: Threat “Compromise mission-critical information” in **Table 2**, Section *Exploit and compromise.*

Risk References and Resources:

ARC-IT Mechanisms: See SI-7.

SI-7 (10), Software, Firmware, and Information Integrity | Protection of Boot Firmware

Responsible Party (M/I): M/I

Justification to Select: Threat “Compromise mission-critical information” in **Table 2**, Section *Exploit and compromise.*

Guidance: The IOO should define the system component(s) that require boot firmware integrity protection at an ATC. The manufacturer/vendor should implement the functionality on the ATC.

Risk References and Resources:

ARC-IT Mechanisms: See SI-7.

SI-7 (12), Software, Firmware, and Information Integrity | Integrity Verification

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate testing of security changes” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions.*

SI-10, Information Input Validation

Responsible Party (M/I): M/I

Justification to Select: Threat “Compromise mission-critical information” in **Table 2**, Section *Exploit and compromise.*

Guidance: The IOO should define the information inputs to the system that require validation. The manufacturer/vendor should implement the functionality of input validation on the ATC based on the IOO’s requirements.

Parameter Value(s):

“All inputs to web/application servers, database servers, and any system or application input that might receive a crafted exploit toward code/command execution or buffer overflow.”

Risk References and Resources:

ARC-IT Mechanisms:

The network stacks that are provided as part of the device platform shall include industry standard input validation protocols for network datagrams.

All applications installed on the device should conduct input validation on inputs received over a network or wireless interface.

SI-10 (5), Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats

Responsible Party (M/I): M/I

Justification to Select: Threat “Compromise mission-critical information” in **Table 2**, Section *Exploit and compromise.*

Guidance: The IOO should define trusted sources (e.g., the TMC) and/or formats of data/packets (e.g., TLS or SNMPv3) that are to be received and processed at the ATC and that require input validation. The manufacturer/vendor should implement the functionality on the ATC.

SI-11, Error Handling

Responsible Party (M/I): M/I

Justification to Select: To preserve security and proper functioning of the ATC, errors need to be sent to and managed by appropriate personnel. In addition, detailed internal error messages such as stack traces, database dumps, and error codes should not be displayed to the user. Such details can provide hackers with important clues on potential flaws in the system.

Guidance: The IOO should define personnel or roles (e.g., privileged operational users) who need to take corrective action to manage error messages. The manufacturer/vendor should implement the functionality on the ATC to send error messages to the centralized system that manages error messages and distributes notifications to the personnel required by the IOO. The manufacturer/vendor should design the ATC such that it does not reveal any more information than is necessary when an error is encountered/caused, such as for failed logon attempts.

Risk References and Resources:

ARC-IT Mechanisms: The device should provide a facility whereby applications and other processes may write to a store that can only be read by an approved administrator.

SI-16, Memory Protection

Responsible Party (M/I): M/I

Justification to Select: The main purpose of memory protection is to prevent a process from accessing memory that has not been allocated to it. This prevents a bug or malware within a process from affecting other processes, or the operating system itself.

Guidance: The IOO should define the controls required to protect the memory at the ATC. The manufacturer/vendor should implement the controls required by the IOO on the ATC.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0950/T0820, T0890, T0866

ARC-IT Mechanisms:

- The device shall implement data execution prevention.
- The device may implement address space layout randomization.
- The implementations shall be hardware-enforced.

SI-17, Fail-Safe Procedures

Responsible Party (M/I): M/I

Justification to Select: Threat “Loss of Safety” in **Table 4**, Physical Object Threat Events.

Guidance: The IOO should define a list of failure conditions and associated fail-safe procedures. The manufacturer/vendor should implement failure reporting functions on the ATC to meet the requirements of the IOO.

Risk References and Resources:

NIST SP 800-82: The selected failure conditions and corresponding procedures may vary among baselines. The same failure event may trigger different responses, depending on the impact level. Mechanical and analog systems can be used to provide mechanisms to ensure fail-safe procedures. Fail-safe states should incorporate potential impacts to human safety, physical systems, and the environment. Related controls: CP-6.

This control provides a structure for the organization to identify its policy and procedures for dealing with failures and other incidents. Creating a written record of the decision process for selecting incidents and appropriate response is part of risk management in light of the changing environment of operations.

ARC-IT Mechanisms: See SI-7, SC-7, SC-24.

SR FAMILY – SUPPLY CHAIN RISK MANAGEMENT

SR-2, Supply Chain Risk Management Plan

Responsible Party (M/I): M/I

Justification to Select: Threat “Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware” in **Table 2**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).*

Guidance: This is an organizational control, but the IOO should also require the ATC manufacturer/vendor to develop and provide for review and approval by the IOO a Supply Chain Risk Management (SCRM) Plan, if there is concern over the trustworthiness of the more critical components of the ATC.

Parameter Value(s):

paragraph b. “at least annually”

SR-3, Supply Chain Controls and Processes

Responsible Party (M/I): M/I

Justification to Select: Threat “Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware” in **Table 2**, Section *Conduct an attack (i.e., direct/coordinate attack tools or activities).*

Guidance: This is an organizational control, but the IOO should also require the ATC manufacturer/vendor to establish supply chain controls and processes and provide for review and approval by the IOO, if there is concern over the trustworthiness of the more critical components of the ATC.

Parameter Value(s):

paragraph a. 1st PV: “key and/or critical system components”

paragraph c. “security plan”

SR-4, Provenance

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under asset management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions*

Guidance: This is an organizational control, but the IOO may want to require the ATC manufacturer/vendor to establish provenance. The IOO should define systems, system components, and associated data and share that information with the manufacturer/vendor of the ATC. In cases where the manufacturer/vendor has already established provenance via their normal acquisition processes, the IOO may require the manufacturer/vendor to provide documentation demonstrating that provenance for review and approval, as necessary.

Parameter Value(s):

“key and/or critical system components”

SR-4(2), Provenance | Track and Trace

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under asset management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions*.

Guidance: The IOO should define systems and critical system components that require unique identification and tracking through the supply chain. The manufacturer/vendor should develop and maintain processes to support this provenance and provide for the IOO to review and approve.

SR-4(3), Provenance | Validate as Genuine and Not Altered

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under asset management” in **Table 5**, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions*.

Guidance: This is an organizational control, but the IOO may want to require the ATC manufacturer/vendor to provide evidence of the more critical ATC components having been validated as not altered.

SR-5, Acquisition Strategies, Tools, and Methods

Responsible Party (M/I): M/I

Justification to Select: Threats, “Insert counterfeit or tampered hardware into the supply chain” and “Insert tampered critical components into organizational systems” in **Table 2**, Section *Deliver/insert/install malicious capabilities*.

Guidance: This is an organizational control, but the IOO should leverage acquisition strategies, methods, and particularly contract tools to ensure the appropriate SCRM language is included in requests for proposal, requests for information, contracts, statements of work, etc., such that the other applicable controls in this family are conveyed to the manufacturer/vendor and satisfied on delivery of the system. The IOO should review and approve manufacturer/vendor processes that meet these requirements.

SR-6, Supplier Assessments and Reviews

Responsible Party (M/I): M/I

Justification to Select: Threats, “Insert counterfeit or tampered hardware into the supply chain” and “Insert tampered critical components into organizational systems” in **Table 2**, Section *Deliver/insert/install malicious capabilities*.

Guidance: This is an organizational control, but the IOO may want to require the ATC manufacturer/vendor to perform supplier assessments and reviews for suppliers of the more critical ATC components.

Parameter Value(s):

“at least annually or as necessitated by events.”

Chapter 5. References

ARC-IT
Architecture Reference for Cooperative and Intelligent Transportation, Version 9.1
https://www.arc-it.net/html/architecture/architecture.html

ARC-IT TM04
Architecture Reference for Cooperative and Intelligent Transportation, *Service Package TM04: Connected Vehicle Traffic Signal System*
https://www.arc-it.net/html/servicepackages/sp43.html#tab-3

ATC 5201
Institute of Transportation Engineers (ITE) / American Association of State Highway and Transportation Officials (AASHTO) / National Electrical Manufactures Association (NEMA), *Advanced Transportation Controller (ATC) Standard 5201 Version 06*
https://www.ite.org/pub/?id=074A20C1-A415-533F-02B9-B0D185D40FA1

ATC 5301
Institute of Transportation Engineers (ITE) / American Association of State Highway and Transportation Officials (AASHTO) / National Electrical Manufactures Association (NEMA), *Advanced Transportation Controller (ATC) Cabinet Standard 5301 Version 02*
https://www.ite.org/technical-resources/standards/its-cabinet/version-2/

ATC 5401
Institute of Transportation Engineers (ITE) / American Association of State Highway and Transportation Officials (AASHTO) / National Electrical Manufactures Association (NEMA), *Application Programming Interface (API) Standard for the Advanced Transportation Controller (ATC) 5401 Version 02A*, July 29, 2020
https://www.ite.org/pub/?id=0A623A34-BF97-B062-FAF2-93FA63FFE46F

ATT&CK
MITRE ATT&CK® for Industrial Control Systems
https://attack.mitre.org/matrices/ics/

CTI 4001
Institute of Transportation Engineers (ITE) / American Association of State Highway and Transportation Officials (AASHTO) / National Electrical Manufactures Association (NEMA) NEMA, Connected Transportation Interoperability (CTI) 4001 v01.00, *Roadside Unit (RSU) Standard,* September 2021
https://www.ite.org/pub/?id=764FB228-0F6C-BA02-6D7B-16A86B1F8108

CTI 4501
Institute of Transportation Engineers (ITE) / American Association of State Highway and Transportation Officials (AASHTO) / National Electrical Manufactures Association (NEMA) NEMA, Connected Transportation Interoperability (CTI) 4501, v01.00, *Connected Intersections Implementation Guide – Guidance to Setting Up and Operating a Connected Intersection (CI),* September 2021
https://www.ite.org/pub/?id=76270782-B7E4-7F75-BC72-D5E318B14C9A

Cybersecurity Framework
Framework for Improving Critical Infrastructure Cybersecurity (also known as the *Cybersecurity Framework*)

https://www.nist.gov/cyberframework

FIPS 140-2
Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001
https://csrc.nist.gov/publications/detail/fips/140/2/final

FIPS 140-3
Federal Information Processing Standard (FIPS) 140-3, *Security Requirements for Cryptographic Modules*, March 22, 2019
https://csrc.nist.gov/publications/detail/fips/140/3/final

FIPS 201-3
Federal Information Processing Standard (FIPS) 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, January 2022
https://csrc.nist.gov/publications/detail/fips/201/3/final

IEEE 1588
Institute of Electrical and Electronics Engineers (IEEE) 15888-2019, *Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, 2016*
https://standards.ieee.org/ieee/1588/6825/

IEEE 1609.2
Institute of Electrical and Electronics Engineers (IEEE) 1609.2-2022, IEEE *Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages*
https://standards.ieee.org/ieee/1609.2/10258/

IEEE 1609.2.1
Institute of Electrical and Electronics Engineers (IEEE) 1609.2.1-2022 - IEEE *Standard for Wireless Access in Vehicular Environments (WAVE)--Certificate Management Interfaces for End Entities*.
https://standards.ieee.org/ieee/1609.2.1/10728/

IG ICS
Center for Internet Security (CIS) Controls™, *Implementation Guide for Industrial Control Systems*, version 7
https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/

ISA IEC 62443
International Society of Automation / International Electrotechnical Commission (ISA/IEC) 62443-4-2, *Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components*
https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c

ISO TS 2177
International Organization for Standards / Technical Standard (ISO/TS) 21177:2023, Intelligent Transport Systems — ITS Station Security Services for Secure Session Establishment and Authentication Between Trusted Devices
https://www.iso.org/standard/81067.html

ITS Control Set Procedures
Intelligent Transportation Systems (ITS) Operating Procedures for Developing Control Sets
https://placeholder

ITS Profile
Intelligent Transportation Systems (ITS) Cybersecurity Framework Profile
https://placeholder

JPO Cyber Glossary
Intelligent Transportation Systems Joint Program Office, *Transportation Cybersecurity Glossary*
https://www.standards.its.dot.gov/DeploymentResources/CyberGlossary

NEMA TS 8
National Electrical Manufacturers Association Technical Standard (NEMA TS) 8-2018, *Cyber and Physical Security for Intelligent Transportation Systems (ITS)*
https://www.nema.org/standards/view/cyber-and-physical-security-for-intelligent-transportation-systems-its

NEMA TS 10
National Electrical Manufacturers Association Technical Standard (NEMA TS) 10-2020, *Connected Vehicle Infrastructure – Roadside Equipment*
https://www.nema.org/standards/view/connected-vehicle-infrastructure-roadside-equipment

NIST Glossary
National Institute of Standards and Technology, Gaithersburg, MD, NIST Internal Report (NISTIR) 7298, Rev. 3, *Glossary of Key Information Security Terms*
https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf
https://csrc.nist.gov/glossary

NTCIP 1202
National Transportation Communications for ITS Protocol (NTCIP) 1202, v03A, *Object Definitions for Actuated Signal Controllers (ASC) Interface,* May 2019
https://www.ntcip.org/file/2019/07/NTCIP-1202v0328A.pdf

NTCIP 1218
National Transportation Communications for ITS Protocol (NTCIP) 1218 v01.38, *Object Definitions for Roadside Units (RSUs)*, Sept 2020.
https://www.ntcip.org/file/2021/01/NTCIP-1218v0138-RSU-toUSDOT-20200905.pdf

NTCIP 9014
National Transportation Communications for ITS Protocol (NTCIP) 9014 v01.20, *Infrastructure Standards Security Assessment (ISSA)*, Aug 2021
https://www.ntcip.org/file/2021/08/NTCIP9014v0120.pdf

RFC 8446
Internet Engineering Task Force (IETF) Request for Comment 8446, *The Transport Layer Security (TLS) Protocol Version 1.3,* August 2018
https://datatracker.ietf.org/doc/html/rfc8446

NIST SP 800-30
National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-30, *Joint Task Force (2012) Guide for Conducting Risk Assessments*.
https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

NIST SP 800-37
National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-37, Revision 2, *Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy*.
https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

NIST SP 800-39
National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-39, *Joint Task Force (2011) Managing Information Security Risk - Organization, Mission, and Information System View*.
https://csrc.nist.gov/publications/detail/sp/800-39/final

NIST SP 800-53 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-53, Revision 5, *Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations*. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST SP 800-53B National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-53B, *Control Baselines for Information Systems and Organizations*, September 2020 (includes updates as of December 10, 2020) https://csrc.nist.gov/publications/detail/sp/800-53b/final

NIST SP 800-56A National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-56A, Revision 3, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*, April 2018 https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final

NIST SP 800-56B National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-56B, Revision 2, *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography*, March 2019 https://csrc.nist.gov/publications/detail/sp/800-56b/rev-2/final

NIST SP 800-56C National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-56C, Revision 2, *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*, August 2020 https://csrc.nist.gov/publications/detail/sp/800-56c/rev-2/final

NIST SP 800-57-1 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-57 Part 1, Revision 5, *Recommendation for Key Management: Part 1 – General*, May 2020 https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

NIST SP 800-57-2 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-57, Part 2, Revision 1, *Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations*, May 2019 https://csrc.nist.gov/publications/detail/sp/800-57-part-2/rev-1/final

NIST SP 800-57-3 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-57, Part 3, Revision 1, *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*, January 2015 https://csrc.nist.gov/publications/detail/sp/800-57-part-3/rev-1/final

NIST SP 800-63B National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication 800-63B, *Digital Identity Guidelines – Authentication and Lifecycle Management*, June 2017 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

NIST SP 800-82, R2 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-82 Revision. 2, *Guide to Industrial Control Systems (ICS) Security,* May 2015. https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

NIST SP 800-82, R3 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-82 Revision 3 (Draft), *Guide to Operational Technology (OT) Security*, April 2022. https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft

NIST SP 800-90A, R1 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-90A Revision 1, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2015 https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final

NIST SP 800-160 V1 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-160 Volume 1, Revision 1, *Engineering Trustworthy Secure Systems*, November 2022 https://csrc.nist.gov/publications/detail/sp/800-160/vol-1-rev-1/final

NIST SP 800-160 V2 National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-160 Volume 2, Revision 1, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, December 2021 https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final

Appendix A. Acronyms

Acronyms and abbreviations used in this document are defined below.

AASHTO	American Association of State Highway and Transportation Officials
AES	Advanced Encryption Standard
AiTM	Adversary in The Middle
API	Application Programming Interface
ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
ASC	Actuated Signal Controller
ATC	Advanced Transportation Controller
BIOS	Basic Input/Output System
CAPEC™	Common Attack Pattern Enumeration and Classification
CI	Connected Intersection
C-I-A	Confidentiality, Integrity, and Availability
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CMU	Cabinet Monitor Unit
CSF	Cybersecurity Framework
CTI	Connected Transportation Interoperability
CVRSE	Connected Vehicle Roadside Equipment
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMS	Dynamic Message Sign
DNS	Domain Name Service
DNSSec	Domain Name Service Security Extensions
DoS	Denial of Service
DSRC	Dedicated Short Range Communications
ECC	Elliptic-Curve Cryptography

ECDHE	Elliptic-curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMP	Electromagnetic Pulse
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GPS	Global Positioning System
GUI	Graphical User Interface
HSM	Hardware Security Module
IACS	Industrial Automation and Control Systems
IBM	International Business Machines
ICS	Industrial Control Systems
ID	Identification
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IOO	Infrastructure Owner/Operator
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISA/IEC	International Society of Automation / International Electrotechnical Commission
ISO	International Organization for Standards
ISSA	Infrastructure Standards Security Assessment
IT	Information Technology
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation Systems
ITSRE	Intelligent Transportation System Roadside Equipment
L-M-H	Low, Moderate, and High
MAC	Media Access Control
NEMA	National Electrical Manufacturers Association
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Internal Report

NTCIP	National Transportation Communications for Intelligent Transportation System (ITS) Protocol
NTP	Network Time Protocol
NVD	National Vulnerability Database
OBE	On-board Equipment
OS	Operating System
OT	Operational Technology
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
POLP	Principle of Least Privilege
PV	Parameter Value
RBAC	Role-Based Access Control
RFC	Request for Comment
RMF	Risk Management Framework
RSA	Rivest, Shamir, and Adleman
RSU	Roadside Unit (see also Roadside Equipment)
RTU	Remote Terminal Units
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
SIU	Serial Interface Unit
SNMP	Simple Network Management Protocol
SP	Special Publication
SPAT	Signal Phase and Timing
SSH	Secure Shell
STIG	Security Technical Implementation Guides
TCP	Transmission Control Protocol
TFCS	Transportation Field Cabinet System
TLS	Transportation Layer Security
TMC	Traffic Management Center
TPM	Trusted Platform Module
TS	Technical Standard

USB	Universal Serial Bus
VDC	Volts Direct Current
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAVE	Wireless Access in Vehicular Environments
WiFi	Wireless Fidelity
WPA	Wi-Fi Protected Access

Appendix B. Control Family Abbreviations

AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Assessment, Authorization, and Monitoring
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
PT	PII Processing and Transparency
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
SR	Supply Chain Risk Management

Appendix C. Glossary

Connected Vehicle (ARC-IT)

A vehicle connected device that is equipped with onboard equipment (OBE) that is active and operational and includes the means to send and receive data to and from other connected devices.

Control Extension

A statement that extends the basic capability of a control by specifying additional functionality, altering the strength mechanism, or adding or limiting implementation options.

Cost/Benefit Analysis

The process of comparing the projected or estimated costs and benefits (or opportunities) associated with a project decision to determine whether it makes sense from a business perspective. Note: For security, it is necessary to balance the cost of applying selected controls (or derived requirements) and benefits gained by reducing risk to an acceptable level.

Device Security Class ARC-IT

A statement of the security requirements for a device in terms of its requirements for Confidentiality, Integrity, and Availability, expressed as Low, Moderate, or High ratings for each of the three

Enterprise Object

An organization or individual that interacts with other Enterprise Objects and/or Physical Objects. An Enterprise Object may be a component of another larger Enterprise Object, which may in turn be a component of a third, even larger, Enterprise Object (e.g., a Traffic Management Center Manager is a component of State Department of Transportation is a component of State Government). Enterprise Objects may participate wholly or in part in other Enterprise Objects (e.g., a Device Developer is a component of Auto Manufacturer but also participates in Standards Body).

Field

Infrastructure proximate to the transportation network which performs surveillance (e.g., traffic detectors, cameras), traffic control (e.g., signal controllers), information provision (e.g., Dynamic Message Signs and local transaction (e.g., tolling, parking) functions. Typically governed by transportation management functions running in centers. Field also includes connected vehicle roadside equipment and other non-DSRC wireless communications infrastructure that provides communications between mobile elements and fixed infrastructure.

Information Flow (ARC-IT)

Information that is exchanged between Physical Objects (subsystems and terminators) in the Physical View of ARC-IT. The terms "information flow" and "architecture flow" are used interchangeably. Information flows are the primary tool that is used to define the ITS architecture interfaces. These information flows and their communication requirements define the interfaces which form the basis for much of the ongoing standards work in the national ITS program.

Intelligent Transportation System

A system composed of technologies that advance transportation safety and mobility and enhance American productivity by integrating advanced communications technologies into transportation infrastructure and into vehicles. (JPO Cyber Glossary)

The system defined as the electronics, communications, or information processing in transportation infrastructure and in vehicles used singly or integrated to improve transportation safety and mobility and enhance productivity. Intelligent transportation systems encompass a broad range of wireless and wire line communications-based information and electronics technologies. (ARC-IT)

On-board Equipment (ARC-IT)

Computer modules, display, and a Dedicated Short-Range Communications radio, that is installed and embedded into vehicles which provide an interface to vehicular sensors, as well as a wireless communication interface to the roadside and back-office environment.

Physical Object (ARC-IT)

Systems or devices that provide ITS functionality that make up the ITS and the surrounding environment. They are defined in terms of the services they support, the processing they include, and their interfaces with other Physical Objects. They are grouped into six classes: Centers, Field, ITS, Support, Travelers, and Vehicles. Example Physical Objects are the Traffic Management Center, the Vehicle Onboard Equipment, and the ITS Roadway Equipment. These correspond to the physical world: respectively traffic operations centers, equipped connected automobiles, and roadside signal controllers. Due to this close correspondence between the physical world and the Physical Objects, the interfaces between them are prime candidates for standardization.

In ARC-IT, Physical Objects are defined with scope such that they are under the control of a single Enterprise Object.

Risk Tolerance (NIST Glossary)

The organization’s or stakeholder’s readiness to bear the risk after risk treatment in order to achieve its objectives. Note: Risk tolerance can be influenced by legal or regulatory requirements.

Roadside Unit (ARC-IT)

A fixed-position cooperative device. This may be a permanent installation or temporary equipment brought on-site for a period of time associated with an incident, road construction, or other event.

Security Control
(NIST Glossary)

Safeguards or countermeasures prescribed for a system or an organization to protect the confidentiality, integrity, and availability of the system and its information.

Service Package
(ARC-IT)

Provides an accessible, service-oriented perspective to ARC-IT and is tailored to fit, separately or in combination, real world transportation problems and needs. Service packages collect one or more Functional Objects that must work together to deliver a given ITS service and the information flows that connect them and other important external systems. In other words, they identify the pieces of the Physical View that are required to implement a particular ITS service. Service packages are implemented through projects (or groups of projects, aka programs) and in transportation planning, are directly related to ITS strategies used to meet regional goals and objectives.

Appendix D. Threats, Vulnerabilities, and Predisposing Conditions

Abroad set of adversarial and non-adversarial threat events down selected and tailored from NIST SP 800-30 that could potentially impact ATCs is provided in **Table 2** (adversarial) and **Table 3** (non-adversarial) below[42]. The properties of ATCs may also present unique opportunities to a threat source, specifically addressing how the threat source can manipulate the process of the ATCs to cause damage or achieve other malicious purposes (e.g., exfiltration of data). **Table 4** provides an overview of potential threat events from NISTSP 800-82 that are more specific to ATCs.

Threat events listed below focus on the ATCs (to include surveillance cameras and message signs), not the larger system comprised of various types of physical objects and other components. Various threat events may ultimately impact ATCs or its mission/operations, either by compromise of the ATC itself or the larger system (e.g., control center). In the case of potential compromise of the larger system, that larger system must implement certain protections to mitigate those risks. Only if the ATCs can implement a protection measure to mitigate the risk will the threat be considered relevant to the ATC itself and, therefore, controls will be selected in this document to mitigate those risks.

Table 2: Adversarial Threat Events

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	**Description**
Perform reconnaissance and gather information.	
Perform perimeter network reconnaissance/scanning.	Adversary uses commercial or free software to scan organizational perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks.
Perform network sniffing of exposed networks.	Adversary with access to exposed wired or wireless data channels used to transmit information, uses network sniffing to identify components, resources, and protections.
Gather information using open-source discovery of organizational information.	Adversary mines publicly accessible information to gather information about organizational systems, business processes, users or personnel, or external relationships that the adversary can subsequently employ in support of an attack.
Perform reconnaissance and surveillance of targeted	Adversary uses various means (e.g., scanning, physical observation) over time to examine and assess organizations and

[42] Reference NIST SP 800-30, Guide for Conducting Risk Assessments

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	**Description**
organizations.	ascertain points of vulnerability.
Perform malware-directed internal reconnaissance.	Adversary uses malware installed inside the organizational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.
Craft or create attack tools.	
Craft phishing attacks.	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or social security numbers (SSNs). Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.
Craft spear phishing attacks.	Adversary employs phishing attacks targeted at high value targets (e.g., senior leaders/executives).
Craft attacks specifically based on deployed information technology environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organizational information technology environment.
Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.
Create and operate false front organizations to inject malicious components into the supply chain.	Adversary creates false front organizations with the appearance of legitimate suppliers in the critical life-cycle path that then inject corrupted/malicious system components into the organizational supply chain.
Deliver/insert/install malicious capabilities.	
Deliver known malware to internal organizational information systems.	Adversary uses common delivery mechanisms to install/insert known malware (e.g., malware whose existence is known) into organizational information systems.
Deliver modified malware to internal organizational information systems.	Adversary uses common delivery mechanisms to install/insert known malware (e.g., malware whose existence is known) into organizational information systems.
Deliver targeted malware for control of internal systems and exfiltration of data.	Adversary uses more sophisticated delivery mechanisms than email (e.g., FTP) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems.
Deliver malware by providing removable media.	Adversary installs malware that is specifically designed to take control of internal organizational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions.
Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware, or commercial information technology products. Adversary is not targeting specific organizations, simply looking for entry points into internal organizational information systems. Note that this is particularly a concern for mobile applications.
Insert targeted malware into organizational information systems and information system components.	Adversary inserts malware into organizational information systems and information system components (e.g., commercial information technology products), specifically targeted to the hardware,

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	**Description**
	software, and firmware used by organizations (based on knowledge gained via reconnaissance).
Insert specialized malware into organizational information systems based on system configurations.	Adversary inserts specialized, non-detectable, malware into organizational information systems based on system configurations, specifically targeting critical information system components based on reconnaissance and placement within organizational information systems.
Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.
Insert tampered critical components into organizational systems.	Adversary replaces, though supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.
Install general-purpose sniffers on organization-controlled systems or networks.	Adversary installs sniffing software onto internal organizational information systems or networks.
Install persistent and targeted sniffers on organizational information systems and networks.	Adversary places within internal organizational systems or networks software designed to (over a continuous period) collect (sniff) network traffic.
Insert subverted individuals into organizations.	Adversary places individuals within organizations who are willing and able to conduct actions to cause harm to organizational missions/business functions.
Insert subverted individuals into privileged positions in organizations.	Adversary places individuals in privileged positions within organizations who are willing and able to conduct actions to cause harm to organizational missions/business functions. Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files) and may leverage access to one privileged capability to get to another capability.
Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware, or commercial information technology products. Adversary is not targeting specific organizations, simply looking for entry points into internal organizational information systems. Note that this is particularly a concern for mobile applications.
Exploit and compromise.	
Exploit poorly configured or unauthorized systems exposed to the Internet.	Adversary gains access through the Internet to systems that are not authorized for Internet connectivity or that do not meet organizational configuration requirements.
Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones).	Adversary takes advantage of fact that transportable information systems are outside physical protection of organizations and logical protection of corporate firewalls, and compromises the systems based on known vulnerabilities to gather information from those systems.
Exploit recently discovered vulnerabilities.	Adversary exploits recently discovered vulnerabilities in organizational information systems in an attempt to compromise the systems before mitigation measures are available or in place.
Exploit vulnerabilities using zero-day attacks.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Zero-day attacks are based on adversary insight into the information systems and applications used by organizations as

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	**Description**
	well as adversary reconnaissance of organizations.
Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	Adversary launches attacks on organizations in a time and manner consistent with organizational needs to conduct mission/business operations.
Compromise critical systems via physical access.	Adversary obtains physical access to organizational information systems and makes modifications.
Compromise systems or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organizations for purposes of subsequently infecting organizations when reconnected.
Compromise software of organizational critical information systems.	Adversary inserts malware or otherwise corrupts critical internal organizational information systems.
Compromise mission-critical information.	Adversary compromises the integrity of mission-critical information, thus preventing or impeding the ability of organizations to which information is supplied, from conducting operations.
Compromise design, manufacture, and/or distribution of system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.
Conduct an attack (i.e., direct/coordinate attack tools or activities).	
Conduct communications interception attacks.	Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing publicly known flaws), targets those communications, and gains access to transmitted information and channels.
Conduct wireless jamming attacks.	Adversary takes measures to interfere with wireless communications to impede or prevent communications from reaching intended recipients.
Conduct attacks using unauthorized ports, protocols, and services.	Adversary conducts attacks using ports, protocols, and services for ingress and egress that are not authorized for use by organizations.
Conduct Distributed Denial of Service (DDoS) attacks.	Adversary uses multiple compromised information systems to attack a single target, thereby causing denial of service for users of the targeted information systems.
Conduct targeted DoS attacks.	Adversary targets DoS attacks to critical information systems, components, or supporting infrastructures, based on adversary knowledge of dependencies.
Conduct physical attacks on organizational facilities.	Adversary conducts a physical attack on organizational facilities (e.g., sets a fire).
Conduct physical attacks on infrastructures supporting organizational facilities.	Adversary conducts a physical attack on one or more infrastructures supporting organizational facilities (e.g., breaks a water main, cuts a power line).
Conduct cyber-physical attacks on organizational facilities.	Adversary conducts a cyber-physical attack on organizational facilities (e.g., remotely changes HVAC settings).
Conduct data scavenging attacks in a cloud environment.	Adversary obtains data used and then deleted by organizational processes running in a cloud environment.
Conduct brute force login attempts/password guessing attacks.	Adversary attempts to gain access to organizational information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	Description
Conduct nontargeted zero-day attacks.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Attacks are not based on any adversary insights into specific vulnerabilities of organizations.
Conduct externally based session hijacking.	Adversary takes control of (hijacks) already established, legitimate information system sessions between organizations and external entities (e.g., users connecting from off-site locations).
Conduct internally based session hijacking.	Adversary places an entity within organizations in order to gain access to organizational information systems or networks for the express purpose of taking control (hijacking) an already established, legitimate session either between organizations and external entities (e.g., users connecting from remote locations) or between two locations within internal networks.
Conduct externally based network traffic modification (man in the middle) attacks.	Adversary, operating outside organizational systems, intercepts/eavesdrops on sessions between organizational and external systems. Adversary then relays messages between organizational and external systems, making them believe that they are talking directly to each other over a private connection, when in fact the entire communication is controlled by the adversary. Such attacks are of particular concern for organizational use of community, hybrid, and public clouds.
Conduct internally based network traffic modification (man in the middle) attacks.	Adversary operating within the organizational infrastructure intercepts and corrupts data sessions.
Conduct insider-based social engineering to obtain information.	Internally placed adversary takes actions (e.g., using email, phone) so that individuals within organizations reveal critical/sensitive information (e.g., mission information).
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom systems and components.
Achieve results (i.e., cause adverse impacts, obtain information)	
Obtain sensitive information through network sniffing of external networks.	Adversary with access to exposed wired or wireless data channels that organizations (or organizational personnel) use to transmit information intercepts communications.
Obtain sensitive information via exfiltration.	Adversary directs malware on organizational systems to locate and surreptitiously transmit sensitive information or insider manually exfiltrates data.
Cause degradation or denial of attacker-selected services or capabilities.	Adversary directs malware on organizational systems to impair the correct and timely support of organizational mission/business functions.
Cause deterioration/destruction of critical system components and functions.	Adversary destroys or causes deterioration of critical system components to impede or eliminate organizational ability to conduct missions or business functions. Detection of this action is not a concern.
Obtain information by externally located interception of wireless network traffic.	Adversary intercepts organizational communications over wireless networks. Examples include targeting public wireless access or hotel networking connections, and drive-by subversion of home or organizational wireless routers.
Obtain unauthorized access.	Adversary with authorized access to organizational systems, gains

Threat Events (Characterized by Tactics, Techniques, and Procedures (TTPs))	**Description**
	access to resources that exceeds authorization.
Obtain sensitive data/information from publicly accessible information systems.	Adversary scans or mines information on publicly accessible servers and web pages of organizations with the intent of finding sensitive information.
Obtain information by opportunistically stealing or scavenging information systems/components.	Adversary steals information systems or components (e. g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organizations or scavenges discarded components.
Maintain a presence or set of capabilities.	
Obfuscate adversary actions.	Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations.
Adapt cyber attacks based on detailed surveillance.	Adversary adapts behavior in response to surveillance and organizational security measures.
Coordinate a campaign of multi-staged attacks (e.g., hopping).	Adversary moves the source of malicious commands or actions from one compromised information system to another, making analysis difficult.
Coordinate a Campaign.	
Coordinate a campaign that combines internal and external attacks across multiple information systems and information technologies.	Adversary combines attacks that require both physical presence within organizational facilities and cyber methods to achieve success. Physical attack steps may be as simple as convincing maintenance personnel to leave doors or cabinets open.
Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome.	Adversary does not limit planning to the targeting of one organization. Adversary observes multiple organizations to acquire necessary information on targets of interest.
Coordinate a campaign that spreads attacks across organizational systems from existing presence.	Adversary uses existing presence within organizational systems to extend the adversary’s span of control to other organizational systems including organizational infrastructure. Adversary thus is in position to further undermine organizational ability to conduct missions/business functions.
Coordinate a campaign of continuous, adaptive, and changing cyber attacks based on detailed surveillance.	Adversary attacks continually change in response to surveillance and organizational security measures.
Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organizational operations.

Table 3 provides a high-level characterization of non-adversarial threat events as adapted from NIST SP 800-30. A non-adversarial threat event is a threat associated with accident or human error, structural failure, or environmental causes. For non-adversarial threat events, the anticipated severity, duration of the event (as included in the description of the event), and range of effects are considered in determining if relevant controls are selected.

Table 3: Non-Adversarial Threat Events

Threat Event	Description
Incorrect privilege settings	Authorized privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low.
Unreadable display	Display unreadable due to aging equipment.
Earthquake at primary facility[43]	Earthquake of organization-defined magnitude at primary facility makes facility inoperable.
Fire at primary facility	Fire (not due to adversarial activity) at primary facility makes facility inoperable.
Fire at backup facility	Fire (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Flood at primary facility	Flood (not due to adversarial activity) at primary facility makes facility inoperable.
Flood at backup facility	Flood (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Hurricane at primary facility	Hurricane of organization-defined strength at primary facility makes facility inoperable.
Hurricane at backup facility	Hurricane of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Resource depletion	Degraded processing performance due to resource depletion.
Introduction of vulnerabilities into software products	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.
Disk error	Corrupted storage due to a disk error.
Pervasive disk error	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.
Windstorm/tornado at primary facility	Windstorm/tornado of organization-defined strength at primary facility makes facility inoperable.
Windstorm/tornado at backup facility	Windstorm/tornado of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.

Table 4 provides an overview of potential threat events that are specific to and even more relevant to the ATCs than the general threats listed in **Table 2** and **Table 3** above. These physical object threat events are adapted from NIST SP 800-82 which addresses OT (was ICS), as ICS are similar in nature and operations to ITS physical objects.

[43] In the context of ITS, this is the primary location of the physical objects in the field, not necessarily a facility that houses typical IT.

Table 4: Physical Object Threat Events

Threat Event	Description
Denial of Control	Temporarily prevents operators and engineers from interfacing with process controls. An affected process may still be operating during the period of control loss, but not necessarily in a desired state.
Spoofed Reporting Message	False information sent to an ITS system operator either for evasion or to impair process control. The adversary could make the defenders and operators think that other errors are occurring to distract them from the actual source of the problem (i.e., alarm floods).
Theft of Operational Information	Adversaries may steal operational information for personal gain or to inform future operations.
Loss of Safety	Adversaries may target and disable safety system functions as a prerequisite to subsequent attack execution or to allow for future unsafe conditionals to go unchecked.
Loss of Availability	Adversaries may leverage malware to delete or encrypt critical data on human-machine interfaces, workstations, or databases.

Table 5 includes or adapts vulnerabilities and predisposing conditions from NIST SP 800-82. A vulnerability is a weakness in a system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Most vulnerabilities can be associated with system- or organization-level controls that either have not been applied (either intentionally or unintentionally) or have been applied but retain some weakness. The focus in this document is on the system-level vulnerabilities, as the organizational-level vulnerabilities typically cannot be mitigated by the engineers or vendors on the physical object itself.

A predisposing condition is a condition that exists within an organization, a mission/business process, enterprise architecture, or system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact. Predisposing conditions include, for example, the location of a facility in a hurricane- or flood-prone region (increasing the likelihood of exposure to hurricanes or floods) or a stand-alone system with no external network connectivity (decreasing the likelihood of exposure to a network-based attack).

Vulnerabilities resulting from predisposing conditions that cannot be easily corrected could include, for example, gaps in contingency plans, use of outdated technologies, or weaknesses/deficiencies in system backup and failover mechanisms.

The groups of vulnerabilities are:

- Policy and Procedures
- System

- Architecture and Design
- Configuration and Maintenance
- Physical
- Software Development
- Communication and Network Configuration

Table 5: Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Policy and Procedure Vulnerabilities and Predisposing Conditions	
Inadequate organizational ownership of risk assessments	Risk assessments should be performed with acknowledgement from appropriate levels within the organization. Lack of understanding of risk could lead to under-mitigated scenarios or inadequate funding and selection of controls.
Inadequate security policy for ITS	Vulnerabilities are often introduced into the ITS environment due to inadequate policies or the lack of policies specifically for ITS security. Controls and countermeasures should be derived from a risk assessment or policy. This ensures uniformity and accountability.
Inadequate ITS security training and awareness program	A documented formal ITS security training and awareness program is designed to keep staff up to date on organizational security policies and procedures as well as threats, industry cybersecurity standards, and recommended practices. Without adequate ongoing training on specific ITS policies and procedures, staff cannot be expected to maintain a secure ITS environment.
Lack of inventory management policy	Inventory policy and procedures should include installation, removal, and changes made to hardware, firmware, and software. An incomplete inventory could lead to unmanaged and unprotected devices within the ITS environment.
Lack of configuration management policy	Lack of policy and procedures for ITS configuration management can lead to an unmanageable and highly vulnerable inventory of hardware, firmware, and software.
Inadequate organizational ownership of risk assessments	Risk assessments should be performed with acknowledgement from appropriate levels within the organization. Lack of understanding of risk could lead to under-mitigated scenarios or inadequate funding and selection of controls.
Inadequate incident detection & response plan and procedures	Incident detection and response plans, procedures, and methods are necessary for rapidly detecting incidents, minimizing loss and destruction, preserving evidence for later forensic examination, mitigating the weaknesses that were exploited, and restoring services. Establishing a successful incident response capability includes continually monitoring for anomalies, prioritizing the handling of incidents, and implementing effective methods of collecting, analyzing, and reporting data.
Lack of redundancy for critical components	Lack of redundancy in critical components could provide single point of failure possibilities.
System Vulnerabilities and Predisposing Conditions	
Architecture and Design Vulnerabilities and Predisposing Conditions	
Inadequate incorporation of security into architecture and design.	Incorporating security into the physical object architecture, design must start with budget, and schedule of the physical object. The security architecture is part of the Enterprise Architecture. The architectures must address the identification and authorization of users, access control

Vulnerability	Description
	mechanism, network topologies, and system configuration and integrity mechanisms.
Inadequate management of change allowing insecure architecture to evolve	The network infrastructure within the ITS environment has often been developed and modified based on business and operational requirements, with little consideration for the potential security impacts of the changes. Over time, security gaps may have been inadvertently introduced within the infrastructure. Without remediation, these gaps may represent backdoors into the ITS. Sensors and controllers that were historically simple devices are now often manufactured as intelligent devices. In some cases, sensors and controllers may be replaced with IIoT devices which allow direct internet connections. Security should be incorporated into change management for all ITS devices, not just traditional IT components.
No security perimeter defined	If the ITS or physical object does not have a security perimeter clearly defined, then it is not possible to ensure that the necessary controls are deployed and configured properly. This can lead to unauthorized access to systems and data, as well as other problems.
Control networks used for non-control traffic	Control and non-control traffic have different requirements, such as determinism and reliability, so having both types of traffic on a single network makes it more difficult to correctly configure the network so that it meets the requirements of the control traffic, and that complexity can create undue risk. For example, non-control traffic could inadvertently consume resources that control traffic needs, causing disruptions in physical object functions. There may also be the potential for lateral movement from the non-control traffic to the control traffic, which could lead to hijacking or other types of attacks.
Control network services dependent on a non-control network	When IT services such as Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) are used by control networks, they are often implemented in the IT network. This causes the ITS network to become dependent on the IT network, which may not have the reliability and availability requirements needed by ITS.
Inadequate collection of event data history	Forensic analysis depends on collection and retention of enough data. Without proper and accurate data collection, it might be impossible to determine what caused a security incident to occur. Incidents might go unnoticed, leading to additional damage and/or disruption. Regular monitoring is also needed to identify problems with controls, such as misconfigurations and failures.
Configuration and Maintenance Vulnerabilities and Predisposing Conditions	
Hardware, firmware, and software not under asset management	The organization does not know what it has (e.g., make, model), where they are, or what version it has, resulting in an inconsistent and ineffective defense posture. To properly secure an ITS, there should be an accurate inventory of the assets in the environment. Procedures should be in place to manage additions, deletions, and modifications of assets, which include asset inventory management. These procedures are critical to executing business continuity and disaster recovery plans.
Hardware, firmware, and software not under configuration management	The organization does not know the patch management status, security settings, or configuration versions that it has, resulting in inconsistent and

Vulnerability	Description
	ineffective defense posture. A lack of configuration change management procedures can lead to security oversights, exposures, and risks. A process for controlling modifications to hardware, firmware, software, and documentation should be implemented to ensure an ITS is protected against inadequate or improper modifications before, during, and after system implementation. To properly secure an ITS, there should be an accurate listing or repository of the current configurations.
Operating System (OS) and vendor software patches may not be developed until significantly after security vulnerabilities are found.	Because of the tight coupling between ITS software and the underlying ITS, changes must undergo expensive and time-consuming comprehensive regression testing. The elapsed time for such testing and subsequent distribution of updated software provides a long window of vulnerability. Vulnerability management procedures should include flexibility for interim alternative mitigations.
Vendor declines to develop patches for vulnerability	Out-of-date OSs and applications may contain newly discovered vulnerabilities that could be exploited. Security patch support may not be available for legacy ITS, so vulnerability management procedures should include contingency plans for mitigating vulnerabilities where patches may never be available or replacement plans.
Lack of a vulnerability management program	Vulnerabilities not considered by the organization could result in exploitation. Vulnerability management procedures should be in place to determine a plan of action or inaction upon discovery of a vulnerability. Some ITS considerations are availability concerns may push patching until the next planned operational downtime; security patch support may not be available for ITS systems that use outdated OSs; isolated systems may not require immediate patching; and ITS exposed to the internet may need prioritized for patching.
Inadequate testing of security changes	Modifications to hardware, firmware, and software deployed without testing could compromise normal operation of the ITS. Documented procedures should be developed for testing all changes for security impact. The live operational systems should never be used for testing. The testing of system modifications may need to be coordinated with system vendors and integrators.
Poor remote access controls	There are many reasons why an ITS may need to be remotely accessed, including vendors and system integrators performing system maintenance functions, and ITS engineers accessing geographically remote system components. The concept of least privilege should be applied to remote access controls. Remote access capabilities must be adequately controlled to prevent unauthorized individuals from gaining access, or authorized individuals from gaining excessive access, to the ITS.
Poor configurations are used	Improperly configured systems may leave unnecessary ports and protocols open. These unnecessary functions may contain vulnerabilities that increase the overall risk to the system. Using default configurations often exposes vulnerabilities and exploitable services. All settings should be examined.
Critical configurations are not stored or backed up	Procedures should be available for restoring ITS configuration settings in the event of accidental or adversary-initiated configuration changes to

Vulnerability	Description
	maintain system availability and prevent loss of data. Documented procedures should be developed for maintaining configuration settings.
Vendor default passwords are used	Most vendor default passwords are easy to discover within vendor product manuals, which are also available to adversaries. Using the default password can drastically increase ITS vulnerability.
Passwords generation, use, and protection not in accord with policy	Password policy and procedure must be followed to be effective. Violations of password policy and procedures can increase physical object vulnerability.
Inadequate access controls applied	Access controls must be matched to the way the organization allocates responsibilities and privilege to its personnel. Poorly specified access controls can result in giving an ITS user too many or too few privileges. The following exemplify each case: • System configured with default access control settings gives an operator administrative privileges • System configured improperly results in an operator being unable to take corrective actions in an emergency
Malware protection not installed or up to date	For physical objects that include an operating system and possibly applications, installation of malicious software, or malware, is a common attack. Malware protection software, such as antivirus software, should be kept current in a very dynamic environment. Outdated malware protection software and definitions leave the system open to malware threats.
Malware protection implemented without sufficient testing	Malware protection software deployed without sufficient testing could impact normal operation of the ITS and block the system from performing necessary control actions.
Denial of service (DoS)	Physical object software could be vulnerable to DoS attacks, resulting in the prevention of authorized access to a system resource or delaying system operations and functions.
Intrusion detection/prevention software not installed	Incidents can result in loss of system availability and integrity; the capture, modification, and deletion of data; and incorrect execution of control commands. Intrusion Detection System / Intrusion Protection System (IDS/IPS) software may stop or prevent various types of attacks, including DoS attacks, and identify attacked internal hosts, such as those infected with worms. IDS/IPS software must be tested prior to deployment to determine that it does not compromise normal operation of the physical object.
Logs not maintained	Without proper and accurate logs, it might be impossible to determine what caused a security event to occur and perform adequate forensics.
Physical Vulnerabilities and Predisposing Conditions	
Unauthorized personnel have physical access to equipment	Physical access to physical object equipment should be restricted to only the necessary personnel, considering safety requirements, such as emergency shutdowns or restarts. Unauthorized access to physical object equipment can lead to any of the following: • Physical theft of data and hardware • Physical damage or destruction of data and hardware • Modification of the operational process • Unauthorized changes to or uses of the functional environment (e.g., data connections use of removable media, adding/removing resources) • Disconnection of physical data links

Vulnerability	Description
	• Undetectable interception of data (keystroke and other input logging)
Radio frequency, electromagnetic pulse (EMP), static discharge, brownouts, and voltage spikes	Without proper shielding, grounding, power conditioning, and/or surge suppression, some hardware used for control systems is vulnerable to radio frequency and EMP, static discharge, brownouts, and voltage spikes. The impact can range from temporary disruption of command and control to permanent damage to circuit boards.
Lack of backup power	Without backup power to critical assets, a general loss of power will shut down the physical object and could create an unsafe situation. Loss of power could also lead to insecure default settings. If the program file or data is stored in volatile memory, the process may not be able to restart after a power outage without appropriate backup power.
Loss of environmental control	Loss of environmental control (e.g., temperatures, humidity) could lead to equipment damage, such as processors overheating. Some processors will shut down to protect themselves; some may continue to operate but in a minimal capacity and may produce intermittent errors, continually reboot, or become permanently inoperable.
Unsecured physical ports	Unsecured universal serial bus and International Business Machines (IBM) personal system two ports could allow unauthorized connection of thumb drives, keystroke loggers, etc.
Software Development Vulnerabilities and Predisposing Conditions	
Improper Data Validation	Physical object software may not properly validate received data to ensure validity. Invalid data may result in numerous vulnerabilities including buffer overflows, command injections, cross-site scripting, and path traversals.
Installed security capabilities not enabled by default	Security capabilities that were installed with the product are useless if they are not enabled or at least identified as being disabled.
Inadequate authentication, privileges, and access control in software	Unauthorized access to configuration and programming software could provide the ability to corrupt a device.
Inadequate data protection between wireless clients and access points	Sensitive data between wireless clients and access points should be protected using strong encryption to ensure that adversaries cannot gain unauthorized access to the unencrypted data.
Communication and Network Configuration Vulnerabilities and Predisposing Conditions	
Firewalls nonexistent or improperly configured	A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and corporate networks, allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping, and providing individuals with unauthorized access to systems.
Inadequate firewall and router logs	Without proper and accurate logs, it might be impossible to determine what caused a security incident to occur.
Standard, well-documented communication protocols are used in plain text	Adversaries that can monitor the physical object network activity, can use a protocol analyzer or other utilities to decode the data transferred by protocols such as telnet, File Transfer Protocol, Hypertext Transfer Protocol, and Network File System. The use of such protocols also makes it easier for adversaries to perform attacks against the physical object and manipulate physical object network activity.
Authentication of users, data or devices is	Without authentication, there is the potential to replay, modify, or spoof data; or to spoof device identities or user identities; or masquerade

Vulnerability	Description
substandard or nonexistent	devices.
Use of unsecure ITS protocols	ITS protocols often have few or no security capabilities, such as authentication and encryption, to protect data from unauthorized access or tampering. Also, incorrect implementation of the protocols can lead to additional vulnerabilities.
Lack of integrity checking for communications	Adversaries could manipulate communications undetected. To ensure integrity, the physical object can use lower-layer protocols (e.g., IPsec) that offer data integrity protection when traversing untrusted physical media.
Inadequate authentication between clients and servers over wireless connection	Strong mutual authentication between clients and servers is needed to ensure legitimate clients do not connect to a rogue access point deployed by an adversary, and to ensure adversary clients do not connect to any of the ITS's wireless networks.
Inadequate data protection between clients and servers over wireless connection	Sensitive data between clients and servers should be protected using strong encryption to ensure that adversaries cannot gain unauthorized access to the unencrypted data.
Sensor, Final Element, and Asset Management Vulnerabilities and Predisposing Conditions	
Unauthorized physical access to sensors or final elements	Physical access to sensors and final elements allows for direct manipulation of the physical process. Many smart devices are configured on a fieldbus such that electronic access to the sensor network allows for manipulation of controlling parameters. Physical access to the whole of the loop should be managed to prevent incidents.
Unauthorized wireless access to sensors or final elements[44]	Wireless access to sensors and final elements allows for direct manipulation of the physical process. Many smart devices allow for wireless configuration (e.g., Bluetooth, Wi-Fi, WirelessHART). Wireless access should be securely configured or disabled using hardware write-protect where possible to protect unauthorized modification of the sensors and final elements which are connected both to the physical process and to the physical object environment.
Inappropriate segmentation of asset management system	Most architectures are designed for PLCs, remote terminal units (RTU)s, distributed control system (DCS), and SCADA controllers to manipulate the process, and for asset management systems to monitor the assets connected to the controllers. Many asset management systems also have the technical ability to modify the configuration of sensors and final elements, although modification may not be their primary function. The asset management system should be controlled appropriately based on its ability (or lack of ability) to manipulate the process.

[44] Examples of sensors are cameras, induction loops, or anything that can be used to detect the presence of people or vehicles, vehicle motion, speed, direction, weight, etc. Examples of final elements are the things that are being controlled, such as red-yellow-green (R-Y-G) lights, pedestrian crossing signals, gates, scales, red light/stop sign/speed cameras, overhead message signs, or variable speed or lane direction signs.

U.S. Department of Transportation
ITS Joint Program Office – HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free "Help Line" 866-367-7487

www.its.dot.gov

[FHWA Document Number]

U.S. Department of Transportation