## ATC Cyber ConOps v01.02

Advanced Transportation Controller (ATC)

# Concept of Operations (ConOps) for the Advanced Transportation Controller Cybersecurity Standard

June 28, 2023



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 |
| --- | --- | --- | --- |
| ATCCyberStd_ConOps_v0102_230628 | 06/28/2023 | Boaz | Draft ConOps distributed to stakeholders prior to technical walkthrough. |
| ATCCyberStd_ConOps_v0101_220908 | 09/08/2022 | Boaz | Initial draft ConOps. |

Add DOT standards statement if desired.


# Acknowledgement

XXXXXX

To be completed.


# 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**

Md Ashraf Ahmed, aahmed@ite.org
Siva Narla, snarla@ite.org
Tatiana Richey, trichey@ite.org

## AASHTO

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

Robert T. White, rwhite@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

Ethan Coxsey, Eberle Design (Co-Chair)
Matt Luker, Utah DOT (Co-Chair)
Matt Barron, Cubic
Mike Bousliman, Montana DOT
Brandon Campbell, City of Tampa
Mike Gallagher, Q-Free America
Jonathan Grant, Yunex
Justin Hatch, Georgia DOT
Herasmo Iñiguez, SWARCO McCain
Jeremy Iwen, Wisconsin DOT
David Lucas, Maricopa County DOT
Marisa Ramon, Southwest Research Inst.
Robert Rausch, TransCore
Jason Tao, District of Columbia
Shea Thompson, Econolite
Paul Tykodi, Massachusetts DOT

## Subject Matter Experts (SMEs)

Ralph Boaz, Pillar Consulting
Tiffany Rad, ELCnetworks
Michaela Vanderveen, Still Waters Consulting

# 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, Committee Members, Task Force co-chairs, and SMEs, there were many others that contributed to the development of this standard and their input and assistance was critical to the final product. The following list includes those who volunteered their time to help both the Task Forces and consultants ensure that the resulting guidance met their needs, and contributed to the input and review during the development of this guide:

To be completed.

In addition to the many volunteer efforts, recognition is also given to the following federal agency that supported the effort by providing funding:

- The United States Department of Transportation

# User Comment Instructions

The term "User Comment" includes any type of written inquiry, comment, question, or proposed revision, from an individual person 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 for clarification of 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 intentionally left blank.>

# Section 1
# General Information [Informative]

## 1.1 Purpose

This Concept of Operations (ConOps) 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 made up of 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) that 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).

This ConOps 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 are intended to provide an open architecture hardware and software platform that can support a wide variety of Intelligent Transportation Systems (ITS) applications including traffic management, safety, security, and other applications. ATC controllers operate in non-ATC cabinet systems. It is expected that many of the issues addressed for the ATC standards will also apply to other ITS standards and specifications. The project follows a systems engineering process which will have interim deliverables of a ConOps, a Systems Requirement Specification (SRS), and a System Design Description (SDD) (to be determined, design material may be in individual standards) for the cybersecurity areas of concern for the three ATC standards. The primary deliverable of the project will be the development of the ATC Cybersecurity Standard.

This ConOps 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 that may be less familiar with such equipment and provides context when identifying cybersecurity needs.

## 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 and 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 connected intersections; 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, and 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 SP 800-53 Rev. 5 | Security and Privacy Controls for Information Systems and Organizations, National Institute of Standards and Technology, 2019 |
| 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 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. |
| Availability | Ensuring timely and reliable access to and use of information. Source NIST SP 800-53r5. |
| Bus Interface Unit | A transportation cabinet device which is used for 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. |

| Term | Definition |
| --- | --- |
| Connected Intersections (CI) | An infrastructure system that broadcasts signal, phase, and timing (SPaT), mapping information and position correction data to On-Board Units and Mobile Units. |
| Confidentiality | Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Source NIST SP 800-53r5. |
| 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.<br><br>Source: *The NTCIP Guide* |
| Interface | A shared boundary across which information is passed.<br><br>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 SP 800-53r5. |
| Interoperability | The ability of two or more systems or components to exchange information and to use the information that has been exchanged.<br><br>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.<br><br>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.<br><br>Source [IEEE 1362-1998] |
| Roadside Unit (RSU) | A transportation infrastructure communications device located on the roadside that provides V2X connectivity between OBUs/MUs and other parts of the transportation infrastructure including traffic control devices, traffic management systems, and back-office systems.<br>Note: Devices that are not part of the transportation infrastructure, such as cellular base stations or satellites, are not RSUs.<br><br>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.<br><br>Source: *ISO/IEC/IEEE 24765:2017 Systems and software engineering-Vocabulary* |

| Term | Definition |
|---|---|
| Serial Interface Unit | A transportation cabinet device which is used for communications within ATC cabinet systems. |
| 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 |
| 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 |
| DCS | Distributed Control System |
| DRAM | Dynamic Random Access Memory |
| DTLS | Datagram Transport Layer Security |
| ECLA | External Control Local Application |
| FHWA | Federal Highway Administration |
| FIPS | Federal Information Processing Standards |
| 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 |
| 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 |
| SDO | Standards Development Organizations |
| 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 |
| SRS | Systems Requirement Specification |
| SSE | Systems Security Engineering |
| SU | Sensor Unit |
| TEES | Transportation Electrical Equipment Specifications |
| TFCS | Transportation Field Cabinet System |
| TLS | Transport Layer Security |
| TMS | Traffic Management System |
| TSC | Traffic Signal Controller |
| UPS | Uninterrupted Power Supply |
| US | United States |
| USB | Universal Serial Bus |
| USDOT | United States Department of Transportation |
| VAC | Volts Alternating Current |
| VDC | Volts Direct Current |

# 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. 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.** This section identifies the cybersecurity user needs for ATC equipment.
- **Section 2.8 Operational Policies and Constraints**. This section describes any operational policies and constraints that apply to the system or situation.
- **Section 2.9 Operational Scenarios**. This section provides any operational scenarios identified for the system.

## 2.2 Background [Informative]

### 2.2.1 General Description of Transportation Field Cabinet Systems

In the 1970s and early 1980s, standards and specifications emerged as a means to perform actuated traffic signal control. These standards defined a system that is located in a cabinet at signalized intersections. There has been an evolution of the standards and specifications of the 1970s and 1980s and new national standards developed. While these new standards have more capabilities and features, they still have the same conceptual operation. The standards and one state specification that have had an influence on this evolution are identified in the order of their original publication date.

- “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 “332-type cabinets” in reference to other models numbers of the same 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 design of the TS 1 Cabinet. This enhancement for TS 1 cabinets is referred to as 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.” It is a successor to the ITS Cabinet but it 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 **Error! Reference source not found.**.

- The “Inputs” element is the part of the system that gathers the indications from various on-street sensor devices in the form of on/off states. There are numerous technologies used for detection such as inductive loops, video image processing, microwave radar, magnetometers, and others. Most commonly, this element is found in TFCSs as “detectors” housed in a “detector rack,” “input assembly,” or “input file” (terms are synonymous).

- The “Controller” element is a field hardened computer that runs the signal control application program and other application programs. The signal control application understands the association of the detection with the turning movements in the intersection. The Controller receives the detection inputs, determines how to safely provide service to the vehicles and sets the field display states (reds, yellows and greens) in the output element of the TFCS.

- The “Outputs” element is a collection of switch packs or load switches (terms are synonymous) which receive the field display states from the controller and enable or disable the flow of electricity to the signal heads accordingly. 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).

- The “Monitoring” element ensures that the field display states are allowable by comparing them to a removable hard-wired program card or programmable memory device installed in the monitor. If signal indications are considered unsafe, the monitor will put the TFCS into a flash condition. Depending on the capabilities of the monitor and the standard used to define the TFCS, the monitor may be able to validate that the controller is operating, that internal cabinet and output voltages are within allowable parameters and many other features. The generic terms for this element are “signal monitor” or “monitor.” The names vary across the standards, this element may be a Conflict Monitor Unit (CMU), Malfunction Management Unit (MMU), or a Cabinet Monitor Unit (CMU).

- The “Power Supply” element provides power for the devices internal to the cabinet system.

- The “Internal Bus” element refers to the “communications” method used between components of the TFCS. In the case of older TFCSs, there is discrete electrical wiring between the elements. In more modern standards, there is serial communications and messaging between the cabinet elements.

- The “Housing” element includes the cabinet body, cabinet finish, cabinet doors, latches/locks, hinges and door catches, gasketing, ventilation, lighting, assembly supports and mounting. Common mountings are base mounts, pole mounts, and pedestal mounts. There are others.

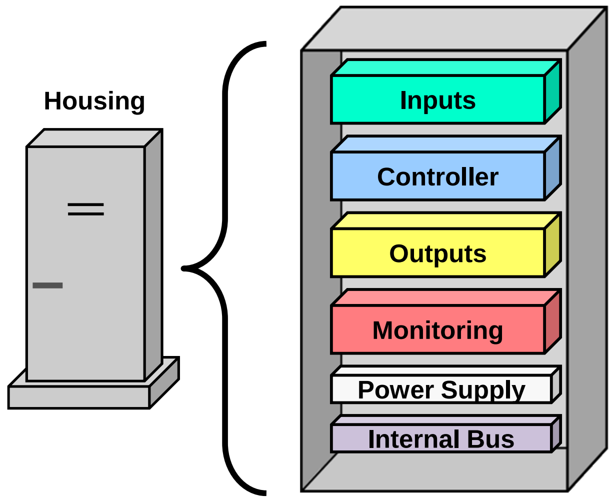



**Figure 1. Elements of a Transportation Field Cabinet System.**

**Error! Reference source not found.** illustrates the basic operation of a TFCS. Steps are as follows:

1) Field sensors detect vehicles, which come in as inputs to the controller
2) The controller determines which turning movements to service according to its programming
3) The controller determines the settings for the display states and sends this information to the outputs
4) The outputs allow power to the field displays (signal heads) according to the states sent from the controller.
5) At the same time, the monitor performs its functions to determine if the cabinet system is operating safely. If it is not, the monitor puts the cabinet into a flash condition.
6) For NEMA TS 2 Cabinets, ITS Cabinets, and ATC Cabinets; the monitor sends the status of the outputs to the controller.

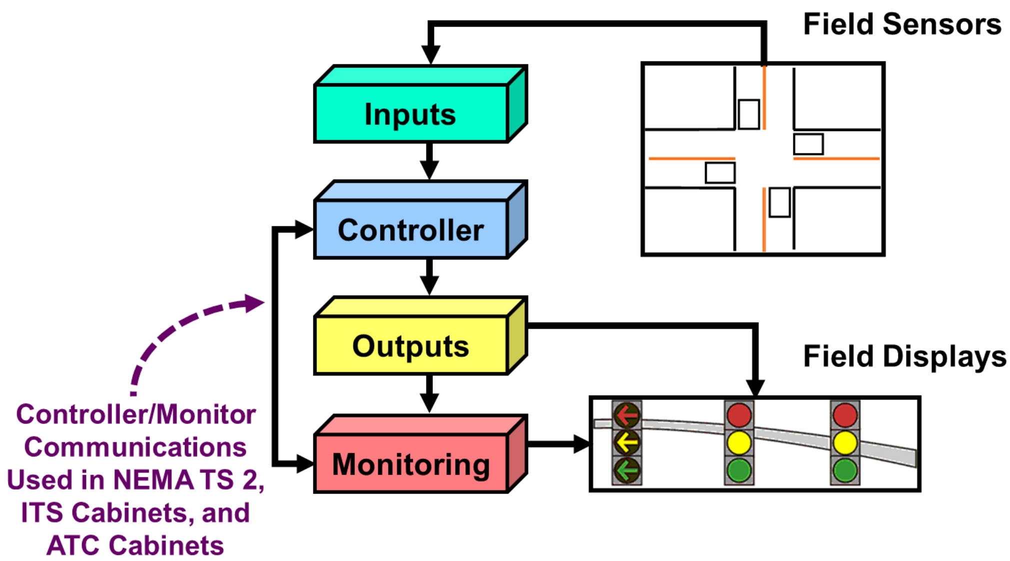



**Figure 2. Basic operation of a Transportation Field Cabinet System.**

TFCSs that are deployed rarely have only equipment covered by ITS standards. Other equipment commonly deployed in TFCSs include the following:

- Networking Equipment – Switches, Routers, Ethernet and Wi-Fi
- Specialized Detection Systems – Sophisticated detection systems such as radar, video, and lidar often use additional equipment within the cabinet to do processing. They may use slots in a detector rack or they may be separate devices emulating a detector rack with communications to the cabinet bus. These devices may also have separate ethernet ports so that they can be monitored or configured remotely.
- Priority and Preemption Devices – There are various ways that agencies will implement transit signal priority and emergency vehicle priority and preemption. A common way is to have an additional device in the TFCSs to receive a signal and generate a priority request to the controller.
- Time Keeping Devices – There are various time keeping devices that connect directly to controllers using a USB cable or RS-232 connection.
- Battery Backup Systems (BBSs) and Uninterrupted Power Supplies (UPSs) – When there is room in a transportation cabinet, many agencies use the available space to include BBSs and UPSs to maintain traffic control during power outages.
- External Control Local Application (ECLA) Devices – ECLA devices are located within a TFCS and exercise control over the signal program running in the controller. They may command the signal program to run specific timing plans, adjust timing parameters, or hold, force-off, or omit movements within the intersection. These devices are often used to run adaptive control programs supplied by a manufacturer other than the controller manufacturer. ECLA devices will also have separate ethernet ports so that they can be monitored or configured remotely.
- Connected Vehicle (CV) Processors / Coprocessors – These devices offload processing demands from the main processor of the ATC unit or an RSU. They may perform some of the processing required to provide Signal Phase and Timing (SPaT) messages, process incoming messages such as the basic safety message, or other functions of a connected intersection (CI). These devices can be co-processors within the controller unit or separate devices within the cabinet system.

### 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 (CV), 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 a controller standard. 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) Eight 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. **Error! Reference source not found.** shows how the Engine Board can be used to create ATC units that work within different families of traffic controller equipment. This concept also allows more powerful Engine Boards to be deployed in the future without changing the overall controller and cabinet architecture.

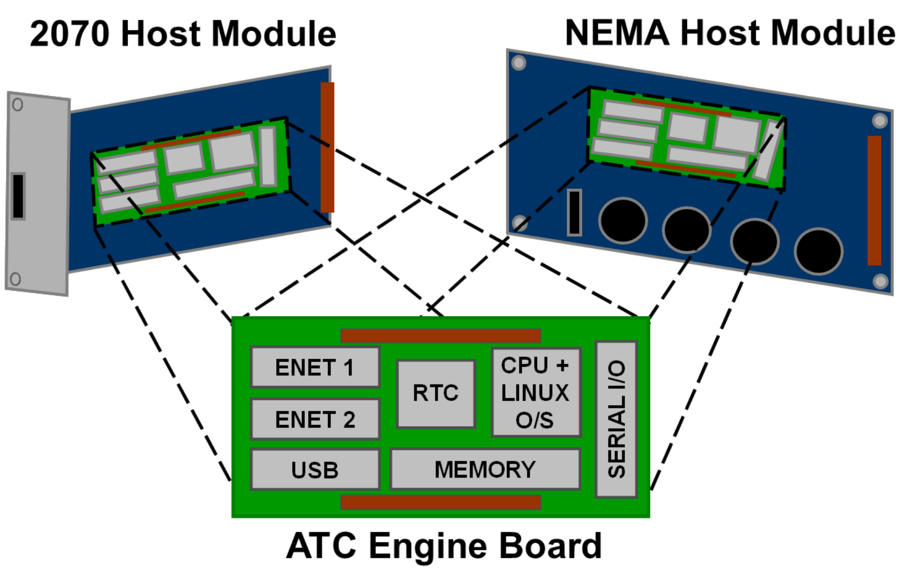



**Figure 3. ATC Engine Board used to support different families of controllers.**

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 **Error! Reference source not found.** (not all named ports are required for different configurations). In the configuration shown, Serial Ports 1-3 are for general use.

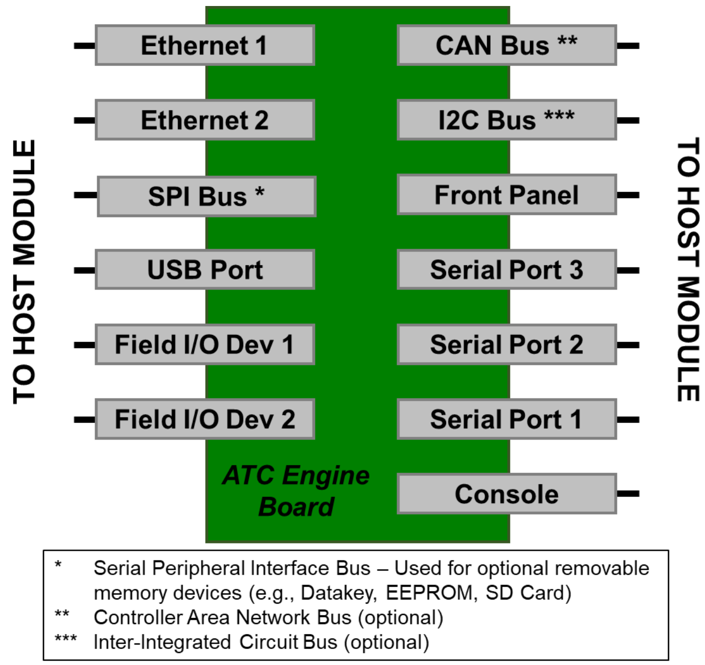



**Figure 4. ATC Engine Board communications ports and their functions.**

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.

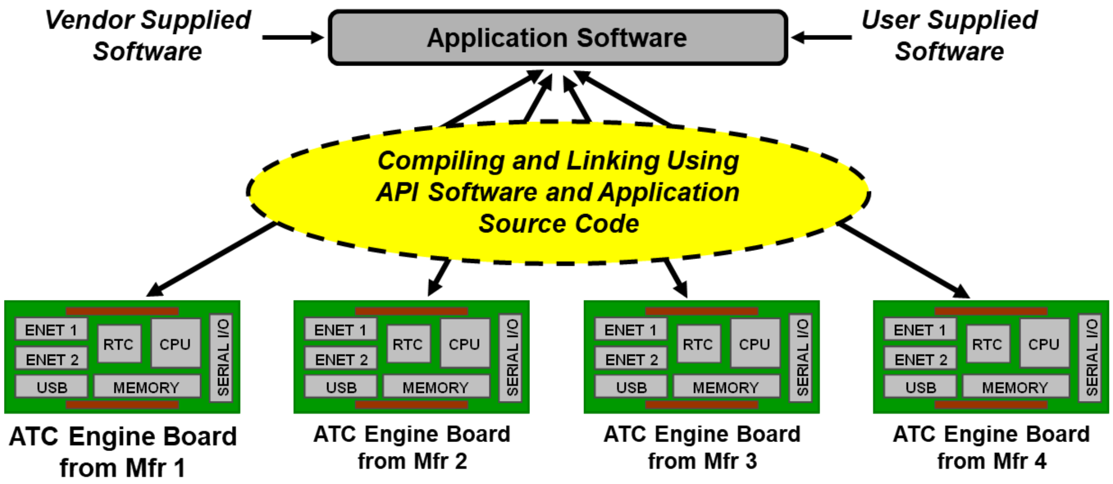



**Figure 5. Application portability through compilation and linking of source code.**

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 **Error! Reference source not found.**, both users and application programs use the API Software to interface to ATC units.

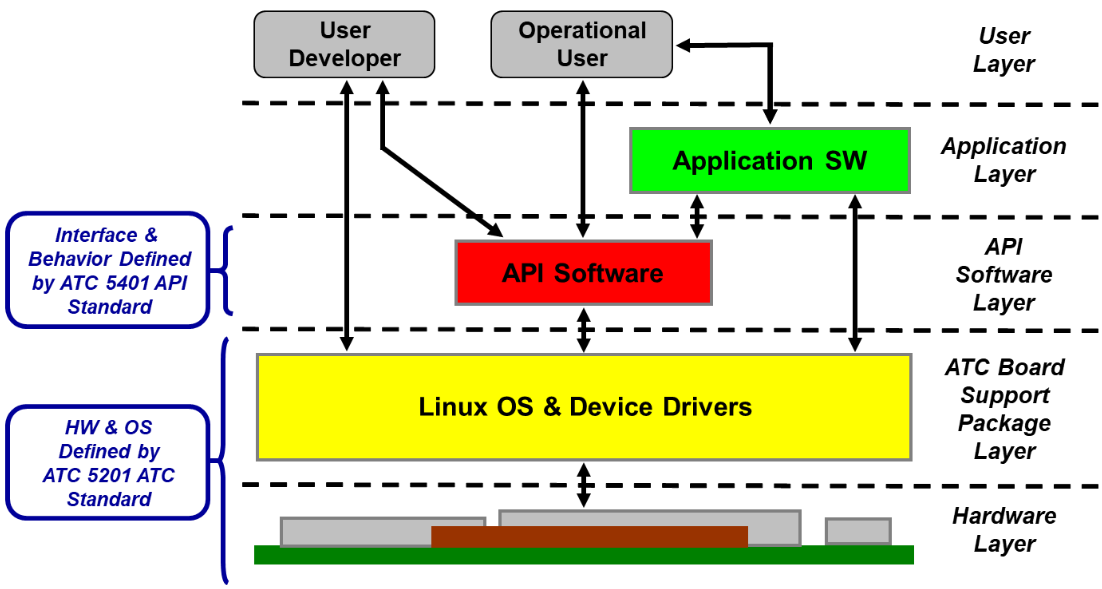



**Figure 6. ATC software layered organization.**

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.

**Error! Reference source not found.** shows 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. **Error! Reference source not found.** shows the ATC Configuration Information window. Users use this window to set and view system wide parameters (e.g., system time, Ethernet ports).

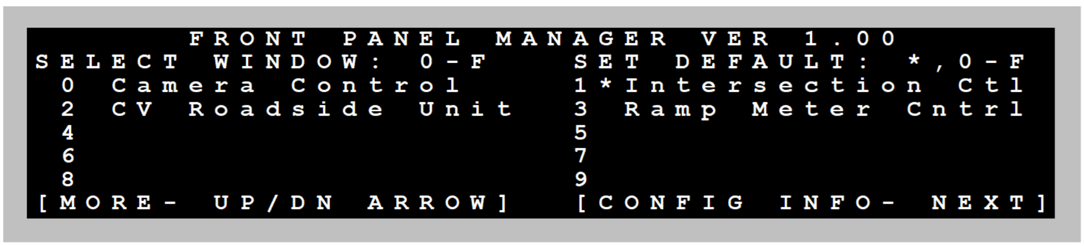



**Figure 7. Front Panel Manager allows users to select an application program to put in view.**

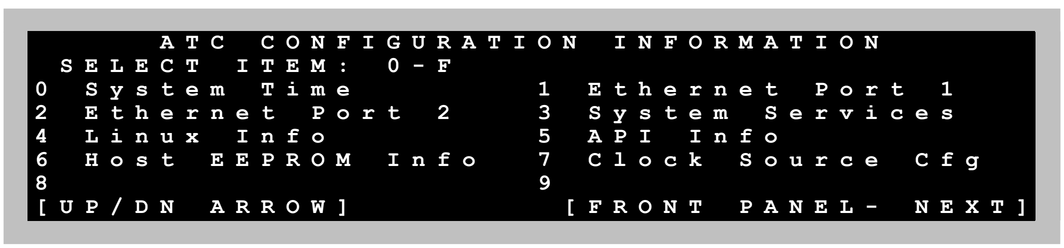



**Figure 8. ATC Configuration Information allows users set and view system wide parameters.**

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. **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 element 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). Controllers from different manufactures will have a different appearance, size and shape.

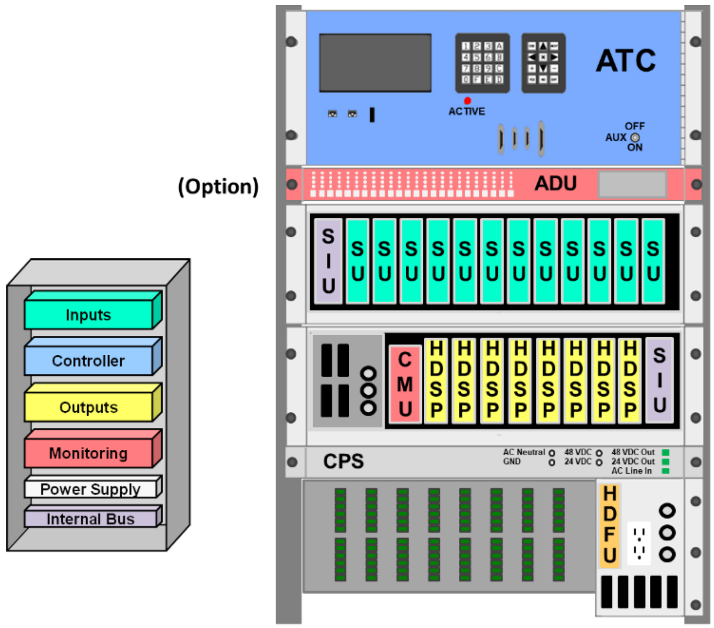
- The Inputs element is shown as an Input Assembly containing Sensor Units (SUs) to perform on-street detection and a Serial Interface Unit (SIU) to communicate the sensor data to the ATC unit. The SUs can be double density detectors that support two input channels for each SU. They are used in some other TFCS architectures. Input assemblies can be different sizes and shapes.

- The Outputs element 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 safety monitoring), and an SIU to allow the ATC unit to command the states of the HDSPs. HDSPs are double density switch packs that can control two output channels for each HDSP. HDSPs also come in high voltage and low voltage models. The high voltage model operates with signals that use 120 VAC. The low voltage model operates with signals that use 48 VDC. The HDSPs are unique to the ATC Cabinet architecture because of the double density and low voltage option. The output assembly can be various shapes and sizes.

- The Monitoring element 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 may not be used at all. In the latter case, a technician may plug a laptop or handheld device into the CMU to see the status of the cabinet system. The CMU performs load current monitoring which can be used to detect dark signal heads. The CMU comes in high voltage and low voltage models. The high voltage version monitors intersections that operate with signals that use 120 VAC. The low voltage model operates with signals that use 60 VDC. This low voltage option is unique to the ATC Cabinet architecture. The load current monitoring and low voltage capabilities are unique to the ATC Cabinet architecture. A removable memory device or a “program card” is used to set the allowable signal state combinations allowed for the intersections.

- The Internal Bus element is High-level Data Link Control (HDLC) at 614 kbps (kilobits per second) between the SIUs on the output and input assemblies, the CMU and the ATC unit.

- The Power Supply element 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 of 120 VAC 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. Our roadway infrastructure helps us respond to natural disasters, contributes to national security across the country, and generally provides 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 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 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 their 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 our largest metropolitan areas cost the 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. Our infrastructure may communicate with external systems outside of an agency including cloud services. All of these developments are inevitably posed to increase both the vulnerability of the transportation infrastructure and the urgency to include cybersecurity measures in our 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. **Error! Reference source not found.** illustrates connections to devices or systems external to the cabinet structure that may exist in installations, 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).

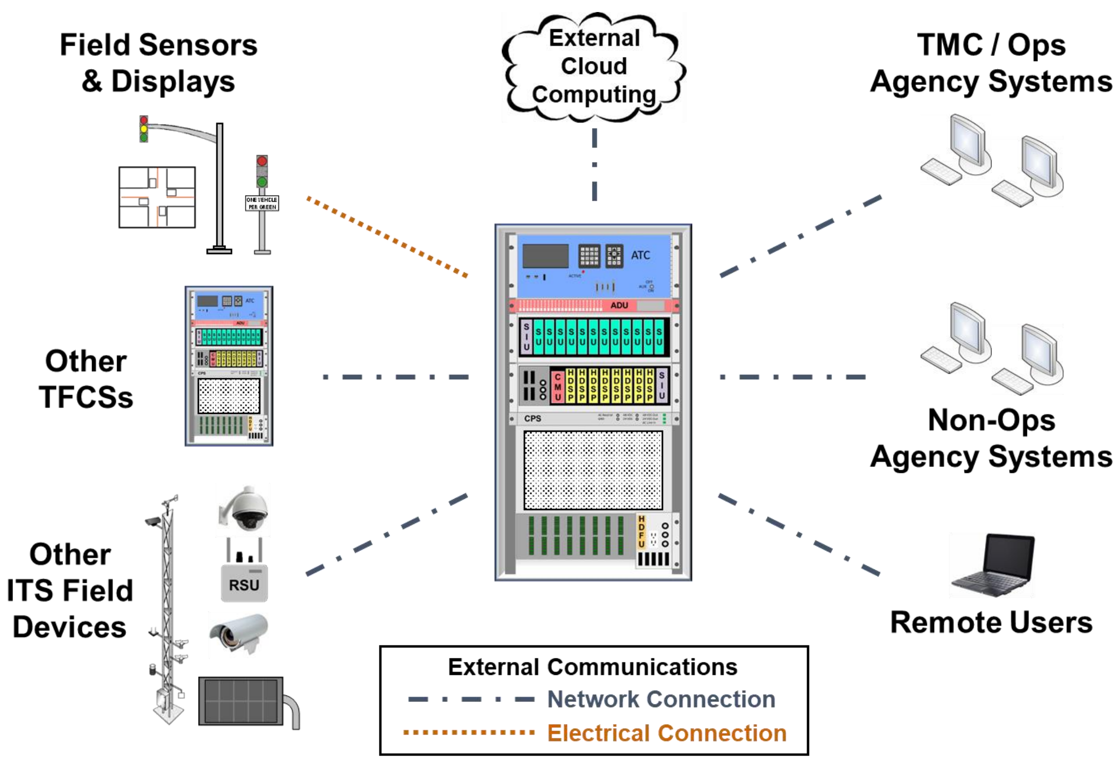



**Figure 10. ATC Cabinet with external operational connections.**

### 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 ConOps but the communications with them are. This is illustrated in **Error! Reference source not found.**. **Error! Reference source not found.** provides an internal view of the ATC Cabinet with areas identified for discovery of ATC cybersecurity needs and requirements.

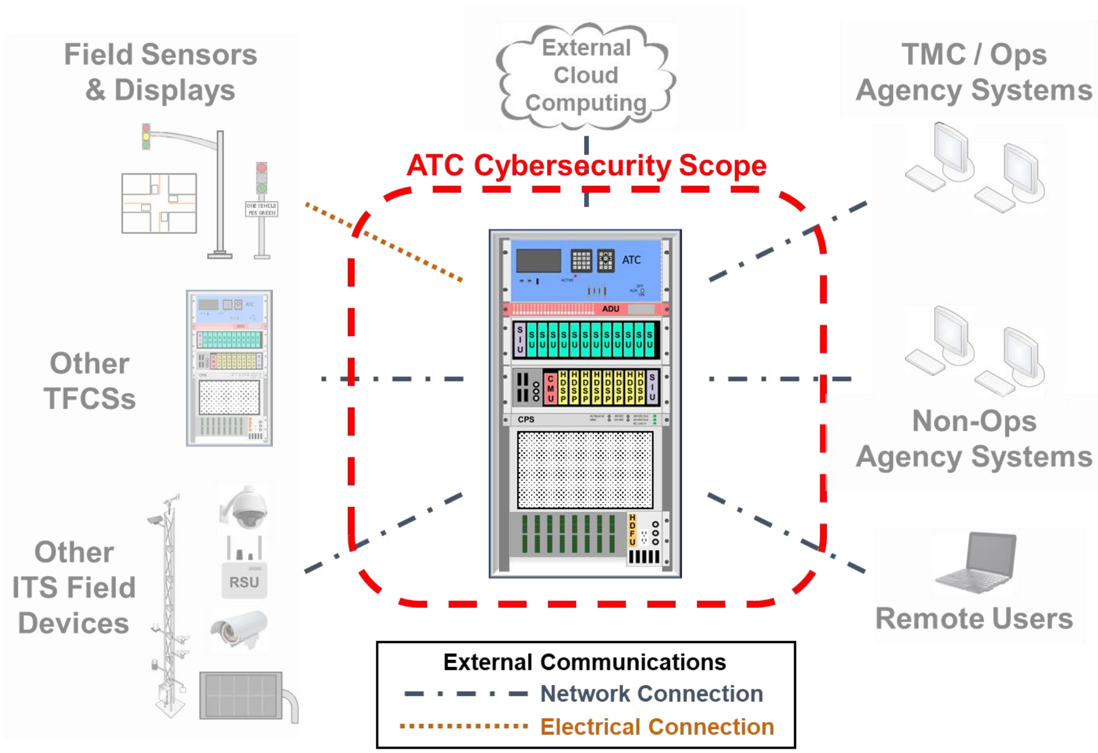



**Figure 11. ATC Cybersecurity Scope includes external communications.**

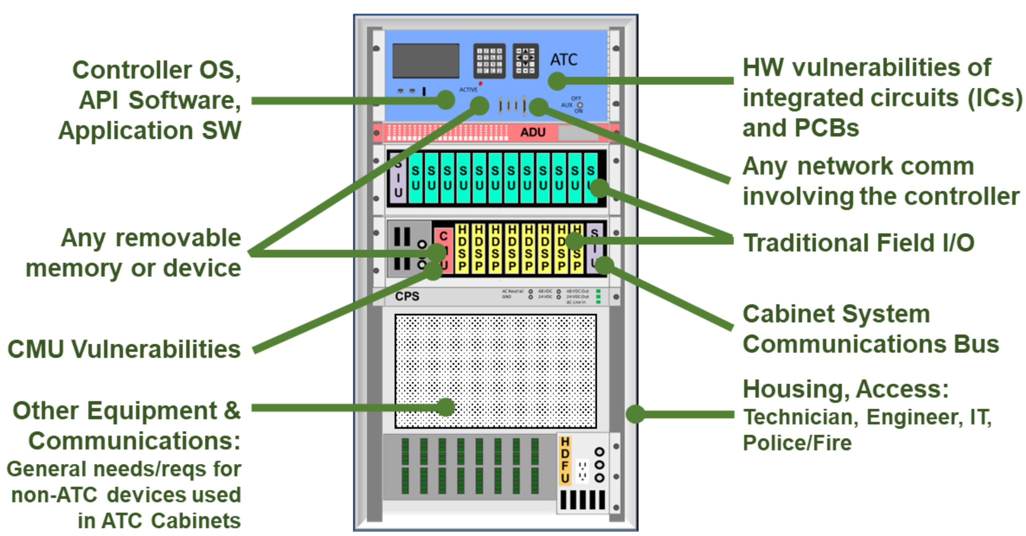



**Figure 12. Areas for discovery of ATC cybersecurity needs and requirements.**

## 2.6 Architectural Constraints

As described in Section 2.2 and its subsections, the ATC 5201 and ATC 5401 standards define a controller that can be used to upgrade any of the major TFCS architectures in use today.

It is out of scope for this ATC Cybersecurity Standard to attempt to impose requirements on non-ATC TFCS designs. Therefore, ATC controllers in cabinet systems that do not conform to ATC 5301 are not formally covered by this ConOps but may still benefit from most of its content.

## 2.7 ATC Cybersecurity Needs

This section identifies the cybersecurity needs to be included in the ATC Cybersecurity Standard. As a system, the needs are assigned to the ATC Cabinet. During requirements development, however, it is expected that requirements will reflect the subsystems, devices, communications or software to which they apply. Each need has a unique number (section number) and title, a sentence stating the need, and a rationale (typically 1-4 sentences) which states the reason for the need and may contain additional clarifying information.

In addition, each need is followed by initial implementation priorities set by the ATC Cybersecurity WG to help plan the requirements phase of development. They are bracketed and written in italics (e.g., *[Implement Now]*). The options are as follows:

- Implement Now – the need is implementable using the current generation of ATC equipment and it is a priority to do so.
- Desired Now – the need may or may not be implementable using the current generation of ATC equipment or it is a lower priority than those identified as Implement Now.
- Next Generation – the need is to be deferred to a new generation of ATC equipment due to the technical requirements or the time needed to carry it out.

<u>The implementation priority is Informative and may change during the development of the ATC Cybersecurity Standard</u>.

### 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.
*[Implement Now]*

#### 2.7.1.2 Signal Monitor Bypass

The ATC Cabinet needs to prohibit the signal monitor device from being bypassed or disabled when installed. The signal monitor is a critical safety device for traffic signal control applications.
*[Implement Now]*

### 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 identifiers such as the model, version, manufacturer, serial number, MAC address (if it is a network capable device), or universally unique identifier (UUID). This is to support asset and configuration management by users. The identifying information will vary depending on the device.
*[Implement Now]*

#### 2.7.2.2 Sourced Bill of Materials

The ATC Cabinet needs its physical devices within the cabinet to come with a bill of materials (BOM) that identifies the components of the device and sources of the components. This may include resistors, diodes, capacitors, integrated circuits, date of manufacture, etc. Sourcing identifies the manufacturer to the receipt of the part. This is to support supply chain risk management (SCRM).
*[Implement Now]*

#### 2.7.2.3 Facilitate Software Inventory

The ATC Cabinet needs to facilitate the inventory and control of any software that is used on a programmable device. 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.
*[Implement Now]*

#### 2.7.2.4 Software Bill of Materials

The ATC Cabinet needs any software that is to be used on a programmable device to come with a software bill of materials (SBOM). An SBOM is a nested inventory of the software components for a given software item. It 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.
*[Implement Now]*

#### 2.7.2.5 Inventory Tool Support

The ATC Cabinet needs 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.
*[Next Generation]*

#### 2.7.2.6 Notice of Unsupported Software

The ATC Cabinet needs vendors to provide 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.
*[Implement Now]*

#### 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 Controllers and Signal Monitors but could include other equipment) remain in expected locations.
*[Desired Now]*

#### 2.7.3 Continuous Vulnerability Management

This section identifies needs that concern continuous vulnerability management.

##### 2.7.3.1 Validate Software Is Authorized

The ATC Cabinet needs a mechanism to ensure only authorized software is installed in 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.
*[Implement Now]*

##### 2.7.3.2 Vulnerability Scanning

The ATC Cabinet needs to continually check for unauthorized changes to software components including additions and removals. Unauthorized manipulation is logged and reported.
*[Implement Now]*

##### 2.7.3.3 Intrusion Detection

The ATC Cabinet needs to detect in a timely manner when a cyber intrusion has been attempted or occurred. Intrusion includes malware activity. The detection capability can be updated with the latest known threats.
*[Next Generation]*

#### 2.7.4 User Accounts and Controlled Use of Administrative Privileges

This section identifies needs that concern user accounts and controlled use of administrative privileges.

##### 2.7.4.1 Uniquely Identify Authorized Users

The ATC Cabinet needs to be able to uniquely identify authorized users of the system. The system may use passwords or multi-factor authentication. The purpose is to verify that the user is authorized.
*[Implement Now]*

##### 2.7.4.2 User Account Management

The ATC Cabinet needs to support the addition, change, and removal of user accounts. This allows the agency to manage access to the entire system.
*[Desired Now]*

##### 2.7.4.3 User Access Control

The ATC Cabinet needs to provide user based access control. The ability to use features and operations (user privileges) can be tailored and restricted for logins and may be time limited. Access and operations may be role-based. This protects the operation and security of the device.
*[Desired Now]*

##### 2.7.4.4 Default Passwords

The ATC Cabinet needs to protect against the use of weak or discoverable default passwords. Default passwords are a security risk.
*[Implement Now]*

#### 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 of its devices. Consistent and accurate time is necessary to analyze logs and perform forensics after a cybersecurity event.
*[Desired Now]*

##### 2.7.5.2 Account Logging

The ATC Cabinet needs to log and report any changes to the accounts on the system or application in a fashion that prevents tampering (unauthorized modification). This is to detect the changes made as soon as they happen as well as in later analysis.
*[Desired Now]*

##### 2.7.5.3 Security Event Logging

The ATC Cabinet needs to perform security event logging. For example, 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.
*[Desired Now]*

##### 2.7.5.4 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.
*[Desired Now]*

##### 2.7.5.5 Security Monitoring

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

##### 2.7.5.6 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.
*[Desired Now]*

##### 2.7.5.7 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.
*[Implement Now]*

#### 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.
*[Implement Now]*

#### 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.
*[Implement Now]*

#### 2.7.6.3 Disabled Protocols, Services, and Ports

The ATC Cabinet needs to contain network capable devices that have protocols, services, and ports disabled by default. This means that users will configure what they need and will be less likely to expose services unintentionally.
*[Implement Now]*

#### 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.
*[Implement Now]*

#### 2.7.6.5 Boundary Protection

The ATC Cabinet needs to restrict or prohibit unauthorized network traffic to critical components. Support the monitoring and control of network communications at managed interfaces within the system and external to the system. 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.
*[Implement Now]*

#### 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 and increased network capacity and bandwidth. Possibly automated rate limiting of devices.
*[Implement Now]*

#### 2.7.6.7 Secure Cloud Services

The ATC Cabinet needs secure cloud services if they are employed. There are additional risks to the systems over which the organization does not have direct control. Zero trust practices should be employed (e.g., authentication by specified services, avoid all bring your own devices). Safety critical applications should not require cloud services.
*[Implement Now]*

### 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 encrypted and integrity protected. This protects the operation of the system.
*[Desired Now]*

#### 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.
*[Desired Now]*

### 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 (encrypted), up-to-date protocols such as TLS 1.3, SFTP, SSH2, and SNMPv3. Unencrypted protocols are not secure.
*[Desired Now]*

#### 2.7.8.2 Valid Credentials

The ATC Cabinet needs to ensure that it uses up-to-date, valid credentials to send and receive information securely (e.g., TLS certificates between devices). Communications with invalid credentials are not secure.
*[Desired Now]*

### 2.7.9 Authentication, Authorization, and Accounting

This section identifies needs that concern the authentication, authorization, and accounting of users and devices.

#### 2.7.9.1 Configure Centralized Point of Authentication

ATC Cabinet needs to provide facilities for remote authentication of users (e.g., active directory, RADIUS, IEEE 802.1x). This allows centralized credential management. For example, when a person leaves the agency, their credentials can be removed from the domain.
*[Desired Now]*

#### 2.7.9.2 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.
*[Implement Now]*

#### 2.7.9.3 Key Material Protection

The ATC Cabinet needs to protect the 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.
*[Next Generation]*

#### 2.7.9.4 Secure Authenticated Sessions

The ATC Cabinet needs to provide best practices for authentication. Use Public Key Infrastructure (PKI) for bidirectional cryptographic authentication, locking accounts after too many failed authentication attempts, and terminating inactive sessions. This inhibits the ability of bad actors to gain access to the system.
*[Desired Now]*

#### 2.7.9.5 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 certificates, lack of responsiveness, excessive network traffic, and other tests. Communications with a device that is not trustworthy is not secure.
*[Desired Now]*

### 2.7.10 Operating Platform and Applications

This section identifies needs that concern the operating platform for ATC units and the application programs that run on them.

#### 2.7.10.1 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.
*[Desired Now]*

#### 2.7.10.2 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.
*[Desired Now]*

#### 2.7.10.3 Application Portability

TFSC needs to facilitate application portability. Portability of application programs allows new security solutions to be used to secure the system.
*[Desired Now]*

#### 2.7.10.4 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. This prevents the misuse of privileged functions.
*[Implement Now]*

#### 2.7.10.5 Facilitate System Software Updates

The ATC Cabinet needs to provide tools to ensure the timeliness and completeness of patching firmware, operating system, and middleware. These tools include options for manual and automated updates. Only allows valid software to be installed and includes the removal of previous versions of the software.
*[Desired Now]*

### 2.7.11 Resiliency

This section identifies needs that concern resiliency.

#### 2.7.11.1 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 data. This is to facilitate recovery from an attack or failure.
*[Desired Now]*

#### 2.7.11.2 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.
*[Implement Now]*

#### 2.7.11.3 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.
*[Desired Now]*

#### 2.7.11.4 Emergency Power

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

## 2.8 Operational Policies and Constraints

There are no operational policies or constraints identified for this ConOps.

## 2.9 Operational Scenarios

There are no operational scenarios identified for this ConOps.

## 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.

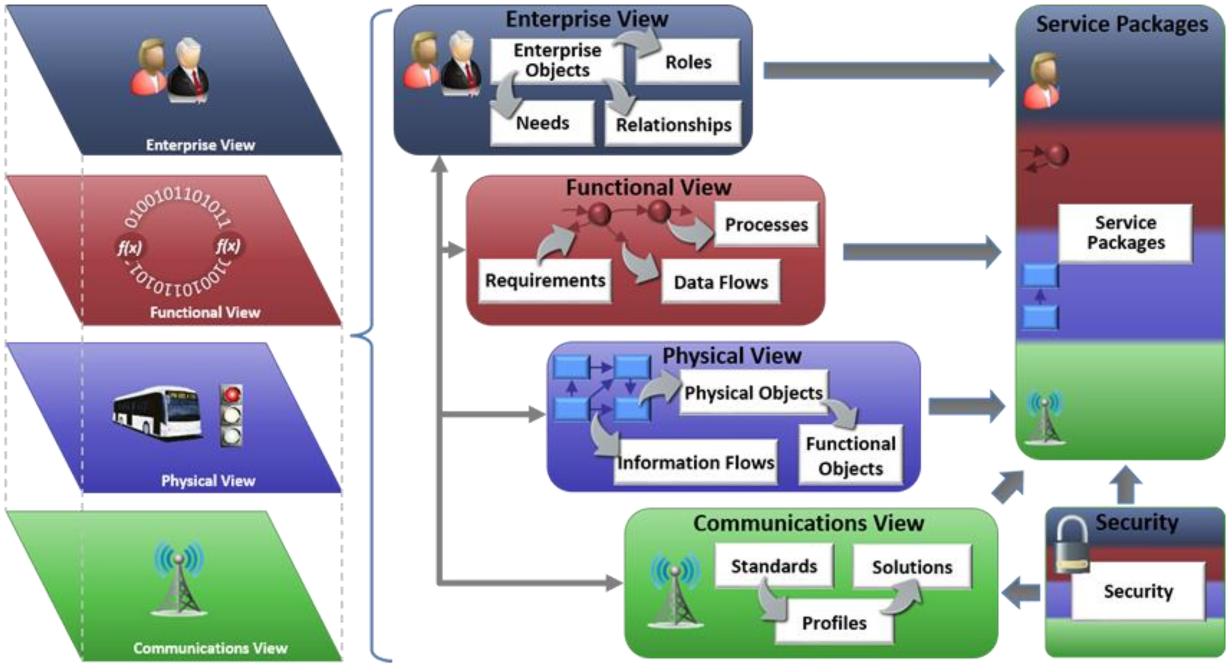



**Figure 13. ARC-IT's interconnected components are organized into four different views of the reference architecture.**

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 800-53 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 800-53 was also performed as part of this 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.**

# Annex A
# Requirement Resources from NIST SP 800-53 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 800-53 organizes security controls into 20 families (see **Error! Reference source not found.**). 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 800-53 of which 206 have been initially identified as resources for requirements development.

**Table 1. NIST 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 800-53 Controls

**Error! Reference source not found.** 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 requirements development, it is recommended that the controls and enhancements listed are reviewed along with any related controls referenced within the descriptions. Table 2 is not intended to be exhaustive.

**Table 2. ATC Cybersecurity User Needs and Supporting NIST SP 800-53 Controls**

| UN # | User Need Title | NIST Controls and Enhancements |
|---|---|---|
| **2.7.1** | **Physical Security** | |
| 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 | Signal 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 | Sourced Bill of Materials | SR-3, SR-3(3), SR-4, SR-4(1), SR-4(2), SR-4(4), SR-5 |
| 2.7.2.3 | Facilitate Software Inventory | CM-8 |
| 2.7.2.4 | Software Bill of Materials | SR-3, SR-3(3), SR-4, SR-4(1), SR-4(2), SR-4(4), SR-5 |
| 2.7.2.5 | Inventory Tool Support | 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** | |
| 2.7.3.1 | Validate Software Is Authorized | 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 | Vulnerability Scanning | CM-11(2), CM-11(3), SI-3, SI-3(4), SI-3(8), SI-7(2), SI-7(6), SI-7(8) |
| 2.7.3.3 | Intrusion Detection | 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) |
| **2.7.4** | **User Accounts and Controlled Use of Administrative Privileges** | |
| 2.7.4.1 | Uniquely Identify Authorized Users | 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) |
| 2.7.4.3 | User Access Control | 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 |
| 2.7.4.4 | Default Passwords | 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) |
| 2.7.5.2 | Account Logging | AU-2, AU-3, AU-3(1) |
| 2.7.5.3 | Security Event Logging | AU-2, AU-3, AU-3(1), AU-12(3), CM-3(5), CM-5(1), SI-11 |

| UN # | User Need Title | NIST Controls and Enhancements |
|---|---|---|
| 2.7.5.4 | 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) |
| 2.7.5.5 | Security Monitoring | SI-4, SI-4(2), SI-4(5), SI-4(7), SI-4(14), SI-4(22), AC-9 |
| 2.7.5.6 | Operating Software Reporting | CM-6, CM-8, SA-10(1), SI-11 |
| 2.7.5.7 | Network Service Status | CM-6, SI-4, SI-4(2), SI-4(22) |
| **2.7.6** | **Networks, Protocols, and Services** | |
| 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 |
| 2.7.6.3 | Disabled Protocols, Services, and Ports | 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 |
| 2.7.6.7 | Secure Cloud Services | 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 |
| 2.7.8.2 | Valid Credentials | IA-9 |
| Error! Reference source not found. | **Authentication, Authorization, and Accounting**Error! Reference source not found. | |
| 2.7.9.1 | Configure Centralized Point of Authentication | AC-3(11), AC-3(12), AC-3(13) |
| 2.7.9.2 | Authentication Protection | AC-3(5), IA-5(7), IA-7, IA-5(13), IA-5(14), IA-6, SI-10(5) |
| 2.7.9.3 | Key Material Protection | AC-3(5), IA-5, IA-5(1), IA-5(2), IA-7 |
| 2.7.9.4 | Secure Authenticated Sessions | 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) |
| 2.7.9.5 | Trustworthiness | AC-4, CM-3(5), IA-3, SI-10(5) |

| UN # | User Need Title | NIST Controls and Enhancements |
|---|---|---|
| **2.7.10** | **Operating Platform and Applications** | |
| 2.7.10.1 | 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 |
| 2.7.10.2 | Application Reporting | AU-2, SI-4, SI-4(7), SI-11 |
| 2.7.10.3 | Application Portability | SC-27 |
| 2.7.10.4 | 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) |
| 2.7.10.5 | Facilitate System Software Updates | SI-2(4), SI-2(5), SI-2(6), SA-10, SA-10(1), SA-10(3), SA-10(6) |
| **2.7.11** | **Resiliency** | |
| 2.7.11.1 | System Backup | CP-9 |
| 2.7.11.2 | System Safe Mode | CP-12, SC-7(18), SC-24, IR-4(5), SI-7(5), SI-17 |
| 2.7.11.3 | Secure System Restore | CP-10, IR-4(5), SA-8(24), SI-17 |
| 2.7.11.4 | Emergency Power | PE-11, PE-11(1), SI-17 |

§