Added Security for your Traffic Signal Network
To Protect Your Traffic Control Devices
Date: 22 September 2014
Document Number: AN2152

Purpose
You can use the information in this document to help secure Internet Protocol (IP) Networks that contain traffic control devices. The focus of this document is IP communications security, not Serial data network security.

Here we summarize basic concepts that concern a Traffic Engineer. It is not our intention to explain network security in detail. To understand the information, you should have a basic knowledge of networking concepts and terms.

Note: We recommend the USDOT/FHWA\(^1\) Office of Operations – Cyber Security Advisory, August 2014, attached\(^2\), as a good supplement to this document.

Introduction
As you make adjustments for network security, a good guide is to “provide enough access so as not to inhibit productivity, yet provide enough restriction to ensure reasonable security.”

This document divides network security into:
- Physical security—access to devices at the intersection
- Logical security—access across a network(s).

Physical Security
Each traffic control cabinet on the street should have an applicable locking mechanism to prevent intrusion. An unauthorized person that enters a traffic control cabinet could access the IP network and have unlimited access to the entire network—both cabinet to cabinet and cabinet to central operations. Central systems, such as Centracs, can monitor the traffic control cabinet and set an alarm when there is an open cabinet door; if authorized personnel were not expected at that location, traffic operation personnel could then investigate the security violation.

Also, within the traffic control cabinet, secure any equipment that has a user interface with a unique Personal Identification Number (PIN) or password. To restrict data access to authorized personnel, you can program the Econolite ASC/3 and Cobalt controllers and a 2070 controller with ASC/3-2070 software with unique passwords.

---

\(^1\) USDOT/FHWA = United States Department Of Transportation/Federal Highway Administration

\(^2\) Refer to the last two pages of this document for the Cyber Security Advisory.
Logical Security

It is important to understand the communications protocols used in Network Security and how best to secure them.

National Transportation Communications for ITS Protocol (NTCIP)

The transportation industry is fully committed to the NTCIP standard. This protocol suite covers a number of ITS devices. The NTCIP protocols have no encryption because it is understood that the devices that use these protocols are on a secure network.

Internet Protocol (IP)

IP is the primary communications protocol for passing information between devices on a network. IP is designed to allow devices from different networks located anywhere in the world to communicate with minimal intervention. If left unsecured, users anywhere could access a computer on a network.

From a high-level network view, threats can come from two distinct locations:

- Outside of your network.
- Inside of your network.

Outside threats can be divided into two areas:

Wired Networks – standard LAN cabling, fiber optic cabling, voice-grade twisted pair cabling and leased circuits: To help restrict unwanted traffic onto the network, firewalls are the easiest first step. Occasionally, leased circuits (such as a DSL) terminate on a public network. If you use DSL, use a Virtual Private Network (VPN) tunnel to securely route data.

Wireless Networks – In addition to the steps taken to secure wired networks, with wireless connectivity we recommend you enable encryption. Also, if it is not needed, disable the Service Set Identification (SSID) Broadcast feature. If you use a cellular service for communication with field devices, be aware of the level of security provided by your cellular service mode. One mode of cellular-based connectivity provides a direct connection to the Internet resulting in worldwide public access; we recommend you secure this connection with a firewall and route all data via a VPN connection, as mentioned above. We highly recommend that you use a private Access Point Name (APN) and Dynamic Mobile Network Routing (DMNR) to securely route IP traffic to/from your operations center to field devices.

3 NTCIP is a joint standardization project between AASHTO, ITE, and NEMA.
4 DSL = Digital Subscriber Line
Possible **inside** threats to the network are people that can connect within the trusted realm of a particular network. For this, consider restricting access by IP subnet and limiting access to ports. You can do this within the configuration of the routers that make up the network.

Consider this diagram:

![Diagram of network](image)

We recommend that you restrict access to the Traffic Signal Field Network by IP subnet and segregate it from the Municipality Wide Area Network (WAN). You can do this easily with an Access Control List (ACL) within the network router. This permits maintenance access for the Traffic Signal Technicians and Administrators without connecting the Traffic Signal Field Network traffic to the Municipality WAN. You can enable more access as needed.

To make sure that your traffic network is compliant with IT standards, we highly recommend that your Traffic Engineers talk with the applicable IT security personnel about policies and procedures.

**File Transfer Protocol (FTP) and TELNET**

You can access some devices in the traffic control cabinet with FTP or Telnet. As well as the security measures mentioned above for securing Internet Protocol, we highly recommended you change the manufacturer default password. Also, if available, we recommended you use SSH\(^5\) as an alternate to Telnet.

For Application Notes and assistance in changing the default username and password for the Econolite Controller Product Line, please contact Econolite Technical Support.

---

\(^5\) SSH = Secure Shell
Purpose of Advisory

The purpose of this advisory is two-fold: 1) To make DOTs aware of a recent article published by the University of Michigan on “a number of security flaws that exist due to systemic failures by the designers” and 2) reinforce and build upon known solutions to hardening the center to field network.

Summary of University of Michigan Paper

The University of Michigan paper is titled, “Green Lights Forever: Analyzing the Security of Traffic Infrastructure” where a number of vulnerabilities in a wirelessly networked traffic signal system were identified, explained, and demonstrated. This was done with cooperation of a local transportation agency (see paper attached). The impacts are significant and push the envelope of safe operation to the MMU and Conflict Monitor in guaranteeing safety. We also feel this research paper provides sufficient information for other attackers to replicate these attacks.

Short term solutions To Hardening Center to Field Wireless Network

The vulnerabilities revealed by University of Michigan and the DMS SUN_HACKER incident both exploit in significant fashion known weakness of improperly configured wireless communication network. Wireless network are still an important component of transportation operations, but they must be operated in a safe and resilient manner. AASHTO, along with members of the Transportation Systems Management and Operations Subcommittee and the Federal Highway Administration, have made recommendations for immediate action in the past. The following steps build upon those recommendations:

1. Devices shall never deploy in the field with factory default passwords
   1.1. This will include all equipment on the communication path, inclusive of edge devices, routers, modems, and traffic management center.
   1.2. Use a strong password based on recommended best practices
   1.3. Tips on stronger password can be found here - https://www.us-cert.gov/sites/default/files/publications/PasswordMgmt2012.pdf

2. Use a VPN to encrypt traffic when using commercial wireless services

3. Immediately enable logging of traffic on the center to field network. Log files are critical for forensic analysis if there is an incident. It is also needed for more advanced protection systems at a later date.

4. Immediately enable any encryption services built into your wireless equipment. Order of preference shall be WPA2-Personal, WPA2-Enterprise, WPA, and finally WEP only if no alternative is available. Please note that WEP security is completely compromised, but the legal repercussion of circumventing encryption could be a deterrent.

5. Disable SSID broadcast from wireless equipment.

6. If possible, randomize the MAC address of the field devices and utilize MAC address filtering where possible.

7. Turn off or disable all unused ports and unnecessary services (telnet, ping, ftp, etc) in all field devices.
These are recommended steps for immediate action that should be taken if wireless communication is utilized in your transportation system. There will be operation and maintenance labor cost to plan and implement these recommendation. There should not be any additional cost to adopt these recommendations, but it could not be ruled out due to the number of different equipment currently in use. There are other steps that can be taken to further harden the transportation network against attack. These steps are not a replacement for a comprehensive cyber security plan.

Where To Report Suspicious Activity

In the near term, the following are the recommended reporting procedures.

1. In cases with **no injuries, property or facility damage**, Suspicious Activities should be reported to ICS-CERT (ics-cert@hq.dhs.gov) and your State’s FHWA Division Office.

2. In cases where **there are injuries, property or facility damage**, Report the incident to Law Enforcement, followed by ICS-CERT (ics-cert@hq.dhs.gov), and your state’s FHWA Division Office.