Application Note AN2013-15

SEL ICON™ Cybersecurity

Ken Fodero, Paul Robertson, and Rhett Smith

INTRODUCTION

The SEL ICON™ synchronous optical network (SONET) multiplexer was designed with an emphasis on communications system requirements for dependable communications for critical infrastructure. SEL has been providing security features in their products from the first relays released in the 1980s and continues to lead the industry with security features.

This application note describes security features built into the ICON and the testing performed to ensure security robustness. Protection against unwanted or unauthorized system access is only one part of a complete solution. It is equally important for equipment to send alarms and keep records to increase situational awareness when events occur.

SECURITY FEATURES

There are many features that come together in the ICON to provide a very high level of security against unauthorized access attempts, as well as provide documentation of these attempts. The following subsections discuss these features and the benefits they provide.

Default Password Protection

Every ICON network has only one set of passwords (no backdoor or service account). If the default passwords are enabled, the system will have a standing alarm indicating that the default user accounts are active. The only way to clear the alarm is to change the passwords.

User Access

SNMPv3 is the only communications protocol supported for network management and craft interface. SNMPv3 provides the encryption and authentication of each frame sent for local and remote access. See [1] for more details about SNMPv3 security.

Disabling of Unused Communications Ports

All communications ports have the ability to be disabled and are disabled by default. Regulations require that all unused ports be disabled. Additionally, the network management access ports on each device can be disabled. This allows for additional security and control of who has access to the network.

Locking of Media Access Control (MAC) Addresses at Ethernet Ports

The ICON is typically deployed in static networks. This means that the control systems connected to the Ethernet ports are static, and connected devices are permanently connected. By locking the MAC addresses per port when the system is commissioned, only the devices connected at the time of lock will be accepted on that port. Additionally, if a device is removed from an active port, an alarm is sent. If a device with a different MAC address is inserted, then communication with the new device is blocked and an additional alarm is sent.

Use of Pipes to Segregate Critical Systems

Data segregation is an important attribute in network management because it controls how bandwidth is allocated to different users and limits which network devices or ports have access to specific data. Data segregation is also important for network security. In networks carrying data for critical systems, it is a recommended best practice to segregate protection traffic or operational technology (OT) traffic from noncritical information technology (IT) traffic. Time-division multiplexing (TDM) provides security by segregating data into separate time slots and transporting the data to dedicated endpoints or ports. The end user or application only sees data that are intended for its use. Ethernet supports the segregation of traffic through the use of virtual local-area networks (VLANs). However, the use of VLAN technology alone does not provide complete traffic segregation within an Ethernet-based network. By combining the attributes of TDM and Ethernet, it is possible to build isolated Ethernet pipes that exist within the TDM structure to completely isolate dedicated Ethernet services.

In a denial-of-service (DoS) attack, the target device is saturated with communications requests that overload the local Ethernet switch message buffers, thereby affecting the target Ethernet pipe and all local Ethernet services. Using pipes for other Ethernet services prevents the attack from saturating Ethernet traffic traveling in other Ethernet pipes that are running on the SONET line transport between other nodes in the network. In addition, TDM allows the network manager to control which Ethernet pipes are dropped at each node, allowing critical services to only be dropped at selected nodes. The network manager can restrict the number of Ethernet pipes that an attacker can target from a single node. This approach maintains the flexibility of Ethernet and adds the dedicated network management and traffic segregation characteristics of TDM. See [2] for more details on how this is accomplished.

Secure Distribution of High-Accuracy Time

Each ICON contains an integrated Global Positioning System (GPS) receiver and local clock for holdover timing. A typical ICON network uses at least two nodes for GPS timing, with one site acting as a primary reference source and the other as a secondary. The GPS receiver provides a Stratum 1 reference that is used for SONET network timing and the generation of high-accuracy (less than 1 microsecond) IRIG-B for distribution to local intelligent electronic devices (IEDs). Figure 1 shows IRIG-B being generated as a timing reference for the SEL-3530 Real-Time Automation Controller (RTAC) and two SEL-411L Advanced Line Differential Protection, Automation, and Control System Relays for line current differential measurements. Multiple GPS clock references combined with holdover clock sources and a wide-area fiber network provide a time distribution network that is resilient against the loss of GPS. The ICON has taken resilient time distribution one step further by implementing methodologies to detect and mitigate GPS spoofing attacks. Through the monitoring of each active GPS receiver on the network, it is possible to detect a spoofing attack and selectively prevent a node with a suspect GPS signal from being used for network timing.

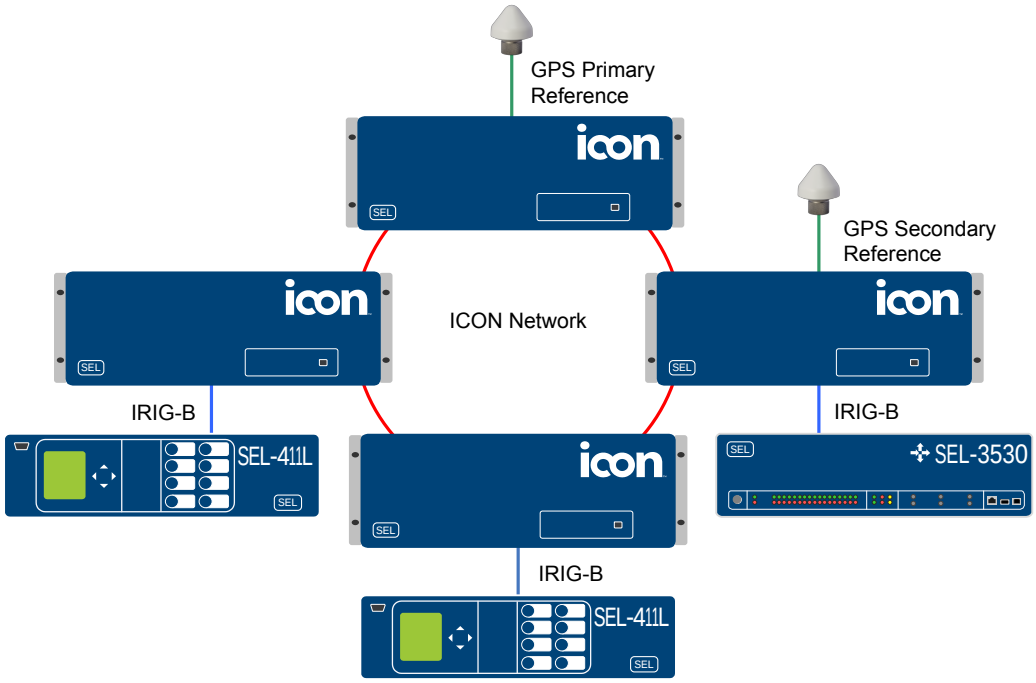

Figure 1 Precise Time Distribution

Encryption of the SONET Transport

The ICON can be optionally equipped with an OC-48 encryption module, which provides strong advanced encryption standard (AES) 256-bit encryption of the SONET payload data. The encryption process introduces a less than 1 microsecond delay, resulting in a negligible increase in overall latency for data circuits running across the network. The ICON Crypto Module (SEL-8029-01) provides additional security beyond the station security perimeter. Audit logs for the session key and session updates are included, providing an audit trail for security reporting procedures.

Logging, Alarming, and Reporting of Events

Each ICON node is capable of storing up to 40,000 nonvolatile time-stamped event records. These records include information about the following:

- Login attempts, both successful and unsuccessful.
- Settings changes.
- Firmware updates, both successful and unsuccessful.
- Disconnection of Ethernet devices from active ports.
- Connection attempts of devices with unauthorized MAC addresses.

A system security report can be generated for all events that have occurred during a selectable time period.

Negative Testing

The ICON network management port is routinely subjected to negative testing. This testing subjects the ICON to known methods of attacks as well as invalid message conditions or intelligent fuzzing. This continued testing is an important part of the development process to verify security robustness in every firmware release.

REFERENCES

[1] K. Fodero, "SNMPv3 Security Features," SEL Application Note (AN2011-01), 2011. Available: http://www.selinc.com.

[2] K. Fodero, "Advantages of Using Ethernet Pipes to Segregate Networks," SEL Application Note (AN2013-14), 2013. Available: http://www.selinc.com.

LAN2013-15

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com