A Project Document of the ATC Cybersecurity Project

ATC Cyber Research Paper v01.02

Summary of Applicable Prior and Ongoing Cybersecurity Research and Practices

September 3, 2022

A report in support of:
USDOT Contract # FHWA 693JJ321D000005
Task Order # 693JJ321F000419

For use by:
Deborah Curtis, Highway Research Engineer
United States Department of Transportation
Task Order Contracting Officer's Representative (TOCOR)

Siva Narla, Senior Director, Transportation Technology
Institute of Transportation Engineers
ATC Program Manager

Nicola Tavares, Technical Products Manager
Institute of Transportation Engineers
Project Manager for the ATC Cybersecurity Project

Members of the ATC Cybersecurity Steering Committee

Project Team for the ATC Cybersecurity Project

CHANGE HISTORY

Version	Date	Editor	Notes
01.02	09/03/22	Ralph Boaz	Updated document based on USDOT comments.
01.01	7/28/2022	Ralph Boaz	Updated document based on USDOT comments.
01.00	6/21/2022	Ralph Boaz	Initial draft version submitted to USDOT for review.

CONTENTS

TABLE OF FIGURES

1 INTRODUCTION

This paper has been prepared 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 primary 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. 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 Concept of Operations (ConOps), a Systems Requirement Specification (SRS), and a System Design Description (SDD) 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.

The purpose of this document is to summarize the investigation into projects, reports, standards, frameworks and other documents that may serve as resources or guidance for the project. The paper is organized in five sections and an appendix. Section 1, “Introduction,” provides an overview of this paper. Section 2, “Background,” provides a description of the intelligent transportation system (ITS) infrastructure covered by the project and terms used to assist readers that are less familiar with the subject. Section 3, “System Scope,” identifies the scope of the project in terms of a physical architecture. Section 4, “Research,” describes the resources investigated. Section 5, “Recommendations,” provides recommendations from the project team. Appendix A, “Acronyms and Abbreviations,” provides definitions of terminology used in this paper.

2 BACKGROUND

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 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.

There are multiple terms used for such systems such as “cabinet,” “field cabinet,” or “traffic cabinet.” The term Transportation Field Cabinet System (TFCS) is in this paper to be consistent with the term used in the ATC 5301 ATC Cabinet Standard. The general elements of a TFCS are described below and illustrated in Figure 1.

- 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.

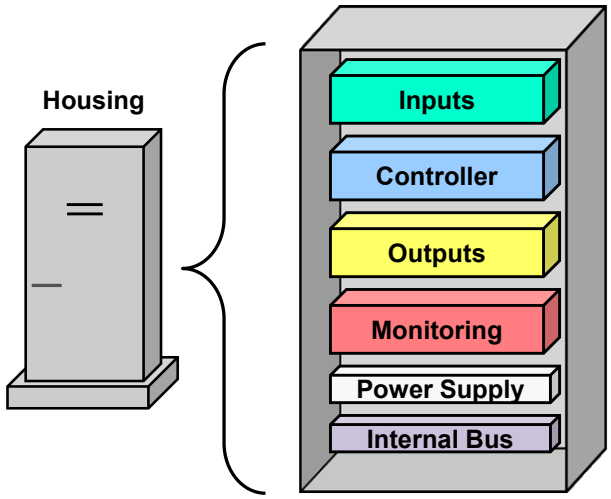

Figure 1. Elements of a Transportation Field Cabinet System.

Figure 2 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.

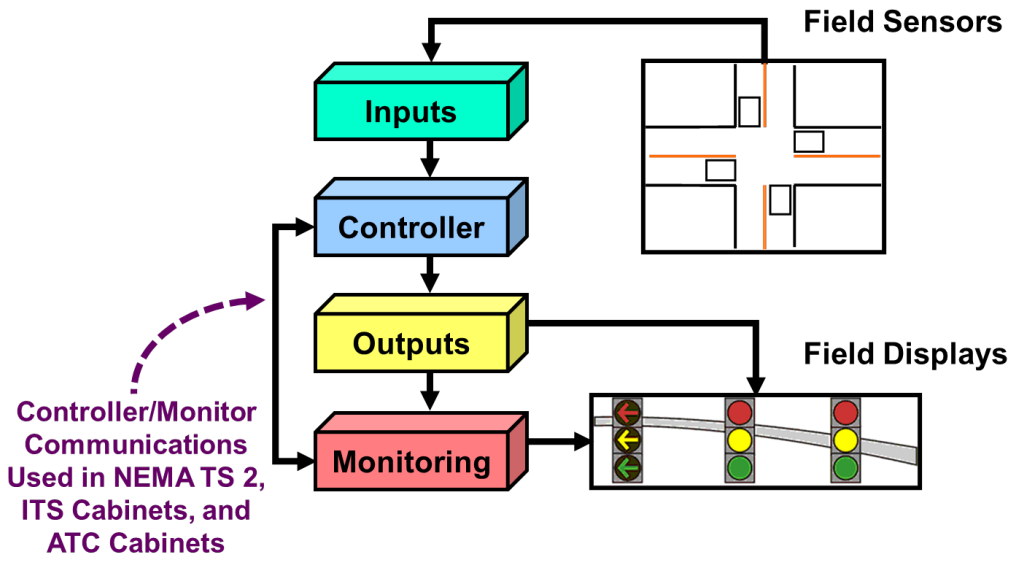

Figure 2. Basic operation of a Transportation Field Cabinet System.

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). They devices can be co-processors within the controller unit or separate devices within the cabinet system.

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 in 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.

2.2.1 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. Figure 3 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. The Engine Board connects to the Host Module using two 50-pin connectors as shown in Figure 4.

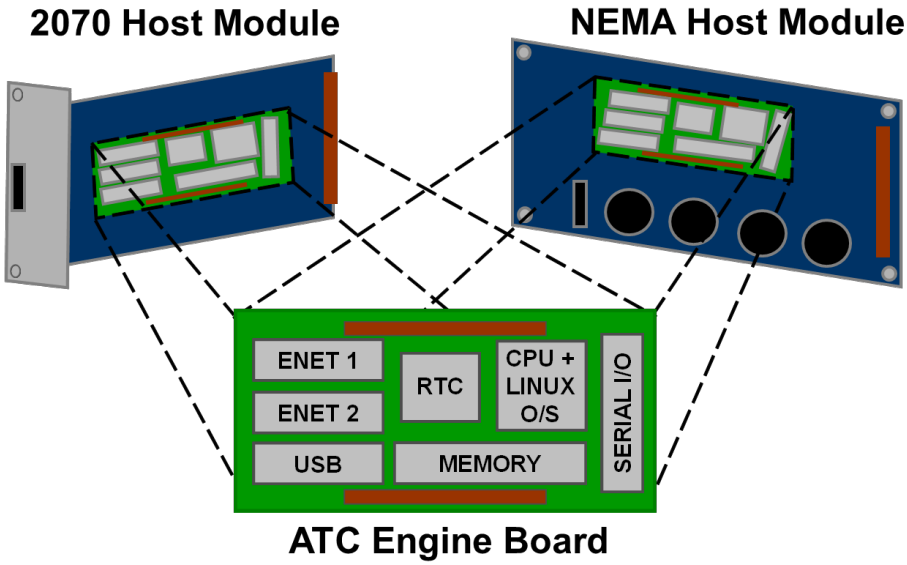

Figure 3. ATC Engine Board used to support different families of controllers.

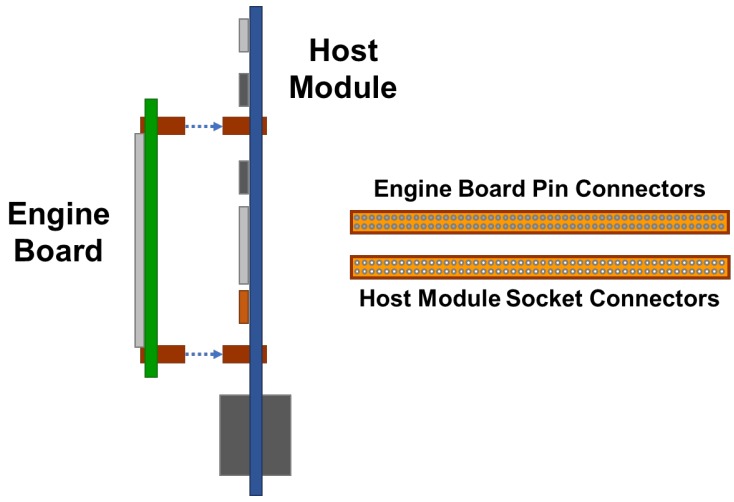

Figure 4. ATC Engine Board / Host Module connection.

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 5 (not all named ports are required for different configurations). In the configuration shown, Serial Ports 1-3 are for general use.

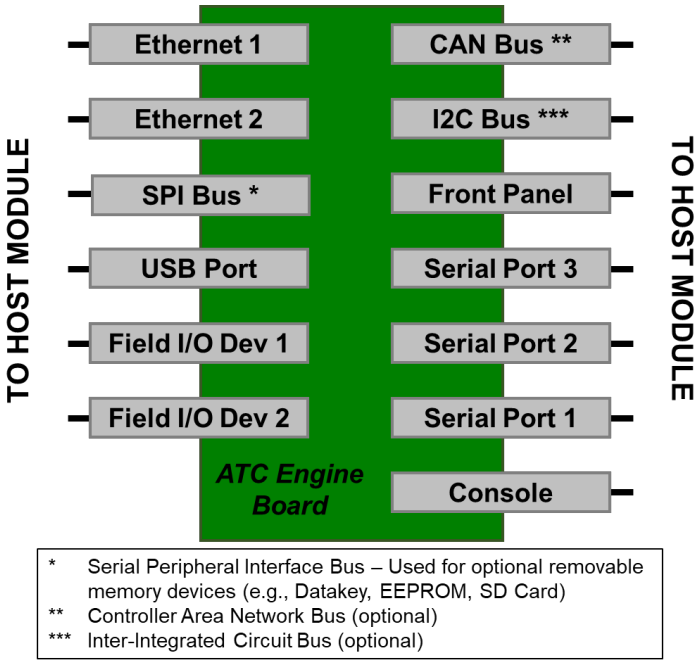

Figure 5. ATC Engine Board communications ports and their functions.

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 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 6.

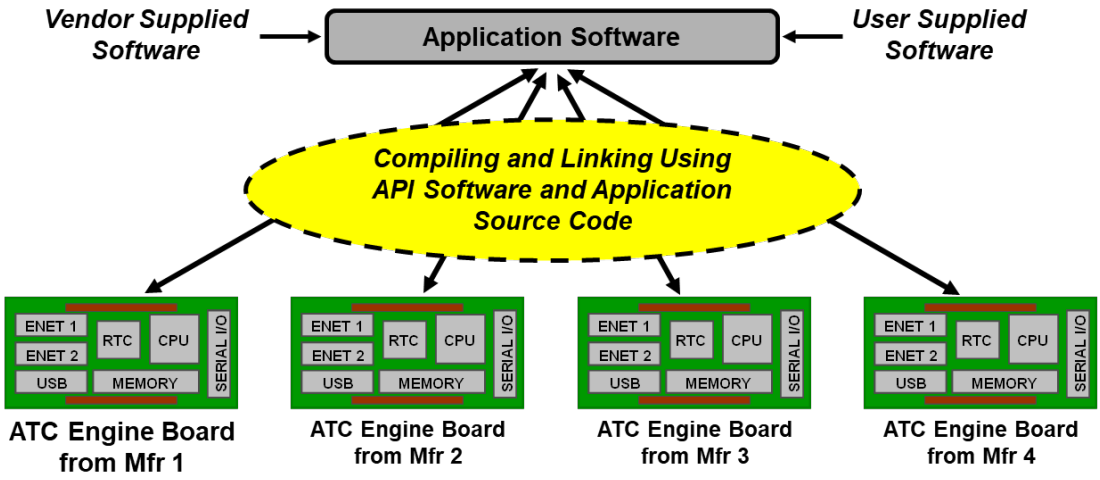

Figure 6. Application portability through compilation and linking of source code.

Figure 7 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 7, both users and application programs use the API Software to interface to ATC units.

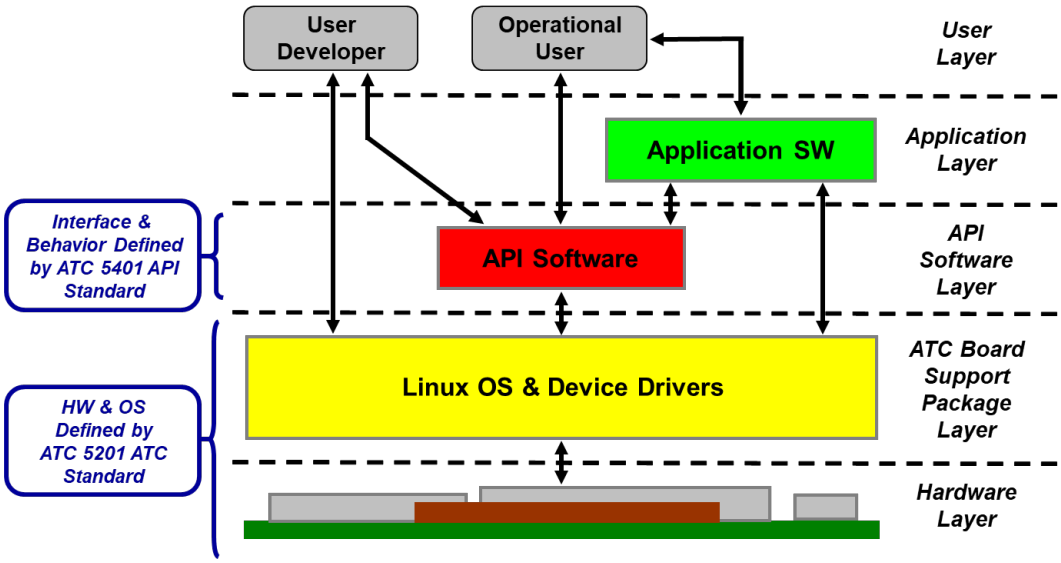

Figure 7. ATC software layered organization.

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 8 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. Figure 9 shows the ATC Configuration Information window. Users use this window to set and view system wide parameters (e.g., system time, Ethernet ports).

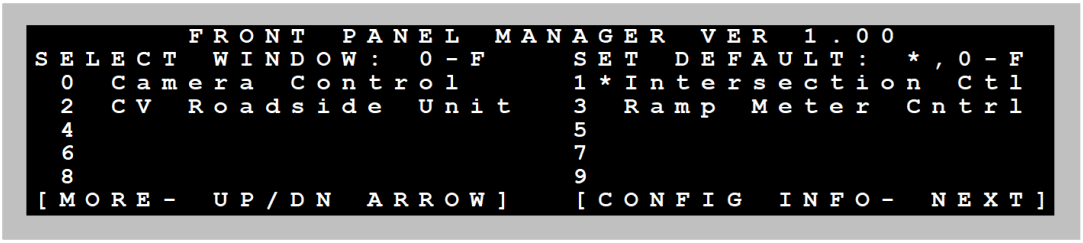

Figure 8. Front Panel Manager allows users to select an application program to put in view.

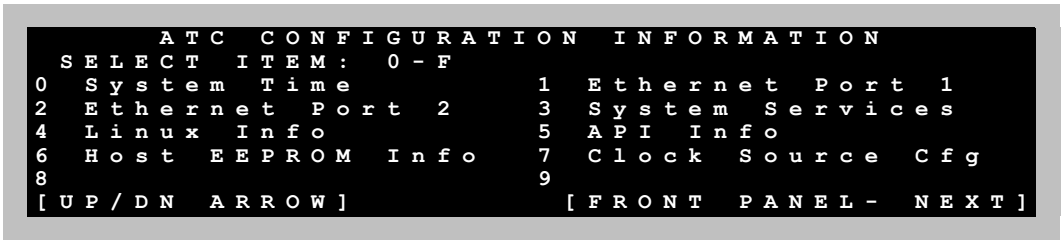

Figure 9. ATC Configuration Information allows users set and view system wide parameters.

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.

2.2.3 ATC 5301 ATC Cabinet Standard

ATC 5301 Advanced Transportation Controller (ATC) Cabinet Standard Version v02 is the latest version of ATC 5301. Figure 10 illustrates an example ATC Cabinet. It must be emphasized that not all cabinets will have this configuration. The components of the cabinet are color coded in a similar fashion to the general TFCS description in Section 2.1.

- 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 a 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.

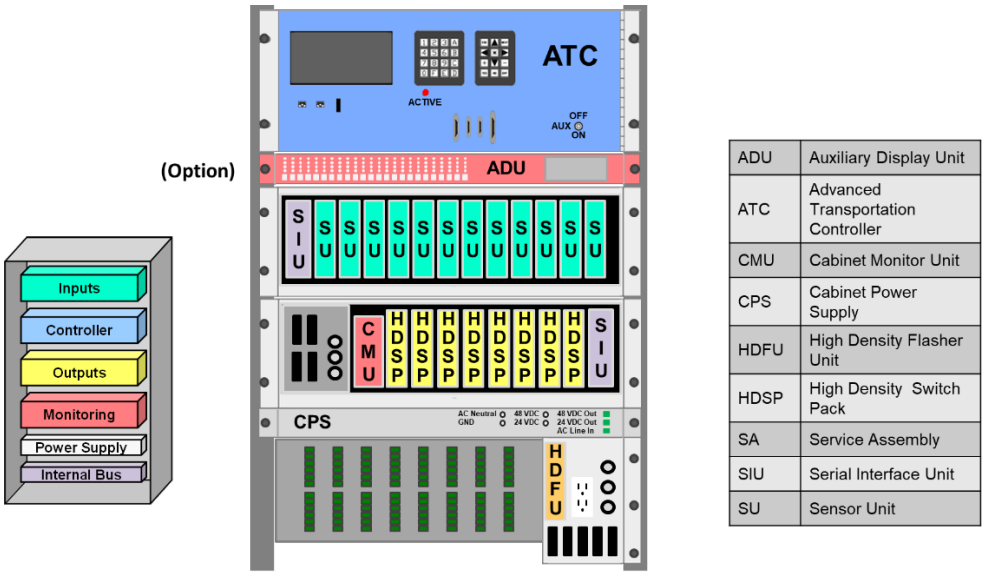

Figure 10. ATC Cabinet and components.

3 ATC CYBERSECURITY SCOPE

The ATC Cybersecurity Project scope is shown in Figure 11. The initial areas to investigate are identified but others may be brought out as the project advances. Cybersecurity requirements will also need to be established for the devices that are outside of the ATC standards but commonly used in cabinet systems (see the end of Section 2.1). Intrinsically, the cybersecurity measures taken in the ATC standards may impose requirements on the users of the equipment. These include engineers, traffic technicians, police, and IT staff.

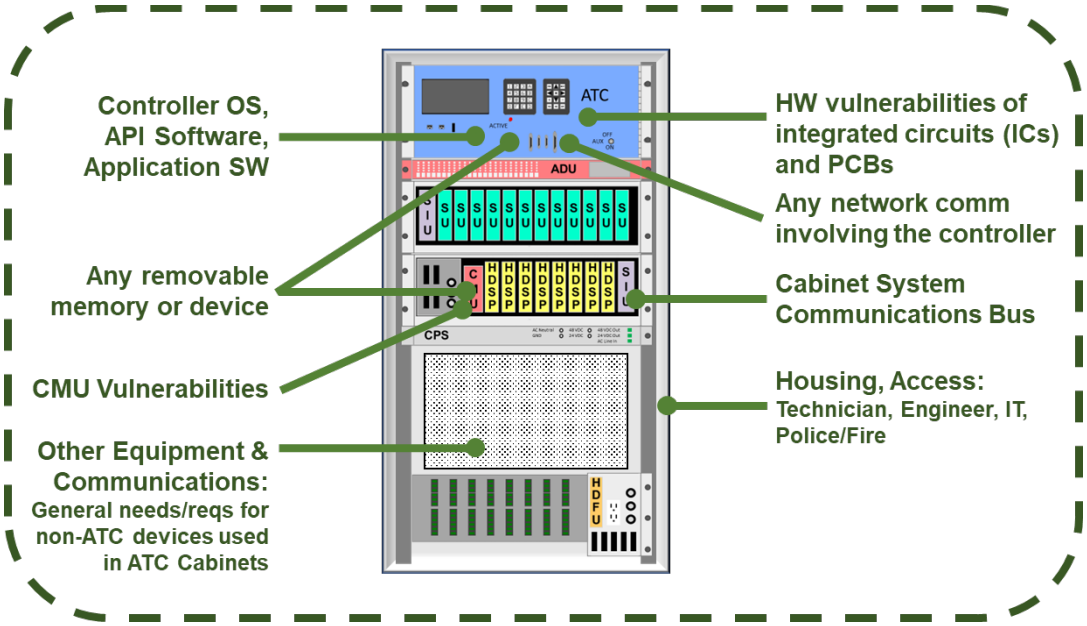

Figure 11. ATC Cybersecurity Project scope and initial areas for investigation.

4 RESEARCH

4.1 Approach

Research material was chosen to support the scope identified in Section 3. The research material consists of cybersecurity standards, threat frameworks, reports and guides, and past projects. An effort was made to narrow down the number of works researched by answering the question of what clear take-away or key point(s) can be extracted therein and used directly in developing a cybersecurity design for the ATC.

4.2 Research Material

4.2.1 Cybersecurity Standards

ANSI/CTA 2088, "Cybersecurity Standard for Devices and Device Systems**"**

This publication lists some basic cybersecurity guidelines for consumer devices such as IoT. The guidelines include device identifiers security, secured access, protection of data while being transmitted or while stored, use of industry standardized protocols for communication and cryptographic algorithms, data validation and event logging, software "patchability," and device reprovisioning capabilities.

NEMA Standards Publication TS 8-2018 Cyber and Physical Security for Intelligent Transportation Systems (ITS)

This standard addresses different aspects of security including those associated with field systems, communications and central systems. Those that pertain to field equipment should be addressed in the project.

4.2.2 Threat Frameworks

Microsoft STRIDE Framework

STRIDE is a threat framework originally developed for software systems, but applicable to cyber-physical systems like the ATC. It takes the perspective of the defender and it categorizes threats at a high level of abstraction, according to: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

This threat framework can help identify possible attacks that could occur against the ATC, in order to formulate cybersecurity needs and requirements.

MITRE ATT&CK ™

ATT&CK™ is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It takes the perspective of the adversary and the procedures are described with a mid level of abstraction. The ATT&CK knowledge base is used to develop specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. MITRE ATT&CK now includes ICS (industrial control systems) as part of its matrices, and this is the reason there is no separate reference to it.

For the ATC, MITRE ATT&CK for Linux and MITRE ATT&CK for ICS are applicable to a large extent. Examining each threat listed therein can help with the exercise of building an attack tree; for example, how an attacker may get the ATC to be in an unsafe state. The attack steps in turn then can inform

mitigations, which feed into requirements and design of cybersecurity.

4.2.3 Reports and Guides

Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) Version 9.1, USDOT

ARC-IT contains high-level designs for requirements for given service packages (i.e., applications). One relevant application for the ATC is under Traffic Management, namely "Traffic Signal Control." When a device is used for this purpose, it has a given set of security and other requirements. ARC-IT denotes it as "ITS Roadway Equipment." The class of device recommended is Device Class 3. The controls applicable to this device class are found in the web page for Device Class 3. One way to distill these controls would be to say that the ATC, as a Device class 3, should meet the following requirements:

- Compliance with National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 Level 3 physical security requirements for its hardware security module (HSM), if equipped with an HSM
- Support for remote and physical management via SNMPv3, requiring role-remote authentication in both cases. (source: Connection Intersections Implementation Guide, v1.0).

CIS Controls V7: Implementation Guide for Industrial Control Systems, Center for Internet Security

This document contains high-level guidance on securing ICS from the Center for Internet Security (CIS). There are 20 security controls, at a mid-level of detail. Some are applicable to the ATC itself as a device, others are applicable to the organization deploying and managing such devices. To use this document, each applicable control should result in a cybersecurity requirement. For example, "Controlled Use of Administrative Privileges" could mean that an ATC should be manageable by a limited number of administrators with certain privileges. This document can be a source of practical needs and requirements for the ATC Cybersecurity Project.

NIST Cybersecurity Framework, Version 1.01, "Framework for Improving Critical Infrastructure Cybersecurity"

This document from the National Institute of Standards and Technology (NIST), provides a set of guidelines for mitigating organizational cybersecurity risks based on existing standards, guidelines, and practices. It is considered a best practice for computer security. This update includes the following:

- Authentication and identity
- Self-assessing cybersecurity risk
- Managing cybersecurity within the supply chain
- Vulnerability disclosure.

It is relevant to the ATC Cybersecurity Project because these topics are applicable to securing the ATC cabinet.

NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"

This NIST document is a catalogue of security controls meant to cover a wide range of industries. It provides a common language for both business stakeholders, information technology (IT), and cybersecurity engineers. Because of its broad and comprehensive nature, it cannot drive the decisions for standards for cybersecurity for a given type of device. Instead, it may help formulate design prescriptions at the last stage of development of the standard. For example, instead of saying "all software updates to the ATC should be signed," one can state it more formally as in section CM-14 of this standard, "SIGNED COMPONENTS Control: Prevent the installation of [….] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization."

NIST SP800-63B, "Digital Identity Guidelines: Authentication and Lifecycle Management"

This NIST document is applicable to the administration and IT support of the ATC devices during operation in the field. It contains requirements for IT management in terms of password ("memorized secret") strength, login timers, single/multi-factor authentication, etc.

NIST SP800-82 Rev. 2, "Guide to Industrial Control Systems (ICS) Security"

This NIST document provides guidance to secure the following: Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). Their unique performance, reliability, and safety requirements are taken into account. This document includes an ICS overview including system topology, and it lists typical threats and vulnerabilities, along with security controls to mitigate the associated risks. This document can serve as a cross check for threats identified (possibly from guidance in other documents), as well as a source for mitigations (security controls) to be recommended as part of the project.

NIST SP800-160 Vol. 1 Rev. 1 (draft), "Engineering Trustworthy Secure Systems"

This NIST guidance attempts to "infuse systems security" into the existing systems engineering processes, making Systems Security Engineering (SSE) as a sub-discipline of Systems Engineering (SE). In essence, this guidance would be most applicable if the ATC standard was now being developed from ground zero, so that security is taken into account from the beginning. Some sections are not directly applicable (e.g., the lifecycle processes of Chapter 3).

The following points are applicable:

- The systems security engineering tasks to be undertaken, as outlined in Section 2.1.
- System security is a holistic property; all system elements have to meet security requirements.
- A system needs only to be "as secure as reasonably practicable" (ASARP). Stakeholder asset-protection needs and security objectives are the starting point.
- Part of security is the concept of intent, which has two parts that both have to be satisfied: design intent and user intent. Security achieves only the authorized and intended system behaviors and outcomes
- Assets and their protection needs must be identified. Protection needs come from stakeholder perspective, system perspective, and engineering perspective. Consequences and type of asset loss must be evaluated.
- Asset protection needs are satisfied via security requirements and security policies.
    - Protective measures may include any aspects of the system: machine part, human portion, and physical environment
- Trustworthiness (demonstrating security) is achieved done via building "assurance cases" for acceptable security and showing that case is satisfied.

NIST SP800-160 Vol. 2 Rev. 1, "*Developing Cyber Resilient Systems: A Systems Security Engineering Approach"*

This NIST guidance focuses on cyber resiliency engineering which is a specialty systems engineering discipline to be applied in conjunction with resilience engineering and systems security engineering to develop more survivable, trustworthy systems.

The cyber resiliency design model incorporates the ability to anticipate, withstand, recover, and adapt to adverse conditions, stresses, attacks or compromises of the system. This is a threat-driven approach to designing cyber systems.

The following sections in Volume 2 are applicable to the ATC project:

- How cyber resiliency concerns can be addressed as part of the life cycle processes in systems security engineering
- Controls in NIST Special Publication 800-53, Revision 5, which directly support cyber resiliency
- An approach for adversary-oriented analysis of a system and applications of cyber resiliency, a vocabulary to describe the current or potential effects of a set of mitigations, and a representative cyber threat coverage analysis for cyber resiliency approaches.

Similar to analysis regarding Volume 1, the second volume would be most applicable to the ATC system if it was being designed from the ground-up for cyber resiliency. However, the MITRE ATT&CK Threat Framework (Section 4.2.2) incorporates a similar resiliency framework as is referenced in Volume 2 and utilizes risk management techniques by incorporating a multitude of facets including assets, threats, vulnerabilities and controls which are to be jointly evaluated with the variables of probability and impact. These evaluations could be done at a later stage of the ATC project and analyzed while taking account of the cyber resiliency design model.

The Minimum Elements for a Software Bill of Materials (SBOM), National Telecommunications and Information Administration, U.S. Department of Commerce, 2021

SBOMs provide those who produce, purchase, and operate software with information that enhances their understanding of the supply chain, which enables the ability to track known and emerging vulnerabilities and risks. An SBOM is the full list of every item that is needed to build an application. It identifies all parts, including direct OSS dependencies, indirect OSS dependencies, open-source packages, vendor agents, vendor APIs, and vendor software development kits. Executive Order 14028 (2021), “Improving the Nation’s Cybersecurity” contains a provision for SBOMs. The ATC Cybersecurity Project will be addressing software.

4.2.4 Past Projects / Papers

CTI 4501 v01.00 Connected Intersection Implementation Guide, Connected Intersections Committee, 2021

This project leveraged the experience of the CV technology deployments and produced a CI Implementation Guide that addresses the gaps, ambiguities, and incongruous practices discovered. The CI Implementation Guide provides guidance to all those active in the CV community to help achieve consistent infrastructure-vehicle interoperability across the United States. This project identified security concerns for connected intersections which can be carried over to the ATC Cybersecurity Project.

“Exposing Congestion Attack on Emerging Connected Vehicle Based Traffic Signal Control,” Qi Alfred Chen, Yucheng Yin, Yiheng Feng, Z. Morley Mao, Henry X. Liu, University of Michigan, 2018

This academic paper references a spoofing attack traffic signal control via connected vehicles (CVs). The researchers targeted the USDOT-sponsored design of a system called Intelligent Traffic Signal (I-SIG) which performs traffic signal control. Their objective was to exploit the I-SIG system via physical access, wireless communications, or malware sent to the traffic signal controller. While this paper mostly focuses on the connection between the CV and the RSU, it does critique weak security for the traffic control system and algorithms.

“Green Lights Forever,” Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman, Electrical Engineering and Computer Science Department, University of Michigan, 2014

The research team for the “Green Lights Forever” project found a few vulnerabilities in traffic light systems including unencrypted wireless connections, default usernames and passwords, and a debugging port left open. The team also discovered that anyone with an SDR (software defined radio) could communicate on

a 5.8 gigahertz frequency and access the entire unencrypted network from a single point of entry. Their recommendations included not using default passwords (in this case, passwords were found via an Internet search) and not using unencrypted communications.

NCHRP 03-127 Cybersecurity of Traffic Management Systems, Task 3 – Penetration Test Results for Adversarial Assessment, National Cooperative Highway Research Program (NCHRP), Transportation Research Board

This NCHRP project performed penetration testing on various transportation field devices including controllers and cabinet systems. The research team identified numerous attack paths and weaknesses. There were significant security shortcomings across all tested devices and manufacturers. This project provides insight into methods used in attacks and lists specific deficiencies in controllers, traffic cabinet system, and other equipment. This applies directly to the ATC Cybersecurity Project.

NTCIP 9014 v01 National Transportation Communications for ITS Protocol (NTCIP) Infrastructure Standards Security Assessment (ISSA), NTCIP Joint Committee

NTCIP standards provide ITS communications for both center-to-field (C2F) and center-to-center (C2C) communications. This project analyzed existing NTCIP C2F Standards and the manner in which they are deployed. It then provided guidance on how best to implement security for NTCIP C2F communications. Historically, C2F communications were based on Simple Network Management Protocol Version 1 (SNMPv1). NTCIP 9014 provides a plan to move the NTCIP C2F standards to base of SNMPv3 which has authentication and encryption built into the protocol. This move to SNMPv3 is already taking place with a follow-on project. Communications will be addressed within the ATC Cybersecurity Project.

Understanding the Security of Traffic Signal Infrastructure, Zhenyu Ning, Fengwei Zhang, and Stephen Remias, COMPASS Lab, Wayne State University, 2019

The Understanding the Security of Traffic Signal Infrastructure paper was the result of a research project that examined the vulnerabilities of traffic signal systems. This paper identified some attack vectors that may be useful to the project.

5 Recommendations

The sources identified in Section 4.2 contain material that will support the ATC Cybersecurity Project in some fashion. Some materials will be primary sources and others will be secondary sources. Further investigation during the course of the project may be undertaken, branching from the sources already listed. Primary sources that are expected to provide direct needs and requirements are as follows:

- NEMA Standards Publication TS 8-2018
- CIS Controls V7: Implementation Guide for Industrial Control Systems
- The Minimum Elements for a Software Bill of Materials (SBOM)
- NCHRP 03-127 Cybersecurity of Traffic Management Systems
- NTCIP 9014 v01 National Transportation Communications for ITS Protocol (NTCIP) Infrastructure Standards Security Assessment (ISSA)
- CTI 4501 v01.00 Connected Intersection Implementation Guide
- Understanding the Security of Traffic Signal Infrastructure

The following sources may assist in performing threat analysis although it is expected that an abbreviated customized methodology will be used:

- MITRE ATT&CK ™
- Microsoft STRIDE Framework

APPENDIX A ACRONYMS AND ABBREVIATIONS

Term	Meaning
AASHTO	American Association of State Highway and 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
ECLA	External Control Local Application
FIPS	Federal Information Processing Standards
HDLC	High-level Data Link Control
HDSP	High-Density Switch Pack
HSM	Hardware Security Module
HW	Hardware
I/O	Input/Output
IC	Integrated Circuit
ICS	Industrial Control System
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
NCHRP	National Cooperative Highway Research Program
NEMA	National Electrical Manufacturers Association
NIST	National Institute of Standards and Technology
NTCIP	National Transportation Communications for ITS Protocol
OS	Operating System
OSS	Open Source Software
PCB	Printed Circuit Board
PLC	Programmable Logic Controller
RTC	Real-Time Clock
RAM	Random Access Memory
RSU	Roadside Unit
SBOM	Software Bill of Materials

SCADA	Supervisory Control and Data Acquisition
SDD	System Design Description
SE	Systems Engineering
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
SW	Software
TEES	Transportation Electrical Equipment Specifications
TFCS	Transportation Field Cabinet System
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