WGD ATC 5501 SyRS v01.03 WTWB

Advanced Transportation Controller (ATC)

Walkthrough Workbook for the System Requirements Specification (SyRS) for the ATC Cybersecurity Standard

March 4, 2026

This document is being distributed to the ATC Cybersecurity Working Group to facilitate the review of the system requirements for ATC 5501 ATC Cybersecurity Standard.

Published by the following organizations:

American Association of State Highway and Transportation Officials
AASHTO

ite
A Community of Transportation Professionals

NEMA
National Electrical Manufacturers Association

Supported/Sponsored By: The United States Department of Transportation (USDOT)

U.S. Department of Transportation

CHANGE HISTORY

Version	Date	Editor	Notes
01	3/4/2026	Ralph Boaz	

TABLE OF CONTENTS

1. PURPOSE

The purpose of this Walkthrough Workbook is to facilitate the ATC Cybersecurity Working Group (WG) review of the Working Group Draft (WGD) System Requirements Specification (SyRS) for the ATC 5501 ATC Cybersecurity Standard. The walkthrough meetings are an essential part of the ITS standards development process. The requirements walkthrough helps the ATC Cybersecurity WG to:

- detect ambiguities, errors, and missing requirements
- establish a shared understanding of the requirements among stakeholders
- reduce the likelihood of issues during system design
- confirm that the requirements can be verified and validated.

2. NEEDS AND REQUIREMENTS

In developing the SyRS, requirements are derived from the needs identified in the Concept of Operations (ConOps). Needs are written from the user's perspective. Needs are typically higher-level and describe what the user wants to accomplish or the problem they need solved. A requirement is a precise, measurable, and testable statement describing what the system must do or how well it must perform to satisfy user needs.

User needs are expressed in a “well-written” fashion and have the following characteristics:

a) Uniquely Identifiable – The need is identified by a unique number and title.
b) Major Desired Capability – A need expresses a desired system capability, regardless of whether the capability currently exists or represents a capability gap.
c) Solution Free – The need is solution-free, providing designers with flexibility and latitude to develop the most appropriate solution.
d) Captures Rationale – The need captures the rationale or intent for why the capability is desired in the system. The rationale may also contain additional information to help clarify the need.

Requirements are said to be “well-formed” when they have the following characteristics:

a) Necessary – The requirement is useful and traceable to needs.
b) Concise – Minimal, understandable, and expressed in a “shall” statement.
c) Attainable – Realistic to achieve within available resources and time.
d) Standalone – The requirement is stated completely in one place.
e) Consistent – Does not contradict itself, nor any other stated requirement.
f) Unambiguous – Susceptible to only one interpretation.
g) Verifiable – Must be able to determine that the requirement has been met through one of four possible methods: inspection, analysis, demonstration, or test.

Good requirements generally take the form: [Actor] [Action] [Target] [Constraint] [Localization]. The localization and constraint portions are important, but not all requirements have both. A constraint limits the range of acceptable solutions for satisfying a requirement. Localization identifies where, when, or to which system elements a requirement applies.

Examples:

- The controller shall log all failed authentication attempts. [no Constraint or Localization]
- The controller shall log all failed authentication attempts within 1 second of detection. [Constraint]
- The controller shall log all failed authentication attempts for remote access sessions. [Localization]
- The controller shall log all failed authentication attempts for remote access sessions within 1 second of detection. [Localization and Constraint]

3. THE WALKTHROUGH

Input

The inputs to the walkthrough process are as follows:

a) Draft SRS
b) Comments submitted prior to the walkthrough meeting
c) SRS Walkthrough Workbook.

Walkthrough Procedure

The following procedure will be used:

1) Review any comments received prior to the walkthrough.
   - Identify resolutions or defer the comments to the appropriate place in the walkthrough workbook.
2) Perform a detailed review of the draft SyRS document using the SRS Walkthrough Workbook
   - Read sections of the SyRS identified in the walkthrough workbook, capturing comments in real-time in the walkthrough workbook and, if appropriate, in the draft SyRS to reflect inputs from walkthrough participants.
   - Review each requirement to ensure that it meets the criteria identified in the walkthrough workbook and, if revisions are necessary, that they are captured in the walkthrough workbook.
   - Collect and document new user needs proposed by participants as agreed upon by the WG.

Output

The outputs from the walkthrough process are as follows:

a) A marked-up walkthrough workbook indicating the changes and decisions made during the walkthrough meeting. For each requirement, the result of its evaluation, and the input provided that resulted in a revision.
b) A SyRS Walkthrough report will be generated.

4. NEW SECTIONS INTRODUCING LEVELS OF CONFORMANCE

In the course of the ATC Cyberecurity Project, the ATC Cyberecurity WG decided implement “Cybersecurity Conformance Levels” to represent higher cybersecurity capabilities for ATC Systems. This concept enables a subset of the standard to be developed and deployed faster. Sections 1.6 and 2.7 of the ATC 5501 SyRS will be reviewed during the walkthrough.

5. EXPANDED NEEDS TO REQUIREMENTS TRACEABILITY MATRIX (NRTM)

The NRTM found in WGD ATC Cyber SyRS v01.03 has been expanded to include the text for the needs and requirements to aid in the review. Needs and requirements that are to be part of the Level 1 version of the standard are identified using the “Level1” predicate in the conformance column of the NRTM. An “:M” or “:O” is appended to the Level1 to indicate if a requirement is Mandatory or Optional (e.g., Level1:M). A predicate “LevelD” indicates that the need or requirement is deferred to a later version of the standard.

Needs to Requirements Traceability Matrix (NRTM)

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
2.7.1	Physical Security			This section identifies needs that concern physical security.		
2.7.1.1	Control Physical Access			The ATC Cabinet needs to control physical access to the cabinet system. This may include authentication, monitoring, and reporting physical access to the cabinet system. Physical access control helps to protect the system from tampering and modified operation.	Level1:M	
		3.3.1.1.1	No #2 Key	When the only method to securing the cabinet door is a physical key, the ATC Cabinet shall not use a #2 key. Guidance: This should be implemented using a physical key distribution plan that is as secure as feasible for the agency. E.g., Distribution based on the agency, contractor, geographic area, group of cabinets, or individual cabinet basis.	Level1:M	
		3.3.1.1.2	Differentiated Physical Cabinet Key	When the only method to securing the cabinet door is a physical key, the locking mechanism shall be configurable for one unique key-lock combination from a minimum possible 10,000 key-lock combinations.	Level1:M	
		3.3.1.1.3	Programmable Cabinet Key	The ATC Cabinet shall secure the cabinet door with an electronic locking system that provides user authentication and authorization.	Level1:O	
		3.3.1.1.4	Detect Open Doors	The ATC Cabinet shall be able to detect whether any door of the cabinet is open. This includes a Police Panel and other special access doors for batteries or other elements.	Level1:M	
		3.3.1.1.5	Log Access Attempts	The ATC Cabinet shall generate a log for all access attempts.	Level1:M	
		3.3.1.1.6	Access Attempt Alerts	If it is connected to a central system, the ATC Cabinet shall send real-time alerts to the central system for all access attempts.	Level1:M	
2.7.1.2	No Cabinet Monitor Bypass			The ATC Cabinet needs to prohibit the CMU from being bypassed or disabled. The CMU is a critical safety device for traffic signal control applications.	Level1:M	
		3.3.1.2.1	No Functional CMU Present	The ATC Cabinet shall maintain a flashing state when there are no CMU response frames received by the controller on Serial Bus #1.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.1.2.2	No Flasher Present Operation	The ATC Cabinet shall allow an operational user to configure the cabinet operation if there are no functional flashers installed. Note: It is the responsibility of the operational user to configure the ATC unit for safe and secure cabinet operation when no operational flashers are present. For example, if an ATC unit is connected to a central system that receives alerts, it is arguable that maintaining the intersection without flashers is safer than keeping the cabinet in flash. Developer Note: Do we want to make an optional requirement to have two flashers?	Level1:M	
		3.3.1.2.3	No Flasher Present Alert	The ATC Cabinet shall send a real-time alert to the central system (if present) when there is no flasher present.	Level1:M	
2.7.2	Inventory and Control of Assets			This section identifies needs that concern inventory and control of assets.		
2.7.2.1	Facilitate Physical Inventory			The ATC Cabinet needs to facilitate the inventory and control of physical devices within the system. This may include support for identifying information such as the model, version, manufacturer, serial number, and MAC address (if it is a network-capable device). This is to support asset and configuration management by users. It is intended to be retrievable electronically. The identifying information will vary depending on the device.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.2.1.1	Inventory Identifiers for ATC Cabinet Standard Devices	The ATC Cabinet shall have the following identifiers for equipment defined in ATC 5301: • Controller – Model, version, manufacturer, serial number, and IP address/MAC address pairs (array of pairs). • Cabinet Monitor Unit (CMU) – Model, version, manufacturer, serial number, and IP address/MAC address pairs (array of pairs). • Serial Interface Unit (SIU) – Model, version, manufacturer, serial number, SB#1 address. • High Density Switch Pack Unit (HDSP) – Model, version, manufacturer, serial number, SB#3 address. • High Density Flasher Unit (HDFU) – Model, version, manufacturer, serial number, SB#3 address. • Auxiliary Display Unit (ADU) – Model, version, manufacturer, serial number, SB#3 address. Note: Detector information is not required for Level 1. Hardware changes are necessary.	Level1:M	
		3.3.2.1.2	Inventory Identifiers for IP-Addressable Non-Standard Devices	IP-addressable non-standard Cabinet Devices shall have the following inventory identifiers: • Model, version, manufacturer, serial number, and IP address/MAC address pairs (array of pairs).	Level1:M	
		3.3.2.1.3	Inventory Identifiers for Attached Non-IP-Addressable Non-Standard Devices	Non-IP-addressable non-standard devices attached to IP-addressable devices shall have the following inventory identifiers at a minimum: • Model, version, manufacturer, and serial number. Note: This would apply to Non-Standard Non-IP Addressable Devices attached to the Controller, as well as those attached to non-standard IP Addressable Devices.	Level1:M	
		3.3.2.1.4	Display Cabinet Inventory on Controller Front Panel	If a front panel is present, the Controller shall display a list of the ATC Cabinet Standard Devices and non-standard non-IP-addressable devices attached to the Controller. Guidance: This does not include non-standard IP-addressable devices and non-IP-addressable devices attached to them.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.2.1.5	Send Cabinet Inventory Remotely	The Controller shall send the current physical inventory remotely when commanded by an authenticated and authorized user or NPE.	Level1:M	
2.7.2.2	List of Programmable Components			The ATC Cabinet needs its physical devices within the cabinet to come with a list that identifies the components of the devices that may impose cybersecurity risks. Examples include microcontrollers, microprocessors, and field programmable gate arrays (FPGAs). This is to support supply chain risk management (SCRM).	Level1:M	
		3.3.2.2.1	List of Programmable Components of Cabinet Devices	The manufacturer of an ATC Cabinet Device shall provide a list of all microcontrollers, microprocessors, and FPGAs within the device identified by the following: Manufacturer Name and Manufacturer Part Number, when delivered.	Level1:M	
2.7.2.3	List of Software Components			The ATC Cabinet needs any software that is to be used in one of its programmable devices to come with an inventory of the software components. This allows users to respond to security, license, and operational risks that come with software including open source and third-party components present in a codebase.	Level1:M	
		3.3.2.3.1	SBOM Provided	The manufacturer of an ATC Cabinet Device shall provide an SBOM for all microcontrollers, microprocessors, and FPGAs within the device, when delivered. Note: This allows an end user to check for current patches and to manage vulnerabilities.	Level1:M	
2.7.2.4	Facilitate Software Inventory			The ATC Cabinet needs to facilitate the inventory and control of any software that is used in one of its programmable devices. Software may include driver software, OS, libraries, a board support package (BSP), file system, middleware, application software, and scripts. It is intended to be retrievable electronically.	Level1:M	
		3.3.2.4.1	Store SBOMs	When software is installed, the Controller shall store the associated SBOMs in protected memory.	Level1:M	
		3.3.2.4.2	Send Cabinet Inventory Remotely	The Controller shall send the current cabinet inventory remotely when commanded by an authenticated and authorized user or NPE.	Level1:M	
2.7.2.5	Inventory Tool Interface				LevelD	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
2.7.2.6	Notice of Unsupported Software			The ATC Cabinet needs vendors to provide advance notices of end of life (EOL) or otherwise unsupported software. Notices may include EOL, expected end of support, or if a delivered software is not a production release (e.g., Beta Version Release). This is typically performed at procurement, but it may be a part of an ongoing relationship with the software provider.	Level1:M	
		3.3.2.6.1	No Unsupported Software	The ATC Devices shall not contain software and hardware components that are not supported by their vendor, manufacturer, or developer due to end-of-life or end-of-support.	Level1:M	
		3.3.2.6.2	Unsupported Software Notification	When ATC devices contain microcontrollers, microprocessors, and FPGAs, the manufacturer of the device shall provide a notice of unsupported software when: • the software provider has determined EOL of the software • the software becomes unsupported for any other reason.	Level1:M	
		3.3.2.6.3	Non-Production Software Notification	The manufacturer of an ATC Cabinet Device shall provide a notice of non-production software when the software of a microcontroller, microprocessor, or FPGA within the device is not a production version (e.g., Alpha, Beta, pre-production, release candidate).	Level1:M	
2.7.2.7	Asset Tracking				LevelD	
2.7.3	Continuous Vulnerability Management			This section identifies needs that concern continuous vulnerability management.		
2.7.3.1	Verify Software Is Authorized				LevelD	
2.7.3.2	Monitor for Unauthorized Changes				LevelD	
2.7.3.3	Intrusion Detection and Prevention Systems				LevelD	
2.7.4	Authentication, Authorization, and User Accounts			This section identifies needs that concern authentication, authorization, and user accounts.		
2.7.4.1	Authenticated and Authorized Users			The ATC Cabinet needs to ensure that users are authenticated and authorized for administrative actions. Users may be authenticated using passwords and/or multi-factor authentication for each user account. This authentication and authorization capability should function with or without requiring a central system. This protects the ATC system from unauthorized changes.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.4.1	User Types	The controller shall have the following user account types: • Device Administrator (Administrator) • System • Discretionary User (User). Note: • Device Administrator (Administrator) – First administrator account that must exist and is set up by the provisioning person who performs the initial configuration of the device. See Section 3.3.6.3.4.1. In the sections that follow, any actions being attributed to the Administrator is to be interpreted as applying to any user group assigned the privilege to perform the particular action. • System – Built in user accounts essential for Linux services, daemons, and system processes that cannot be administered by the Device Administrator. These accounts provide service resource isolation; they are configured by the manufacturer and are not to be used for any type of access. See Section 3.3.4.7.1. • Discretionary User (User) – These are accounts created at the discretion of the Device Administrator to delegate responsibilities including system administration and operational duties for both human-to-machine (H2M) and machine-to-machine (M2M) purposes.	Level1:M	
		3.3.4.2	Authentication Levels	The controller shall apply AAL levels as described by NIST SP 800-63B-4.	Level1:M	
		3.3.4.3.1	Minimum Administrator Authentication Level	The controller shall require that the minimum authentication for the Administrator to be AAL2.	Level1:M	
		3.3.4.3.2	No Authentication for System Accounts	The controller shall prohibit authentication for system accounts.	Level1:M	
		3.3.4.3.3	Minimum User Authentication Level	The controller shall require that the minimum authentication for a user to be AAL1.	Level1:M	
		3.3.4.4.1	Assigning User Group Privileges	Only an Administrator shall be able to assign any privilege to a User Group.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.4.4.2	Removing User Group Privileges	Only an Administrator shall be able to remove any privilege from a User Group.	Level1:M	
		3.3.4.5.1	Minimum User Group Membership	The Controller shall require that a user is a member of at least one user group.	Level1:M	
		3.3.4.5.2	Adding User Group Membership	Only an Administrator shall be able to add a user to any user group.	Level1:M	
		3.3.4.5.3	Removing User Group Membership	Only an Administrator shall be able to remove a user from a user group.	Level1:M	
		3.3.4.5.10	User Credential Expiration	Only an Administrator shall be able to immediately expire user credentials. Note: This is to allow the administrator to force a user to change their credentials.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.4.7.1	Access Modes	The controller shall have at least one of the following access modes: • Physical Local Access • Human-to-Machine (H2M) • Machine-to-Machine (M2M). Note: • Physical Local Access – This is access through physical peripherals that are directly attached to the controller using the keypad, display, connected keyboard, or serial console. This excludes access over a network. – Technician changes timing plan at controller. – Technician uses automated script that runs commands over serial console. • Human-to-Machine (H2M) – This is access over a network connection that is initiated by a human. – Technician accesses the traffic application webserver running the controller to change the timing plan. – Support engineer accesses the controller via SSH console to make changes to the OS. – Technician uses SFTP to retrieve measure of effectiveness (MOE) logs from the controller. • Machine-to-Machine (M2M) – This is access over a network connection that is initiated and controlled by a program or process; i.e., Non-Person Entity (NHI). – Engineer in TMC access the central system to initiate a software installation conducted by the central system. In this case, the engineer's access to the central system is H2M, but the central system's access to the controller is M2M. Guidance: M2M cryptographic authentication is desirable but not required at this time for Level 1 conformance. When technically possible, use of cryptographic authentication is recommended to authenticate M2M connection to reduce vulnerability to Man-in-The-Middle (MiTM) attacks and unauthorized remote access.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.4.7.2	No Access for System Accounts	The controller shall prohibit system accounts from all access modes.	Level1:M	
		3.3.4.8.1	Local Authorization of Users	The controller shall authorize users without requiring the use of a central system.	Level1:M	
		3.3.4.8.2	Central Authorization of Users	When a controller is connected to a Central System that provides user authorizations, the controller shall authorize users based on information obtained from the central system.	Level1:M	
		3.3.4.6.1.4	Configure User Credential Expiration	Only an Administrator shall be able to configure the expiry of user credentials.	Level1:M	
		3.3.4.6.2.4	Enforce User Credential Expiration	The Controller shall expire user credentials per configuration.	Level1:M	
		3.3.4.9.1	User Credential Protection	The Controller shall protect all user credentials from tampering. Note: Standard Linux OS already does this by default.	Level1:M	
		3.3.4.9.2	User Privilege Protection	The Controller shall protect user privilege configuration from tampering.	Level1:M	
2.7.4.2	User Account Management			The ATC Cabinet needs to support the timely addition, modification, lock/unlock, and removal of user accounts. This allows the agency to manage access to the entire system.	Level1:M	
		3.3.4.4.3	User Group Addition	Only an Administrator shall be able to add a User Group.	Level1:M	
		3.3.4.4.4	User Group Deletion	Only an Administrator shall be able to delete a User Group.	Level1:M	
		3.3.4.4.5	User Group Modification	Only an Administrator shall be able to modify a User Group. Note: Modification refers to a change in any property or attribute of a user group that does not involve assignment or removal of privileges.	Level1:M	
		3.3.4.4.6	User Group Cloning	Only an Administrator shall be able to create a new User Group by cloning an existing User Group.	Level1:M	
		3.3.4.5.1	Minimum User Group Membership	The Controller shall require that a user is a member of at least one user group.	Level1:M	
		3.3.4.5.2	Adding User Group Membership	Only an Administrator shall be able to add a user to any user group.	Level1:M	
		3.3.4.5.3	Removing User Group Membership	Only an Administrator shall be able to remove a user from a user group.	Level1:M	
		3.3.4.5.4	User Addition	Only an Administrator shall be able to add a User.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.4.5.5	User Deletion	Only an Administrator shall be able to delete a User. Note: This also deletes the User from all associated user groups.	Level1:M	
		3.3.4.5.6	User Lock Out	Only an Administrator shall be able to lock a User. Note: Locking a user account is where authentication and authorization is prohibited and all active sessions are terminated.	Level1:M	
		3.3.4.5.7	User Unlock	Only an Administrator shall be able to unlock a User.	Level1:M	
		3.3.4.5.8	User Modification	Only an Administrator shall be able to modify a User. Note: Modification refers to a change in any property or attribute of a user account that does not involve assignment or removal of privileges.	Level1:M	
		3.3.4.5.9	User Cloning	Only an Administrator shall be able to create a new user by cloning an existing user. Note: This is a “quality of life” feature that speeds the creation of new users where the only differences are the name and authentication credentials.	Level1:M	
		3.3.4.5.10	User Credential Expiration	Only an Administrator shall be able to immediately expire user credentials. Note: This is to allow the administrator to force a user to change their credentials.	Level1:M	
2.7.4.3	Default User Accounts			The ATC Cabinet needs any default user accounts to be modifiable and removable. No default accounts should exist except for first time provisioning. This is to prevent unauthorized access to the controller unit with easily discoverable credentials.	Level1:M	
		3.3.6.3.3.2	Manufacturer Identified Provisioning Services	The manufacturer shall identify the minimum services and accounts required to provision the controller.	Level1:M	
		3.3.6.3.3.5	User Accounts Deleted in Unprovisioned State	When reset to an unprovisioned state, the controller shall ensure all discretionary user accounts are deleted except those required to facilitate the provisioning process.	Level1:M	
		3.3.6.3.4.4	Delete or Disable Provisioning User Accounts	The controller shall delete or disable any discretionary user accounts created strictly for facilitating the provisioning process as identified by the manufacturer.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
2.7.4.4	Authenticated and Authorized Programs, Processes, and Services			The ATC Cabinet needs to ensure that programs, processes, and services (non-person entities or NPEs) are authenticated and authorized for administrative actions. This authentication and authorization capability should function with or without requiring a central system. This protects the ATC system from unauthorized operation of the system and applications.	Level1:M	
		3.3.4.1	User Types	The controller shall have the following user account types: • Device Administrator (Administrator) • System • Discretionary User (User). Note: • Device Administrator (Administrator) – First administrator account that must exist and is set up by the provisioning person who performs the initial configuration of the device. See Section 3.3.6.3.4.1. In the sections that follow, any actions being attributed to the Administrator is to be interpreted as applying to any user group assigned the privilege to perform the particular action. • System – Built in user accounts essential for Linux services, daemons, and system processes that cannot be administered by the Device Administrator. These accounts provide service resource isolation; they are configured by the manufacturer and are not to be used for any type of access. See Section 3.3.4.7.1. • Discretionary User (User) – These are accounts created at the discretion of the Device Administrator to delegate responsibilities including system administration and operational duties for both human-to-machine (H2M) and machine-to-machine (M2M) purposes.	Level1:M	
		3.3.4.2	Authentication Levels	The controller shall apply AAL levels as described by NIST SP 800-63B-4.	Level1:M	
		3.3.4.3.2	No Authentication for System Accounts	The controller shall prohibit authentication for system accounts.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.4.3.3	Minimum User Authentication Level	The controller shall require that the minimum authentication for a user to be AAL1.	Level1:M	
		3.3.4.4.1	Assigning User Group Privileges	Only an Administrator shall be able to assign any privilege to a User Group.	Level1:M	
		3.3.4.4.2	Removing User Group Privileges	Only an Administrator shall be able to remove any privilege from a User Group.	Level1:M	
		3.3.4.5.1	Minimum User Group Membership	The Controller shall require that a user is a member of at least one user group.	Level1:M	
		3.3.4.5.2	Adding User Group Membership	Only an Administrator shall be able to add a user to any user group.	Level1:M	
		3.3.4.5.3	Removing User Group Membership	Only an Administrator shall be able to remove a user from a user group.	Level1:M	
		3.3.4.5.10	User Credential Expiration	Only an Administrator shall be able to immediately expire user credentials. Note: This is to allow the administrator to force a user to change their credentials.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.4.7.1	Access Modes	The controller shall have at least one the following access modes: • Physical Local Access • Human-to-Machine (H2M) • Machine-to-Machine (M2M). Note: • Physical Local Access – This is access through physical peripherals that are directly attached to the controller using the keypad, display, connected keyboard, or serial console. This excludes access over a network. – Technician changes timing plan at controller. – Technician uses automated script that runs commands over serial console. • Human-to-Machine (H2M) – This is access over a network connection that is initiated by a human. – Technician accesses the traffic application webserver running the controller to change the timing plan. – Support engineer accesses the controller via SSH console to make changes to the OS. – Technician uses SFTP to retrieve measure of effectiveness (MOE) logs from the controller. • Machine-to-Machine (M2M) – This is access over a network connection that is initiated and controlled by a program or process; i.e., Non-Person Entity (NHI). – Engineer in TMC access the central system to initiate a software installation conducted by the central system. In this case, the engineer's access to the central system is H2M, but the central system's access to the controller is M2M. Guidance: M2M cryptographic authentication is desirable but not required at this time for Level 1 conformance. When technically possible, use of cryptographic authentication is recommended to authenticate M2M connection to reduce vulnerability to Man-in-The-Middle (MiTM) attacks and unauthorized remote access.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.4.7.2	No Access for System Accounts	The controller shall prohibit system accounts from all access modes.	Level1:M	
		3.3.4.8.1	Local Authorization of Users	The controller shall authorize users without requiring the use of a central system.	Level1:M	
		3.3.4.8.2	Central Authorization of Users	When a controller is connected to a Central System that provides user authorizations, the controller shall authorize users based on information obtained from the central system.	LevelD	
		3.3.4.6.1.4	Configure User Credential Expiration	Only an Administrator shall be able to configure the expiry of user credentials.	Level1:M	
		3.3.4.6.2.4	Enforce User Credential Expiration	The Controller shall expire user credentials per configuration.	Level1:M	
		3.3.4.9.1	User Credential Protection	The Controller shall protect all user credentials from tampering. Note: Standard Linux OS already does this by default.	Level1:M	
		3.3.4.9.2	User Privilege Protection	The Controller shall protect user privilege configuration from tampering.	Level1:M	
2.7.4.5	Local-Based Access Control			The ATC Cabinet needs to provide local-based access control. The ability to use features and operations (privileges) can be tailored and restricted for access and may be time limited. Access and operations may be role-based. This protects the operation and security of the device.	Level1:M	
		3.3.4.4.1	Assigning User Group Privileges	Only an Administrator shall be able to assign any privilege to a User Group.	Level1:M	
		3.3.4.4.2	Removing User Group Privileges	Only an Administrator shall be able to remove any privilege from a User Group.	Level1:M	
		3.3.4.5.1	Minimum User Group Membership	The Controller shall require that a user is a member of at least one user group.	Level1:M	
		3.3.4.5.2	Adding User Group Membership	Only an Administrator shall be able to add a user to any user group.	Level1:M	
		3.3.4.5.3	Removing User Group Membership	Only an Administrator shall be able to remove a user from a user group.	Level1:M	
		3.3.4.6.1.1	Configure Automatic Inactive User Logout	Only an Administrator shall be able to configure an inactivity logout timer. Note: This is the period after which an inactive user session is terminated. See NIST SP 800-63B-4.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.4.6.1.2	Configure Failed Authentication Delay	Only an Administrator shall be able to configure the delay imposed after each successive failed authentication attempt.	Level1:M	
		3.3.4.6.1.3	Configure Failed Authentication Lockout	Only an Administrator shall be able to configure the number of repeated failed authentication attempt before a user is locked out.	Level1:M	
		3.3.4.6.2.1	Enforce Automatic Inactive User Logout	The Controller shall log out an inactive user per configuration.	Level1:M	
		3.3.4.6.2.2	Enforce Failed Authentication Delay	The Controller shall impose a delay after each successive failed authentication attempt per configuration.	Level1:M	
		3.3.4.6.2.3	Enforce Failed Authentication Lockout	The Controller shall lock out users after repeated failed authentication attempts per configuration.	Level1:M	
		3.3.4.6.2.5	Reset Failed Authentication Attempts on Successful Authentication	The Controller shall reset the failed authentication count after a successful authentication.	Level1:M	
		3.3.4.6.2.6	Reset Failed Authentication Attempts on User Unlock	The Controller shall reset the failed authentication count when a user is unlocked.	Level1:M	
		3.3.4.9.2	User Privilege Protection	The Controller shall protect user privilege configuration from tampering.	Level1:M	
2.7.4.6	Authentication Protection			The ATC Cabinet needs to protect the authentication capability of the system. Locally stored user credentials and privileges are stored in a secure fashion. Allow configurable expiration of credentials. Secure storage of locally stored credentials and privileges helps protect against unauthorized access to the system.	Level1:M	
		3.3.4.5.10	User Credential Expiration	Only an Administrator shall be able to immediately expire user credentials. Note: This is to allow the administrator to force a user to change their credentials.	Level1:M	
		3.3.4.6.1.4	Configure User Credential Expiration	Only an Administrator shall be able to configure the expiry of user credentials.	Level1:M	
		3.3.4.6.2.4	Enforce User Credential Expiration	The Controller shall expire user credentials per configuration.	Level1:M	
		3.3.4.9.1	User Credential Protection	The Controller shall protect all user credentials from tampering. Note: Standard Linux OS already does this by default.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.4.9.2	User Privilege Protection	The Controller shall protect user privilege configuration from tampering.	Level1:M	
2.7.4.7	Key Material Protection				LevelD	
2.7.4.8	Secure Authenticated Sessions			The ATC Cabinet needs to employ modern, currently deemed secure, protocols and algorithms for authentication. Use Public Key Infrastructure (PKI) for bidirectional cryptographic authentication. Terminate inactive sessions or those no longer valid (e.g., credentials have expired or have been revoked after a connection was made). This inhibits the ability of adversaries to gain access to the system.	Level1:M	
			This User Need is addressed by User Need 2.7.4.4.		Level1:M	
2.7.4.9	Trustworthiness				LevelD	
2.7.5	Logging, Monitoring, and Reporting			This section identifies needs that concern logging, monitoring, and reporting.		
2.7.5.1	Consistent and Accurate Time			The ATC Cabinet needs to maintain consistent and accurate time among all its devices. Consistent and accurate time is necessary to analyze logs and perform forensics after a cybersecurity event.	Level1:M	
		3.3.5.1.1	GNSS Time Source	The controller shall synchronize its system time with an authenticated and authorized GNSS time source.	Level1:M	
		3.3.5.1.2	NTP	The controller shall synchronize its system time using NTPv4 or later. Note: The ATC unit updates its RTC when the system time is updated.	Level1:M	
		3.3.5.1.3	Time Synchronization Log	The controller shall log each instance of synchronization with the GNSS time source.	Level1:M	
		3.3.5.1.4	Time Discrepancy Check	The controller shall check for a time discrepancy greater than 100 ms between the GNNS time source and the system time at user-defined periodicity.	Level1:M	
		3.3.5.1.5	Time Discrepancy Alert	The controller shall issue an alert if it fails the time discrepancy check.	Level1:M	
2.7.5.2	Security Event Logging			The ATC Cabinet needs to perform security event logging. For example, system or application accounts activity and modifications, denial-of-service, port scans, temporary changes due to an attack, etc. Logging needs to be enabled by default and securely stored so that it is accessible to privileged accounts only and prevents tampering.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.5.2.1	Security Event Log Record	The controller shall record the following information, at a minimum, for all security events: • Timestamp • Event Type • Severity. Development Note: Further event details to be developed in the design stage of the project. Different event types will require additional information.	Level1:M	

	3.3.5.2.2	Security Event Logs	The controller shall maintain a security event log that records, at a minimum, the following security events: 1)Access Control and Authentication Events: • All successful and failed login attempts (username, source IP/interface, authentication method used) • Login method and authentication mechanism used (password, SSH key, certificate, etc.) • Password changes, reset attempts, and account modifications • Account lockouts due to failed login attempts • Failed authentication attempts with reason (including patterns indicating brute force attacks) • Privilege escalation attempts (sudo/su usage) • SSH key additions, modifications, and deletions • SSH connection attempts and session establishments • Session timeouts or forced terminations 2)Account Management: • User account creation, including creator identity and assigned privileges • Account deletions and reason for removal • Group membership modifications • Permission/privilege changes • Account status changes (disabled, expired, locked, unlocked) • Password policy changes at user level • Changes to account-specific settings • Account lockout duration modifications 3)Session Management: • Session start and end times • Terminal/TTY information • Remote access session details (SSH, serial console, etc.) • Source IP and interface for remote sessions • Session termination reason (timeout, user logout, forced) • Privilege level changes during session 4)System Security Configuration: • Changes to PAM (Pluggable Authentication Modules) configuration • Modifications to /etc/passwd, /etc/shadow, or /etc/group files • Changes to sudoers configuration	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
				• Updates to SSH configuration files • Modifications to login.defs • System-wide security policy changes • Changes to access control lists (ACLs) • Firewall rule modifications and violations • Network interface configuration changes 5)File System Security: • Changes to critical system files and configurations • Access attempts to sensitive files or directories • File permission modifications on important system files • File integrity alerts for security-critical files • Mount/unmount operations, especially for external storage • Creation or modification of setuid/setgid binaries 6)Network Security: • Unusual network connections or port access attempts • DHCP lease assignments and network configuration changes • Unexpected ARP or DNS activities 7)Process and System Operations: • Service starts, stops, and crashes • System boot and shutdown events • Installation or removal of software packages • Kernel module loading/unloading • Process crashes or unexpected terminations 8)Resource Usage and System Health: • Memory exhaustion events • CPU usage spikes • Disk space warnings • I/O errors or unusual patterns • Temperature or power-related alerts (if applicable) 9)Security Subsystem Events: • Integrity check failures • Certificate-related events (expiration, validation failures) • Crypto subsystem failures or warnings. Developer Note: Further event details to be developed in the design stage of the project.		

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.5.2.3.1	Enabling Security Event Types	Only an administrator shall be able to enable the security event types to be logged.	Level1:M	
		3.3.5.2.3.2	Disabling Security Event Types	Only an administrator shall be able to disable the security event types to be logged.	Level1:M	
		3.3.5.2.3.3	Setting Security Event Severity	Only an administrator shall be able to set the security event severity threshold for when to log an event per event type. Note: • Configuration parameters may be adjusted over time based on operational experience, including modification of event selection, verbosity, storage allocation, and retention policy (if supported) to better support agency security monitoring and forensic needs. • Changes to security event log configuration parameters are security-relevant events and may be logged.	Level1:M	
		3.3.5.2.4	Minimum Security Log Capacity	The controller shall have a minimum capacity of 8000 security events. Note: It is estimated that there would be 2000 to 4000 security events over a four-week period with additional capacity of 4000 events for retention purposes when there is incident.	Level1:M	
		3.3.5.2.5	Security Log Rollover	The controller shall overwrite the oldest of security event records when the capacity is reached subject to any retention policy (See Section 3.3.5.2.6).	Level1:M	
		3.3.5.2.6	Security Log Retention Policy	Only an Administrator shall be able to configure retention criteria and duration for selected security event records. Note: This allows the administrator to prioritize which records are critical to their operational needs.	Level1:O	
		3.3.5.2.7	Security Log Access Control	The controller shall restrict access to the security log to privileged accounts.	Level1:M	
		3.3.5.2.8.1	Security Log Modification Protection	The controller shall protect security logs from log modification. Notes: This excludes rollover and retention policies. This covers appending and trimming. Examples are hashing, signatures, or integrity monitoring. See NIST SP 800-53, SI-7.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.5.2.8.2	Security Log Deletion Protection	Only an Administrator shall be able to delete the security log.	Level1:M	
		3.3.5.2.9.1	Security Log Physical Local Access	Only an Administrator shall be able to review the security log at the Controller.	Level1:M	
		3.3.5.2.9.2	Security Log Local Retrieval	Only an Administrator shall be able to copy the security log to removable storage.	Level1:M	
		3.3.5.2.9.3	Security Log Remote Retrieval	Only an Administrator shall be able to copy the security log over a network.	Level1:M	
2.7.5.3	Support Security Audits				LevelD	
2.7.5.4	Security Monitoring				LevelD	
2.7.5.5	Operating Software Reporting				LevelD	
2.7.5.6	Network Service Status				LevelD	
2.7.5.7	Security Alerts			The ATC Cabinet needs to provide alerts for security events that occur within the cabinet system. Alerts are to be provided both locally and remotely. Only trusted users should see the entire reason why it failed. Otherwise, hackers may get sufficient info to help inform their next step.	Level1:M	
		3.3.5.7	Security Alerts	The controller shall generate security alerts that notify authorized incident response personnel without disclosure of details that could be exploited by an attacker. Developer Note: Add a new definition for incident response personnel. Discuss.	Level1:M	
2.7.6	Networks, Protocols, and Services			This section identifies needs that concern networks, protocols and services.		
2.7.6.1	Secure Remote Access			If remote access is supported by the system, the ATC Cabinet needs to provide secure connections and communications. For example, Internet proxy. This reduces the attack surface.	Level1:M	
		3.3.6.1.1	Restricted Root Login	The controller shall restrict a root user (or equivalent highest privileged user) to physical local access only.	Level1:M	
2.7.6.2	Wireless Security				LevelD	
2.7.6.3	No Open Network Services			The ATC Cabinet needs unused network services to be disabled when equipment is delivered. This means that users will configure what they need and will be less likely to expose network services unintentionally.	Level1:M	
		3.3.6.3.1.1	Services Disabled by Default	The controller shall have all services disabled by default. Note: Provisioning exception see Section 3.3.9.8.1.3.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.6.3.1.2	Networking Disabled by Default	The controller shall have all network settings disabled by default. Note: Provisioning exception see Section 3.3.9.8.1.4.	Level1:M	
		3.3.6.3.2.1	Enable Services	Only an administrator shall be able to enable a service.	Level1:M	
		3.3.6.3.2.2	Disable Services	Only an administrator shall be able to disable a service.	Level1:M	
		3.3.6.3.2.3	Configure Network Settings	Only an administrator shall be able to configure network settings.	Level1:M	
		3.3.6.3.3.1	Resettable to Unprovisioned State	The controller shall be resettable to an unprovisioned state only through local physical access. Note: Privileges could be required to reset a controller to unprovisioned state.	Level1:M	
		3.3.6.3.3.2	Manufacturer Identified Provisioning Services	The manufacturer shall identify the minimum services and accounts required to provision the controller.	Level1:M	
		3.3.6.3.3.3	Service Restrictions in Unprovisioned State	When reset to an unprovisioned state, the controller shall disable all services except those required to facilitate the provisioning process as identified by the manufacturer.	Level1:M	
		3.3.6.3.3.4	Networking Restrictions in Unprovisioned State	When reset to an unprovisioned state, the controller shall disable all network settings except those required to facilitate the provisioning process as identified by the manufacturer.	Level1:M	
		3.3.6.3.3.5	User Accounts Deleted in Unprovisioned State	When reset to an unprovisioned state, the controller shall ensure all discretionary user accounts are deleted except those required to facilitate the provisioning process.	Level1:M	
		3.3.6.3.4.1	Device Administrator Creation Required	The controller shall require the device administrator account to be created to complete the provisioning process.	Level1:M	
		3.3.6.3.4.2	Device Administrator Authentication Required	The controller shall require the device administrator authentication to be configured to complete the provisioning process.	Level1:M	
		3.3.6.3.4.3	Operation Restriction in Unprovisioned State	The controller shall perform no other function or operation except what is required to facilitate the provisioning process until the provisioning process is completed.	Level1:M	
		3.3.6.3.4.4	Delete or Disable Provisioning User Accounts	The controller shall delete or disable any discretionary user accounts created strictly for facilitating the provisioning process as identified by the manufacturer.	Level1:M	
2.7.6.4	Manufacturer-Stated Network Services			The ATC Cabinet needs to have the network features of all network-capable devices documented by the manufacturer. This allows agencies to understand the device's capabilities, how to configure them, and how to maintain them.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.6.4.1	Documented Network Features	The manufacturer of an ATC Cabinet Device shall provide a list of all required network protocols and services containing at least the following information: •protocol handlers and services needed for the operation of network product •their open ports and associated services •a description of their purposes.	Level1:M	
2.7.6.5	Boundary Protection			The ATC Cabinet needs to restrict or prohibit unauthorized network traffic to critical components. This includes the support of monitoring and control of network communications at managed interfaces. Managed interfaces include the use of gateways, routers, firewalls, guards, and other network management methods. Support the use of VLANs or multiple physical networks. This allows a LAN to be configured to only connect devices of similar security sensitivity.	Level1:M	
		3.3.6.5.1	Firewall	Only an Administrator shall be able to configure the firewall. Note: This does not restrict an external firewall from being used.	Level1:M	
		3.3.6.5.2	No Unmanaged Network Devices	The ATC Cabinet shall not use unmanaged network devices. Note: E.g., Unmanaged switches, hubs, unmanaged cell modems. Guidance: Currently deployed equipment that has unmanaged switches cannot be used to extend the network.	Level1:M	
2.7.6.6	Denial-of-Service Protection				LevelD	
2.7.6.7	Use of Cloud Services				LevelD	
2.7.6.8	External Media Startup Software			The ATC Cabinet needs to prohibit the automatic execution of any script or executable program from any external device. Automatically executing a script from an external device is a security risk.	Level1:M	
		3.3.6.8.1	No Auto-Execution from External Media	The controller shall not auto-execute software from an external device. Note: This prohibits ATC 5201 Section B.4.1.1.	Level1:M	
2.7.7	Data At Rest Protection			This section identifies needs that concern data at rest protection.		

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
2.7.7.1	Secure Data At Rest			The ATC Cabinet needs to have all sensitive data at rest protected from modification. This protects the operation of the system.	Level1:M	
		3.3.7.1.1	Data at Rest Modification Protection	The controller shall protect data at rest from log modification. Note: E.g., hashing, signatures, or integrity monitoring.	Level1:M	
		3.3.7.1.2	Data at Rest Deletion Protection	Only an Administrator shall be able to delete data at rest.	Level1:M	
2.7.7.2	Removable Storage Security				LevelD	
2.7.8	Data in Transit Protection			This section identifies needs that concern data in transit protection.		
2.7.8.1	Secure Data in Transit			The ATC Cabinet needs to utilize secure communications between network capable devices. At a minimum, use secure (integrity protected), up-to-date protocols such as (D)TLS 1.3, SFTPv3, SSH2, and SNMPv3. Unencrypted protocols are not secure. Note: SDLC communications is exempted for current generation ATC equipment.	Level1:M	
		3.3.8.1.1	Protected Network Communications	The ATC Cabinet shall use the following protocols, at a minimum, for encrypted network communications: (D)TLS 1.3, SFTPv3, SSH2, and SNMPv3 or later.	Level1:M	
2.7.8.2	Verifiable Credentials			The ATC Cabinet needs to ensure that it uses up-to-date, verifiable credentials to send and receive information securely (e.g., TLS certificates between devices). Communications with unverified credentials are not secure.	Level1:M	
		3.3.8.2.1	Verify Endpoint Credentials	The data-carrying communication link between the controller and another endpoint shall be protected based on the exchange of verifiable credentials from both sides.	Level1:M	
2.7.9	Operating Platform and Applications			This section identifies needs that concern the operating platform for ATC units and the application programs that run on them.		
2.7.9.1	Application and Process Isolation			If the ATC Cabinet is running multiple applications, then the resources used by the applications need to be isolated, controlled, and privileges restricted. If one application is compromised or malfunctions, it will not affect the other applications.	Level1:M	

	3.3.9.1.1	Resource Allocation	The Controller shall allow a system administrator to allocate the controller's resources to the application programs as described below: 1)CPU Resources • CPU time/scheduling priority using cgroups or nice values • CPU affinity (binding specific applications to certain cores) • Real-time scheduling policies for time-critical applications 2)Memory Resources • RAM allocation limits using cgroups memory subsystem • Memory protection boundaries 3)Storage Resources • Disk space quotas • I/O bandwidth throttling • I/O scheduling priorities 4)Network Resources • Bandwidth allocation/QoS • Network interface prioritization • Socket buffer sizes 5)Power Management • CPU frequency scaling policies per application • Sleep states for non-critical applications 6)Device Access • Access controls to specific hardware peripherals • Device binding for critical applications 7)Inter-process Communication Resources • Semaphore limits • Shared memory segments • Message queue sizes. Note: The following definitions are provided. Affinity (CPU Affinity): The binding of a specific application or process to one or more designated CPU cores, ensuring that the application always executes on the assigned cores. Control Groups (cgroups): A Linux kernel feature that limits, prioritizes, and isolates the resource usage (CPU, memory, I/O, etc.) of process groups. Device Binding: The practice of associating a critical application exclusively with a designated hardware device to ensure reliable and prioritized access.		

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
				Nice Values: A numerical value that influences a process's scheduling priority on Linux systems, where lower values result in higher priority and higher values yield to other processes. Quality of Service (QoS): The ability to prioritize certain network traffic over others to ensure that critical communications receive adequate bandwidth and low latency. Semaphores: Synchronization primitives used by applications to coordinate access to shared resources and prevent conflicts between concurrent processes.		
2.7.9.2	Application Logging				LevelD	
2.7.9.3	Application Reporting				LevelD	
2.7.9.4	Application Portability				LevelD	
2.7.9.5	Separation of System, Security, and User Functionality				LevelD	
2.7.9.6	Facilitate System Software Updates			The ATC Cabinet needs to provide tools to ensure the timeliness and completeness of updating firmware, operating system, and middleware. These tools include options for manual and automated updates. Only allows verified software to be installed and includes the removal of previous versions of the software.	Level1:M	
		3.3.9.6.1	Software Update Capability	The Controller shall provide a mechanism to install updates of the system software including the update of firmware, operating system, and middleware. Note: This applies only to devices capable of updates.	Level1:M	
		3.3.9.6.2	Manual Software Updates	Only an Administrator shall be able to perform a software update.	Level1:M	
		3.3.9.6.3	Automated Software Updates		LevelD	
		3.3.9.6.4.1	Digital Certificate Additions	Only an Administrator shall be able to add digital certificates that verify software updates.	Level1:M	
		3.3.9.6.4.2	Digital Certificate Removals	Only an Administrator shall be able to remove digital certificates that verify software updates.	Level1:M	
		3.3.9.6.4.3	Update Package Integrity	The Controller manufacturer shall provide a mechanism to verify the integrity of a software package. Note: For example, the manufacturer provides a file containing a hash of the install package that has been signed by a digital certificate.	Level1:M	

UN ID	UN	Sys Req ID	System Requirement	User Need / System Requirement	Conform	Additional Specifications
Well-formed? Logically consistent w/UN & parent/sib Req? Necessary? Concise? Attainable? Standalone? Consistent? Unambiguous? Verifiable?						
		3.3.9.6.4.4	Update Package Integrity Verification	The Controller manufacturer shall verify the integrity (e.g., hash, signature) of the software update package before installation.	Level1:M	
		3.3.9.6.5	Removal of Previous Versions	The Controller shall remove the previous version of software upon a successful update.	Level1:M	
2.7.9.7	Stable Linux Kernel and Board Support Package			The ATC Cabinet needs to use stable and reliable versions of the Linux and Board Support Package. Linux kernel support for a minimum of five years ensures that bug and security patches will continue. The board support package should come from a reliable source.	Level1:M	
		3.3.9.7.1	Board Support Package Security Updates	The Controller manufacturer shall provide security updates for devices until the EOL is reached. Note: Section 3.3.2.6.2 is a requirement for manufacturers to provide a notice when software becomes unsupported for any reason.	Level1:M	
2.7.10	Resiliency			This section identifies needs that concern resiliency.		
2.7.10.1	System Backup				LevelD	
2.7.10.2	System Safe Mode				LevelD	
2.7.10.3	Secure System Restore				LevelD	
2.7.10.4	Power Interruption Response				LevelD	

§