

# *Securing Critical Industrial Systems With SEL Solutions*

Tom Bartman and Kevin Carson

---

## **INTRODUCTION**

The overall security of critical infrastructure around the world is essential to ensuring the safe, reliable, and available services that society relies on for daily life. Without security, the services provided could be disrupted, greatly impacting their availability. Industrial control systems (ICSs) are responsible for the safe and reliable operation of these services. ICSs are the backbone of the electric power system, water and gas systems, and manufacturing and production systems. It is imperative that these systems be built and maintained with security in mind. Threats against integrated systems can come from hackers, terrorists, and countries with sophisticated information warfare plans and capabilities [1].

The systems that monitor, control, and protect modern ICSs have come under increased risk. This increased risk can be attributed to products becoming more complex, with more electronic capabilities and more communications. The energy sector is also under the increased risk of security incidents. Since the development of the communications protocols used in data acquisition, protection, and control, threats have emerged that put the availability of services and assets at risk. Therefore, it is necessary to make every effort to provide protection against these threats.

While the protection and security of physical assets are important, the threat of a loss of availability is equally crucial for industries. A loss of availability is a loss of revenue and could lead to a significant impact to an organization. Some attacks are intended for sabotage while other attacks are intended for espionage. Therefore, when planning for security, it is important to recognize both tangible and intangible assets.

Many attacks target communications. Without secure communications, companies face significant risks. For example, substations in the electric power industry communicate over copper wire, fiber, radio frequency (RF), and satellites. Unfortunately, many of these communications paths are not adequately protected. When older legacy communications protocols were established, little-to-no emphasis was placed on security because the protocols were designed for closed-loop systems and relied on physical security. Because of their simplicity, legacy protocols are still widely used. Without proper safeguards, these protocols put communications at risk of data modification, unauthorized access, eavesdropping, or denial of service. Transmission Control Protocol-based (TCP-based) communications offer greater connectivity with less wiring; however, it is important to have an understanding of the methods required to secure them.

The belief that supervisory control and data acquisition (SCADA) communications are secure due to obscurity is no longer valid. The methods that attackers use today are very real and must be well understood in order to be countered.

SCADA systems are used in all critical industrial sectors, including electric power, chemical, manufacturing, mining, forest and paper, transportation, water and sewer, nuclear, petrochemical, and oil and gas. The electrical sector, focusing primarily on generation and transmission, has been regulated with mandated security requirements.

Schweitzer Engineering Laboratories, Inc. (SEL) provides cost-effective, highly reliable cybersecurity solutions for critical infrastructure systems. The purpose of this paper is to detail the cybersecurity risks on ICSs and discuss how to detect and counter these risks by applying processes and technology to keep the ICSs safely operating. The paper is an expansion of the technical paper titled “Securing Communications for SCADA and Critical Industrial Systems” [2].

## SCADA SYSTEMS

Communications protocols are necessary for the movement of electric power, gas, and oil and for transportation. Among communications protocols, SCADA is an attractive target for attacks. In recent years, much attention has been given to several computer viruses that specifically targeted programmable logic controller (PLC) and SCADA systems. Even today, SCADA protocols rarely use any authentication or encryption methods and often use cleartext communications to conduct their communications. This presents a vulnerability, allowing the insertion of illegitimate commands or the capture, modification, and replay of system commands by an attacker. Security controls to address this vulnerability are discussed later in this paper.

Since the revelation of these threats and the execution of successful attacks, attention has been given to the security of SCADA systems. According to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), in the first half of 2013, with regard to critical infrastructure sectors, the highest percentage of security incidents involved the energy sector, as shown in Figure 1 [3].

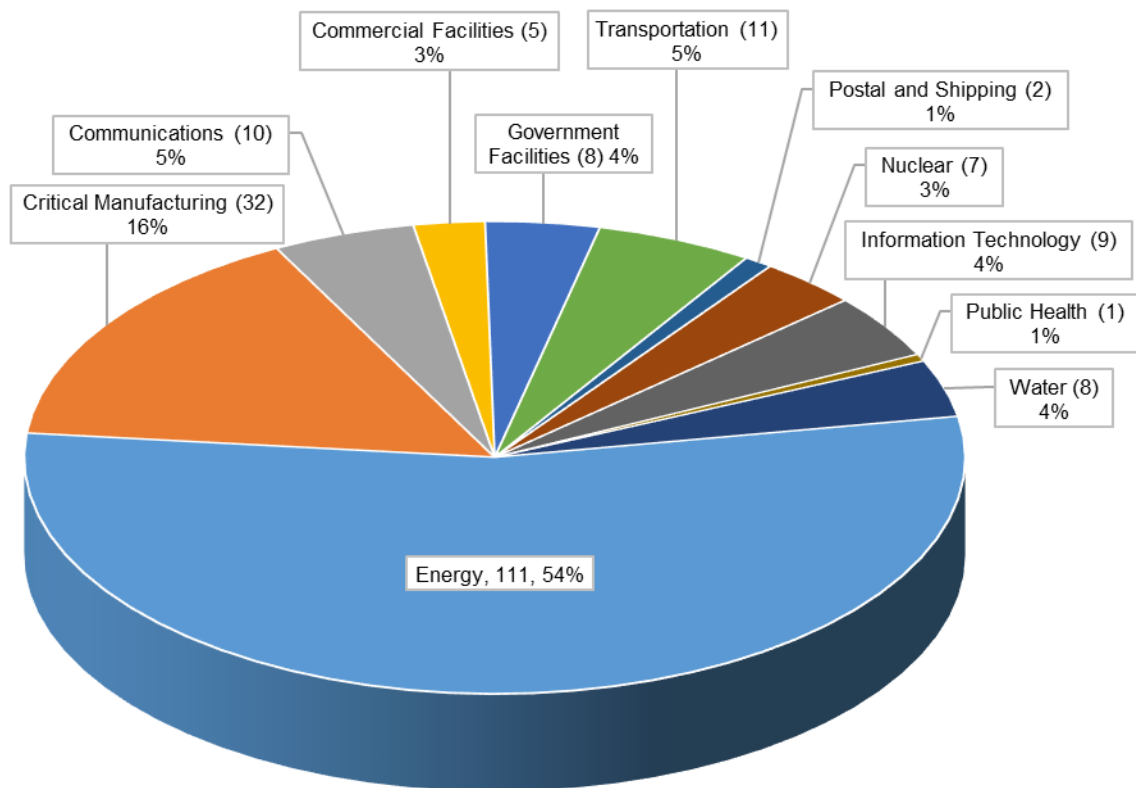


Figure 1 Security incidents by industry, 2013

It should be noted that not every incident is an attack. An incident is an event that disturbs the normal operation of equipment. An incident may be unintentional, whereas an attack is intentional. Incident also include unsuccessful attacks, such as foiled attempts at access.

With the market growth of SCADA products projected at 10 percent over next 5 years, it is essential that the security of these systems be addressed [4]. As new protocols have emerged, Ethernet has become popular in the electrical industry. Because the use of SCADA products is expected to increase, and because more systems are becoming connected on networks, special care must be taken to ensure that these systems are not vulnerable.

Online threats against SCADA pose as much risk as physical attacks. As cybercriminals become more sophisticated and understand more about SCADA and ICSs, the risk of attack becomes greater. In order to defend against such an attack, the sequence of events and methods that allow an attacker to be successful must be learned.

In addition to SCADA systems presenting information to an operator, the systems acquire data from remote locations. Communications between devices are the foremost attack avenue. Communications in ICSs and SCADA systems come in many forms, such as Internet protocols, RF, fiber, Bluetooth<sup>®1</sup>, and older technologies such as telephone networks.

Not only must the power system be protected by tripping breakers, or moving gas be protected by opening valves, but these systems must also be protected from espionage and physical attacks.

## THREAT VECTORS

This section discusses several threat vectors—the methods or means that attackers use to accomplish their goals. Understanding threat vectors is important in order to counter and protect against them. The loss of sensitive information is a threat to any organization. There are several key threat vectors that must be understood to ensure that the appropriate security is applied.

### Replay Attack

In 2011, the manufacturer of an industrial PLC fixed a vulnerability that allowed attackers to intercept passwords and make unauthorized changes to a specific device [5]. The attack vector, known as a replay attack, allowed an unauthorized user to take control of the control system. A replay attack occurs when a malicious user eavesdrops, intercepts, and stores communications, such as passwords or data transmissions, to replay at a later time. One example is an intruder who captures wireless communications to a SCADA device to replay at a later time. The key concept behind a replay attack is that the same legitimate operation is performed at a later time. Another example is the capture of a SCADA command, such as a trip command, to play back anytime. Replay attacks do not require a good understanding of the communications protocol. Unless mitigated, the replayed message is processed as a legitimate message, resulting in unauthorized access or control.

---

<sup>1</sup> The Bluetooth<sup>®</sup> word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by SEL is under license.

## Man-in-the-Middle Attack

Man-in-the-middle attacks are another way attackers take control. In a man-in-the-middle attack, the attacker places himself between two users or devices. This is accomplished in several steps. As shown in Figure 2, the attacker first makes an independent connection to the network. Next, the attacker breaks the connection of the user or device under attack. Using a method known as Address Resolution Protocol (ARP) spoofing, the attacker impersonates the connection to which the victim was connected. The connection is reestablished through the attacker, and the data from the victim are forwarded to the original endpoint. As shown in Figure 2, for a man-in-the-middle attack to be performed, the attacker needs access to the physical network.

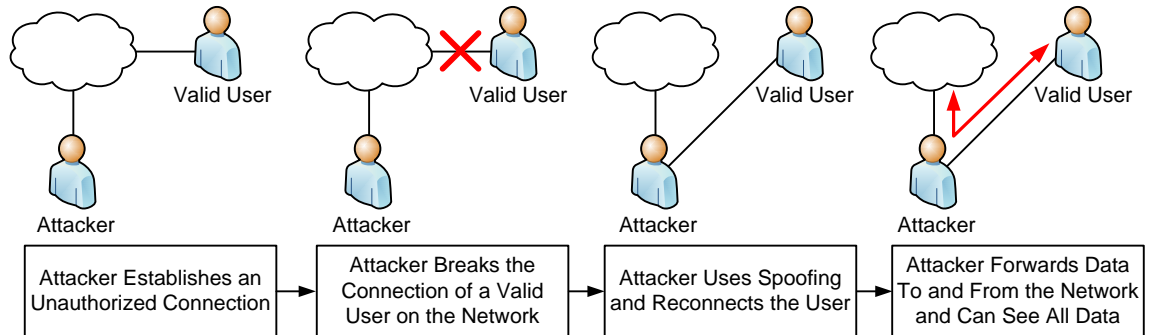


Figure 2 Man-in-the-middle attack scenario

Man-in-the-middle attacks exploit a lack of authentication. Once the new connection is established, the attacker can control the connection, eavesdrop on the data passing through, and inject false messages. Encryption without authentication will not prevent a man-in-the-middle attack. An attacker can modify an encrypted packet even though the attacker may not know what the change will do. For example, a modified encrypted packet may trip a breaker. However, with authentication, because the packet has been changed, it is ignored. For this reason, both encryption and authentication should be implemented. Internet Protocol security (IPsec), which is discussed later in this paper, provides a method of both encryption and authentication.

## Brute Force Attack

Brute force attacks target both encrypted data and/or passwords. A brute force attack attempts to decode encrypted messages by using all possible key combinations. This attack requires time to cycle through the entire key space. Key space refers to the set of all possible keys. Brute force attacks are very common. In February 2013, ICS-CERT issued a security alert after a researcher published a password-cracking tool used for PLCs in SCADA systems [6]. The report also noted a sharp increase in brute force attacks against critical infrastructure.

## Dictionary Attack

Another method of breaking passwords is through a dictionary attack. Dictionary attacks attempt to break passwords by trying each one in a long list of predefined words. This type of attack is very successful for short or simple passwords. Adding a few digits to a simple word (e.g., Password999) creates a weak password that a dictionary attack can easily exploit. Fortunately, there are countermeasures (discussed later in this paper) to dictionary, brute force, and the other threat vectors.

## Eavesdropping

Eavesdropping occurs through many forms. Although some techniques are at a higher technical level, simple techniques can prove very effective. For an attack against a SCADA system, the responsible party must first obtain information about the system or the company itself. Intercepting a fax or unencrypted videoconference call can yield valuable information. Intercepting and analyzing communications packets can yield information about the system in the information gathering phase of an attack. The core of eavesdropping is to silently listen to valid communications to learn about the system.

## Distributed Denial-of-Service Attacks (DDoS)

Denial-of-service attacks are performed with the intent of halting the availability of services. The attack floods a network with an abundance of requests so that the network becomes saturated and cannot respond to legitimate traffic. In a DDoS attack, multiple computers are used to generate massive amounts of data targeted at the network with the aim of slowing it to a halt. In 2012, a European electric power grid operator was targeted with a DDoS attack [7]. The attack rendered the company's Internet communications unusable for a short while. These types of attacks are very inexpensive, yet effective. A DDoS employs a botnet (a large number of compromised computers) to simultaneously send requests to the target system. Some attacks can employ over 10,000 computers. Recently, an anti-spam website was the victim of the largest recorded DDoS attack, which peaked at over 300 gigabits per second. Denial-of-service attacks are not limited to a flood of data. Vulnerabilities in products can be triggered by an attacker that take the product out of service. This method is not a flood of data, but it is still a denial-of-service attack.

## War Dialing

War dialing is a technique, often with malicious intent, of identifying modems. Modems are a popular target of attackers because they often connect to the internal network or electronic equipment of a company. In a war dialing attack, a computer program dials an unknown number in a known area code and listens for a modem to respond. A range of phone numbers are called with the intent of discovering modems and logging their numbers for future uses, such as attempting to gain access. Once a connection is made, the attacker can obtain a prompt. If a banner is included in the prompt, information can be learned from it, such as the device and location.

Modem communications still play a role in many power system communications systems. For instance, digital services may not be available in some rural areas. Modems are often directly attached to intelligent electronic devices (IEDs) in these scenarios.

## Default Passwords

Default passwords could be the greatest risk to the systems of an organization. As simple as it seems to never use default passwords, this practice is not always observed. Manufacturer-specific devices use default passwords that should never be assumed to be secret. A prominent manufacturer of controllers for critical infrastructure had their default credentials leak to the Internet, where they circulated for years. Stuxnet malware took advantage of default passwords, allowing the access and control of the targeted SCADA system. Keeping default passwords in any SCADA equipment poses a significant risk of unauthorized access. Using strong passwords is necessary for a defense-in-depth strategy.

## Electromagnetic Emanations

Emanations, if not controlled, can provide an eavesdropper with information. All electronic devices emit, or emanate, electromagnetic radiation. In some instances, this radiation can be captured and reconstructed to reveal the information being transmitted from or received by a device. With sophisticated and highly sensitive receiving equipment, an eavesdropper can capture emanations from distances of over 100 meters. The distance at which an eavesdropper can capture information increases if the emanations are coupled into the power line from which the device is powered.

The example in Figure 3 illustrates emanations on a Modbus® communications cable. The emanations are apparent due to an unshielded, inexpensive cable. A Modbus communications packet (blue) is overlaid with the emanation (yellow). Note that the rising and falling edges of the communication generate emissions that are easily picked up with a very simple, portable piece of equipment.

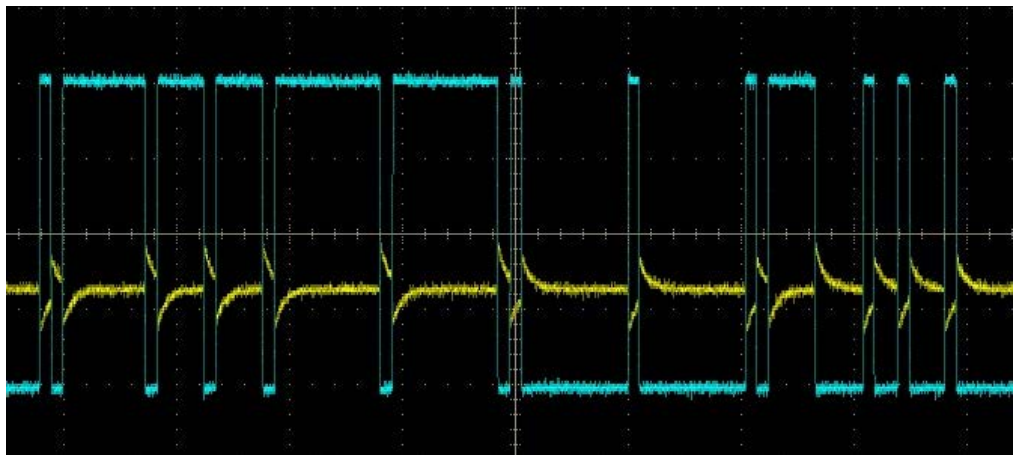


Figure 3 Modbus emanations with unshielded cable

The emanations in this example can be reconstructed to determine the content of the data without physically accessing the device.

Figure 4 shows the same device with a quality, shielded cable. From legacy protocols using hard-wired copper communications to Ethernet-based protocols, quality, shielded cables are necessary to minimize the risk of emanations.

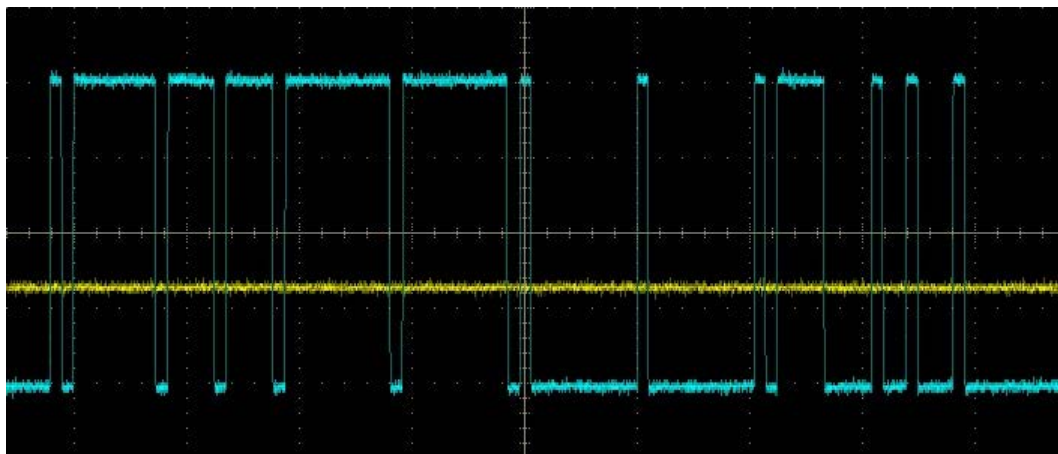


Figure 4 Modbus emanations with shielded cable

## Data Modification

Data modification, also known as data diddling or data injection, involves changing data before they are processed at their destination. Although data modification commonly occurs in data-entry environments, it cannot be ruled out in SCADA systems. For example, some legacy protocols will respond to any host. What would be the impact if the date or time were changed on devices on a Modbus communications bus? The risk of data modification is mitigated in Ethernet protocols with encryption.

## Platform Vulnerabilities

Platform vulnerabilities refers to unpatched Microsoft® Windows® and Linux® operating systems as well as application software. As the SCADA industry transitions from dedicated communications to shared communications links using Internet Protocol-based (IP-based) protocols, platform vulnerabilities are often overlooked in the security sense. A robust security system offers little protection if the platforms it resides on are not properly patched and protected. An unpatched computer can provide an entry point for system flaws to be exploited. In 2011, ICS-CERT issued advisories within 12 hours after a researcher released dozens of flaws in four SCADA products. The exploitation of these flaws in the software that monitors and controls SCADA systems could be used to corrupt memory, modify data, and execute commands.

Patching older legacy systems can be a challenge. A chief technology officer for a major United States security firm estimated that only 10 percent of its customers downloaded the PLC patches that it issued [8]. The reasons for the lack of urgency can be debated. Some experts say it is a lack of education, while others say that not many are willing to touch legacy systems that are over 30 years old. A compromised computer and its trusted connection can be used to expand the reach of an attack. Every company must evaluate the benefits and risks of patch management. Any security patches, settings, and security measures recommended by manufacturers need to be tested extensively and vetted before being applied in a production environment.

## The Age of Designer Threats

Another threat to the secure operation of SCADA systems is called an advanced persistent threat (APT). The origin of this type of well-funded long-term threat is toolkits that are capable of combining all of the attack methods previously examined. They are delivered via a well thought out attack vector, such as an email with a link to what appears to be a website but, in fact, is a launch platform for a cyberattack on the targeted infrastructure. The goal of an APT is to gain access to a system and move slowly and deliberately enough to not be noticed. Once system access has been accomplished, the APT will not trigger the attack until a specific reason or time has surfaced. This makes it very difficult to know that the system has been compromised. The APT attack is designed to swiftly accomplish the desired goal so that it cannot be stopped before the goal is met. Because of the high complexity of an APT, they are generally targeted at organizations for political reasons or because of nation state-level conflicts.

Once an APT enters an industrial network, it expands in stages to different networks and tries to discover equipment. It may even be able to contact outside resources or the attacking group that created it for updates or commands. This is one reason that business and operational networks should be strictly separated. Allowing email and Internet traffic on an operational network is never a safe practice.

Risks to SCADA and ICSs are not limited to the attack vectors described in this paper. Although no risk can be completely eliminated, a proper operations security implementation will mitigate the threats outlined in this paper. Risks are diminished by safeguarding data, preventing unauthorized access, and securing communications. The remainder of this paper focuses on the methods used to prevent, detect, and counter these individual attack methods and to thwart those that come packaged in a 21st-century wrapper, such as an email.

## SECURING IP

Several methods are used with malicious intent to eavesdrop, sabotage, or access systems. Many of these methods are associated with IP communications. Before a discussion of prevention can be presented, a basic understanding of encryption methods must be established. This section presents a basic overview of IPsec, X.509, message hashing, Advanced Encryption Standard (AES) encryption, and public key infrastructure (PKI).

### Secure Communications

To understand the methods used by attackers and how to defend against them, a basic knowledge of public-key cryptography is necessary. The public-key encryption that is used for secure communication requires two mathematically linked codes, referred to as keys. This key pair is responsible for the secrecy of messages across a nonsecure network. One key encrypts a cleartext message, while the other key decrypts the ciphertext message, as shown in Figure 5. This can be thought of as one key locking a box while another key can unlock the box. Because both keys cannot perform the same function, this method of two unique keys is classified as asymmetric key encryption. Encryption is achieved by the use of the public key, and the public key is widely dispersed. Decryption, however, is only achieved through the private key.

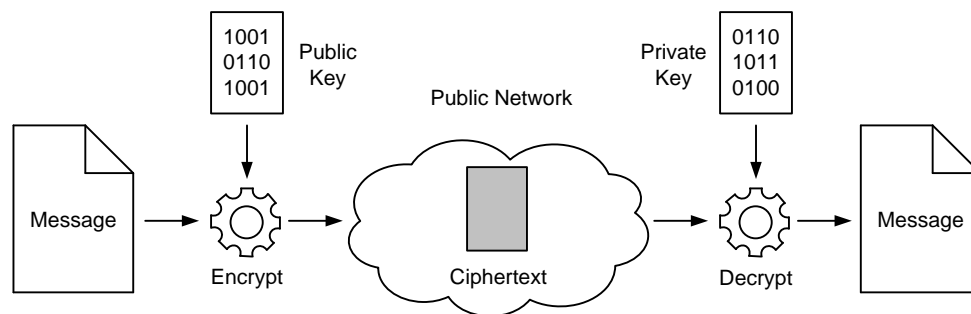


Figure 5 Public key encryption concept

Confidentiality is achieved through the secrecy of the private key. If the private key is compromised, confidentiality is at risk.

Public key encryption and the use of asymmetric key encryption not only provide stronger security but also offer many other benefits. Because a private key is specific to a user or device, its identity can be verified. Digital signatures allow for the verification of identity, message integrity, and origin.

A digital signature is simply a message signed with the private key of the sender. Signing a message digitally is partially accomplished by a process known as a hash. Hashing means that the entire message is put through a one-way process that cannot be reversed. The resulting hash, or string of characters, is known as a message digest. The message digest is a fixed-length hash value, regardless of the input data size.



In theory, each message has a unique hash result. In the example in Figure 6, both messages have distinctly different hash values despite very little difference between the messages.

Text	<b>Never use default passwords</b>
Hash Value	3D5DC3D68B90122917B87B952A153331 F521B9C21E27DAB5FF2B9629521ER74A
Modified Text	<b>never use default passwords</b>
Hash Value	0677DF348635164ABDD628B8F1F84B5A 78464E63996BD2D50D68AE1FD84D76F6

Figure 6 Example of a message digest or hash

If any part of the message is tampered with or modified, the message digest changes. A digital signature is created by hashing the entire message with the private key of the sender, as shown in Figure 7.

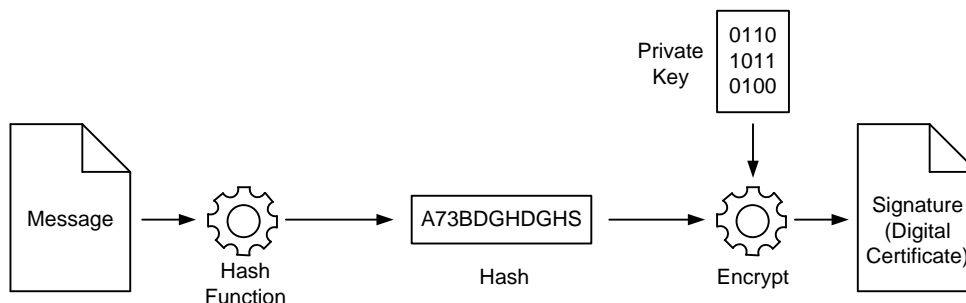


Figure 7 Generating a digital signature

Because the private key, specific to the sender, is used, it is assumed that the message associated with it is valid. Data integrity is also verified. If the message digest remains unchanged from the sender to the recipient, it is assumed that the message has not been altered or modified.

Another method used is symmetric key encryption. Symmetric encryption uses the same key for locking and unlocking, or encryption and decryption. Because the same key is used for both functions, symmetric encryption is much less of a burden on processing and greater speeds are achieved. Security, however, is weaker. If the single key is compromised in a symmetric key system, confidentiality and data integrity are at risk.

## IPsec

IPsec is a standardized framework for securing IP communications over a trusted or untrusted network. IPsec provides confidentiality, integrity, and authentication. Confidentiality is provided through strong encryption algorithms while integrity is provided by the use of message validation schemes known as checksums and hashes.

Developed by the Internet Engineering Task Force (IETF), IPsec builds a secure tunnel of communications between two endpoints, as shown in Figure 8. This is accomplished with the use of a protocol that exchanges keys between the two endpoints. IPsec works by the sending and receiving devices sharing a public key. Once the tunnel is established, the sender and receiver agree on the encryption algorithm to use.

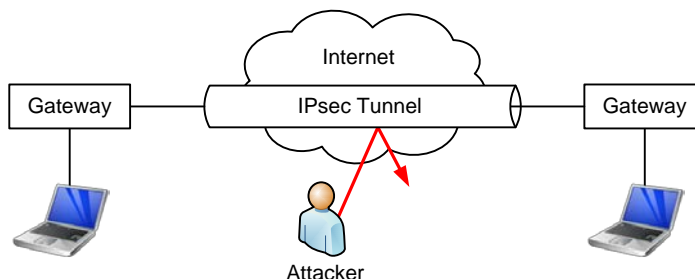


Figure 8 Secure IPsec tunnel

IPsec uses the following two protocols for data transfer, as shown in Figure 9:

- Authentication header (AH) is used to authenticate IP traffic but performs no encryption. The authentication is performed by calculating hashed messages over the packet of data.
- Encapsulating security payload (ESP) provides confidentiality by encrypting the data. In addition to confidentiality, ESP provides authentication, integrity, and anti-replay. ESP can be used with or without AH protocol.

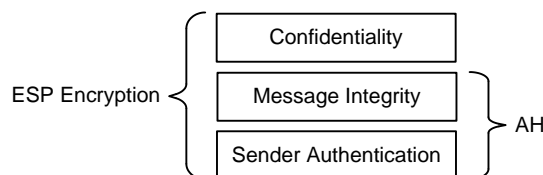


Figure 9 ESP and AH work together

IPsec can be deployed on a SCADA network to secure communications between gateways that protect end devices, such as PLCs or relays.

## AES Encryption

AES is a United States government-accepted, and globally recognized, standard for encoding data. AES operates by splitting data into blocks called matrices and operating on each one. The AES algorithm performs multiple rounds of scrambling the data by substituting data, shifting rows, and mixing columns.

As with the goal of any encryption, AES provides data confidentiality. AES encryption is the most widely-used symmetric key algorithm.

## X.509

X.509 is a standard that defines the context and arrangement of a digital certificate. A digital certificate binds a public key to the entity of a person or device, ensuring the validity of the communication and preventing an impersonation. X.509 also includes a system of certificate authorities for issuing the certificates. An X.509 certificate typically includes information about the entity, such as name, organization, and country. Digital certificates are common on devices with a web interface and provide security for access to those devices. Digital certificates provide confidentiality, authentication, nonrepudiation, and user-based access control.

## Secure Shell (SSH) and Secure Sockets Layer (SSL)

Before much emphasis was placed on security, Telnet was a popular protocol for accessing remote devices. Developed in 1969, Telnet is inherently nonsecure in that usernames and passwords are sent in cleartext. Because of this glaring security flaw, SSH was specifically developed to replace Telnet. SSH is a protocol for secure access to a remote device via public key cryptography. Because SSH communications are encrypted with public key cryptography, they provide confidentiality and data integrity over an untrusted network. The most common applications for SSH are for devices with web interfaces, such as remote computers and IEDs.

SSL is a protocol developed by Netscape to provide communications security over the Internet. SSL uses digital certificates and asymmetric cryptography for confidentiality and authentication. Like SSH, SSL is commonly used for remote access via a web interface. The URLs for SSL connections use Hypertext Transfer Protocol Secure (https) rather than Hypertext Transfer Protocol (http). How SSL is used in authenticating a request for access from an engineer is discussed later in this paper.

## Logging and Audits

One of the single most important aspects of security is the ability to detect unauthorized activity. The strongest security imaginable is incomplete without the capability to detect malicious activity.

Many attacks are intended to be silent and gather information. Espionage is a key phase of an attack and can last for a long period of time. It is important to understand that espionage can either be the sole purpose of an attack or can precede a malicious event. The malicious event occurs after enough needed information has been gained.

Security logs provide the means of detecting intrusion attempts. Knowing that an unauthorized person is attempting to access a device is important. The log report in Figure 10 reveals a failed intrusion attempt and the IP address of the user.

Timestamp	Tag	Severity	Facility	Message
2010-07-30 22:48:26.652197+00	Login	Notice	SECURITY	Login to web: successful by admin at 192.168.1.3
2010-07-30 22:48:19.891215+00	Login	Notice	SECURITY	Login to web: failed from 192.168.1.3
2010-07-30 22:48:15.361319+00	Login	Notice	SECURITY	Login to web: failed from 192.168.1.3
2010-07-30 22:48:12.002449+00	Login	Notice	SECURITY	Login to web: failed from 192.168.1.3
2010-07-30 22:48:09.748182+00	Login	Notice	SECURITY	Login to web: failed from 192.168.1.3
2010-07-30 22:48:07.228703+00	Login	Notice	SECURITY	Login to web: failed from 192.168.1.3
2010-07-30 22:48:04.734423+00	Login	Notice	SECURITY	Login to web: failed from 192.168.1.3
2010-07-30 22:48:02.339213+00	Login	Notice	SECURITY	Login to web: failed from 192.168.1.3

Figure 10 Syslog reveals failed intrusion attempt

Many devices available today contain event logging. Logs contain information, such as a history of logins, about the state of a device. Syslog is a protocol used for sending these events to a data collection server or a security information and event management (SIEM) server. Because syslog is standardized, software packages can analyze the data to generate reports and security metrics.

All SEL cybersecurity solutions feature logging that addresses the requirements of regulatory bodies and good security practices. Also, SEL has implemented denial-of-service monitoring in new products, such as the SEL-3530 Real-Time Automation Controller (RTAC). This safeguard

monitors Ethernet traffic for bandwidth spikes and bursts that may be denial-of-service attacks. If the amount of Ethernet traffic addressed to the RTAC causes processing exceeding 80 percent of the configured watchdog time-out, the RTAC logs a special alert message and adjusts system priorities to compensate. The RTAC prevents any time-out condition by modulating nonessential traffic and dialing down the noise. After five minutes of lowered priorities, if the traffic has diminished, the priorities are reset to normal and the RTAC logs a message that operations have been restored to their normal state.

If the traffic continues at the same or greater volume and rate, the watchdog timer expires and logs a message stating that the system watchdog has expired. In addition to the denial-of-service monitoring in the RTAC, the SEL-2730M 24-Port Managed Ethernet Switch allows traffic throttling with bandwidth guards on virtual local-area networks (VLANs).

## MITIGATION TECHNIQUES

The objective of any security plan is to reduce risk. The numerous methods attackers use to gain access, gather intelligence, and execute malicious activity were discussed previously. Each form of attack has a mitigation technique, as summarized in Table 1.

Table 1 Attack types and mitigation techniques

Attack Type	Mitigation Technique
Replay attack	Message sequencing (IPsec), time stamps
Man-in-the-middle attack	Strong encryption (IPsec) with PKI
Brute force attack	Strong password policy, account locking and delaying
Dictionary attack	Strong password policy, account lockout
Eavesdropping	Strong encryption and authentication
Denial of service or DDoS	Rapid detection, IP filtering (firewall)
War dialing	Switched-in modem when needed, enabled modem callback option, inbound call whitelisting
Default passwords	Use of unique passwords, strong password policy
Emanations (and tapping)	Shielded copper cables, limited fiber bend radius
Data modification (or injection)	Hash-based Message Authentication Code (HMAC) authentication
Platform vulnerabilities	Patching via security operations policy, asset management and change control
Unauthorized access	Stateful firewall, access controls (Lightweight Directory Access Protocol [LDAP])

In a replay attack, an intercepted password or data transmission is replayed. With IPsec, a sequence number is incremented for each packet sent. These sequence numbers built into IPsec prevent replay attacks. A message received with an out-of-sequence number will be dropped.

A similar technique exists for man-in-the-middle attacks. Defense against such attacks is accomplished through authentication. The use of strong encryption and authentication together can provide adequate defense.

Data modification and data injection defenses also rely on authentication. One method of authentication is an HMAC used within IPsec. Using a hash function along with a key, a message

authentication code is generated. An HMAC is used to verify both the integrity and authenticity of the data. Because the authentication code is based on the contents of the data, if the data are changed, the authentication code will not match from source to destination, indicating that the data are not authentic.

In the past, dial-up access to substation IEDs was frequently accomplished using modems over a plain old telephone system (POTS) circuit. This practice is still in use at some utilities but is becoming less popular for several reasons, security being one of the main reasons. Because the phone circuits are normally provided by the local telephone company, the communication is established over infrastructure that is not under the control of the utility. This presents the risk of unauthorized access. Keeping the phone number secret is not enough. War dialing software is available for an attacker to identify modems. Although war dialing cannot be prevented, the end goal of war dialing can be defeated. The best practice is to disconnect modems when not in use. Some utilities require a phone call to an operations center to request access to the modem. After access is granted, the modem is physically switched into the system. If this method of switching is not possible, inbound numbers can be whitelisted. Another possibility is to enable the call-back feature. Call back enables more security on dial-in lines. It functions by connecting, logging in, and then hanging up. Next, the host rings back. In this mode, the caller has to be at a phone number that is known and authorized. Utilities are moving toward building their own communications infrastructure, such as synchronous optical network (SONET) systems, which will be discussed in the next section. This has resulted in Ethernet becoming more widely available. Securing Ethernet through the use of virtual private networks (VPNs) and firewalls is becoming more popular with utilities.

Defending against attacks on passwords, such as dictionary and brute force attacks, requires strong passwords. Recent breaches into physical devices were successful because the passwords were never changed from the factory defaults. Attackers know the factory default passwords of manufacturer equipment, and it is critical to change these to strong passwords. A good password policy should include a requirement for a minimum number of characters, one or more symbols, and both uppercase and lowercase characters. Passwords like **Oaks Sub\$tat1on Deliv3rs!** make dictionary and brute force attacks difficult. Note that some characters are replaced with numbers to strengthen the secrecy of the password.

Denial-of-service and DDoS attacks require special attention. A denial-of-service attack can typically be defeated by filtering and rejecting the source IP address. However, a DDoS attack is much more difficult because the traffic is coming from many devices and must be handled by a network team.

Another concept in mitigation controls is firewalls. In simple terms, firewalls allow or deny traffic to relays, IEDs, or other devices. A firewall analyzes data packets and, based on a set of rules, determines if the data are allowed to pass to the device. There are several types of firewalls, including a type known as a stateful firewall, which inspect data packets and keep track of the state of the connection by storing attributes of the connection such as IP addresses, port numbers, and the sequence numbers of the packets.

Computer systems, and the platforms they operate under, can contain newly discovered vulnerabilities. These vulnerabilities are a serious risk because computer systems reside inside an organization and are potentially connected to equipment. As new vulnerabilities are discovered, firms work to issue patches. According to the National Institute of Standards and Technology (NIST), timely patching for security issues is generally recognized as critical to maintaining operational availability. Most major attacks in the past few years have targeted known vulnerabilities for which patches existed before the outbreaks [9]. Before beginning a patch and vulnerability management program, an inventory of all of the devices on the system is required—an unpatched and unaccounted-for computer is at risk of being exploited. Organizations should use automated patch management tools to fix potential vulnerabilities.

## PROTECTING SCADA COMMUNICATIONS

The following sections outline threats to SCADA systems and how attackers are able to execute malicious attacks on the systems from a technical perspective. This section brings together the previous discussions and presents the application of countermeasures. In addition, a discussion of secure communications is presented with examples. Mitigating the risk to a system is the main goal in security, and this section makes the best effort to outline the requirements to accomplish this goal.

### Dependable Communications for Critical Infrastructure

The SEL ICON® Integrated Communications Optical Network SONET multiplexer provides dependable communications for critical infrastructure. SONET communicates over fiber-optic rings that provide redundant paths should a fiber break. In the example in Figure 11, four sites at different locations are linked through a SONET communications ring.

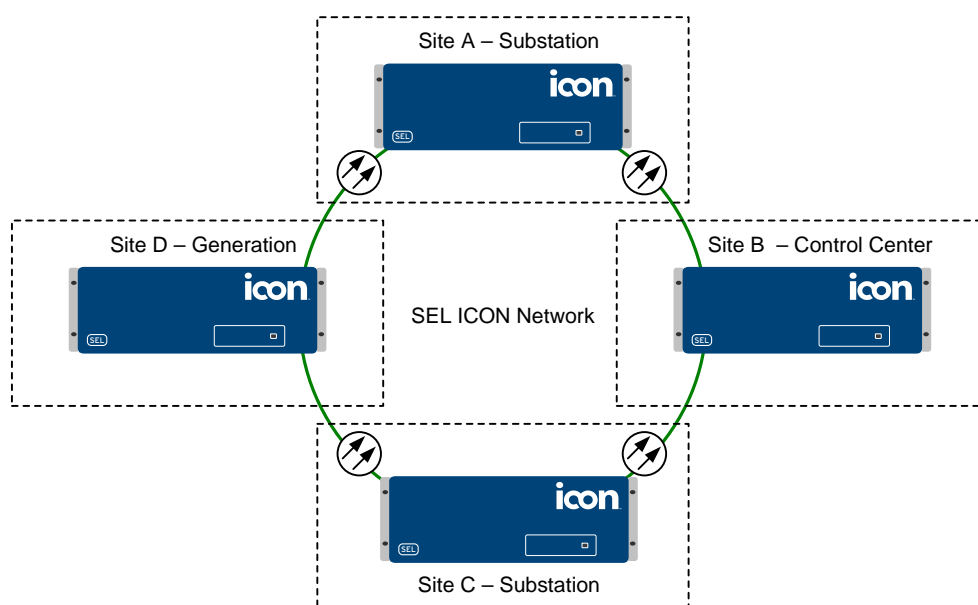


Figure 11 Core communications on an example utility network as an ICON SONET ring

The ICON supports the optional application of AES security on the SONET ring. The SONET transmission is strongly encrypted between adjacent ICON nodes. SEL has developed an innovative SEL SONET Encryption Protocol (SSEP). This protocol implements AES encryption that is configurable to 128-bit or 256-bit key strengths, and it adds very little latency. SEL engineers design encryption solutions specifically to meet the needs and latency requirements of the electrical utility industry.

The ICON encryption has been certified as meeting the Federal Information Processing Standard (FIPS). The system was designed and built to meet the stringent FIPS 140-2 Level 2 requirements for encryption devices.

The encryption on the SONET ring protects the most exposed portion of the communications channel: the fiber that forms the rings and runs between substations and control centers. Much of this fiber is not in a building that provides physical security, making it a potential target. This encryption provides a formidable deterrent to tapping and protects the fiber medium from eavesdropping.

In the example ICON ring in Figure 11, four sites are connected. Each site, or node, uses a different form of communication, each of which will be discussed in further detail.

Site A in Figure 11 is a substation that uses Ethernet protocol for communications.

### Ethernet Communications Security

The first step in Ethernet security is access control. The example in Figure 12 demonstrates the access authorization of relays and an IED by means of a security gateway. The SEL-3620 Ethernet Security Gateway supports Remote Authentication Dial-In User Service (RADIUS) protocol for centralized authentication. It also supports LDAP. Most organizations use LDAP as their database of authorized user accounts and passwords. The following scenario illustrates the value of using this method (no local or forgotten accounts or passwords) and the security of the system (accounts can be managed in a centralized location).

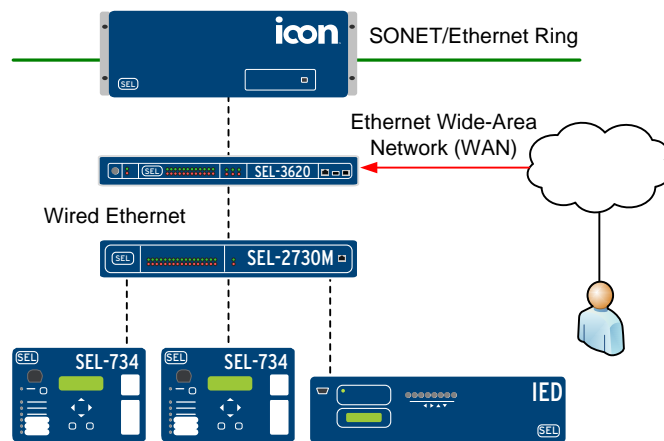


Figure 12 Ethernet communications security concept

Consider the example of a relay engineer logging into relays through the SEL-3620. The engineer logs in to the SEL-3620 using SSL, authenticates to the Microsoft Active Directory® service, and manages the connections securely. The engineer logs in with Active Directory or LDAP credentials via a connection to a user password repository, as shown in Figure 13.

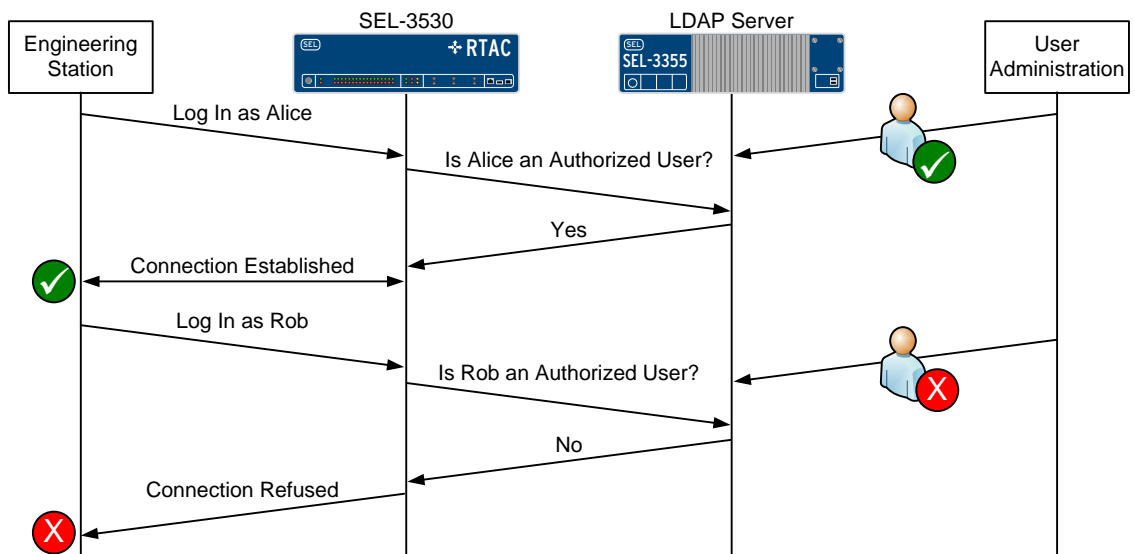


Figure 13 LDAP provides access to company databases of employee user accounts

The SEL-3620 provides a two-factor authentication with RSA SecurID® key tokens.

The SEL-3622 Security Gateway is a security device with a small form factor (see Figure 14). Like the larger SEL-3620, it helps to manage IED passwords and ensures that passwords are changed regularly and conform to complexity rules for stronger security. The SEL-3622 authentication proxy feature provides user-based single-sign-on access to several Ethernet and serial devices. The small footprint of the SEL-3622 allows it to be used in enclosures and structures where space is limited, such as the control cabinet of a pole-top recloser.

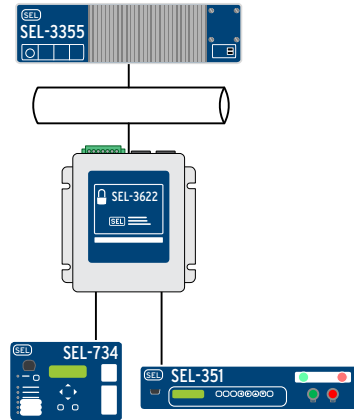


Figure 14 An SEL-3622 installed in an example utility network (serial connections from the IEDs are sent securely by Ethernet networks to the operator)

Ethernet communications confidentiality is obtained through encryption. An attacker cannot effectively eavesdrop on the encrypted communications on the link between SEL-3620 units, nor can the attacker capture an encrypted session with a packet capture tool and replay it because of the anti-replay protections built into the SEL protocols and the encryption standards. The attacker is further thwarted from passing through the SEL-3620 interface to the hosts inside.

Authentication is also provided, making it impossible to inject frames into the encrypted stream of protected packets. The attacker will be foiled and any traffic will be dropped at the interface because a barrier is in place, consisting of a combination of authentication and encryption. Recall the example of AH in the Securing IP section of this paper. The applied result of this method is an authentication failure of the forged packet, which prevents the attack, as shown in Figure 15. It is like the protective seal found on a bottle of pain killers at the store. If the protective seal is broken, it is thrown away. This is what authentication, such as HMAC, does programmatically.

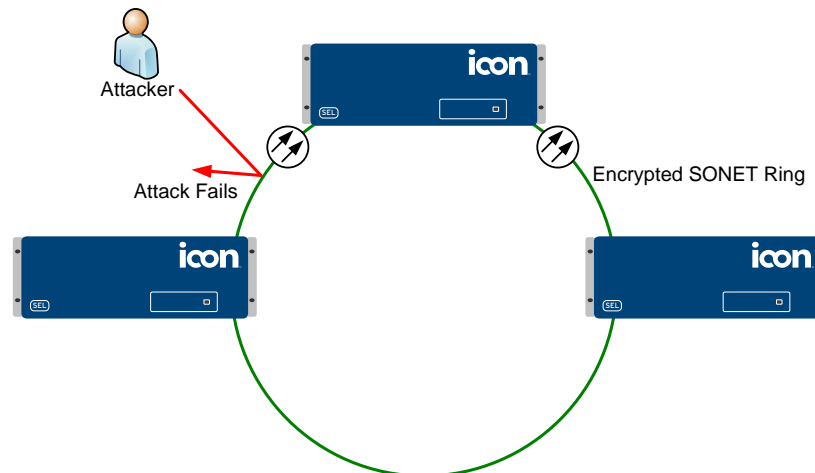


Figure 15 Attacker foiled in forged packet attempt



Another layer in Ethernet security is access through switching. Media Access Control (MAC) address security is built into the SEL-2730M Switch. Most MAC security systems are manually entered in a whitelist of allowed hosts for a particular port. Once the allowed address is entered, the switch port will allow only that address to communicate. The security operator must gather the allowed MAC addresses and program them into the switch configuration on a per-port basis.

The SEL-2730M supports flexible methods to gather the addresses to allow and apply them as needed on the correct ports. After building an Ethernet network in a substation, the operator can enable the SEL-2730M to learn the MAC addresses on the switch ports. There are several methods available to simplify MAC security and prevent errors. One method is called count lock. To implement count lock, the operator enters the total number of MAC addresses to learn. The switch will gather MAC addresses until the counter reaches the parameter that the operator has entered. The second method is time lock. Time lock is used by entering a time period for the switch port to learn new MAC addresses, and after the time expires, the MAC addresses of the connected devices will be locked into the switch. The operator can use this feature to capture the endpoints in an initial network during commissioning.

As operators add new equipment to the network, the switch can easily relearn or add endpoints to adjust to the changes that have been made. For security reasons, a user with administrative privileges should make this change.

MAC security is most effective when a single host is connected to a dedicated port and when the system does not go through many changes (i.e., has a relatively static connection).

There are some caveats to using MAC security. It is possible to spoof MAC addresses on particular computer platforms (such as Linux) by changing the address to pretend to be a different host. Nevertheless, MAC security is still a viable security measure when combined with other layered security measures.

All Ethernet communications devices should have monitoring and auditing enabled. For instance, the SEL-2730M logs keep track of any changes made to the device, such as the addition of a user, a changed password, or a change in a port state. This information can be fed to network intrusion detection systems or remote logging servers. The SEL-2730M features user roles for accounts. The possible roles for a user are Administrator, Account Manager, Engineer, or View Only, each of which has varying levels of rights. Any username can be created for authorized individuals and then the user is assigned to a role.

## Port Servers

Port servers, also known as terminal servers, are purpose-built devices with a high port capacity that historically have provided Telnet-to-serial connections to multiple devices. Port servers are inherently a nonsecure platform and unfortunately also widely used. The SEL-3610 Port Server provides a large number of serial ports and updates the communications to be flexible and secure by allowing serial products to communicate securely through Ethernet networks. A wide variety of IEDs can be managed securely with an SEL-3610. The SEL-3610 is used to securely manage meters, communications devices, relays, and other IEDs that support only serial communications. The port server tunnels serial data over an Ethernet connection using SSH. One or more logical Ethernet ports are mapped to a single or multiple physical serial ports. Multiple protocol options and session filtering can be configured to support Ethernet protocol sessions where the preferred communications are over Ethernet and IP.

SEL security gateways are extremely effective when connected directly to legacy devices where a weak password is built into the system. SEL security gateways are also extremely effective for tunneling nonsecure protocols to secure protocols, such as tunneling Telnet over SSH. Instead of passing through the communications channel in cleartext over potentially hundreds of miles, the

cleartext communication occurs over a short stretch of cable. The security gateway proxies the weak password locally and uses strong encryption and strong password authentication to make the connection through the WAN.

## Serial Communications Security

Site B in the communications ring in Figure 11 is a control center that uses serial communications.

Serial networks are well-established throughout the power grid and are an important part of the communications infrastructure. Until SEL developed serial encryption devices, tapping, intercepting, and replaying commands on a serial line were simple. The introduction of serial encryption devices for EIA-232, EIA-422, and EIA-485 has solved this problem, and using them closes a serious avenue of attack. The newest entry to the family of serial encryption solutions is the SEL-3025 Serial Shield®, which prevents data injection and replay attacks using the methods discussed throughout this paper. AH and ESP methods work against the hacker in the SEL-3025.

The SEL-3025 prevents replay attacks and data modification via authentication that uses an HMAC included in the Secure SCADA Communications Protocol (SSCP). Figure 16 shows an example of secure serial communications. Communications over the SCADA network are protected with AES encryption.

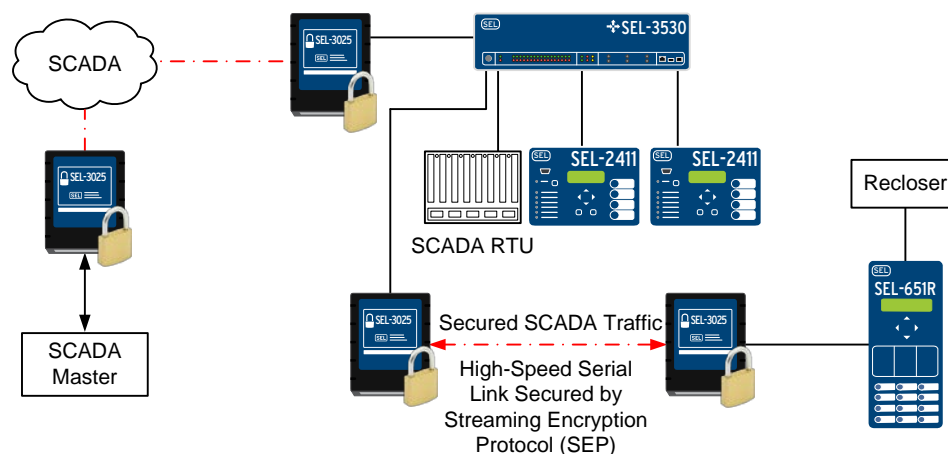


Figure 16 Serial secure communications

For cases where latency is an issue, such as for fast communications, streaming encryption protocol (SEP) is used in the SEL-3025. Using MIRRORRED BITS® communications for a transmission line protection scheme is one example where low-latency encryption is desirable. SEP uses AES encryption, which is suitable for securing data. SEP was designed to minimize the latency that the encryption of communications can introduce. SSCP, mentioned previously, has some additional latency because each message is authenticated. This requires the message to be stored briefly to perform the authentication, which introduces some latency. SEP authenticates the session, but not each message, which allows SEP to have lower latency. SSCP is used for engineering access (people-to-machine communications) and SEP, having a low latency, is used for machine-to-machine (M2M) communications. SEL provides a quantitative analysis of the minimal latency introduced by the SEL-3025 (available at <https://www.selinc.com>).

AES 256-bit session keys are generated through a FIPS 186-2 digital signature standard-compliant method. Key exchange is via the Diffie-Hellman key exchange protocol. X.509 digital certificates are used for confidentiality and authentication and nonrepudiation (the digital signature is hashed with the sender private key).

## Wireless Communications Security

Site C in the communications ring in Figure 11 is a substation that uses wireless communications.

Wireless communications have been used in SCADA networks because of the convenience and flexibility in reaching remote installations where other communications cannot be established. Private wireless communications offer attractive cost savings. Even though the predominant methods are point-to-point wireless connections, interception remains a concern. Wireless technologies clearly offer significant value and cost savings from a maintenance and safety standpoint, but what about security?

In the example in Figure 17, two remote sites (a substation and a utility protective relay) are linked via a secure wireless scheme.

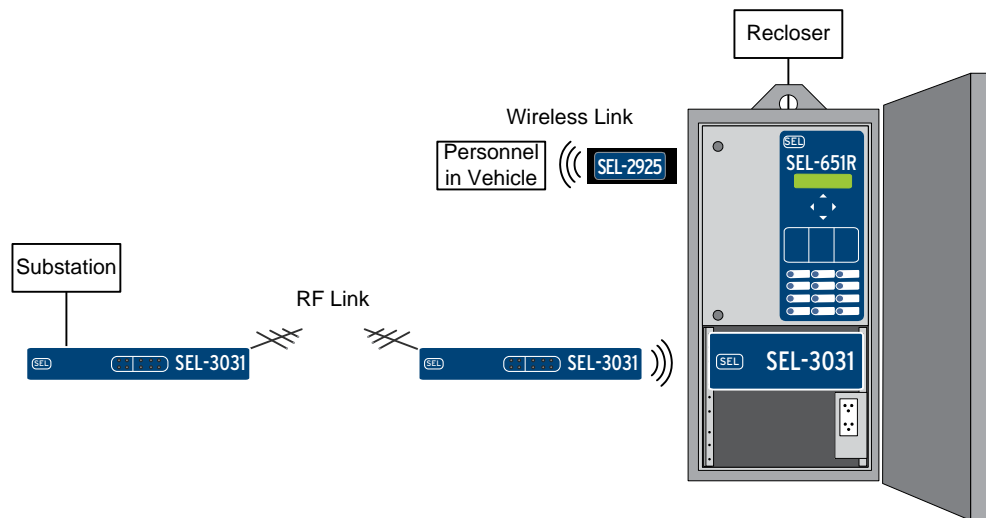


Figure 17 RF, Bluetooth wireless secure communications

Many electric utilities use RF communications. In doing so, it is important to secure the transmissions over the air. In order to prevent malicious attacks, or information gathering via eavesdropping, authentication and encryption must be implemented. SEL wireless devices provide this type of effective security.

The SEL-3031 Serial Radio Transceiver optionally supports session authentication and strong 256-bit AES technology. For applications requiring wireless Ethernet, the SEL-3060 Ethernet Radio is designed for SCADA and engineering access. The SEL-3060 provides communications within a 15-mile range and operates in the 900 MHz license-free industrial, scientific, and medical (ISM) frequency bands. Security is provided via AES 128-bit encryption.

In addition to wireless RF, field service vehicles communicate with remote devices via Bluetooth. Bluetooth communications enable a field technician to access equipment from their service vehicle. Pole-mounted equipment can be accessed for maintenance without climbing or opening the enclosure. Bluetooth is a wireless protocol that operates in the 2.5 GHz frequency band. SEL Bluetooth serial adapters are secure by design, using Bluetooth v2.1 + Enhanced Data Rate (EDR) security—a version with strengthened security. The wireless adapter requires an 8- to 16-character encryption personal identification number (PIN). An extra level of security is provided by secure simple pairing (SSP). Secure pairing ensures that only Bluetooth devices with v2.1 and EDR are able to connect. The SEL-2924 Portable Bluetooth Serial Adapter and SEL-2925 Bluetooth Serial Adapter use elliptic curve Diffie-Hellman encryption, making them secure for SCADA applications.

## Secure Remote Access to SCADA Devices

Site D in the communications ring in Figure 11 is a generation site that requires remote access to SCADA devices. Remote access to SCADA and industrial control networks is a mission-critical need. Reliable remote access is necessary in the event of a SCADA system failure or network problem. Remote access, however, is an attack channel and must be secured. Secure remote access requires access control, authentication, and encryption. Endpoints should be protected by a firewall.

Figure 18 illustrates secure engineering access to a remote substation from a control center. The control center is able to establish communications to its devices over an untrusted network via an SEL-3620. The SEL-3620 provides a central point of entry with user-based access control and detailed activity logs. Authentication and encryption are also provided.

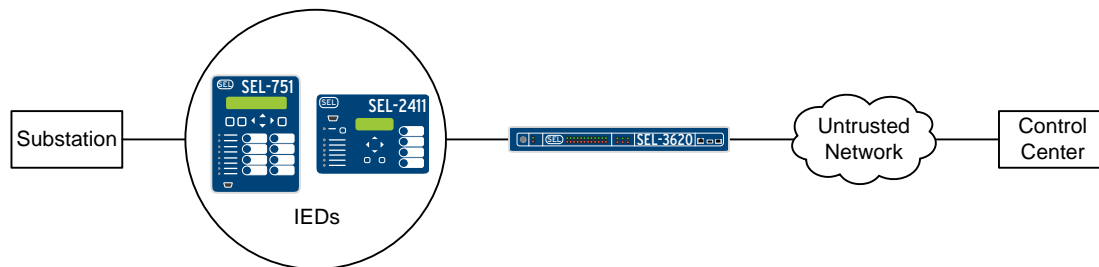


Figure 18 Engineering access over an untrusted network

Serial communications over older nonsecure public access channels must also be protected. Securing meters, relays, PLCs, remote terminal units (RTUs), and port servers is essential.

For an application of remote access via a POTS circuit, dial-up connections via a modem are considered untrusted. An attacker can access and alter the communications by injecting malicious data.

The SEL-3025 cryptographic transceiver with PC Serial Security Kit solves this problem. Installed on the engineering workstation, the PC Serial Security Kit provides the hardware and software required to communicate with remote SEL-3025 devices. An encryption card provides the capability to secure the communications to and from the engineering workstation. ACCELERATOR QuickSet® SEL-5030 Software securely generates and stores cryptographic keys and manages the distribution of the keys [10].

In Figure 19, the SEL-3025 and PC Serial Security Kit (including an SEL-3045 Secure SCADA Card) provide a secure SCADA link by authenticating and optionally encrypting the communications. Communications are protected from unauthorized access by rejecting requests from sources that fail the encrypted session authentication. In addition, communications are protected from eavesdropping and unauthorized control by protecting against forged, modified, or replayed messages.

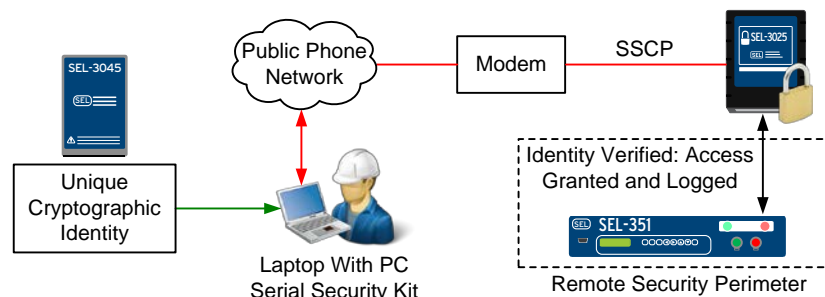


Figure 19 Dial-up secure remote access

Finally, with remote engineering access, auditing is never forgotten. Who has accessed the network and devices can be determined. Not only the rejected logins, but also the accepted logins can be analyzed.

## Machine-to-Machine Communications

The concept of devices and machines communicating with each other is certainly nothing new. However, as newer networking technologies have emerged, modern networking technology has expanded into many devices used in the protection, control, monitoring, and automation of essential applications. M2M communications enable wireless and wired systems to communicate with other devices. Some examples of M2M communications are smart meters, ICS devices, relays, and PLCs. Typical media for M2M communications are Ethernet and cellular.

M2M communications have two attack vectors—the communications channel and a physical attack on the endpoints. M2M attacks should not be thought of as specific to the communications channel—data can be skewed at the physical endpoint. Industries must increase the focus on physical attacks on devices, especially those in remote locations. The need for physical security is discussed in the Physical Security section later in this paper. Protecting M2M communications begins with the communications channels, and data protection is achieved through encryption. Ethernet and wireless communications should use authenticated encryption, such as AES encryption, to protect from man-in-the-middle and replay attacks. Securing M2M for critical applications, such as SCADA and automation, may need further controls such as monitoring devices. For example, a device sending a lot more data than anticipated should trigger an investigation of the cause.

Many analyst firms predict that the number of M2M-connected devices will grow to 50 billion by 2020. Keeping these devices secure will require authentication and encryption. Older technologies will be at risk from the threats fixed in newer technologies. For such legacy devices, compensating controls should be used, such as an encryption wrapper.

## New Generation of Computers

Availability and reliability are critical for SCADA, ICSs, automation, data concentration, monitoring, and control. A new generation of industrial computers has been introduced that has an anticipated mean time between failures (MTBF) many times that of typical industrial computers. The SEL-3355 Computer is an example of such a computer.

The reliability of the SEL-3355 results from the lack of moving parts, such as fans and spinning drives. Solid-state drives reduce wear and tear and can be used in a redundant array of independent disks (RAID) configuration. Error-correcting code (ECC) memory protects against bit flips that produce digital logic errors. The SEL-3355 withstands harsh environments and extreme temperature ranges by using new thermal designs that allow for quick heat dissipation without fans or vents. The SEL-3355 also operates correctly when exposed to electrostatic discharges, vibrations, shocks, bumps, or large electromagnetic fields or RF interference.

These computers have a wide range of applications to increase the security of an office, substation, or industrial plant. One application is that of a centralized authentication server, such as a local LDAP server. Other applications include industrial automation, information processing, data concentration, and intrusion detection.

## Network Intrusion Detection

A network intrusion detection system (IDS) is a very important piece of the security framework within an organization. While firewalls and antivirus protection are a must for protecting SCADA networks, the ability to know if a network has even been breached relies on an IDS. An IDS monitors both inbound and outbound communications on a network and between devices and records events such as unauthorized access attempts, port scans, probes, buffer overflows, operating system (OS) fingerprinting, and other forms of attack.

In addition to detecting malicious threats, an IDS is also valuable in the detection of policy violations. For example, security incidents have occurred in which a utility engineer placed an Ethernet cable with Internet access into a device on a secure network with the intention of using the connection temporarily to update the device. The cable was forgotten and found months later after allowing the system to be exposed to the outside world. An IDS would have detected this policy violation.

A rule-based IDS uses predefined rules to analyze traffic on the SCADA or ICS network. The IDS inspects each packet for information such as the source and destination, protocol, port, and message content based on the rule shown in Figure 20. The rule contains information on how to inspect each packet and alert if action is necessary.

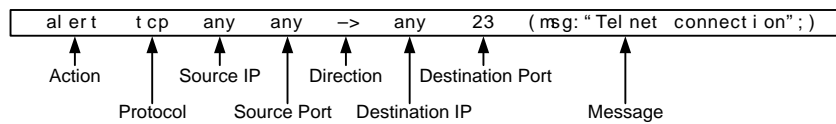


Figure 20 Intrusion detection rule

Some threats may originate from within an organization. These threats can be discovered because an IDS also analyzes traffic between devices. In the example in Figure 21, the rule is used to detect a possible buffer overflow or DDoS attack. Because the maximum size of a Modbus® TCP packet is 260 bytes, the rule checks for a packet size greater than 300 bytes. In the event that the packet in Figure 21 is seen, a formatted log event will be generated.

```
al er t t cp $MODBUS_Client any -> $MODBUS_Server \
502 (dsi ze:>300; msg: "I l l e g a l M o d b u s T C P P a c k e t S i z e";)
```

Figure 21 Buffer overflow rule

Deploying an IDS is accomplished by mirroring an Ethernet port with a managed switch, such as the SEL-2730M, as shown in Figure 22. The network traffic passing through the switch port is sent on to its intended destination and is also mirrored to another port where the IDS is listening.

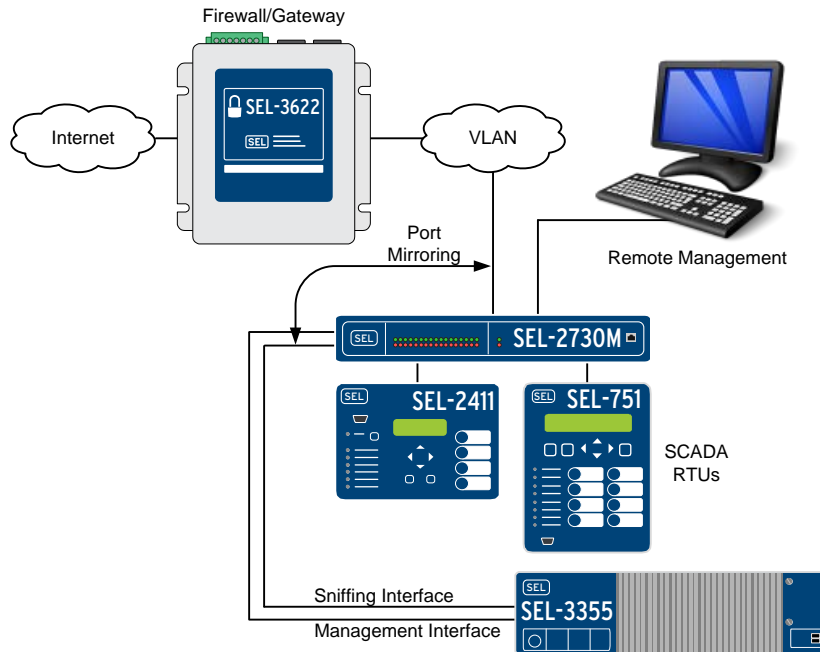


Figure 22 Intrusion detection with port mirroring

Managed Ethernet switches, coupled with reliable computers such as the substation-hardened SEL-3355, make an IDS a practical addition to SCADA and ICS networks. In addition, the availability of SCADA rules makes applying an IDS more efficient.

For more information on deploying an IDS using SEL technology, refer to [11].

## Whitelist Technology

Traditional anti-malware solutions are performed with blacklist antivirus software. The downfalls of blacklist antivirus software are system scans and constant updates. Blacklist antivirus software is also vulnerable to zero-day exploits (i.e., vulnerabilities that have yet to be patched).

The U.S. Department of Energy and several partners, including SEL, developed new technology based on whitelist malware protection. This technology is now available in secure Ethernet gateway devices, such as the SEL-3620 and SEL-3622. The technology uses a secure kernel to prevent unauthorized access to or modification of system data. It also monitors system services to detect unexpected activity caused by unauthorized modifications to the device program. Whitelist technology mitigates risks from rootkits, malware, and zero-day exploits. Because it establishes a known baseline to prevent unauthorized executables from running, it eliminates frequent antivirus signature patches. This technology results in updates being needed only when firmware updates are performed.

## IEC 61850 SECURITY

IEC 61850 is a standard for the automation of electrical substations. The data structures of the standard map operational data points to specific protocols. Ethernet and TCP/IP communications are playing an important role in IEC 61850 deployments.

The RTAC is a complete automation platform. Not only is the RTAC built with complete support for IEC 61850, but it also supports the cutting-edge security features described in IEC 62351.

The RTAC is the SEL flagship automation system for programmability, flexibility, and security. Some of its security features include unique login accounts and profiles for role-based user authorization. There is even an innovative feature for consultants and consulting engineers, which sets the temporary account to deactivate after a defined period of time. This means that consultant access is automatically removed on a future date that the operator specifies. The RTAC also makes it easy to send security information to the control center alongside the process SCADA information. This gives operators and security officers security status information in real time.

IEC 62351 is a standard that was developed for the security of IEC 61850. Some of the security features of IEC 62351 include Transport Layer Security (TLS) encryption, node authentication, message authentication, role-based access control, key management, and mandatory VLAN use for Generic Object-Oriented Substation Event (GOOSE) messages.

Robust communications network and system security is built into the RTAC. The RTAC features permissive and restrictive settings that are configurable per port, as shown in Figure 23. Web access to the RTAC is safeguarded through the use of https over TLS. HTTPS is a secure connection method that encrypts the traffic between the operator and the RTAC web interface and prevents man-in-the-middle attacks.





Interfaces						
Status	Interface Name	IP Address	Default Gateway	MAC Address	Enable Ping Enable ODBC Access Enable Web Access	Options
	Eth_01	172.16.1.150/24	172.16.1.1	00:30:a7:08:92:3d	False True True	<a href="#">Edit</a>
	Eth_02	192.168.2.2/24	192.168.2.1	00:30:a7:08:92:3e	True True True	<a href="#">Edit</a>
	Eth_F	0.0.0.0		00:30:a7:08:92:3f	True True True	<a href="#">Edit</a>
	USB_B1	172.29.131.1/24		00:30:a7:08:92:40	True True True	<a href="#">Edit</a>

Figure 23 RTAC ports can be set to allow and deny specific protocols

The vulnerabilities of cleartext communications were discussed previously. To mitigate this threat, remote engineering access sessions over Ethernet are protected by SSH between the RTAC and the calling computer. When using SSH, the RTAC will disconnect a client after three failed authentication attempts. Other network connections to the RTAC are encrypted with TLS.

The RTAC supports data communications security when using Manufacturing Message Specification (MMS).

The new IEC 62351-11 standard defines security for Extensible Markup Language (XML). XML is a method of creating common information exchange formats containing data and is used in IEC 61850 to define objects, methods, and protocol attributes.

## PHYSICAL SECURITY

Critical communications can originate, pass through, and terminate in remote sites. Physical sites are often the endpoints of communications, and isolated substations are usually not manned by employees. Pole-mounted equipment, like that shown in Figure 24, could also be a target for break-in or tampering.





Figure 24 Pole-mounted equipment

Physical security protects these assets and the sensitive communications carried over the communications network.

With the development of the SEL-3622, SEL introduced hardware and software features that help protect pole-mounted systems from physical tampering and vandalism. The SEL-3622 can report door opening by using a binary sensor or by detecting a change in light conditions using an optical sensor. An internal accelerometer detects physical events such as a jolt or movement. The SEL-3622 generates syslog events and Simple Network Management Protocol (SNMP) traps when the sensors are triggered. Secure remote access to pole-mounted equipment is available with the SEL-2925. The adapter allows personnel to keep doors closed, and security is provided with an 8- to 16-character key.

Other points to consider in physical security include the following:

- Restricting the number of technicians who can perform maintenance.
- Verifying that isolated engineering and control networks do not have the ability to connect to other networks.
- Establishing intrusion detection systems with around-the-clock monitoring.
- Locating and identifying remote telephone, fiber-optic, Ethernet, and radio links that could be tapped.
- Identifying wireless access points and verifying that authentication is enabled.
- Conducting physical security surveys at periodic intervals.

## OPERATIONAL SECURITY

Promoting a culture of security awareness is important in every organization. Where possible, physical security and cybersecurity efforts should be merged. An emerging trend in the industry is the convergence of security and information technology functions. In critical industries, it makes sense to strengthen the capability to counter security threats by unifying the management of building access, alarms, and other physical countermeasures with information security operations with an eye toward efficiency gains, increased security, and a workable security lifecycle.

Security resources are available on the SEL website at <https://www.selinc.com/cybersecurity>. These methods and training resources include items such as security awareness and training

posters and USB lockout tags (see Figure 26) that remind employees about the dangers of connecting USB devices.



Figure 25 USB lockout tags

Equipment should support contact I/O alarming on failed logins as well as privilege escalation. SEL equipment uses a range of logging notification methods ranging from contact alarm outputs that can trigger on annunciator panels to audible alarms, syslog, and Sequence of Events (SOE) reports. SEL manufactures a wide range of annunciators designed to display alarm conditions. The SEL-2523 Annunciator Panel and the space-efficient SEL-2533 Annunciator are used for indicating alarm conditions in control centers.

The security methods used by equipment manufacturers should be tested. Equipment from SEL uses the same strong methods to protect a login via a serial port or on a network port. Equipment should also support multiple levels of tiered passwords. For instance, SEL equipment for critical electric power relay systems has at least two tiers of password authentication—a nonprivileged first-tier password and a unique second-tier password for other levels of privileged operation. A first-tier password allows Level One access that only allows the user to view settings. A second-tier password allows Level Two access, which allows an elevated privilege such as the ability to change settings or perform control operations.

New innovations are occurring every day as companies create products that support increased security postures for industrial communications networks. SEL equipment features have been designed to address the unique needs of SCADA networks and for automation. One of the goals that SEL has met is to make regulatory compliance less costly and available without major process changes. For instance, the RTAC is designed as a programmable automation system. It is also a device with advanced security features, including intrusion detection, detailed notifications, event records, and logging.

New equipment should be evaluated for the security features and safeguards discussed in this paper. Security evaluation should be part of the criteria considered for each and every system purchase.

## CONCLUSION

All of the mitigation techniques and technologies presented in this paper are examples of a defense-in-depth strategy. For a SCADA protocol to be secure, it must provide end-to-end authentication, integrity, and nonrepudiation. If the protocol cannot provide these security features, then a secure wrapper (encryption) must be provided to encapsulate the communications.

Compensating controls (such as placing an encryption wrapper around serial protocols) are additional steps that must be taken to secure systems that are inherently nonsecure. They are a necessity for legacy systems. The operational security practices and controls put in place also protect SCADA systems from harm. Implementing data and user authentication and authorization with strong encryption provides a network with data integrity assurance.

Upgrades or replacement projects can also help to mitigate threats from older, legacy systems by migrating to more capable and secure platforms. Prior to this, the point application of effective security devices like the SEL-3620 can be used to proxy and protect the interfaces of vulnerable legacy systems.

This paper demonstrated that SCADA and industrial communications security is achievable with the addition of digital safeguards, layered security, and good practices, even on legacy systems.

## REFERENCES

- [1] E. O. Schweitzer, III., “Ten Tips for Improving the Security of Your Assets,” Schweitzer Engineering Laboratories, Inc., November 2009. Available: <https://www.selinc.com>.
- [2] T. Bartman and K. Carson, “Securing Communications for SCADA and Critical Industrial Systems,” proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2015.
- [3] U.S. Department of Homeland Security, “Incident Response Activity,” ICS-CERT Monitor, April–June 2013. Available: <https://ics-cert.us-cert.gov/monitors/ICS-MM201306>.
- [4] K. Coleman, “The Increased Threat of Attacks on SCADA Systems,” DefenseTech, September 2011. Available: <http://defensetech.org/2011/09/26/the-increased-threat-of-attacks-on-scada-systems>.
- [5] U.S. Department of Homeland Security, “ICS-ALERT-11-186-01: Siemens SIMATIC Controllers Password Protection Vulnerability,” ICS-CERT, July 2011. Available: <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-11-186-01>.
- [6] U.S. Department of Homeland Security, “ICS-ALERT-13-016-02: Offline Brute-Force Password Tool Targeting Siemens S7,” ICS-CERT, December 2013. Available: <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-016-02>.
- [7] F. Lüke, “Power Grid Operators Attacked Via DdoS,” The H, December 2012. Available: <http://www.h-online.com/security/news/item/Power-grid-operators-attacked-via-DDoS-1767170.html>.
- [8] K. J. Higgins, “The SCADA Patch Problem,” *Information Week*, January 2013. Available: <http://www.darkreading.com/vulnerabilities---threats/the-scada-patch-problem/d/d-id/1138979?>
- [9] P. Mell, T. Bergeron, and D. Henning, “Creating a Patch and Vulnerability Management Program, Version 2.0,” National Institute of Standards and Technology, November 2005. Available: <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>.
- [10] G. Masters, “Securing Dial-Up Modems Using ACSELERATOR QuickSet® SEL-5030 Software With the SEL-3025 and the PC Serial Security Kit,” Schweitzer Engineering Laboratories, Inc., January 2013. Available: <https://www.selinc.com>.
- [11] T. Bartman and J. Kraft, “Deploying a Network Intrusion Detection System (IDS) on an SEL Rugged Computing Platform,” Schweitzer Engineering Laboratories, Inc., December 2014. Available: <https://www.selinc.com>.

## BIOGRAPHIES

**Tom Bartman** joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2006 as an engineering technician. He is now an application specialist in communications. Prior to joining SEL, he served in the U.S. Navy as an electronics technician with an emphasis on avionics and secure communications. After leaving the Navy, he worked for Harris Corporation as an electronics engineering technician in the broadcast communications division. He has a degree in computer science, is a member of ISSA and (ISC)<sup>2</sup>, and obtained his Certified Information Systems Security Professional (CISSP) certification in 2013. Tom holds a patent for validation of arc-flash protection.

**Kevin Carson** is an alumnus of Washington State University. He has worked in the software industry as a project manager and has performed software quality assurance consulting for major software development companies. In 1997, he received a master's degree in public administration from the University of Idaho and then joined Schweitzer Engineering Laboratories, Inc. (SEL) in 1999. He is a Certified Information Systems Security Professional (CISSP) and has extensive experience in industrial security. He is currently a network engineer in security and information services at SEL. He received his first SEL patent in 2010.

© 2018 by Schweitzer Engineering Laboratories, Inc. All rights reserved.

All brand or product names appearing in this document are the trademark or registered trademark of their respective holders. No SEL trademarks may be used without written permission.

SEL products appearing in this document may be covered by US and Foreign patents.

### 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

