WGD ATC 5501 SyRS v01.03

Advanced Transportation Controller (ATC)

Working Group Draft (WGD)

System Requirements Specification (SyRS) for the Advanced Transportation Controller Cybersecurity Standard v01.03

February 23, 2026

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

Recent Minor Version Revision History

Filename	Date	Author	Notes
ATC5501v01_SyRSv0103_260223	02/23/2026	Boaz	WG Draft for Review and Walkthrough
ATC5501v01_SyRSv0102_251203	12/03/2025	Boaz	Internal WG Draft

Add DOT standards statement if desired. May occur later in document.

Acknowledgment

XXXXXX

May be covered later.

Foreword

To be completed.

Standard Development Organizations

The Standards Development Organizations (SDOs) supporting this standard include the following:

ITE

1627 Eye Street, NW, Suite 600
Washington, DC. 20006

Matt Jasnosz, mjasnosz@ite.org
Patrick Morrison, pmorrison@ite.org
Siva Narla, snarla@ite.org

AASHTO

555 12th Street NW, Suite 1000
Washington, DC 20004

Syed Ahnaf Morshed, amorshed@aashto.org

NEMA

1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209

Brian Doherty, brian.doherty@nema.org
Steve Griffith, steve.griffith@nema.org

Groups

ATC Cybersecurity Steering Committee Members

Dave Miller, Yunex Traffic (Co-Chair)
(Co-Chair)
XXX, YYYY
To be completed.

ATC Cybersecurity Working Group Voting Members

Matt Luker *	UDOT	Shea Tomsin *	Econolite
Justin Hatch	GDOT	Mike Gallagher	Q-Free America
David Lucas	MAG	Mark Simpson	SWARCO McCain
Jason Tao	DDOT (DC)	Matt Barron	Cubic
Jeremy Iwen	WisDOT	Wolfgang Buckel	Yunex
James Danila	MassDOT	Bob Rausch	TransCore
Brandon Campbell	City of Tampa	Kenneth Tinsley	Synapse ITS
Robert White	Nashville DOT	* Co-Chair of ATC Cyber Working Group	

Subject Matter Experts (SMEs)

Ralph Boaz	Pillar Consulting
Himaja Nimmagadda	Gurus Infotech
Tiffany Rad	ELCnetworks
Michela Vanderveen	Still Waters Consulting

ATC Cybersecurity Quick Response Group (QRG)

Matt Barron, Cubic
Wolfgang Buckel, Yunex
Badii Ennouri, Tech. University of Vienna
Edward Fok, Cipher Roadways
Matt Luker, Utah DOT
Jonathan Grant, Yunex
Marisa Ramon, Toyota
Shea Tomsin, Econolite
Paul Tykodi, MassDOT
David West, TxDOT
Robert White, Nashville DOT
Subject Matter Experts (see above)

ATC Cybersecurity Draft Team

Matt Barron, Cubic
Ethan Coxsey, SynapseITS
Matt Luker, Utah DOT
Mike Gallagher, Q-Free America
Jonathan Grant, Yunex
Jim Rose, Econolite
Mark Simpson, SWARCO McCain
Tom Spiegel, Econolite
Shea Tomsin, Econolite
Subject Matter Experts (see above)

Copyright Notice

NRTM and RTM Distribution Permission

To be completed.

To the extent that these materials are distributed by AASHTO / ITE / NEMA in the form of a Needs to Requirements Traceability Matrix (“NRTM”), AASHTO / ITE / NEMA extend the following permission:

a) you may make or distribute unlimited copies, including derivative works of the NRTM, provided that each copy you make or distribute contains the citation “Based on **[PUT IN STANDARD HERE]** NRTM. Used by permission. Original text © AASHTO / ITE / NEMA.";

b) you may only modify the NRTM by adding text Additional Specifications columns for project-unique or vendor-unique features; and

c) if the NRTM excerpt is made from an unapproved draft, add to the citation "NRTM excerpted from a draft document containing preliminary information that is subject to change."

This limited permission does not include reuse in works offered by other standards developing organizations or publishers, and does not include reuse in works-for-hire, compendiums, or electronic storage devices that are not associated with procurement documents, or commercial hardware, or commercial software products intended for field installation. The NRTM is completed to indicate the features that are supported in an implementation. Contact ITE for information on electronic copies of the NRTM.

Content and Liability Disclaimer

The information in this publication was considered technically sound by the consensus of persons engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document. AASHTO, ITE, and NEMA standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While AASHTO, ITE, and NEMA administer the process and establish rules to promote fairness in the development of consensus, they do not write the document and they do not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in their standards and guideline publications. AASHTO, ITE, or NEMA disclaim liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. AASHTO, ITE, and NEMA disclaim and make no guaranty or warranty, express or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any of your particular purposes or needs. AASHTO, ITE, and NEMA do not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, AASHTO, ITE, or NEMA are not undertaking to render professional or other services for or on behalf of any person or entity, nor are they undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

AASHTO, ITE, and NEMA have no power, nor do they undertake to police or enforce compliance with the contents of this document. AASHTO, ITE, and NEMA do not certify, test, or inspect products, designs, or installations for safety or health purposes. Any certification or other statement of compliance with any health or safety–related information in this document shall not be attributable to AASHTO, ITE, or NEMA and is solely the responsibility of the certifier or maker of the statement.

Additional Contributors and Reviewers

In addition to the SDOs the ATC Cybersecurity WG voting members, and SMEs, there were many others that contributed to the development of this standard as non-voting WG members. Their input and assistance was critical to the final product.

Recognition is also given to the United States Department of Transportation that sponsored this effort and also provided guidance and support.

User Comment Instructions

The term “User Comment” includes any type of written inquiry, comment, question, or proposed revision, from an individual or organization, about any ATC Cybersecurity Standard content. A “Request for Interpretation” is also classified as a User Comment. User Comments are solicited at any time. In preparation of this standards publication, input from users and other interested parties was sought and evaluated. User Comments are generally referred to the Committee responsible for developing and/or maintaining the ATC Cybersecurity Standard. The ATC Cybersecurity Committee chairpersons, or their designee, may contact the submitter to clarify the User Comment. When the ATC Cybersecurity Committee chairpersons or designee reports the ATC Cybersecurity Committee's consensus opinion related to the User Comment, that opinion is forwarded to the submitter. ATC Cybersecurity chairpersons may report that action on the User Comment may be deferred to a future ATC Cybersecurity Committee meeting and/or a future revision of the standards publication.

A User Comment should be submitted to this address:

Institute of Transportation Engineers (ITE)
1627 Eye Street, NW, Suite 600
Washington, DC 20006
e-mail: standards@ite.org

A User Comment should be submitted in the following form:

Standard Publication number and version:
Section, Paragraph:
Editorial or Substantive:
Suggested Alternative Language:
Reason:

Please include your name, organization, and email address in your correspondence.

Table of Contents

Table of Figures

List of Tables

<This page was intentionally left blank.>

Section 1
General Information [Informative]

1.1 Purpose

This System Requirement Specification (SyRS) has been developed for the Advanced Transportation Controller (ATC) Cybersecurity Project under the United States Department of Transportation (USDOT) Contract # DTFH61-16-D-00055, Work Order # 19-0403. The purpose of the project is to identify and address cybersecurity needs in the ATC family of standards comprising the ATC 5201 ATC Standard, the ATC 5401 ATC Application Programming Interface (API) Standard, and the ATC 5301 ATC Cabinet Standard. The ATC standards are being developed and maintained under the direction of the ATC Joint Committee (JC), which is composed of representatives from the American Association of State Highway and Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE) and the National Electrical Manufacturers Association (NEMA).

This SyRS has been prepared by the ATC Cybersecurity Working Group (WG), a technical subcommittee of the ATC Cybersecurity Committee. It establishes a common understanding of the user needs for the cybersecurity elements to be applied to the three ATC standards for the following:

a) The local, state, and federal transportation agencies who specify and use ATC equipment;
b) The manufacturers, software developers and integrators who create equipment, software, and systems that use ATC equipment; and
c) The public who benefits from the deployment of ATC equipment and who directly or indirectly pays for these products.

1.2 Scope

The ATC family of standards provide an open architecture hardware and software platform that can support a wide variety of Intelligent Transportation Systems (ITS) applications including those for traffic management, safety, and security. It is expected that many of the cybersecurity issues addressed for the ATC standards will also apply to other ITS standards and specifications.

The project follows a systems engineering process. Its interim deliverables are a Concept of Operations (ConOps), an SyRS, and a System Design Description (SDD) for the cybersecurity areas of concern for the three ATC standards. The primary deliverable of the project is the ATC Cybersecurity Standard.

This SyRS provides high level background material on how transportation field cabinet systems (TFCSs) operate and descriptions of the three current ATC standards. This aids participants in the ATC Cybersecurity Project who may be less familiar with such equipment and provides context when identifying cybersecurity needs and developing requirements.

1.3 References

1.3.1 Normative References

Normative references contain provisions that, when they are specifically referenced in other sections of this document, constitute provisions of this standard. At the time of publication, the versions indicated for the references were valid. All references are subject to revision. Parties using this document are encouraged to investigate the possibility of applying the most recent versions of the references listed.

Identifier	Title
ATC 5201 v06A	Advanced Transportation Controller (ATC) Standard Version v06A, AASHTO / ITE / NEMA, 29 July 2020.
ATC 5301 v02	Advanced Transportation Controller (ATC) Cabinet Standard Version v02, AASHTO / ITE / NEMA, 18 March 2019.
ATC 5401 v02B	Application Programming Interface (API) for the Advanced Transportation Controller (ATC), AASHTO / ITE / NEMA, 16 February 2023.

1.3.2 Other References

The following documents and standards may provide the reader with a more complete understanding of transportation architecture, ITS field equipment, communications, and security; however, these documents do not contain direct provisions that are required by the ATC Cybersecurity Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision. Parties to agreements based on the ATC Cybersecurity Standard are encouraged to investigate the possibility of applying the most recent editions of the standard listed.

Identifier	Title
ARC-IT 9.1	Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT), USDOT, https://arc-it.net
Caltrans TEES 2020	Caltrans Transportation Electrical Equipment Specifications (TEES), California Department of Transportation, 5 November 2020.
CIS Controls v7.1	Implementation Guide for Industrial Control Systems, Center for Internet Security, 2019
CTI 4001 v01	Roadside Unit (RSU) Standard v01, AASHTO / ITE / NEMA / SAE, 11 November 2021.
CTI 4501 v01	Connected Intersections Implementation Guide v01, AASHTO / ITE / NEMA / SAE, September 2021.
ISO/IEC 15408-1:2022	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model, ISO/IEC. 2022
ISO/IEC/IEEE 29148:2011	Systems and software engineering — Life cycle processes — Requirements engineering
ISO/IEC 9899:2018	Information technology -- Programming languages -- C, ISO/IEC, 2018
ITS Cabinet Standard v01	Intelligent Transportation System (ITS) Standard Specification for Roadside Cabinets v01.02.17b, AASHTO / ITE / NEMA, 16 November 2006.
NEMA TS 1-1989	Traffic Control Systems. National Electrical Manufacturers Association, 1989
NEMA TS 2-2016	Traffic Controller Assemblies with NTCIP Requirements—Version 03.07, National Electrical Manufacturers Association, 2016.
NEMA TS 8-2018	Cyber and Physical Security for Intelligent Transportation Systems (ITS), National Electrical Manufacturers Association, April 2020.
NIST CSRC Online Glossary	NIST Computer Security Resource Center (CSRC) Online Glossary, https://csrc.nist.gov/glossary/
NIST SP 800-53 Rev. 5	Security and Privacy Controls for Information Systems and Organizations, National Institute of Standards and Technology, 2019
NIST SP 800-63B-4	Digital Identity Guidelines: Authentication and Authenticator Management, National Institute of Standards and Technology, 2025
NTCIP 9001 v04	The NTCIP Guide v04, AASHTO / ITE / NEMA, July 2009.

1.3.3 Contact Information

1.3.3.1 Architecture Reference for Cooperative and Intelligent Transportation

The Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) may be viewed online at:

https://arc-it.net

1.3.3.2 FHWA Documents

Documents from the USDOT Federal Highway Administration (FHWA) (with designations FHWA-JPO-…) are available at the USDOT National Transportation Library, Repository & Open Science Access Portal (ROSA P):

https://rosap.ntl.bts.gov/

1.3.3.3 IEEE Standards

Standards from the Institute of Electrical and Electronics Engineers (IEEE) standards may be purchased online in electronic format or printed copy from the following:

Techstreet
6300 Interfirst Dr.
Ann Arbor, MI 48108
(800) 699-9277
www.techstreet.com/ieee

1.3.3.4 Internet Documents

Request for Comment (RFC) electronic documents may be obtained from several repositories on the World Wide Web, or by “anonymous” File Transfer Protocol (FTP) with several hosts. Browse or FTP to the following:

www.rfc-editor.org
https://www.rfc-editor.org/retrieve/

1.3.3.5 ISO/IEC Standards

Standards from the International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) may be purchased online in electronic format or printed copy from the following:

Techstreet
6300 Interfirst Dr.
Ann Arbor, MI 48108
(800) 699-9277
www.techstreet.com/ieee

1.3.3.6 ITE Standards

Standards from the Institute of Transportation Engineers (ITE) may be obtained from the following:

Institute of Transportation Engineers
1627 Eye Street, NW, Suite 550
Washington, DC 20006

(202) 785-0060
https://www.ite.org/technical-resources/topics/standards/

1.3.3.7 NIST Standards

Standards from the National Institute of Standards and Technology (NIST) may be obtained from the following:

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
301-975-2000
https://csrc.nist.gov/publications/

1.3.3.8 NTCIP Standards

Standards that are a part of the National Transportation Communications for ITS Protocol (NTCIP) family of standards may be obtained from the following:

NTCIP Coordinator
National Electrical Manufacturers Association
1300 17th Street North, Suite 900
Arlington, Virginia 22209
www.ntcip.org
e-mail: ntcip@nema.org

1.4 Terms

The following terms, definitions, acronyms, and abbreviations are used in this document.

Term	Definition
2070	A traffic signal controller that meets the California Department of Transportation (Caltrans) Transportation Electrical Equipment Specifications (TEES) for a Model 2070.
API Managers	API Software that manages an ATC resource for use by concurrently running application programs.
API Software	The body of software that conforms to the API Standard. This software includes API Managers, API Utilities, the functions defined in this standard, and any libraries necessary to implement the standard.
API Utilities	API Software not included in the API Managers that is used for configuration purposes.
Application Program	Any program designed to perform a specific function directly for the user or, in some cases, for another application program. Examples of application programs include word processors, database programs, Web browsers and traffic control programs. Application programs use the services of a computer's OS and other supporting programs such as an application programming interface.
ATC Cabinet Device	Any device that falls under the ATC family of standards.

Term	Definition
ATC Device Drivers	Low-level software not included in standard Linux distributions that is necessary for ATC-specific devices to operate in a Linux OS environment.
ATC Unit	The term used for a traffic signal controller that conforms to the ATC 5201 Standard.
Availability	Ensuring timely and reliable access to and use of information. Source: *NIST CSRC Online Glossary*.
Bus Interface Unit	A transportation cabinet device which is used for SDLC communications within NEMA TS 2 cabinet systems.
Board Support Package	Software usually provided by processor board manufacturers which provides a consistent software interface for the unique architecture of the board. In the case of ATC units, the Board Support Package also includes the OS.
Connected Intersections (CI)	An infrastructure system that broadcasts signal, phase, and timing (SPaT) information, mapping information and position correction data to On-Board Units and Mobile Units. Source: *CTI 4501*.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Source: *NIST CSRC Online Glossary*.
Cybersecurity Risk	An effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. Source: *NIST CSRC Online Glossary*.
Data At Rest (DAR)	Data that is not actively moving from device to device or network to network such as data stored on a hard drive, flash drive, or archived/stored in some other way.
Data In Transit (DIT)	Data that is actively moving from one location to another such as across the internet, through a private network, or between devices. Also, called Data in Motion.
Interchangeability	The capability to exchange devices of the same type on the same communications channel and have those devices interact with other devices of the same type using standards-based functions. Source: *The NTCIP Guide*
Interface	A shared boundary across which information is passed. Source: *IEEE Std 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology, 1990.*
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Source: *NIST CSRC Online Glossary*.

Term	Definition
Interoperability	The ability of two or more systems or components to exchange information and to use the information that has been exchanged. Source: *IEEE Std 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology, 1990.*
Mobile Unit (MU)	A device used to wirelessly communicate with other devices for safety and mobility purposes carried by a pedestrian, bicyclist, work zone worker, or other traveler. Source: *RSU Standard v1.0.*
Operational Scenario	A scenario is a step-by-step description of how the proposed [system] should operate and interact with its users and its external interfaces under a given set of circumstances. Operational Scenarios help readers understand how all pieces of the system interact to provide operational capabilities. Source: *IEEE 1362-1998.*
Provisioning	Provisioning is the process by which a system, device, service, or resource is prepared and made ready for use, including the allocation and configuration of required capabilities (e.g., network connectivity, storage, software components, security credentials, and user accounts), deployment into the target environment, and the enablement of access for authorized entities. A resource is considered provisioned once it has been successfully configured, deployed, and made operational within its intended environment. Source: *Adapted from usage in NIST SP 800-145, NIST SP 800-63B, IETF RFC 7642-7644, and NIST SP 1800-36.*
Roadside Unit (RSU)	A transportation infrastructure communications device located on the roadside that provides vehicle-to-everything (V2X) connectivity between OBUs/MUs and other parts of the transportation infrastructure including traffic control devices, traffic management systems, and back-office systems. Note: Devices that are not part of the transportation infrastructure, such as cellular base stations or satellites, are not RSUs. Source: *RSU Standard v1.0*.
Robustness	Degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions. Source: *ISO/IEC/IEEE 24765:2017 Systems and software engineering-Vocabulary.*
Serial Interface Unit	A transportation cabinet device which is used for SDLC communications within ATC cabinet systems.

Term	Definition
Synchronous Data Link Control (SDLC)	A protocol that is used for transferring synchronous, code-transparent, serial-by-bit information over a communications line. Transmission exchanges can be duplex or half-duplex over switched or nonswitched lines. The configuration of the connection can be point-to-point, multipoint, or loop. Source: *IBM Documentation https://www.ibm.com/docs/en*.
Transport Layer Security (TLS)	A cryptographic protocol that provides secure communication over a computer network. It can be implemented in any application or protocol that requires secure communications. The latest version, TLS 1.3, is faster and more secure than previous versions.
Transportation Field Devices	Devices and electronic systems that monitor and control traffic operations on a roadway.

1.5 Abbreviations

The abbreviations and acronyms used in this document are defined below.

AASHTO	American Association of State Highway Transportation Officials
ADU	Auxiliary Display Unit
API	Application Programming Interface.
APIRI	API Reference Implementation
APIVS	API Validation Suite
ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
ASARP	As Secure As Reasonably Practicable
ATC	Advanced Transportation Controller
BBS	Battery Backup System
BIU	Bus Interface Unit
BSM	Basic Safety Message
BSP	Board Support Package
C2C	Center-To-Center
C2F	Center-To-Field
CI	Connected Intersection
CIS	Center for Internet Security
CMU	Cabinet Monitor Unit or Conflict Monitor Unit
CPS	Cabinet Power Supply
ConOps	Concept of Operations
CV	Connected Vehicle
DAR	Data at Rest

DCS	Distributed Control System
DIT	Data in Transit
DRAM	Dynamic Random Access Memory
DTLS	Datagram Transport Layer Security
ECLA	External Control Local Application
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
HDLC	High-level Data Link Control
HDSP	High-Density Switch Pack
HSM	Hardware Security Module
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
ICS	Industrial Control System
IOO	Infrastructure Owner/Operator
I-SIG	Intelligent Traffic Signal
ISSA	Infrastructure Standards Security Assessment
IT	Information Technology
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation System or Systems
JC	Joint Committee
Kbps	Kilobits per second
MAC	Media Access Control
MMU	Malfunction Management Unit
MU	Mobile Units
NCHRP	National Cooperative Highway Research Program
NEMA	National Electrical Manufacturers Association
NIST	National Institute of Standards and Technology
NRTM	Needs to Requirements Traceability Matrix
NTCIP	National Transportation Communications for ITS Protocol
OBU	On-Board Units
OS	Operating System
OSS	Open Source Software
PCB	Printed Circuit Board

PLC	Programmable Logic Controller
RA	Registration Authority
RAM	Random Access Memory
RSU	Roadside Unit
RTC	Real-Time Clock
SBOM	Software Bill of Materials
SCADA	Supervisory Control and Data Acquisition
SCMS	Security Credentials Management System
SDD	System Design Description or Software Design Description
SDO	Standards Development Organizations
SDLC	Synchronous Data Link Control
SE	Systems Engineering
SEP	Systems Engineering Process
SIU	Serial Interface Unit
SNMP	Simple Network Management Protocol
SPaT	Signal Phase and Timing
SRAM	Static Random Access Memory
SyRS	System Requirements Specification
SSE	Systems Security Engineering
SU	Sensor Unit
SyRS	System Requirements Specification
TEES	Transportation Electrical Equipment Specifications
TFCS	Transportation Field Cabinet System
TLS	Transport Layer Security
TMS	Traffic Management System
TSC	Traffic Signal Controller
UPS	Uninterruptible Power Supply
US	United States
USB	Universal Serial Bus
USDOT	United States Department of Transportation
V2X	Vehicle-to-Everything
VAC	Volts Alternating Current
VDC	Volts Direct Current

1.6 Using this Standard

This section describes how this standard is organized, how its content is interpreted, and how it is referenced in procurement documents or conformance claims. It also explains the use of Cybersecurity Conformance Levels, the deprecation policy for User Needs, Requirements, and Design Elements, and how this standard relates to other ATC and non-ATC cabinet architectures.

1.6.1 Cybersecurity Conformance Levels

This standard uses **Cybersecurity Conformance Levels** to represent progressively higher cybersecurity capability for ATC systems. These levels apply to Devices, User Needs, System Requirements, and Design Elements defined throughout this document. The Conformance Levels used in this version are as follows:

a) Conformance Level 1

Represents the baseline cybersecurity capability defined in this version of the standard. Devices conforming to **Level 1** implement all requirements and design elements assigned to Level 1 that are applicable to the device.

b) Conformance Level *N* (where N is any Conformance Level higher than Level 1)

Represents a future, higher cybersecurity capability that expands upon Level 1 and reflects the maturation of cybersecurity protections over time. Devices conforming to **Level *N*** implement all requirements and design elements assigned to Levels 1 through N that are applicable to the device.

c) Conformance Level D (Deferred)

Represents User Needs or System Requirements identified by the ATC Cybersecurity Working Group that are intentionally not addressed in this version of the standard to expedite delivery of the Level 1 capabilities. Deferred User Needs do not generate requirements or design elements in this version and are intended to be assigned to a numbered Conformance Level in a future revision.

These levels support gradual industry adoption, reflect legacy field deployments, and provide a structured path for future cybersecurity enhancements.

1.6.2 Deprecation of User Needs, Requirements, and Design Elements

As this standard evolves, certain User Needs, System Requirements, or Design Elements may become obsolete, superseded, or no longer applicable. To maintain numbering continuity and preserve traceability, this standard applies the same deprecation approach to all three types of content.
When a User Need, Requirement, or Design Element becomes deprecated:

1. Only its identifier and title appear in the main body, marked "**[Deprecated]**".
2. Its full historical content appears in a dedicated Informative Annex of Deprecated Items.
3. Deprecated items are non-normative and do not contribute to cybersecurity conformance at any Conformance Level.
4. Deprecation occurs only when an item is formally removed from the active conformance baseline.

Revisions made solely for clarification, correction, or editorial improvement do not constitute deprecation.
A Requirement is deprecated only when all the User Needs from which it is derived are deprecated.
A Design Element becomes deprecated when sufficient Requirements originally associated with it are no longer active, such that the design no longer provides functional value.

Deprecated items are retained to preserve historical records, support backward compatibility, and help ensure continuity with earlier versions of the standard.

1.6.3 Specifying this Standard

Any formal claim of conformance or compliance to this standard, by a manufacturer, vendor, agency, or procurement document, uses the following reference form:

"**ATC 5501" *[Name]* "v" or "Version" *[MM.mm]* "Conformance Level" or "Level" *[N]*** where:

- *Name* is "ATC Cybersecurity Standard" (optional)
- *MM* is the two-digit major version number
- *mm* is the two-digit minor version number
- *N* is the Conformance Level number

Examples:

- "This device conforms to ATC 5501 ATC Cybersecurity Standard v01.11, Conformance Level 1."
- "This device conforms to ATC 5501 Version 01.40, Conformance Level 2."
- "This device conforms to ATC 5501 v01.40, Level 2."

Phrases such as *"meets ATC specifications," "ATC compliant,"* or other ambiguous language do not constitute valid conformance claims.

Manufacturers or vendors may state that a device "meets or exceeds" a particular Conformance Level when it satisfies all requirements and design elements for that Level, includes additional cybersecurity features provided by the manufacturer or vendor, and does not meet a higher Conformance Level defined by the standard.

A valid conformance claim clearly identifies the highest Conformance Level implemented by the device.

1.6.4 Relationship to Other Standards

The ATC Cybersecurity Standard (ATC 5501) defines cybersecurity expectations for the ATC Cabinet System and for devices that operate within or interface with that system. These include, but are not limited to, devices defined in:

- ATC 5201 ATC Standard (Controller Standard)
- ATC 5301 ATC Cabinet Standard
- ATC 5401 ATC Application Programming Interface (API) Standard.

ATC 5201 controllers may be used in cabinet architectures such as ATC 5301, NEMA TS 1, NEMA TS 2 (Type 1 or Type 2), and Type 332 family cabinets, depending on agency preference, legacy systems, and manufacturer offerings. Likewise, ATC 5301 cabinets may be populated with ATC units of varied vintages and capabilities, including controllers that may not support modern cybersecurity protections.
ATC 5501 does not assume that existing ATC 5201 or ATC 5301 equipment deployed in the field can meet the cybersecurity capabilities defined in this standard. Agencies wishing to ensure cybersecurity conformance should specify ATC 5501 explicitly.

Future revisions of ATC 5201, ATC 5301, and ATC 5401 are expected to align with ATC 5501 so the ATC platform functions as a unified secure system. Because the ATC standards follow differing update cycles, alignment occurs over time; once alignment is complete, procurement of an ATC-conformant cabinet or controller inherently includes the cybersecurity expectations defined in ATC 5501.

Section 2
Concept of Operations [Normative]

2.1 Tutorial [Informative]

In systems engineering, the different stages of the definition and design process are captured in documents specific to the stage of development of the system (or device). A ConOps is a document that describes characteristics for the proposed system from the user's perspective. This ConOps section serves this purpose. The goal is to have a common understanding between the users of the system and the developers of requirements for the system. User needs for the system are identified via collaboration of a broad base of stakeholders and some are drawn from existing documents. Each user need is captured in the ConOps in a formal manner along with the rationale which justifies the inclusion of the need and may also provide other clarifying information so that the user need is understood in subsequent stages of development.

This ConOps has been prepared as part of the development of the ATC Cybersecurity Standard. The terms “Normative” and “Informative” are used to distinguish parts of this ConOps that must be conformed to (Normative) and those that are there for informational purposes (Informative). It is possible for a section to be identified as Normative but have subsections that are identified as Informative. If a section is identified as Normative, then all of its subsections are to be considered Normative unless identified otherwise.

The remaining sections of this ConOps are as follows:

- **Section 2.2 Background [Informative].** This section provides background information on how transportation field cabinet systems operate and descriptions of the three current ATC standards.
- **Section 2.3 Current Situation and Problem Statement [Informative].** This section describes the current situation and the need for an ATC Cybersecurity Standard.
- **Section 2.4 ATC Cabinet Operational Architecture [Informative].** This section describes the operational architecture of an ATC Cabinet in relation to other systems and devices.
- **Section 2.5 ATC Cybersecurity Scope [Informative].** This section provides the scope for the ATC Cybersecurity Standard and identifies areas being addressed.
- **Section 2.6 Architectural Constraints [Informative]**. This section identifies constraints on the architecture for the ATC Cybersecurity Standard.
- **Section 2.7 ATC Cybersecurity Needs [Normative].** This section identifies the cybersecurity user needs for ATC equipment.
- **Section 2.8 Operational Policies and Constraints [Normative]**. This section describes any operational policies and constraints that apply to the system or situation.
- **Section 2.9 Operational Scenarios [Informative].** This section provides any operational scenarios identified for the system.
- **Section 2.10 ARC-IT and Security [Informative].** This section provides security resource information available on the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT).

2.2 Background [Informative]

2.2.1 General Description of Transportation Field Cabinet Systems

Starting in the 1970s, standards and specifications emerged for actuated traffic signal control. These standards and specifications defined systems that are located in cabinets at signalized intersections.

Since that time, these standards and specifications have evolved, and new national standards have been developed to add capabilities and features while preserving the same general concepts as their predecessors.

There are six major TFCS standards and specifications. From oldest to newest, they are:

- "NEMA TS 1 Traffic Control Systems," National Electrical Manufacturers Association (NEMA). Commonly called a "TS 1 Cabinet." This standard was originally published in 1976 and last published in 1989.
- "Caltrans Transportation Electrical Equipment Specifications (TEES)," California Department of Transportation. Commonly called the "Model 332 Cabinet" or "Model 33x Cabinets" to refer to other cabinets of the same general style. This specification was originally published in 1978 and last published 2020.
- "NEMA TS 2 Traffic Controller Assemblies," NEMA. Commonly called a "TS 2 Cabinet" or "TS 2 Type 1 Cabinet." The standard also provides some feature enhancements for the older TS 1 Cabinet, called a "TS 2 Type 2 Cabinet." This standard was originally published in 1992 and last published in 2016.
- "Intelligent Transportation System (ITS) Standard Specification for Roadside Cabinets," ATC Joint Committee. Commonly called the "ITS Cabinet." The standard was published in 2006.
- "ATC 5301 Advanced Transportation Controller (ATC) Cabinet Standard," ATC Joint Committee. Commonly called the "ATC Cabinet (ATCC)." A successor to the ITS Cabinet, the ATCC has significant additional features and design changes. This standard was originally published in 2016 and last published in 2019.

The general elements of a TFCS are described below and illustrated in Figure 1.

- **Inputs** supply information to the Controller from external (field) sensors in the form of on/off states. There are numerous sensor technologies including inductive loops, video, radar, and magnetometers. Most commonly, Inputs consist of "sensor units" or "detectors" housed in a "detector rack," "input assembly," or "input file" (terms are synonymous). Cabinets can also include additional input functionality capable of receiving information from additional sources.

- The **Controller** is a field hardened computer that runs the signal control application and other applications. The signal control application associates Inputs with movements through the intersection. The Controller reads the Inputs, determines how to safely provide right of way to road users, and switches signal indications (reds, yellows and greens) via the Outputs. Not shown, Controllers will also communicate with a Roadside Unit (RSU) to support a connected intersection (CI) environment.

- **Outputs** are switches grouped in components called "switch packs" or "load switches" (terms are synonymous) that are switched by the Controller to enable or disable the flow of electricity to signal indications, turning them on and off. Switch packs/load switches may be plugged into a "cabinet back panel," "load bay," or "terminal and facilities area" (terms are synonymous); or in an "output assembly," "output rack," or "output file" (terms are synonymous). Cabinets can also include additional output functionality capable of driving auxiliary devices.

- The **Monitor** (or signal monitor) ensures that the signal indications are non-conflicting by comparing them to pre-configured safe states programmed by the user using either hardware "program cards" or in software programmable flash memory devices (e.g., "data keys"). If conflicting signal indications are sensed, the monitor transfers the TFCS to a fault state, which changes the signal indications from normal operation to flash. Depending on the type of TFCS, the monitor may also be able to validate that the Controller is operating, and that internal cabinet and output voltages are within allowable parameters. Depending on the type of TFCS, the

Monitor may be called a Conflict Monitor Unit (CMU), Malfunction Management Unit (MMU), or Cabinet Monitor Unit (CMU). Monitors may have auxiliary communication ports.

- The **Power Supply** provides power for the devices internal to the TFCS.

- The **Internal Bus** interconnects the Input, Output, Controller, and Monitor elements. Older TFCSs (e.g., TS 1, Model 33x) have "parallel buses" with discrete electrical wiring between the elements. More modern TFCSs (e.g., TS 2, ITS, ATCC) have "serial buses" that use synchronous data link control (SDLC) communications to exchange data between the elements.

- The **Enclosure** includes the cabinet housing, doors, latches/locks, hinges and door catches, gasketing, ventilation, lighting, internal assembly mounting, and external mounting (e.g., foundation/base, pole, or pedestal).

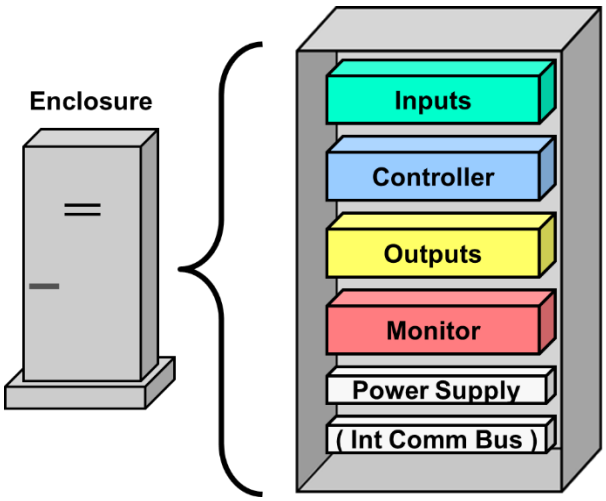


Figure 1. Elements of a Transportation Field Cabinet System.

Figure 2 illustrates the basic operation of a TFCS. Steps are as follows:

1) Field sensors detect vehicles which are provided as inputs to the controller.
2) The controller determines which movements should receive right of way according to its programming.
3) The controller determines the signal indications and turns them on or off via the outputs.
4) The outputs switch power to the signal indications according to the commands from the controller.
5) At the same time, the monitor verifies that the signal indications are not in conflict and that the other elements of the TFCS are operating correctly. If they are not, the monitor transfers the TFCS to a fault state.
6) For NEMA TS 2 Cabinets, ITS Cabinets, and ATC Cabinets, the monitor sends the status of the outputs to the controller (voltage in TS 2, voltage and current in ITS and ATCC).

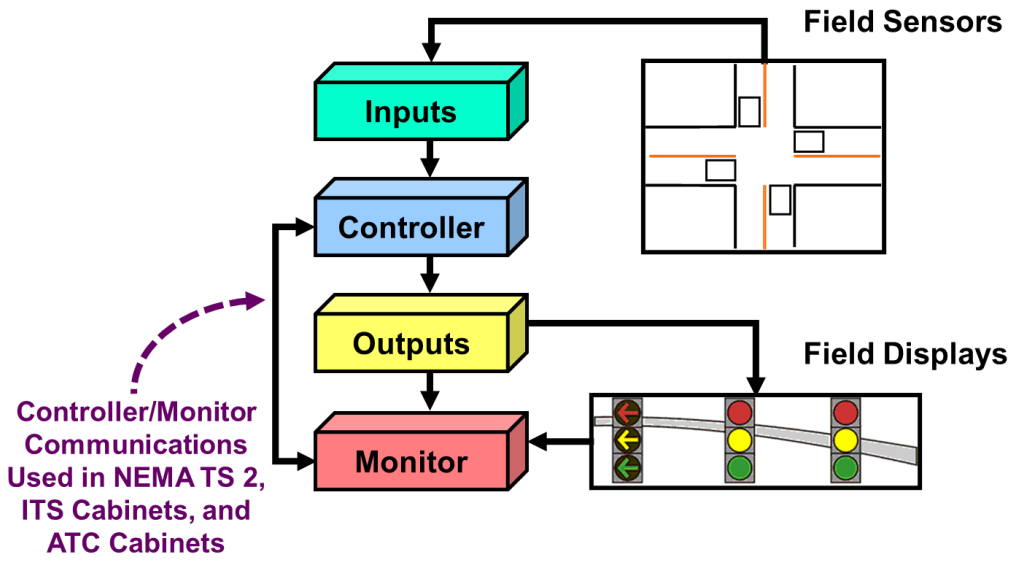


Figure 2. Basic operation of a Transportation Field Cabinet System.

TFCSs typically have additional equipment that is not defined by ITS standards such as:

- **Networking Equipment** including switches, routers, Ethernet, Wi-Fi, fiber optics, and cellular devices.
- **Advanced Detection Systems** that typically have dedicated processors including non-intrusive detectors installed above or beside the roadway (e.g., radar, video, and lidar) and sophisticated intrusive detectors (e.g., magnetometers). They may actuate inputs via sensor units in the detector rack or they may connect to the serial bus. Their processors may have Ethernet ports for remote management, monitoring, and configuration.
- **Priority and Preemption Systems** implement transit signal priority and emergency vehicle preemption using equipment in TFCSs that receives data from vehicles and sends requests to the controller inputs via either sensor units in the detector rack or the serial bus.
- **Clock Sync Devices and GPS Time Sources** connect directly to controllers via USB, asynchronous serial (EIA-232), or Ethernet. These devices may set the controller's clock or the controller may poll them at regular intervals to update its clock.
- **Battery Backup Systems (BBSs) and Uninterruptible Power Supplies (UPSs)** are used at some TFCSs to sustain signal indications during power outages. These devices typically have Ethernet ports for remote management, monitoring, and configuration.
- **External Control Local Application (ECLA) Devices** are used at some TFCSs to modify the controller's operation by changing its timing plan (pattern), adjusting its timing parameters, and issuing it real-time signal control commands such as holds, force-offs, and omits. ECLA devices often run adaptive control programs from a manufacturer other than the controller manufacturer. ECLA devices have Ethernet ports for remote management, monitoring, and configuration.
- **Connected Vehicle (CV) Processors / Coprocessors** are devices that offload processing demands for connected intersections (CIs) from the main processor of the controller or an RSU. They may perform some of the processing required to provide Signal Phase and Timing (SPaT) messages, process incoming messages such as BSMs, or other functions of a connected intersection (CI). These devices can be co-processors within the controller or separate devices within the cabinet system. These devices may have Ethernet ports for remote management, monitoring, and configuration.

2.2.2 Description of ATC Standards

The Advanced Transportation Controller (ATC) family of standards provide an open architecture hardware (HW) and software (SW) platform that can support a wide variety of Intelligent Transportation Systems (ITS) applications including traffic management, support for connected vehicles (CVs), specialized data collection, safety, security, and other applications. The ATC standards are being developed and maintained under the direction of the ATC Joint Committee (JC) which is made up of representatives from the American Association of State Highway and Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE), and the National Electrical Manufacturers Association (NEMA).

Historically, the transportation industry has had a relatively slow growth in controller computing power compared to edge products in other industries. Some of the factors were as follows:

- Controllers were viewed as single application devices. Controllers evolved from mechanical timers in the 1940s. Early microprocessors and the cost and size of memory seemed marginally bigger than the needs of the signal programs.
- Some standards and specifications identified specific processors for controllers that were obsolete soon after the documents were published. When these standards and specifications were in development, it was important to be able to purchase the controller hardware and the application software from different manufacturers and developers. The solution at the time was to identify a specific processor within the standard. However, it was underestimated how long such documents took to develop and the reluctance to change things once they were adopted. For instance, there are controllers being bought new in the United States today that are based on 1980s technology.
- Some standards treated the controller as a closed architecture device which meant that only software produced by the manufacturer could run on the controller.

The ATC Standards Program was started help mitigate these factors.

The ATC Program concept for a controller (including OS and enabling software) was to define a general-purpose field computing platform for transportation applications. The design goals were:

- Open architecture – Any manufacturer or developer can build a controller that meets the internal architecture defined in the standard.
- Modular – This means that the internal structure of the controller has a separation in subsystems or assemblies and flexibility in the way they are combined. Modularity can increase the maintainability of a system, the utility of a system, and the testability of a system.
- Multi-process / Multi-application – Multi-process means that the controller can run multiple application programs at the same time. Multi-application means these programs may be used for different purposes.
- Application Portability – Portability means that there is low effort required for applications to run on ATC units from different vendors.
- Grow in Capability – The standard allows controllers to evolve with better processors and memory and still conform to the standard.
- Upgrade Legacy TFCSs – The controller can provide contemporary performance and capabilities for all of the nationally recognized TFCSs being used in the United States.

The ATC Program also set out to create a new TFCS standard based on lessons learned and technology improvements over the legacy TFCS standards. The design goals were the following:

- Focus on increasing value to end users – This means providing more capability for the same or reduced cost.
- Flexibility within the standard for innovative designs – This means that the placement of the assemblies and components is not set within the standard. The size of components is not specified unless interchangeability is intended.
- Higher density – Able to put more inputs and outputs in a smaller space.
- Increased technician safety – Protect technicians.
- Increased public safety – Protect the public.
- Enhanced monitoring functionality – Monitor more aspects of the TFCS and provide more information to the end user.

- Increased cabinet power efficiency – Potential power conservation.
- Provide LED signal compatibility – Potential power conservation and alternative power sources.

The ATC 5201 ATC Standard and the ATC 5401 ATC Application Programming Interface (API) Standard were developed to meet the goals for ATC units. The ATC 5301 ATC Cabinet Standard was developed to meet the goals for a new TFCS standard.

2.2.2.1 ATC 5201 ATC Standard

ATC 5201 Advanced Transportation Controller (ATC) Standard Version v06A is the latest version of ATC 5201. The standard specifies a controller architecture where the computational components reside on a 5” x 4” printed circuit board (PCB), called the “Engine Board,” with standardized connectors and pinout. The Engine Board contains the following items:

a) CPU
b) Linux Operating System (OS) and Device Drivers
c) Non-Volatile (Flash) Memory
d) Dynamic and Static RAM (DRAM and SRAM)
e) Real-Time Clock (RTC)
f) Two Ethernet ports (manufacturers add Ethernet switches outside of the Engine Board to make more external Ethernet connections available on a controller)
g) One Universal Serial Bus (USB) port that is used for a portable memory device
h) Seven serial ports (some are designated for special interfaces and others general purpose).

The Engine Board plugs into a “Host Module” that supplies power and physical connection to the I/O devices of the controller. While the mechanical and electrical interfaces to the Engine Board are completely specified, the Host Module may be different shapes and sizes to accommodate controllers of various designs. Figure 3 shows how the Engine Board can be used to create ATC units that work within different families of traffic signal controller equipment. This concept also allows more powerful Engine Boards to be deployed in the future without changing the overall controller and cabinet architecture.

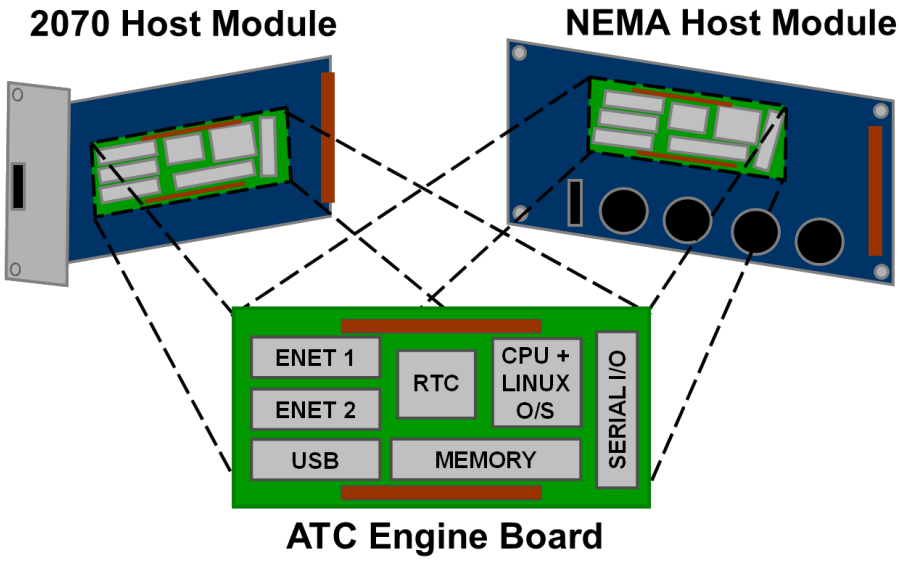


Figure 3. ATC Engine Board is used to support different families of controllers.

ATC 5201 specifies a minimum level of processing capability for the Engine Board. It also specifies the minimum physical and communication requirements for the Host Module. The Engine Board

communication ports and their typical functions are illustrated in Figure 4 (not all named ports are required for different configurations). In the configuration shown, Serial Ports 1-3 are for general use.

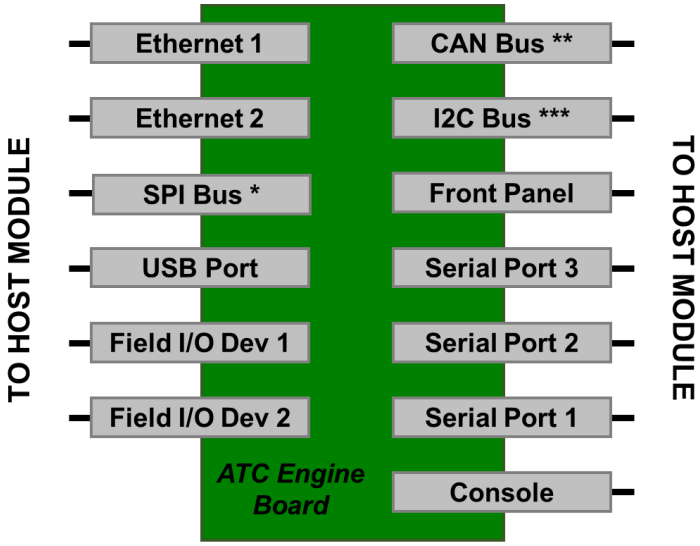


Figure 4. ATC Engine Board communications ports and their functions.

A controller that conforms to ATC 5201 alone usually runs a single application program. While Linux is a multi-process OS, ATC 5201 does not provide for multiple applications running concurrently from different software providers. This is because there is no capability to share the resources of the front panel and the TFCS internal communications. This capability is addressed in ATC 5401 as described in Section 2.2.2.2.

2.2.2.2 ATC 5401 ATC Application Programming Interface Standard

ATC 5401 Advanced Transportation Controller (ATC) Application Programming Interface (API) Standard Version v02A is the latest version of ATC 5401. ATC 5401 defines API Software that enables application programs to share access to the front panel of the controller and the field I/O devices of the TFCS. The API Software has “managers” for the front panel and field I/O devices that are active when the controller is operating. Application programs interact with these managers through functions specified in ATC 5401 using the C programming language. These functions are implemented in the source code of the API Software. ATC 5201 requires that manufacturers provide the libraries and build chain required to create programs for their ATC hardware. Portability of application programs to ATC Engine Boards from different manufacturers is achieved by application developers compiling and linking their application source code and the API Software source code for the targeted manufacturer. See Figure 5.

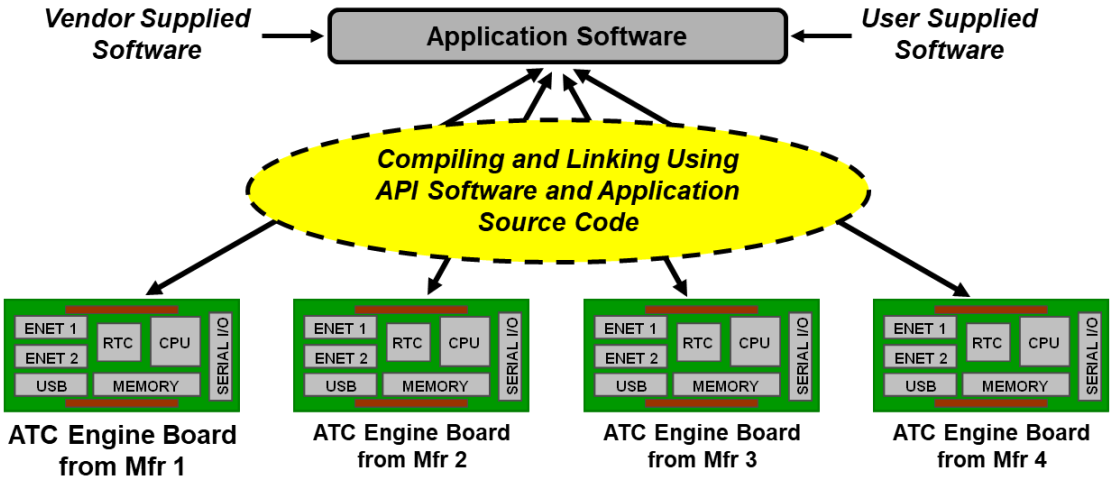


Figure 5. Application portability through compilation and linking of source code.

Figure 6 illustrates the organization and layered architecture of ATC software. The "Linux OS and Device Drivers" reflects a specification of the Linux OS defined in the ATC Board Support Package (BSP) in ATC 5201. This includes functions for things typical in any computer system such as file I/O, serial I/O, interprocess communication, and process scheduling. It also includes the specification of the device drivers necessary for the Linux OS to operate on the ATC hardware. "API Software" refers to the software specified ATC 5401. As shown in Figure 6, both users and application programs use the API Software to interface to ATC units.

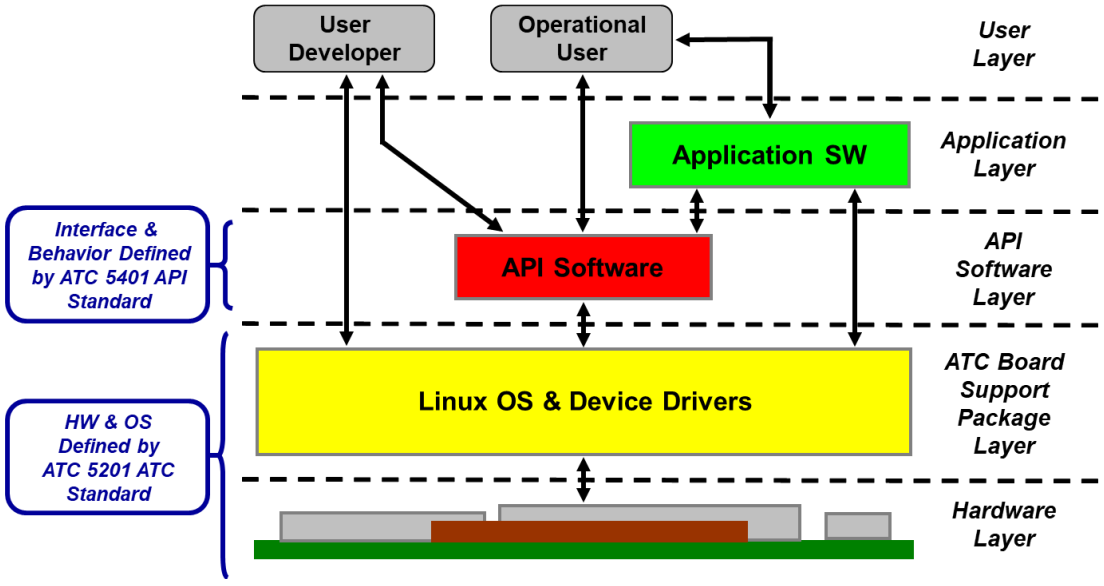


Figure 6. ATC software layered organization.

The division of the ATC software into layers helps to ensure consistent behavior of the software environment between ATC architectures and also provides a migration path to new ATCs in the future. The relationship between the Hardware Layer and ATC BSP Layer is maintained, for the most part, by the Linux operating system community of users and the manufacturers of the Engine Board. Linux source code licenses are free to the public and there are strong market incentives for Linux users to maintain the

Linux standard and ensure consistent functionality of the Linux commands for the operating system. The relationship between the ATC BSP Layer and the API Software Layer is maintained by the transportation community through the ATC standards. Functions in the API Software Layer access the ATC unit through the functions in the ATC BSP Layer. If programs written for the Application Layer only reference the ATC unit through the functions specified in the API Software Layer and ATC BSP Layer, they will be able to operate on any ATC provided the source code is recompiled for the target ATC's processor. Users of the API Software are: a) the operational users that interact with the application programs and the technicians or engineers who configure the system settings (e.g., system time, Ethernet ports, systems services) and b) the user developers who use the API Software to develop applications.

Figure 7 shows an example of the Front Panel Manager window that allows users to select which application program running on the ATC unit to display on the screen. In this example, there are four application programs running: Camera Control, Intersection Control, CV Roadside Unit, and Ramp Meter Control. The application program with the asterisk next to its name is the default application to be displayed when the controller is powered up. Figure 8 shows an example of the ATC Configuration Information window. Users use this window to set and view systemwide parameters (e.g., system time, Ethernet ports).

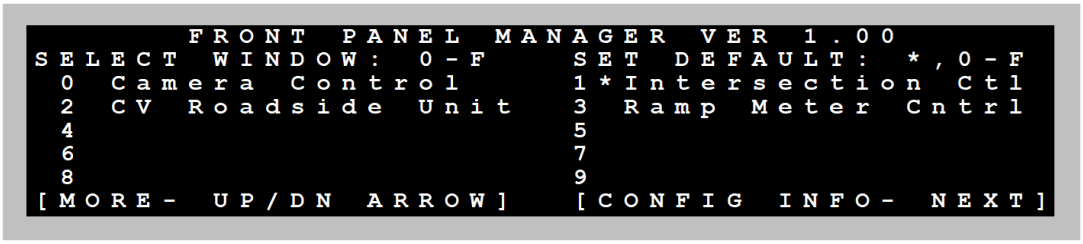


Figure 7. Front Panel Manager allows users to select an application program to put in view.

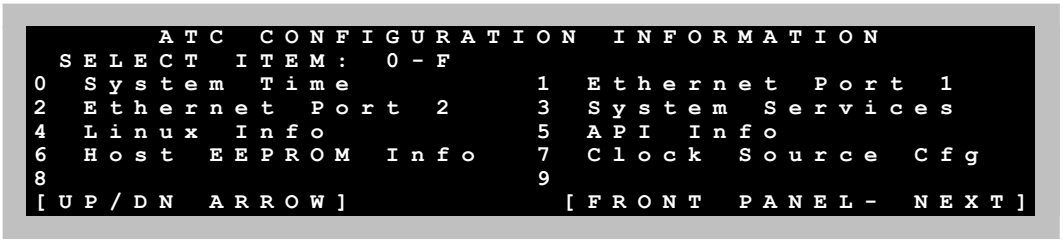


Figure 8. ATC Configuration Information allows users to set and view systemwide parameters.

The USDOT sponsored a project to develop an open source software (OSS) reference implementation of the API Software called the API Reference Implementation (APIRI) and an OSS validation software called the API Validation Suite (APIVS). They are publicly available at https://github.com/apiriadmin/APIRI and https://github.com/apiriadmin/APIVS respectively.

2.2.2.3 ATC 5301 ATC Cabinet Standard

ATC 5301 Advanced Transportation Controller (ATC) Cabinet Standard Version v02 is the latest version of ATC 5301. Figure 9**Error! Reference source not found.** illustrates an example ATC Cabinet System (ATC Cabinet). It must be emphasized that not all ATC Cabinets will have this configuration. The components of the cabinet are color coded in a similar fashion to the general TFCS description in Section 2.2.1.

- The **Controller** is shown as an ATC unit. This refers to the Advanced Transportation Controller unit that conforms to ATC 5201 and ATC 5401 (multi-application support option). ATC units from different manufactures will have a different appearance, size, and shape.

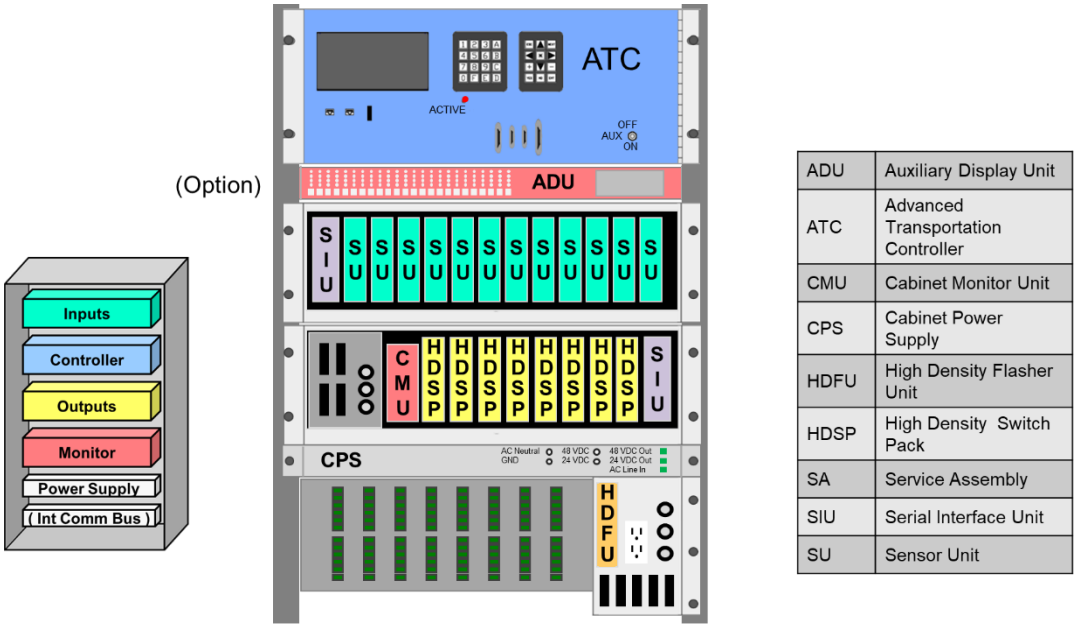
- **Inputs** is shown as an Input Assembly containing Sensor Units (SUs) to perform on-street detection and a Serial Interface Unit (SIU) to communicate the sensor data to the ATC unit. The SUs can be double or quad density detectors that support two or four input channels for each SU. Input assemblies can be different sizes and shapes.

- **Outputs** is shown as an Output Assembly containing High-Density Switch Packs (HDSPs) to control power to signals and other devices, a Cabinet Monitor Unit (CMU) to ensure that there are no conflicting signals (and other monitoring), and an SIU to allow the ATC unit to command the states of the HDSPs. HDSPs can control two output channels for each HDSP. HDSPs also come in high voltage (120 VAC), very high voltage (220 VAC), and low voltage (48 VDC) models. The HDSPs are unique to the ATC Cabinet architecture because of the support for two channels and multiple voltage options. The output assembly can be various shapes and sizes.

- The **Monitor** is shown as a CMU and an optional Auxiliary Display Unit (ADU). The ADU allows technicians to easily see the status of the cabinet system. The ADU may have various designs or the ADU functionality may be achieved through a laptop, handheld device, or the ATC unit. In the latter case, a technician may plug a laptop or handheld device into the CMU or the ATC unit may have a utility to see the status of the cabinet system. The CMU performs load current monitoring which can be used to detect dark signal heads. CMUs come in high voltage (120 VAC), very high voltage (220 VAC), and low voltage (48 VDC) models. The load current monitoring and multiple voltage options are unique to the ATC Cabinet architecture. A removable memory device is used to set the allowable signal state combinations allowed for an intersection in the CMU.

- The **Internal Bus** uses SDLC communications at 614 Kbps (kilobits per second) between the SIUs on the output and input assemblies, the CMU, and the ATC unit.

- The **Power Supply** is shown as the Cabinet Power Supply (CPS). There are several models of CPSs in ATC 5301 and manufacturer-specific designs are also allowed. The CPS converts service power to 48/24/12 VDC to power devices in the ATC Cabinet.



ADU	Auxiliary Display Unit
ATC	Advanced Transportation Controller
CMU	Cabinet Monitor Unit
CPS	Cabinet Power Supply
HDFU	High Density Flasher Unit
HDSP	High Density Switch Pack
SA	Service Assembly
SIU	Serial Interface Unit
SU	Sensor Unit

Figure 9. ATC Cabinet System and Components.

2.3 Current Situation and Problem Statement [Informative]

The United States Cybersecurity and Infrastructure Security Agency (CISA) has identified the US roadway transportation system as one of "16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." It is fundamental to the US economy to be able to transfer goods to market and allow people to go to work and conduct business. The roadway infrastructure is a critical resource in responding to natural disasters, contributing to national security across the country, and generally providing quality of life for the US population. There are over 4 million miles of interstate highways, strategic highways, arterial roadways and intermodal connectors. There are approximately 350,000 signalized intersections.

For most of the computer age, the roadway transportation infrastructure has been protected by its relative obscurity compared to financial institutions, large corporations, and non-transportation government entities. In the middle 1990s, when other sectors were using high-end workstations, fiber networks, and Internet protocols; most of the roadway networks of the transportation sector had single application traffic signal controllers with proprietary operating systems, low-end processors, and used proprietary communications over serial lines. This was due to many factors such as the high cost of replacing infrastructure, the long and complex effort needed to acquire large project funds, and the internal resistance to change by practitioners who maintained such systems. Today, however, this is no longer the case. Most transportation agencies have fiber networks and use Internet protocols. Older traffic signal controllers are being replaced by ATC units that are Linux computers. Operationally, they may be used for different applications and run multiple application programs concurrently.

The exponential rise in the number and sophistication of cyber threats affects all of the US critical infrastructure sectors. IOOs can no longer depend on obscurity to protect the roadway infrastructure. Large transportation agencies are thwarting tens of thousands attacks a day. About one third of state transportation agencies have reported cyber incidents. Traffic delays in metropolitan areas may cost a region hundreds of thousands of dollars per hour. There are demands for more and better data that may expose agencies to more risk. Important societal and economic efforts such as Smart Cities and multi-

modal transportation depend on improved collection, analysis, and distribution of transportation information. Safety efforts such as the Connected Vehicle (CV) program depend on accuracy, precision, and timing where an intrusion could be more detrimental than an all-out failure of the system. Transportation infrastructure may communicate with external systems outside of an agency including cloud services. All of these developments inevitably increase both the vulnerability of the transportation infrastructure and the urgency to include cybersecurity measures in the latest transportation field cabinet systems and subsystems.

2.4 ATC Cabinet Operational Architecture [Informative]

This section identifies the operational architecture of an ATC Cabinet in the field. The description of how TFCSs operate and the introduction to the ATC Cabinet, Controller and API standards have already been provided in Section 2.2 and its subsections. Generally, the internal configurations of an ATC Cabinet will be similar at a subsystem level (e.g., inputs, controller, outputs) but will vary based on the applications being supported, the roadway characteristics, and the connections to other systems. Figure 10 illustrates ATC Cabinet connections to external devices and systems that may exist . This illustration is not intended to be exhaustive. All of the external connections shown are network-type connections except for those used by traditional signal detection and displays which use power from the input and output devices in the cabinet to perform their function (e.g., loop detectors, signal displays, beacons, simple changeable message signs).

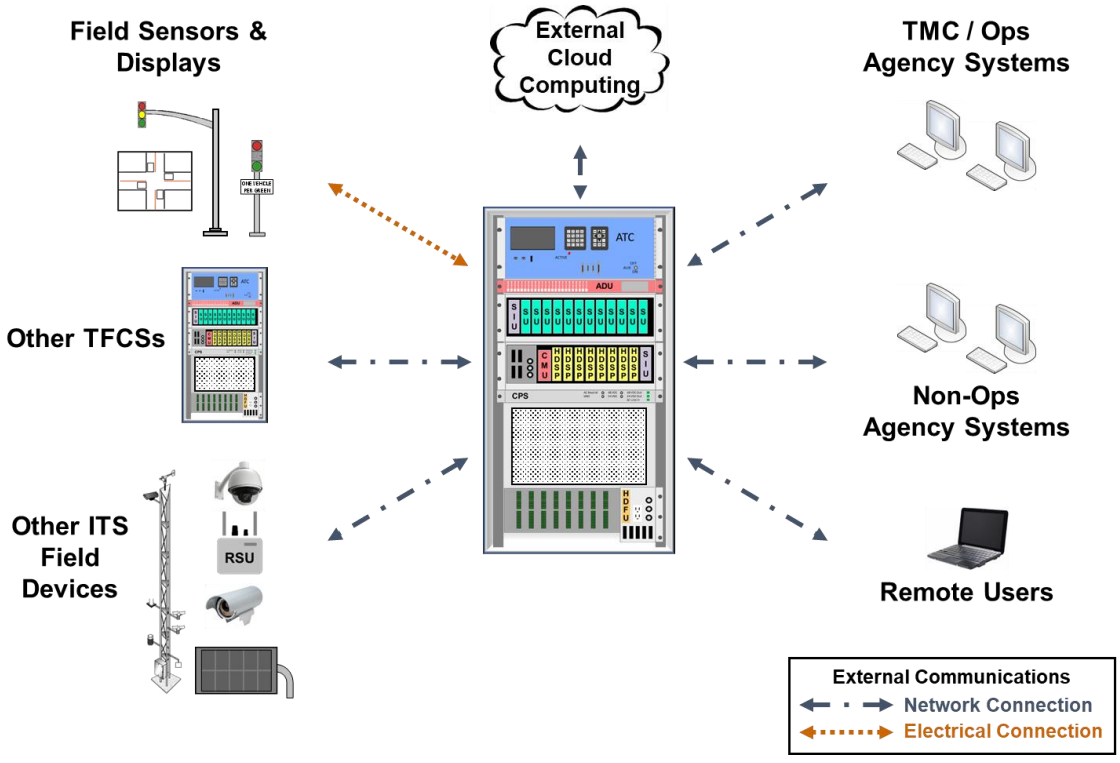


Figure 10. ATC Cabinet with external operational connections.

2.5 ATC Cybersecurity Scope [Informative]

Cybersecurity evaluations for an ATC Cabinet focus on all equipment and communications within cabinet, and all communications with devices and systems that are external to the cabinet. The external systems and devices themselves are not a subject of this SyRS but the communications with them are. This is

illustrated in Figure 11. Figure 12 provides an internal view of the ATC Cabinet with areas identified for discovery of ATC cybersecurity needs and requirements.

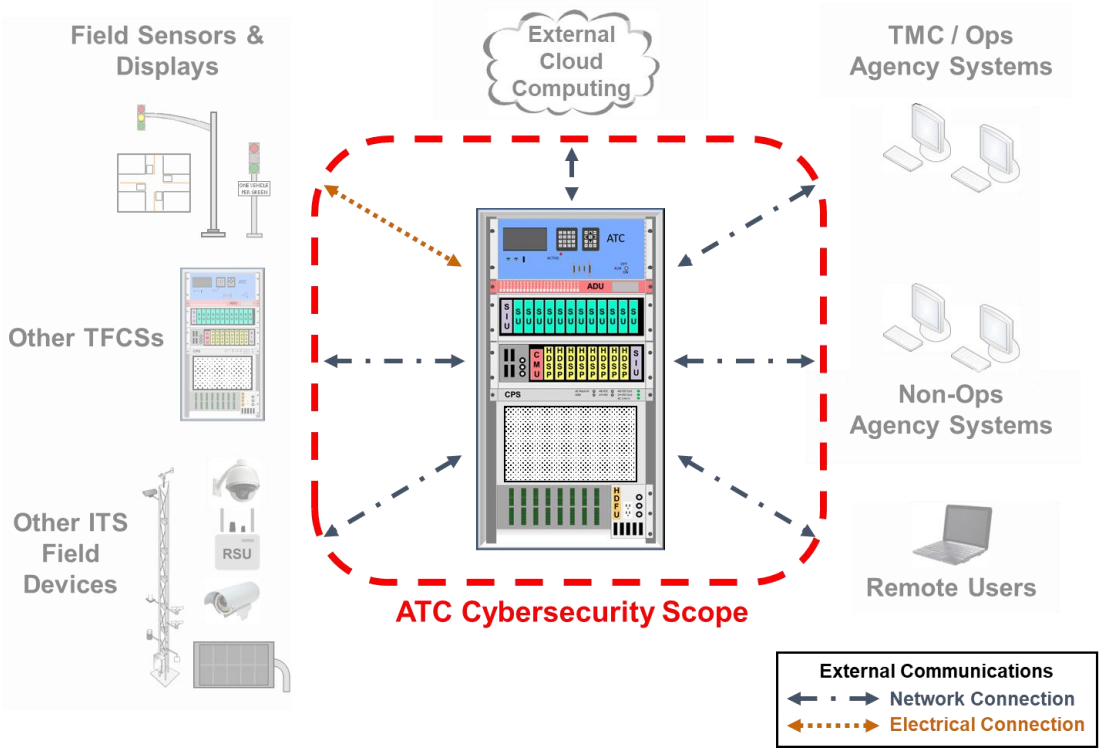


Figure 11. ATC Cybersecurity Scope includes needs and requirements for the ATC Cabinet system and external communications.

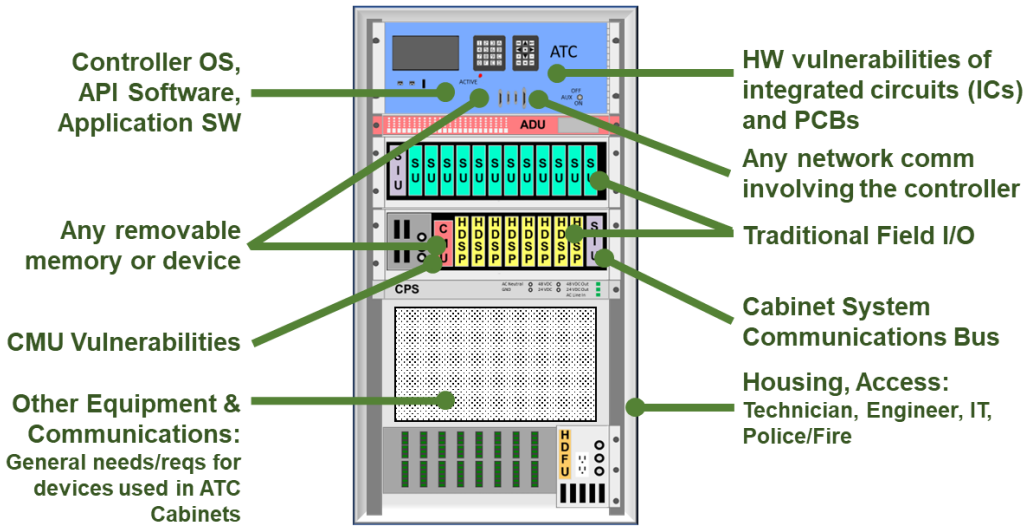


Figure 12. Areas for discovery of ATC cybersecurity needs and requirements.

2.6 Architectural Constraints [Informative]

This ATC Cybersecurity Standard applies to the ATC family of standards. Attempting to impose requirements on non-ATC TFCS designs is out of scope. Therefore, ATC units in cabinet systems that do not conform to ATC 5301 are not formally covered by this SyRS but may still benefit from most of its content.

2.7 ATC Cybersecurity Needs [Normative]

This section identifies the cybersecurity User Needs for the ATC Cabinet System. Each User Need represents a system-level capability or condition required to support secure operation of ATC devices, software, and communications. User Needs reflect expectations from agencies, operators, manufacturers, software developers, integrators, and other stakeholders.

Each User Need includes:

- a unique identifier and title,
- a statement of the need, and
- a rationale (typically 1–4 sentences) explaining the purpose of the need and providing additional context or clarifying information.

As a system, the User Needs are assigned to the ATC Cabinet. In Section 3, System Requirements reflect the subsystems, devices, communications, or software to which they apply.

Each User Need is followed by a Conformance Level, formatted in italic brackets (e.g., *[Level 1]* or *[Level D]*), indicating whether the need is included in this version of the standard or deferred to a future revision. Conformance Levels are defined in Section 1.6.1.

- User Needs assigned Conformance Level 1 lead to System Requirements in Section 3.
- User Needs assigned Conformance Level D (Deferred) do not generate System Requirements or design elements in this version of the standard.

User Needs marked *[Deprecated]* retain their identifier and title but are listed in the Deprecated Items Annex as described in Section 1.6.2.

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.
[Level 1]

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.
[Level 1]

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.
[Level 1]

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).
[Level 1]

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.
[Level 1]

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.
[Level 1]

2.7.2.5 Inventory Tool Interface

The ATC Cabinet needs a means to supply the identifying information of its devices electronically. Identifying information may include the current location of the device. This is to allow users to use automated tools for asset management.
[Level D]

Developer Note: This need was intended to interface using some specialized inventory tool support.

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.
[Level 1]

2.7.2.7 Asset Tracking

The ATC Cabinet needs to include asset tracking capabilities for selected components. Asset location technologies can help ensure that critical assets (especially ATC units and CMUs but could include other equipment) remain in expected physical locations.

[Level D]

2.7.3 Continuous Vulnerability Management

This section identifies needs that concern continuous vulnerability management.

2.7.3.1 Verify Software Is Authorized

The ATC Cabinet needs a mechanism to ensure only authorized software is executed on the system. Software may include driver software, OS, libraries, a board support package (BSP), file system, middleware, application software, and scripts. Identifiers may include the software name, version, publisher, install date, and other identification. This is to protect against the unauthorized loading of software.
[Level D]

2.7.3.2 Monitor for Unauthorized Changes

The ATC Cabinet needs to continually check for unauthorized changes to software components including additions and removals. This is to protect against unauthorized manipulation.
[Level D]

2.7.3.3 Intrusion Detection and Prevention Systems

The ATC Cabinet needs to detect in a timely manner when a cyber intrusion has been attempted or occurred. This is done to identify and prevent the unauthorized use of functions, protocols, ports, and services.
[Level D]

Developer Note: We may want to add a user need for Vulnerability Scanning here. However, there are multiple references to “scanning” in the document. We need to make sure we are consistent with our intentions when using the term and we are not saying the same thing in multiple places. Look at including this as a new need. “The ATC cabinet needs to be able to be scanned a set of its components for applicable vulnerabilities as they are discovered”, but it may be an IOO issue, not a vendor one.

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.
[Level 1]

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.
[Level 1]

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.
[Level 1]

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.
[Level 1]

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.
[Level 1]

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.
[Level 1]

2.7.4.7 Key Material Protection

The ATC Cabinet needs to protect sensitive cryptographic material (e.g., private keys for TLS certificates) of the system. Locally stored cryptographic material is stored in a secure fashion. This could be a security module. Secure storage of locally stored cryptographic material helps protect the system from unauthorized use.
[Level D]

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.
[Level 1]

2.7.4.9 Trustworthiness

The ATC Cabinet needs to ensure that it does not exchange data to/from devices that are no longer trustworthy. The system may halt communications with a device due to expired or revoked certificates, lack of responsiveness, excessive network traffic, and other tests. Communications with a device that is not trustworthy is not secure.
[Level D]

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.
[Level 1]

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.
[Level 1]

2.7.5.3 Support Security Audits

The ATC Cabinet needs to support the secure auditing of the cabinet system. For example, adding a user or changing the configuration. This provides historical and forensic support.
[Level D]

2.7.5.4 Security Monitoring

The ATC Cabinet needs to provide security monitoring of the system operation. This includes automated scanning, alerts, and notifications. This may be through a front panel display, or a message sent to another device.
[Level D]

2.7.5.5 Operating Software Reporting

The ATC Cabinet needs to report all currently running software when queried. This can confirm proper operations and can protect the system from unauthorized software.
[Level D]

2.7.5.6 Network Service Status

The ATC Cabinet needs to provide the current status of the network features. This allows agencies to understand the device's capabilities that are enabled and disabled. Network features may include the webservices provided, the protocols supported (e.g., HTTP, HTTPS, SSH2, FTP, SFTP), and the ports used.
[Level D]

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.
[Level 1]

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.
[Level 1]

2.7.6.2 Wireless Security

The ATC Cabinet needs to employ secure wireless protocols when using wireless communications. This is to secure data in transit. For example, WPA3. Wireless communications are to be secure by default. This reduces the vulnerabilities associated with wireless communications.
[Level D]

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.
[Level 1]

Developer Note: This must be reworked to incorporate the concept of secure by design.

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.
[Level 1]

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.
[Level 1]

2.7.6.6 Denial-of-Service Protection

The ATC Cabinet needs to protect against denial-of-service (DoS) attacks. This ensures the applications running within the cabinet system perform their required operations in the expected fashion. Mitigations may be boundary protection devices, increased network capacity and bandwidth, and automated rate limiting of communicating devices.
[Level 1]

2.7.6.7 Use of Cloud Services

The ATC Cabinet needs to maintain uninterrupted operation of safety critical applications (e.g., traffic signal control) if cloud services become unavailable. Non-critical features that rely on cloud services may not be available. This protects the ATC Cabinet system from failed or compromised cloud services.
[Level D]

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.
[Level 1]

2.7.7 Data At Rest Protection

This section identifies needs that concern data at rest protection.

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.
[Level 1]

2.7.7.2 Removable Storage Security

If removable storage is supported, the ATC Cabinet needs to protect sensitive data at rest on removable storage devices. Examples may be to require that the user has privileges to access devices and encrypt/decrypt files. Ports are to be disabled when not in use.
[Level D]

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.
[Level 1]

Note: SDLC communications is exempted for current generation ATC equipment.

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.
[Level 1]

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.
[Level 1]

2.7.9.2 Application Logging

The ATC Cabinet needs to provide a capability for applications to perform logging of security relevant data and events. This could be used by application programs to identify safety and security risks.
[Level D]

2.7.9.3 Application Reporting

The ATC Cabinet needs to provide a capability for applications to report faulty operation. This could be used by application programs to identify safety and security risks.
[Level D]

2.7.9.4 Application Portability

The ATC Cabinet needs to facilitate application portability. Application portability and the ability to reconstitute on different platforms increase the availability of mission-essential functions. For example, mission critical software on a compromised ATC unit from one manufacturer could be reconstituted on a non-compromised ATC unit from another manufacturer. Also, portability of application programs allows new security solutions to be used to secure the system.
[Level D]

2.7.9.5 Separation of System, Security, and User Functionality

The ATC Cabinet needs to separate user functionality, including user interface services, from system management functionality. The separation of user functions from system and security management functions may be physical or logical and may be separated by using different computers, instances of operating systems, central processing units, or network addresses and protocols. This prevents the misuse of privileged functions.
[Level D]

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.
[Level 1]

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.
[Level 1]

2.7.10 Resiliency

This section identifies needs that concern resiliency.

2.7.10.1 System Backup

The ATC Cabinet needs to provide a method for system backups. Backups may include system state information, operating system software, middleware, application software, licenses, user and system documentation, and configuration data. This is to facilitate recovery from an attack or failure.
[Level D]

2.7.10.2 System Safe Mode

The ATC Cabinet needs to provide a safe mode of operation. It may be activated automatically or manually. It restricts the operations that systems can execute when conditions such as an unauthorized intrusion, a failure, or other conditions are encountered. Examples could be disabling network capabilities, front panel display, keyboard, and others.
[Level D]

2.7.10.3 Secure System Restore

The ATC Cabinet needs to allow an authorized user or trusted installer to revert to a trusted configuration. This may be a recovery method from unauthorized software being installed or a trusted environment that has become corrupted.
[Level D]

2.7.10.4 Power Interruption Response

The ATC Cabinet needs to provide a method for continued operations when there are service power interruptions. This may provide for orderly shutdown of the system or a transition to an alternate power source. This protects system devices and may continue operation of the system.
[Level D]

2.8 Operational Policies and Constraints [Normative]

There are no operational policies or constraints identified.

2.9 Operational Scenarios [Informative]

There are no operational scenarios identified.

2.10 ARC-IT and Security [Informative]

The Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) is the reference architecture for intelligent transportation systems in the United States. It allows planners and engineers to conceive, design and implement systems using four “Views” (viewpoints) of a system that are all tied to the common reference architecture. It also provides “Services” which represent elements of the Physical View that address specific ITS services along with their functional objects and information flows. Security applies to all physical objects and information flows, impacts all enterprise objects, and affects the structure and content of communications profiles. See Figure 13.

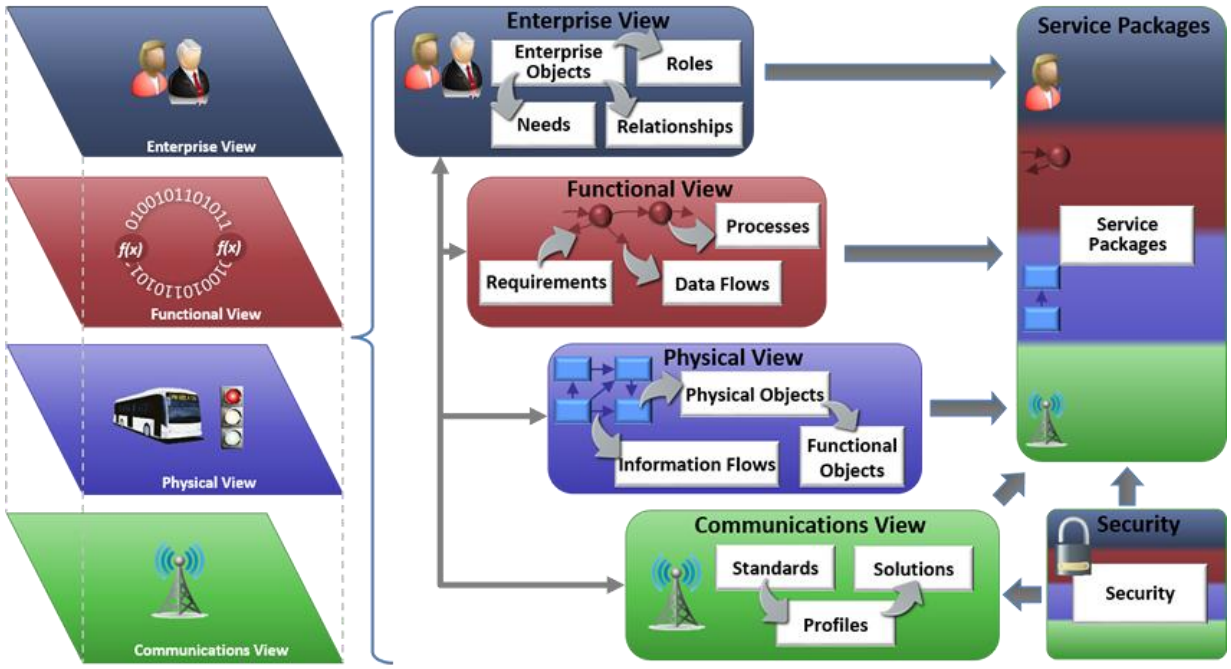
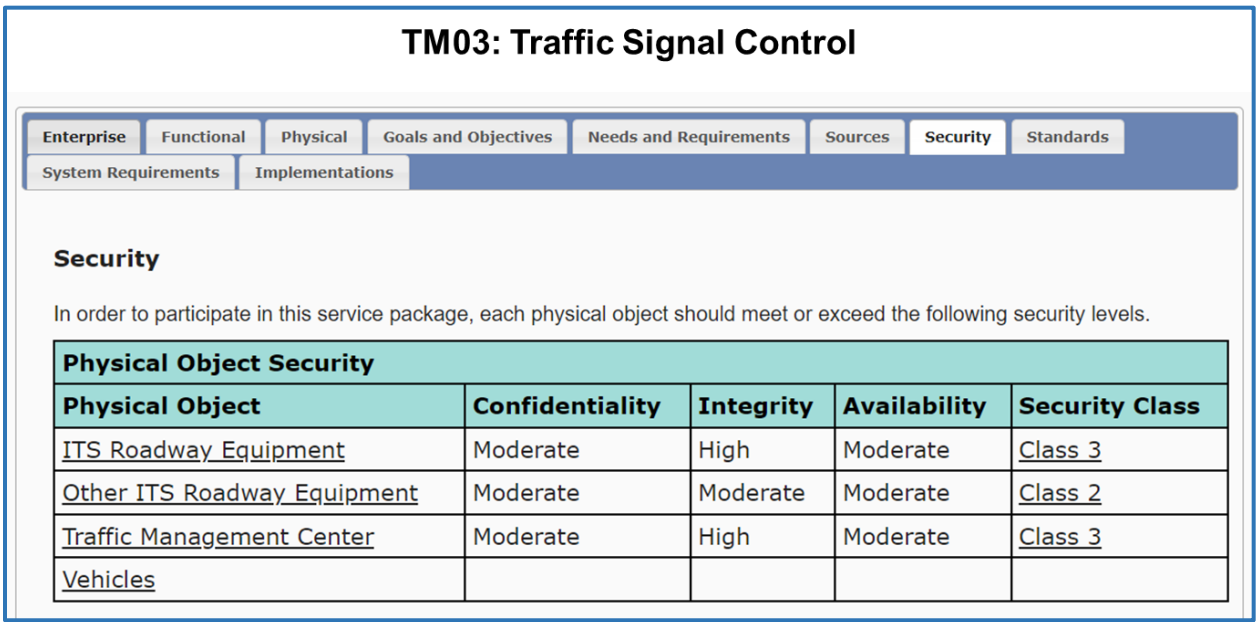


Figure 13. ARC-IT's interconnected components are organized into four views of the reference architecture.

ARC-IT defines five physical device security classes (also called "device classes" or "classes") based on the requirements for Confidentiality, Integrity, and Availability for the device. The classes are a collection of security controls from which security requirements can be developed. Class 5 devices have the highest level of security controls. Every physical object represented in ARC-IT is covered by a device class that matches or exceeds its security requirements. The control documentation for ARC-IT is largely sourced from NIST SP 800-53r3 Security and Privacy Controls for Information Systems and Organizations. The most common starting point when using ARC-IT is through the Services. Figure 14 is a portion of the screen from the Security tab of the Traffic Signal Control service. This shows that ITS Roadway Equipment is Class 3. Selecting Class 3 and then subsequently "Detailed Controls," will list the NIST controls that ARC-IT has identified for Class 3 devices. The ATC standards specify devices and software that fall under this class. A separate analysis of NIST SP 800-53r5 was also performed as part of the ConOps development (see Annex A).



TM03: Traffic Signal Control

Enterprise | Functional | Physical | Goals and Objectives | Needs and Requirements | Sources | Security | Standards | System Requirements | Implementations

Security

In order to participate in this service package, each physical object should meet or exceed the following security levels.

Physical Object Security				
Physical Object	**Confidentiality**	**Integrity**	**Availability**	**Security Class**
ITS Roadway Equipment	Moderate	High	Moderate	Class 3
Other ITS Roadway Equipment	Moderate	Moderate	Moderate	Class 2
Traffic Management Center	Moderate	High	Moderate	Class 3
Vehicles				

Figure 14. Physical object security for the ARC-IT Traffic Signal Control service. ATC standards are a part of ITS Roadway Equipment Security Class 3.

Section 3
System Requirements [Normative]

Developer Note: Sections 3.1 through Section 3.2.3 are to be reworked to simplify the NRTM for this standard.

Section 3 defines the System Requirements based on the user needs identified in the Concept of Operations.

Section 3 includes the following:

a) A tutorial.
b) Needs to Requirements Traceability Matrix (NRTM). This tool provides a mapping from the user needs to the requirements that fulfill the need. The NRTM provides symbols used to indicate if a requirement is may mandatory, conditional, or optional. Additional symbols are used to group requirements for particular functionality.
c) Requirements. These are requirements that collectively satisfy the user needs identified in Sections 2.7.

Section 3 is intended for all readers, including the following:

a) Transportation Managers
b) Transportation Operators
c) Transportation Engineers
d) System Integrators
e) Device Manufacturers
f) Application Developers.

3.1 Tutorial [Informative]

This system requirements section defines the formal requirements that are intended to satisfy the user needs identified in Section 2.7. This is achieved through the development of a NRTM that traces each user need to one or more requirements defined in this section. The details of each requirement are then presented following the NRTM.

3.2 Needs to Requirements Traceability Matrix

The NRTM, provided in Section 3.2.3, maps the user needs defined in Section 2 to the requirements defined in Section 3. The NRTM may be used by the following:

a) A user or specification writer to indicate which requirements are to be implemented in a project-specific implementation
b) The device manufacturer and user, as a detailed indication of the capabilities of the implementation
c) A user, as a basis for initially checking the potential interoperability with another implementation
d) A tester, as a checklist to compare against a specification and provide basis for test planning

3.2.1 Notation [Informative]

The following notations and symbols are used to indicate status and conditional status in the NRTM. Not all of these notations and symbols may be used within this standard.

3.2.1.1 Conformance Symbols

The symbols in Table 1 are used to indicate status under the Conformance column in the NRTM.

Table 1. Conformance Symbols

Symbol	Status
M	Mandatory
M.#	Support of every item of the group labeled by the same numeral # is required, but only one is active at a time
O	Optional
O.# (range)	Part of an option group. Support of the number of items indicated by the '(range)' is required from all options labeled with the same numeral #
C	Conditional
NA	Not-applicable (i.e., logically impossible in the scope of the standard)
X	Excluded or prohibited

The O.# (range) notation is used to show a set of selectable options (e.g., O.2 (1..*) would indicate that one or more of the option group 2 options shall be implemented). Two-character combinations are used for dynamic requirements. In this case, the first character refers to the static (implementation) status, and the second refers to the dynamic (use); thus, "MO" means "mandatory to be implemented, optional to be used."

3.2.1.2 Conditional Status Notation

The predicate notations in Table 2 may be used.

Table 2. Conditional Status Notation

Predicate	Notation
<predicate>:	This notation introduces a single item that is conditional on the <predicate>.
<predicate>::	This notation introduces a table or a group of tables, all of which are conditional on the <predicate>.
(predicate)	This notation introduces the first occurrence of the predicate. The feature associated with this notation is the base feature for all options that have this predicate in their conformance column.

The <predicate>: notation means that the status following it applies only when the NRTM states that the feature or features identified by the predicate are supported. In the simplest case, <predicate> is the identifying tag of a single NRTM item. The <predicate> notation may precede a table or group of tables in a section or subsection. When the group predicate is true then the associated section shall be completed. The symbol <predicate> also may be a Boolean expression composed of several indices. "AND," "OR," and "NOT" shall be used to indicate the Boolean logical operations.

The predicates used in this standard map to the sections indicated in Table 3.

Table 3. Predicate Mapping

Predicate	Section
Level1	Throughout the NRTM
LevelD	Throughout the NRTM

3.2.1.3 Support Column Symbols

The Support column in the NRTM can be used by a procurement specification to identify the required features for the given procurement or by an implementer to identify which features have been implemented. In either case, the user circles the appropriate answer (Yes, No, or N/A) in the support column:

Table 4. Support Column Entries

Entry	Identifier
Yes	Supported by the implementation
No	Not supported by the implementation
N/A	Not applicable

3.2.2 Instructions for Completing the NRTM [Informative]

In the 'Support' column, each response shall be selected either from the indicated set of responses (for example: Yes / No / NA), or it shall reference additional items that are to be attached (for example, list of traffic signal controllers to be supported by an implementation). If a conditional requirement is inapplicable, use the Not Applicable (NA) choice.

Note: A specification can allow for flexibility in a deliverable by leaving the selection in the Support column blank for a given row.

3.2.2.1 Conformance Definition

To claim "Conformance" to this standard, the manufacturer shall minimally fulfill the mandatory requirements as identified in the NRTM (see Section 3.2.3).

Note: The reader and user of this standard is advised that 'conformance' to ATC 5501 should not be confused with 'compliance' to a specification. An agency specification needs to identify the requirements of a particular project and needs to require the support of those requirements. This means that requirements defined as 'optional' in ATC 5501 might need to be selected in a specification (in effect made 'mandatory' for the project-specific specification).

A conformant device may offer additional (optional) features, as long as they are conformant with the requirements of ATC 5501 and the standards it references (e.g., *NIST SP 800-63B-4*). For example, to claim conformance to additional features, an implementation shall conform to all of the mandatory and selected optional requirements that trace to the subject user needs in the NRTM, AND shall fulfill the requirement by using all of the dialogs and data elements traced to the subject requirement in the Requirements Traceability Matrix (RTM).

Note: Off-the-shelf interoperability and interchangeability can only be obtained through well-documented features broadly supported by the industry as a whole. Designing a system that uses features not defined in a standard or not typically deployed in combination with one another inhibits the goals of interoperability and interchangeability, especially if the documentation of these features is not available for distribution to system integrators. Standards allow the use of additional features to support innovation, which is constantly needed within the industry; but users should be aware of the risks involved with using such features.

3.2.3 NRTM

In addition to the Conformance column and the Support column which were discussed in Sections 3.2.1.1 and 3.2.1.3, the additional columns in the NRTM table are the User Need ID and User Need columns, System Requirement ID and System Requirement columns, and the Additional Specifications column.

a) **User Need ID** - the number assigned to the user need statement. The user needs are defined within Section 2 and the NRTM is based upon the user needs within that Section.
b) **User Need** – a short descriptive title identifying the user need.
c) **Sys Req ID** – the number assigned to the functional requirement statement. The requirements are defined within Section 3 and the NRTM references the traces from user needs to these requirements.
d) **System Requirement** – a short descriptive title identifying the functional requirement.
e) **Additional Specifications** - identifies other requirements to fulfill, including user selectable range values. The "Additional Specifications" column may (and should) be used by a procurement specification to provide additional notes and requirements for the product to be procured or may be used by an implementer to provide any additional details about the implementation. In some cases, default text already exists in this field, which the user should complete to fully specify the equipment. However, additional text can be added to this field as needed to fully specify a feature.

Table 5. Needs to Requirements Traceability Matrix (NRTM)

User Need ID	User Need	Sys Req ID	System Requirement	Conformance	Support	Additional Specifications
2.7	ATC Cybersecurity Needs [Normative]					
2.7.1	Physical Security					
2.7.1.1	Control Physical Access			Level1:M		
		3.3.1.1.1	No #2 Key	Level1:M		
		3.3.1.1.2	Differentiated Physical Cabinet Key	Level1:M		
		3.3.1.1.3	Programmable Cabinet Key	Level1:O		
		3.3.1.1.4	Detect Open Doors	Level1:M		
		3.3.1.1.5	Log Access Attempts	Level1:M		
		3.3.1.1.6	Access Attempt Alerts	Level1:M		
2.7.1.2	No Cabinet Monitor Bypass			Level1:M		
		3.3.1.2.1	No Functional CMU Present	Level1:M		
		3.3.1.2.2	No Flasher Present Operation	Level1:M		
		3.3.1.2.3	No Flasher Present Alert	Level1:M		
2.7.2	Inventory and Control of Assets					
2.7.2.1	Facilitate Physical Inventory			Level1:M		
		3.3.2.1.1	Inventory Identifiers for ATC Cabinet Standard Devices	Level1:M		
		3.3.2.1.2	Inventory Identifiers for IP-Addressable Non-Standard Devices	Level1:M		
		3.3.2.1.3	Inventory Identifiers for Attached Non-IP-Addressable Non-Standard Devices	Level1:M		
		3.3.2.1.4	Display Cabinet Inventory on Controller Front Panel	Level1:M		
		3.3.2.1.5	Send Cabinet Inventory Remotely	Level1:M		
2.7.2.2	List of Programmable Components			Level1:M		
		3.3.2.2.1	List of Programmable Components of Cabinet Devices	Level1:M		
2.7.2.3	List of Software Components			Level1:M		
		3.3.2.3.1	SBOM Provided	Level1:M		
2.7.2.4	Facilitate Software Inventory			Level1:M		
		3.3.2.4.1	Store SBOMs	Level1:M		
		3.3.2.4.2	Send Cabinet Inventory Remotely	Level1:M		
2.7.2.5	Inventory Tool Interface			LevelD		
2.7.2.6	Notice of Unsupported Software			Level1:M		
		3.3.2.6.1	No Unsupported Software	Level1:M		
		3.3.2.6.2	Unsupported Software Notification	Level1:M		

User Need ID	User Need	Sys Req ID	System Requirement	Conformance	Support	Additional Specifications
		3.3.2.6.3	Non-Production Software Notification	Level1:M		
2.7.2.7	Asset Tracking			LevelD		
2.7.3	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					
2.7.4.1	Authenticated and Authorized Users			Level1:M		
		3.3.4.1	User Types	Level1:M		
		3.3.4.2	Authentication Levels	Level1:M		
		3.3.4.3.1	Minimum Administrator Authentication Level	Level1:M		
		3.3.4.3.2	No Authentication for System Accounts	Level1:M		
		3.3.4.3.3	Minimum User Authentication Level	Level1:M		
		3.3.4.4.1	Assigning User Group Privileges	Level1:M		
		3.3.4.4.2	Removing User Group Privileges	Level1:M		
		3.3.4.5.1	Minimum User Group Membership	Level1:M		
		3.3.4.5.2	Adding User Group Membership	Level1:M		
		3.3.4.5.3	Removing User Group Membership	Level1:M		
		3.3.4.5.10	User Credential Expiration	Level1:M		
		3.3.4.7.1	Access Modes	Level1:M		
		3.3.4.7.2	No Access for System Accounts	Level1:M		
		3.3.4.8.1	Local Authorization of Users	Level1:M		
		3.3.4.8.2	Central Authorization of Users	Level1:M		
		3.3.4.6.1.4	Configure User Credential Expiration	Level1:M		
		3.3.4.6.2.4	Enforce User Credential Expiration	Level1:M		
		3.3.4.9.1	User Credential Protection	Level1:M		
		3.3.4.9.2	User Privilege Protection	Level1:M		
2.7.4.2	User Account Management			Level1:M		
		3.3.4.4.3	User Group Addition	Level1:M		
		3.3.4.4.4	User Group Deletion	Level1:M		
		3.3.4.4.5	User Group Modification	Level1:M		
		3.3.4.4.6	User Group Cloning	Level1:M		
		3.3.4.5.1	Minimum User Group Membership	Level1:M		
		3.3.4.5.2	Adding User Group Membership	Level1:M		
		3.3.4.5.3	Removing User Group Membership	Level1:M		
		3.3.4.5.4	User Addition	Level1:M		

User Need ID	User Need	Sys Req ID	System Requirement	Conformance	Support	Additional Specifications
		3.3.4.5.5	**Error! Reference source not found.**	Level1:M		
		3.3.4.5.6	User Lock Out	Level1:M		
		3.3.4.5.7	User Unlock	Level1:M		
		3.3.4.5.8	User Modification	Level1:M		
		3.3.4.5.9	User Cloning	Level1:M		
		3.3.4.5.10	User Credential Expiration	Level1:M		
2.7.4.3	Default User Accounts			Level1:M		
		3.3.6.3.3.2	Manufacturer Identified Provisioning Services	Level1:M		
		3.3.6.3.3.5	User Accounts Deleted in Unprovisioned State	Level1:M		
		3.3.6.3.4.4	Delete or Disable Provisioning User Accounts	Level1:M		
2.7.4.4	Authenticated and Authorized Programs, Processes, and Services			Level1:M		
		3.3.4.1	User Types	Level1:M		
		3.3.4.2	Authentication Levels	Level1:M		
		3.3.4.3.2	No Authentication for System Accounts	Level1:M		
		3.3.4.3.3	Minimum User Authentication Level	Level1:M		
		3.3.4.4.1	Assigning User Group Privileges	Level1:M		
		3.3.4.4.2	Removing User Group Privileges	Level1:M		
		3.3.4.5.1	Minimum User Group Membership	Level1:M		
		3.3.4.5.2	Adding User Group Membership	Level1:M		
		3.3.4.5.3	Removing User Group Membership	Level1:M		
		3.3.4.5.10	User Credential Expiration	Level1:M		
		3.3.4.7.1	Access Modes	Level1:M		
		3.3.4.7.2	No Access for System Accounts	Level1:M		
		3.3.4.8.1	Local Authorization of Users	Level1:M		
		3.3.4.8.2	Central Authorization of Users	LevelD		
		3.3.4.6.1.4	Configure User Credential Expiration	Level1:M		
		3.3.4.6.2.4	Enforce User Credential Expiration	Level1:M		
		3.3.4.9.1	User Credential Protection	Level1:M		
		3.3.4.9.2	User Privilege Protection	Level1:M		
2.7.4.5	Local-Based Access Control			Level1:M		
		3.3.4.4.1	Assigning User Group Privileges	Level1:M		
		3.3.4.4.2	Removing User Group Privileges	Level1:M		
		3.3.4.5.1	Minimum User Group Membership	Level1:M		
		3.3.4.5.2	Adding User Group Membership	Level1:M		
		3.3.4.5.3	Removing User Group Membership	Level1:M		
		3.3.4.6.1.1	Configure Automatic Inactive User Logout	Level1:M		

User Need ID	User Need	Sys Req ID	System Requirement	Conformance	Support	Additional Specifications
		3.3.4.6.1.2	Configure Failed Authentication Delay	Level1:M		
		3.3.4.6.1.3	Configure Failed Authentication Lockout	Level1:M		
		3.3.4.6.2.1	Enforce Automatic Inactive User Logout	Level1:M		
		3.3.4.6.2.2	Enforce Failed Authentication Delay	Level1:M		
		3.3.4.6.2.3	Enforce Failed Authentication Lockout	Level1:M		
		3.3.4.6.2.5	Reset Failed Authentication Attempts on Successful Authentication	Level1:M		
		3.3.4.6.2.6	Reset Failed Authentication Attempts on User Unlock	Level1:M		
		3.3.4.9.2	User Privilege Protection	Level1:M		
2.7.4.6	Authentication Protection			Level1:M		
		3.3.4.5.10	User Credential Expiration	Level1:M		
		3.3.4.6.1.4	Configure User Credential Expiration	Level1:M		
		3.3.4.6.2.4	Enforce User Credential Expiration	Level1:M		
		3.3.4.9.1	User Credential Protection	Level1:M		
		3.3.4.9.2	User Privilege Protection	Level1:M		
2.7.4.7	Key Material Protection			LevelD		
2.7.4.8	Secure Authenticated Sessions			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					
2.7.5.1	Consistent and Accurate Time			Level1:M		
		3.3.5.1.1	GNSS Time Source	Level1:M		
		3.3.5.1.2	NTP	Level1:M		
		3.3.5.1.3	Time Synchronization Log	Level1:M		
		3.3.5.1.4	Time Discrepancy Check	Level1:M		
		3.3.5.1.5	Time Discrepancy Alert	Level1:M		
2.7.5.2	Security Event Logging			Level1:M		
		3.3.5.2.1	Security Event Log Record	Level1:M		
		3.3.5.2.2	Security Event Logs	Level1:M		
		3.3.5.2.3.1	Enabling Security Event Types	Level1:M		
		3.3.5.2.3.2	Disabling Security Event Types	Level1:M		
		3.3.5.2.3.3	Setting Security Event Severity	Level1:M		
		3.3.5.2.4	Minimum Security Log Capacity	Level1:M		
		3.3.5.2.5	Security Log Rollover	Level1:M		
		3.3.5.2.6	Security Log Retention Policy	Level1:O		
		3.3.5.2.7	Security Log Access Control	Level1:M		

User Need ID	User Need	Sys Req ID	System Requirement	Conformance	Support	Additional Specifications
		3.3.5.2.8.1	Security Log Modification Protection	Level1:M		
		3.3.5.2.8.2	Security Log Deletion Protection	Level1:M		
		3.3.5.2.9.1	Security Log Physical Local Access	Level1:M		
		3.3.5.2.9.2	Security Log Local Retrieval	Level1:M		
		3.3.5.2.9.3	Security Log Remote Retrieval	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			Level1:M		
		3.3.5.7	Security Alerts	Level1:M		
2.7.6	Networks, Protocols, and Services					
2.7.6.1	Secure Remote Access			Level1:M		
		3.3.6.1.1	Restricted Root Login	Level1:M		
2.7.6.2	Wireless Security			LevelD		
2.7.6.3	No Open Network Services			Level1:M		
		3.3.6.3.1.1	Services Disabled by Default	Level1:M		
		3.3.6.3.1.2	Networking Disabled by Default	Level1:M		
		3.3.6.3.2.1	Enable Services	Level1:M		
		3.3.6.3.2.2	Disable Services	Level1:M		
		3.3.6.3.2.3	Configure Network Settings	Level1:M		
		3.3.6.3.3.1	Resettable to Unprovisioned State	Level1:M		
		3.3.6.3.3.2	Manufacturer Identified Provisioning Services	Level1:M		
		3.3.6.3.3.3	Service Restrictions in Unprovisioned State	Level1:M		
		3.3.6.3.3.4	Networking Restrictions in Unprovisioned State	Level1:M		
		3.3.6.3.3.5	User Accounts Deleted in Unprovisioned State	Level1:M		
		3.3.6.3.4.1	Device Administrator Creation Required	Level1:M		
		3.3.6.3.4.2	Device Administrator Authentication Required	Level1:M		
		3.3.6.3.4.3	Operation Restriction in Unprovisioned State	Level1:M		
		3.3.6.3.4.4	Delete or Disable Provisioning User Accounts	Level1:M		
2.7.6.4	Manufacturer-Stated Network Services			Level1:M		
		3.3.6.4.1	Documented Network Features	Level1:M		
2.7.6.5	Boundary Protection			Level1:M		
		3.3.6.5.1	Firewall	Level1:M		
		3.3.6.5.2	No Unmanaged Network Devices	Level1:M		
2.7.6.6	Denial-of-Service Protection			LevelD		

User Need ID	User Need	Sys Req ID	System Requirement	Conformance	Support	Additional Specifications
2.7.6.7	Use of Cloud Services			LevelD		
2.7.6.8	External Media Startup Software			Level1:M		
		3.3.6.8.1	No Auto-Execution from External Media	Level1:M		
2.7.7	Data At Rest Protection					
2.7.7.1	Secure Data At Rest			Level1:M		
		3.3.7.1.1	Data at Rest Modification Protection	Level1:M		
		3.3.7.1.2	Data at Rest Deletion Protection	Level1:M		
2.7.7.2	Removable Storage Security			LevelD		
2.7.8	Data in Transit Protection					
2.7.8.1	Secure Data in Transit			Level1:M		
		3.3.8.1.1	Protected Network Communications	Level1:M		
2.7.8.2	Verifiable Credentials			Level1:M		
		3.3.8.2.1	Verify Endpoint Credentials	Level1:M		
2.7.9	Operating Platform and Applications					
2.7.9.1	Application and Process Isolation			Level1:M		
		3.3.9.1.1	Resource Allocation			
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			Level1:M		
		3.3.9.6.1	Software Update Capability	Level1:M		
		3.3.9.6.2	Manual Software Updates	Level1:M		
		3.3.9.6.3	Automated Software Updates	Level1:M		
		3.3.9.6.4.1	Digital Certificate Additions	Level1:M		
		3.3.9.6.4.2	Digital Certificate Removals	Level1:M		
		3.3.9.6.4.3	Update Package Integrity	Level1:M		
		3.3.9.6.4.4	Update Package Integrity Verification	Level1:M		
		3.3.9.6.5	Removal of Previous Versions	Level1:M		
2.7.9.7	Stable Linux Kernel and Board Support Package			Level1:M		
		3.3.9.7.1	Board Support Package Security Updates	Level1:M		
2.7.10	Resiliency					
2.7.10.1	System Backup			LevelD		
2.7.10.2	System Safe Mode			LevelD		
2.7.10.3	Secure System Restore			LevelD		

User Need ID	User Need	Sys Req ID	System Requirement	Conformance	Support	Additional Specifications
2.7.10.4	Power Interruption Response			LevelD		

3.3 Requirements

This section specifies the System Requirements derived from the cybersecurity User Needs defined in Section 2.7. Each Requirement represents a verifiable capability, behavior, or condition necessary to support secure operation of the ATC Cabinet System and the devices, software, and communications that operate within or interface with it.

Each Requirement includes:

- a unique identifier and title and
- a statement of the requirement.

Requirements trace to one or more User Needs, and a single User Need may generate multiple Requirements. A traceability table at the beginning of this section maps each Requirement to its originating User Needs.

Requirements are assigned Conformance Levels, formatted in italic brackets (e.g., *[Level 1]*), consistent with the levels defined in Section 1.6.1. Requirements assigned Conformance Level 1 contribute to Level 1 conformance claims. Requirements assigned to a higher Conformance Level in future revisions will contribute to conformance at that level once defined.

Requirements marked [Deprecated] retain their identifier and title in this section but do not include requirement text. Their full historical content is provided in the Deprecated Items Annex, as described in Section 1.6.2.

Requirements are written so that each one:

- is verifiable through inspection, analysis, demonstration, or test
- supports at least one active User Need, and
- applies only to the subsystems, devices, interfaces, or software components for which it is relevant.

Requirements that are not applicable to a particular device or subsystem do not impose obligations on that component.

3.3.1 Physical Security Requirements

The requirements for the ATC Cabinet physical security are as follows.

3.3.1.1 Control Physical Access Requirements

The requirements for controlling physical access to the ATC Cabinet are as follows.

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.
[Level 1]

Guidance: This should be implemented using a physical key distribution plan that is a secure as feasible for the agency. E.g., Distribution based on the agency, contractor, geographic area, group of cabinets, or individual cabinet basis.

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.

[Level 1]

Guidance: This should be implemented using a physical key distribution plan that is a secure as feasible for the agency. E.g., Distribution based on the agency, contractor, geographic area, group of cabinets, or individual cabinet basis.

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.
[Level 1]

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.
[Level 1]

3.3.1.1.5 Log Access Attempts

The ATC Cabinet shall generate a log for all access attempts.
[Level 1]

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.
[Level 1]

3.3.1.2 No Cabinet Monitor Bypass Requirements

The requirements for prohibiting the bypass of the CMU functionality are as follow.
[Level 1]

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.
[Level 1]

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.
[Level 1]

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?

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.
[Level 1]

3.3.2 Inventory and Control of Assets Requirements

The requirements for the inventory and control of assets are as follows.

3.3.2.1 Facilitate Physical Inventory Requirements

The requirements for facilitating the ATC Cabinet physical inventory are as follows.

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.

[Level 1]

Note: Detector information is not required for Level 1. Hardware changes are necessary.

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).

[Level 1]

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.
[Level 1]

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.
[Level 1]

Guidance: This does not include non-standard IP-addressable devices and non-IP-addressable devices attached to them.

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.
[Level 1]

3.3.2.2 List of Programmable Components Requirements

The requirements for a programmable components list are as follows.

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.
[Level 1]

3.3.2.3 Software Bill of Materials Requirements

The requirements for a software bill of materials (SBOM) are as follows.
[Level 1]

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.
[Level 1]

Note: This allows an end user to check for current patches and to manage vulnerabilities.

3.3.2.4 Facilitate Software Inventory Requirements

The requirements for facilitating software inventory are as follows.

3.3.2.4.1 Store SBOMs

When software is installed, the Controller shall store the associated SBOMs in protected memory.
[Level 1]

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.
[Level 1]

3.3.2.5 Inventory Tool Interface Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.2.6 Notice of Unsupported Software Requirements

The requirements for unsupported software are as follows.

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.
[Level 1]

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.

[Level 1]

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).
[Level 1]

3.3.2.7 Asset Tracking Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.3 Continuous Vulnerability Management Requirements

The requirements for continuous vulnerability management are as follows.

3.3.3.1 Verify Software is Authorized Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.3.2 Monitor for Unauthorized Changes Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.3.3 Intrusion Detection and Prevention Systems Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.4 Authentication, Authorization, and User Accounts

The requirements for authentication, authorization, and user accounts follow.

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 **Error! R eference source not found.**.

  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.

3.3.4.2 Authentication Levels

The controller shall apply AAL levels as described by NIST SP 800-63B-4.

3.3.4.3 Minimum Authentication Levels

The requirements for minimum authentication levels follow.

3.3.4.3.1 Minimum Administrator Authentication Level

The controller shall require that the minimum authentication for the Administrator to be AAL2.
[Level 1]

3.3.4.3.2 No Authentication for System Accounts

The controller shall prohibit authentication for system accounts.
[Level 1]

3.3.4.3.3 Minimum User Authentication Level

The controller shall require that the minimum authentication for a user to be AAL1.
[Level 1]

3.3.4.4 User Group Management

The requirements for User Group Management follow.
[Level 1]

3.3.4.4.1 Assigning User Group Privileges

Only an Administrator shall be able to assign any privilege to a User Group.
[Level 1]

3.3.4.4.2 Removing User Group Privileges

Only an Administrator shall be able to remove any privilege from a User Group.
[Level 1]

3.3.4.4.3 User Group Addition

Only an Administrator shall be able to add a User Group.

3.3.4.4.4 User Group Deletion

Only an Administrator shall be able to delete a User Group.
[Level 1]

3.3.4.4.5 User Group Modification

Only an Administrator shall be able to modify a User Group.
[Level 1]

Note: Modification refers to a change in any property or attribute of a user group that does not involve assignment or removal of privileges.

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.
[Level 1]

3.3.4.5 User Management

The requirements for User Management follow.

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.
[Level 1]

3.3.4.5.2 Adding User Group Membership

Only an Administrator shall be able to add a user to any user group.
[Level 1]

3.3.4.5.3 Removing User Group Membership

Only an Administrator shall be able to remove a user from a user group.
[Level 1]

3.3.4.5.4 User Addition

Only an Administrator shall be able to add a User.
[Level 1]

3.3.4.5.5 User Deletion

Only an Administrator shall be able to delete a User.
[Level 1]

Note: This also deletes the User from all associated user groups.

3.3.4.5.6 User Lock Out

Only an Administrator shall be able to lock a User.

[Level 1]

Note: Locking a user account is where authentication and authorization is prohibited and all active sessions are terminated.

3.3.4.5.7 User Unlock

Only an Administrator shall be able to unlock a User.
[Level 1]

3.3.4.5.8 User Modification

Only an Administrator shall be able to modify a User.
[Level 1]

Note: Modification refers to a change in any property or attribute of a user account that does not involve assignment or removal of privileges.

3.3.4.5.9 User Cloning

Only an Administrator shall be able to create a new user by cloning an existing user.
[Level 1]

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.

3.3.4.5.10 User Credential Expiration

Only an Administrator shall be able to immediately expire user credentials.
[Level 1]

Note: This is to allow the administrator to force a user to change their credentials.

3.3.4.6 User Access Management

The requirements for User Access Management follow.

3.3.4.6.1 User Access Configuration

The requirements for User Access Configuration follow.
[Level 1]

3.3.4.6.1.1 Configure Automatic Inactive User Logout

Only an Administrator shall be able to configure an inactivity logout timer.
[Level 1]

Note: This is the period after which an inactive user session is terminated. See NIST SP 800-63B-4.

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.
[Level 1]

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.
[Level 1]

3.3.4.6.1.4 Configure User Credential Expiration

Only an Administrator shall be able to configure the expiry of user credentials.
[Level 1]

3.3.4.6.2 User Access Enforcement

The requirements for User Access Enforcement follow.

3.3.4.6.2.1 Enforce Automatic Inactive User Logout

The Controller shall log out an inactive user per configuration.
[Level 1]

3.3.4.6.2.2 Enforce Failed Authentication Delay

The Controller shall impose a delay after each successive failed authentication attempt per configuration.
[Level 1]

3.3.4.6.2.3 Enforce Failed Authentication Lockout

The Controller shall lock out users after repeated failed authentication attempts per configuration.
[Level 1]

3.3.4.6.2.4 Enforce User Credential Expiration

The Controller shall expire user credentials per configuration.
[Level 1]

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.
[Level 1]

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.
[Level 1]

3.3.4.7 Access

The requirements for access follow.

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).

[Level 1]

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.

3.3.4.7.2 No Access for System Accounts

The controller shall prohibit system accounts from all access modes.
[Level 1]

3.3.4.8 Authorization Entity

The authorization entity requirements follow.
[Level 1]

3.3.4.8.1 Local Authorization of Users

The controller shall authorize users without requiring the use of a central system.
[Level 1]

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.
[Level D]

3.3.4.9 Authentication Protection Requirements

The Authentication Protection Requirements follow.

3.3.4.9.1 User Credential Protection

The Controller shall protect all user credentials from tampering.
[Level 1]

Note: Standard Linux OS already does this by default.

3.3.4.9.2 User Privilege Protection

The Controller shall protect user privilege configuration from tampering.
[Level 1]

3.3.4.10 Key Material Protection Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.4.11 Secure Authenticated Sessions Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.4.12 Trustworthiness Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.5 Logging, Monitoring, and Reporting Requirements

The requirements for logging, monitoring, and reporting are as follows.

3.3.5.1 Consistent and Accurate Time Requirements

The requirements for consistent and accurate time are as follows.
[Level 1]

3.3.5.1.1 GNSS Time Source

The controller shall synchronize its system time with an authenticated and authorized GNSS time source.
[Level 1]

3.3.5.1.2 NTP

The controller shall synchronize its system time using NTPv4 or later.
[Level 1]

Note: The ATC unit updates its RTC when the system time is updated.

3.3.5.1.3 Time Synchronization Log

The controller shall log each instance of synchronization with the GNSS time source.
[Level 1]

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.
[Level 1]

3.3.5.1.5 Time Discrepancy Alert

The controller shall issue an alert if it fails the time discrepancy check.
[Level 1]

3.3.5.2 Security Event Logging Requirements

The requirements for security event logging are as follows.

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.

[Level 1]

Development Note: Further event details to be developed in the design stage of the project. Different event types will require additional information.

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

- 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.

[Level 1]

Developer Note: Further event details to be developed in the design stage of the project.

3.3.5.2.3 Security Event Log Configuration

The security event configuration requirements follow.

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.
[Level 1]

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.
[Level 1]

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.
[Level 1]

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.

3.3.5.2.4 Minimum Security Log Capacity

The controller shall have a minimum capacity of 8000 security events.
[Level 1]

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.

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).
[Level 1]

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.

3.3.5.2.7 Security Log Access Control

The controller shall restrict access to the security log to privileged accounts.
[Level 1]

3.3.5.2.8 Security Log Integrity

The security log integrity requirements follow.

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.

3.3.5.2.8.2 Security Log Deletion Protection

Only an Administrator shall be able to delete the security log.

3.3.5.2.9 Security Log Accessibility

The security log accessibility requirements follow.

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.

3.3.5.2.9.2 Security Log Local Retrieval

Only an Administrator shall be able to copy the security log to removable storage.

3.3.5.2.9.3 Security Log Remote Retrieval

Only an Administrator shall be able to copy the security log over a network.

3.3.5.3 Support Security Audits Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.5.4 Security Monitoring Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.5.5 Operating Software Reporting Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.5.6 Network Service Status Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

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.
[Level 1]

Add a new definition for incident response personnel. Discuss.

3.3.6 Networks, Protocols, and Services Requirements

The requirements for networks, protocols, and services are as follows.

3.3.6.1 Secure Remote Access Requirements

The requirements for secure remote access are as follows.

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.

[Level 1]

3.3.6.2 Wireless Security Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.6.3 Secure by Design

The requirements for secure by design follow.

Note: Services refers to all processes, applications, and features that exist to perform a function or operation.

3.3.6.3.1 Disabled by Default

The disabled by default requirements follow.

3.3.6.3.1.1 Services Disabled by Default

The controller shall have all services disabled by default.
[Level 1]

Note: Provisioning exception see Section **Error! Reference source not found.**.

3.3.6.3.1.2 Networking Disabled by Default

The controller shall have all network settings disabled by default.
[Level 1]

Note: Provisioning exception see Section **Error! Reference source not found.**.

3.3.6.3.2 Configuring Networking and Services

The requirements for networking and services follow.

3.3.6.3.2.1 Enable Services

Only an administrator shall be able to enable a service
[Level 1]

3.3.6.3.2.2 Disable Services

Only an administrator shall be able to disable a service
[Level 1]

3.3.6.3.2.3 Configure Network Settings

Only an administrator shall be able to configure network settings
[Level 1]

3.3.6.3.3 Unprovisioned State

The unprovisioned state requirements follow.

3.3.6.3.3.1 Resettable to Unprovisioned State

The controller shall be resettable to an unprovisioned state only through local physical access.
[Level 1]

Note: Privileges could be required to reset a controller to unprovisioned state.

3.3.6.3.3.2 Manufacturer Identified Provisioning Services

The manufacturer shall identify the minimum services and accounts required to provision the controller.
[Level 1]

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.
[Level 1]

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.
[Level 1]

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.
[Level 1]

3.3.6.3.4 Provisioning Process

The provision process requirements follow.

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.
[Level 1]

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.
[Level 1]

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.
[Level 1]

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.

[Level 1]

3.3.6.4 Manufacturer-Stated Network Services Requirements

The requirements for no open network services are as follows.

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.

[Level 1]

3.3.6.5 Boundary Protection Requirements

The requirements for boundary protection are as follows.

3.3.6.5.1 Firewall

Only an Administrator shall be able to configure the firewall.
[Level 1]

Note: This does not restrict an external firewall from being used.

3.3.6.5.2 No Unmanaged Network Devices

The ATC Cabinet shall not use unmanaged network devices.
[Level 1]

Note: E.g., Unmanaged switches, hubs, unmanaged cell modems.

Guidance: Currently deployed equipment that has unmanaged switches cannot be used to extend the network.

3.3.6.6 Denial-of-Service Protection Requirements

The requirements for denial-of-service protection are as follows.

3.3.6.6.1 Segregated Management Interfaces

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.6.7 Use of Cloud Services Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.6.8 External Media Startup Requirements

The requirements for external media startup software are as follows.

3.3.6.8.1 No Auto-Execution from External Media

The controller shall not auto-execute software from an external device.
[Level 1]

Note: This prohibits ATC 5201 Section B.4.1.1.

3.3.7 Data at Rest Protection Requirements

The requirements for data at rest protection are as follows.

Integrity requirement.

3.3.7.1 Secure Data at Rest Requirements

The Data at Rest Integrity requirements follow.

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.

3.3.7.1.2 Data at Rest Deletion Protection

Only an Administrator shall be able to delete data at rest.

3.3.7.2 Removable Storage Security Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.8 Data in Transit Protection Requirements

The requirements for data in transit protection are as follows.

3.3.8.1 Secure Data in Transit Requirements

The requirements for external media startup software are as follows.

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.
[Level 1]

3.3.8.2 Verifiable Credentials Requirements

The verify credentials requirements follow.

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.
[Level 1]

3.3.9 Operating Platform and Applications Requirements

The requirements for the operating platform and applications are as follows.

3.3.9.1 Application and Process Isolation Requirements

The requirements for application and process isolation are as follows.

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.

[Level 1]

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.

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.

3.3.9.2 Application Logging Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.9.3 Application Reporting Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.9.4 Application Portability Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.9.5 Separation of System, Security, and User Functionality Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.9.6 Facilitate System Software Updates Requirements

The requirements for facilitating system software updates are as follows.

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.

3.3.9.6.2 Manual Software Updates

Only an Administrator shall be able to perform a software update.
[Level 1]

3.3.9.6.3 Automated Software Updates

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.9.6.4 Software Update Integrity

The requirements for software update integrity follow.

Note: Public key storage is to facilitate software package integrity.

3.3.9.6.4.1 Digital Certificate Additions

Only an Administrator shall be able to add digital certificates that verify software updates.
[Level 1]

3.3.9.6.4.2 Digital Certificate Removals

Only an Administrator shall be able to remove digital certificates that verify software updates.
[Level 1]

3.3.9.6.4.3 Update Package Integrity

The Controller manufacturer shall provide a mechanism to verify the integrity of a software package.
[Level 1]

Note: For example, the manufacturer provides a file containing a hash of the install package that has been signed by a digital certificate.

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.
[Level 1]

3.3.9.6.5 Removal of Previous Versions

The Controller shall remove the previous version of software upon a successful update.
[Level 1]

3.3.9.7 Stable Linux Kernel and Board Support Package Requirements

The requirements for a stable Linux kernel and board support package are as follows.

3.3.9.7.1 Board Support Package Security Updates

The Controller manufacturer shall provide security updates for devices until the EOL is reached.
[Level 1]

Note: Section 3.3.2.6.2 is a requirement for manufacturers to provide a notice when software becomes unsupported for any reason.

3.3.10 Resiliency Requirements

The requirements for the operating platform and applications are as follows.

3.3.10.1 System Backup Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.10.2 System Safe Mode Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.10.3 System Restore Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

3.3.10.4 Power Interruption Response Requirements

[These requirements are not part of the Level 1 capability. They will be developed in a subsequent effort.]
[Level D]

Annex A
Requirement Resources from NIST SP 800-53r5 Controls [Informative]

A.1 Introduction

During the development of the ConOps, an analysis was performed of the security controls found in NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations. This was in order to discover additional user needs and to identify controls that could serve as a resource for requirements to be developed for the ATC Cybersecurity Standard. As discussed in Section 2.10, NIST SP 800-53 serves as the security resource for ARC-IT.

NIST SP 800-53r5 organizes security controls into 20 families (see Table 6). The families contain base controls and control "enhancements" which either add functionality or specificity to a base control or increase the strength of a base control. There are a total of 1006 controls and enhancements in NIST SP 800-53r5 of which 206 have been initially identified as resources for requirements development.

Table 6. NIST SP 800-53r5 Security and Privacy Control Families

ID	Control Family	ID	Control Family
AC	Access Control	**PE**	Physical and Environmental Protection
AT	Awareness and Training	**PL**	Planning
AU	Audit and Accountability	**PM**	Program Management
CA	Assessment, Authorization, and Monitoring	**PS**	Personnel Security
CM	Configuration Management	**PT**	PII Processing and Transparency
CP	Contingency Planning	**RA**	Risk Assessment
IA	Identification and Authentication	**SA**	System and Services Acquisition
IR	Incident Response	**SC**	System and Communications Protection
MA	Maintenance	**SI**	System and Information Integrity
MP	Media Protection	**SR**	Supply Chain Risk Management

A.2 User Needs and NIST SP 800-53r5 Controls

Table 7 lists the user needs identified within the ConOps and the NIST controls and enhancements that may serve as resources for requirements development. The controls and enhancements have the form "*ID-n(e)"* where *ID* is the family, *n* is the base control number, and *e* is the enhancement number. During development of this standard, it is recommended that the controls and enhancements listed are reviewed along with any related controls referenced within the descriptions. Table 7 is not intended to be exhaustive.

Developer Note: Table 7 below is to be updated due to revisions in the user needs section.

Table 7. ATC Cybersecurity User Needs and Supporting NIST SP 800-53r5 Controls

UN #	User Need Title	NIST Controls and Enhancements
	Error! Reference source not found.	
2.7.1.1	Control Physical Access	CM-3(8), CM-5(1), IA(11), PE-2(1), PE-3(1), PE-3(4), PE-4, PE-6(1), AC-2(11), AC-2(12), IA-11
2.7.1.2	No Cabinet Monitor Bypass	CM-3(8), PE-3(5), PE-4, PE-6(1)
2.7.2	**Inventory and Control of Assets**	
2.7.2.1	Facilitate Physical Inventory	CM-7(9), CM-8
2.7.2.2	List of Programmable Components	SR-3, SR-3(3), SR-4, SR-4(1), SR-4(2), SR-4(4), SR-5
2.7.2.4	Facilitate Software Inventory	CM-8
Error! Reference source not found.		SR-3, SR-3(3), SR-4, SR-4(1), SR-4(2), SR-4(4), SR-5
Error! Reference source not found.		CM-8, SA-10(3), SA-10(6)
2.7.2.6	Notice of Unsupported Software	SA-22, SA-5
2.7.2.7	Asset Tracking	PE-20
2.7.3	**Continuous Vulnerability Management**	
		CM-7, CM-7(1), CM-7(2), CM-7(4), CM-7(5), CM-7(7), IA-9, SI-7, SI-7(1), SI-7(2), SI-7(5), SI-7(6), SI-7(8), SI-7(9), SI-7(10), SI-7(12), SI-7(15)
2.7.3.2	Monitor for Unauthorized Changes	CM-11(2), CM-11(3), SI-3, SI-3(4), SI-3(8), SI-7(2), SI-7(6), SI-7(8)
Error! Reference source not found.	**Error! Reference source not found.**	CM-11(2), CM-11(3), SC-7, SC-7(3), SC-7(4), SC-7(5), SC-35, SI-3, SI-3(4), SI-3(8)
	Error! Reference source not found.	
		AC-4(17), AC-2(1), AC-2(3), AC-2(4), AC-2(7), AC-2(12), AC-3, AC-3(8), AC-24, AC-24(1), AC-24(2), IA-2, IA-2(1), IA-2(2), IA-2(5), IA-2(6), IA-2(13), IA-5, IA-5(1), IA-5(5), IA-5(7), IA-7, IA-8, IA-10, IA-11
2.7.4.2	User Account Management	AC-2(1), AC-2(3), AC-2(4), AC-2(7), AC-2(11), AC-2(12), AC-3, AC-3(8), AC-3(13)

UN #	User Need Title	NIST Controls and Enhancements
		AC-2(7), AC-2(11), AC-2(12), AC-3(7), AC-2(7), AC-3(8), AC-3(13), AC-6(10), AC-7(4), AC-24, AC-24(1), AC-24(2), CM-3(8), CM-5(1), CM-11(2), SC-4
		AC-7(4), IA-5(5)
2.7.5	**Logging, Monitoring, and Reporting**	
2.7.5.1	Consistent and Accurate Time	SC-45, SC-45(1), SC-45(2)
		AU-2, AU-3, AU-3(1)
2.7.5.2	Security Event Logging	AU-2, AU-3, AU-3(1), AU-12(3), CM-3(5), CM-5(1), SI-11
2.7.5.3	Support Security Audits	AU-3, AU-3(1), AU-4, AU-4(1), AU-5, AU-5(1), AU-5(2), AU-7, AU-7(1), AU-8, AU-9, AU-9(3), AU-9(6), AU-12, AU-12(3) AC-6(9), CM-3(8), CM-3(5), CM-5(1)
2.7.5.4	Security Monitoring	SI-4, SI-4(2), SI-4(5), SI-4(7), SI-4(14), SI-4(22), AC-9
2.7.5.5	Operating Software Reporting	CM-6, CM-8, SA-10(1), SI-11
2.7.5.6	Network Service Status	CM-6, SI-4, SI-4(2), SI-4(22)
2.7.6.1	Secure Remote Access	AC-3, AC-17(1), AC-17(2), AC-17(3), AC-17(10), AC-20, AC-20(1), AC-20(2), AC-20(3), IA-2(13), IA-3, MA-4(4), SC-7(8), SC-7(11), SC-7(15), SC-10, SC-11
2.7.6.2	Wireless Security	AC-18, AC-18(1), AC-18(3), AC-18(4), SC-7(3), SC-7(5), SC-11, SC-40
		AC-18(3), CM-6, CM-7, CM-7(1), SA-4(5), SC-7(5), SC-41
2.7.6.4	Manufacturer-Stated Network Services	SA-5
2.7.6.5	Boundary Protection	AC-3(5), AC-4, AC-4(1), IA-5(2), SC-4, SC-5, SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(8), SC-7(11), SC-7(12), SC-7(13), SC-7(15), SC-7(16), SC-7(18), SC-7(21), SC-7(23), SC-7(28), SC-7(29), SC-11, SC-47, SI-3
2.7.6.6	Denial-of-Service Protection	SC-5, SC-5(1), SC-5(2), SC-5(3), SC-6, SC-7
		AC-3(5), AC-20, AC-20(1), AC-20(3), AC-20(4)
2.7.7	**Data At Rest Protection**	
2.7.7.1	Secure Data At Rest	AC-3(11), AC-20(2), AC-20(4), MP-2, MP-7, SC-4, SC-13, SC-28, SC-28(1)
2.7.7.2	Removable Storage Security	AC-20(2), AC-20(5), AC-3(11), MP-2, MP-7, SC-4, SC-28, SC-28(1), SC-41
2.7.8	**Data in Transit Protection**	
2.7.8.1	Secure Data in Transit	AC-17(2), AC-17(3), SC-8, SC-8(1), SC-13
		IA-9

UN #	User Need Title	NIST Controls and Enhancements
		AC-3(11), AC-3(12), AC-3(13)
		AC-3(5), IA-5(7), IA-7, IA-5(13), IA-5(14), IA-6, SI-10(5)
		AC-3(5), IA-5, IA-5(1), IA-5(2), IA-7
		AC-7, AC-2(5), AC-11, AC-12, AC-12(1), AC-12(3), IA-3(1), IA-5(14), IA-7, SC-17, SC-21, SC-23, SC-23(1), SC-23(3), SC-23(5)
		AC-4, CM-3(5), IA-3, SI-10(5)
2.7.9.1	Application and Process Isolation	SC-2, SC-2(1), SC-5, SC-6, SC-7(21), SC-18, SC-39, AC-3(12), AC-6(4), AC-6(10), SI-16
2.7.9.3	Application Reporting	AU-2, SI-4, SI-4(7), SI-11
2.7.9.2	Application Logging	AU-2, AU-3, AU-3(1), AU-12(3), CM-5(1), SI-11
		SC-27
2.7.9.5	Separation of System, Security, and User Functionality	SC-2, SC-2(1), SC-3, SC-3(1), SC-3(2), SC-3(3), SC-3(4), SC-3(5), AC-6(8), AC-6(10) SC-7(21)
2.7.9.6	Facilitate System Software Updates	SI-2(4), SI-2(5), SI-2(6), SA-10, SA-10(1), SA-10(3), SA-10(6)
2.7.10.1	System Backup	CP-9
2.7.10.2	System Safe Mode	CP-12, SC-7(18), SC-24, IR-4(5), SI-7(5), SI-17
2.7.10.3	Secure System Restore	CP-10, IR-4(5), SA-8(24), SI-17
2.7.10.4	Power Interruption Response	PE-11, PE-11(1), SI-17

Annex B
Future Enhancements [Informative]

§