Securing Communications for SCADA and Critical Industrial Systems

Tom Bartman and Kevin Carson
Schweitzer Engineering Laboratories, Inc.

Presented at the
Automation Fair
Chicago, Illinois
November 18–19, 2015

Previously presented at the
51st Annual Minnesota Power Systems Conference, November 2015,
and 2nd Annual PAC World Americas Conference, September 2015

Originally presented at the
Power and Energy Automation Conference, March 2015

Securing Communications for SCADA and Critical Industrial Systems

Tom Bartman and Kevin Carson, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Secure communications within the electric power system are critical to ensuring safe and reliable electric power. Additionally, secure communications are critical to the safe flow of oil and natural gas. Around the globe, automation and communications networks face a growing number of threats that can result in malicious acts, such as unauthorized access and espionage. Most industrial sectors are in transition from legacy protocols to Internet Protocol-based (IP-based) communications. An unintended consequence of adopting IP communications is that supervisory control and data acquisition (SCADA) and industrial control systems (ICSs) have become very popular targets of attack. Access to the devices in these networks must be secured or critical equipment and information face the risk of compromise.**

In 2013, attacks on the energy sector were the highest percentage of reported security incidents among critical infrastructure. This paper investigates the risks to SCADA and industrial communications and the real-world threats these risks pose. It first discusses basic communications security concepts. It then discusses the methods used by attackers to exploit vulnerabilities in SCADA and ICSs, in addition to the state of real threats to the security and stability of electric power systems. Lastly, the paper describes how to mitigate each threat with the appropriate application of countermeasures and new technologies to keep systems secure.

I. Introduction

The overall security of critical infrastructure is essential for ensuring safe, reliable, and available services. Without viable security in place, major attacks against industrial sectors can cause significant damage. Supervisory control and data acquisition (SCADA) and industrial control systems (ICSs) are responsible for the availability of these services. SCADA refers to the collection and monitoring of sensors and systems with the purpose of helping control and/or supervise processes. ICSs are the nerve center of electric power, water, and gas systems, as well as manufacturing and production systems. It is critical that these systems have security built in from design plans to commissioning and operations.

The systems that monitor, control, and protect ICSs have come under increased threat. The intent of attacks ranges from sabotage to espionage. Therefore, when planning for security, it is important to recognize both tangible and intangible assets.

Many attacks target communications. The lack of secure methods in industrial communications presents a significant risk. For example, substations in the electric power industry communicate over copper wire, fiber, radio frequency (RF), or Ethernet. When older legacy communications protocols were established, little to no emphasis was placed on security. Due to their simplicity, these 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 security with less wiring; however, it is important to have an understanding of the methods required to secure them.

The methods that attackers use today are very real, and the threats they pose must be well understood in order to be countered. SCADA and ICSs are key components 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 electric power sector, which is focused primarily on generation, is required to meet mandated security requirements. However, solutions are available that can lower the cost of providing effective deterrence to real cyberthreats for industries that use SCADA and ICSs.

The purpose of this paper is to detail the threats that these systems face, how to detect and counter those threats, and how to apply countermeasures, new technologies, and safe practices in SCADA and ICSs.

II. SCADA and ICSs

SCADA is a popular target for attacks. Communications protocols are necessary for the movement of electric power, gas, oil, and transportation, and great interest in these systems has yielded several attacks in recent years. Some attacks were viruses specifically targeting programmable logic controller (PLC) and SCADA systems.

Even though there are proven and reliable encryption systems designed for industrial use, the overwhelming majority of SCADA systems in use do not use any authentication or encryption methods. In addition, they often use cleartext communications. This presents an attack vector, allowing the insertion of illegitimate commands or the capture, modification, and replay of system commands by an attacker. Another problem that is rarely discussed is that SCADA systems tend to be promiscuous—endpoints and concentrators accept data from any host (authorized or not). This particular weakness is the weak link exploited in nearly every major cyberattack.

As more sophisticated and successful cyberattacks are launched, more attention is being given to the security and protection of SCADA systems. According to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the energy sector is a popular avenue for cyberattacks. Attacks on the energy sector increased in 2013, and in the first half of that year, the highest percentage of

security incidents within critical infrastructure involved the energy sector [1].

Given the projected growth in the electric power market in the near future, it is essential that the security of these systems be addressed [2]. As new protocols have emerged, Ethernet has become popular in the electric power industry. With more systems connected by networks, operators must take special care to ensure that these systems are not vulnerable.

Online threats to 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 attacks, users must learn the sequence of events and methods by which an attacker is able to be successful.

SCADA systems, in addition to presenting information to operators, acquire data from remote locations. These kinds of communications between devices are the foremost attack avenue for criminals. Communications in ICSs, as well as SCADA systems, come in many forms, such as Internet protocols, RF, fiber, Bluetooth®, and older technologies, such as telephone networks.

The widespread use of encryption is new to the electric power industry. Today, encrypted protocols are in use by some progressive utilities. Relays and breakers are essential to the safe and secure transmission of electrical power. The gas in a pipeline is protected by sensors and valve controls. These systems require protection from espionage and attack from illegitimate operation commands.

III. Threat Vectors

Attackers have several methods to exploit vulnerabilities and gain unauthorized access to critical systems. This section of the paper discusses several threat vectors (i.e., the methods or means that attackers use). Understanding threat vectors is important for countering and protecting against them. There are several key threat vectors which must be understood to ensure that the appropriate security is applied.

A. Replay Attack

A replay attack occurs when a malicious user intercepts, captures, and stores communications for later reuse. For example, when the attacker faces a prompt for a password, the stored data (e.g., the captured password) is sent. Another example is an intruder who captures a wireless communications stream sent to a SCADA device plays back the command later. Replay attacks do not require a good understanding of the communications protocol. For example, a captured breaker-open command can be replayed even if it is encrypted. Unless proper mitigations are in place, the replayed message has the same effect as a legitimate message, resulting in unauthorized access or control.

B. Man-in-the-Middle Attack

In a man-in-the-middle attack, the attacker places himself between two users or devices. This is accomplished in several steps. The attacker makes an independent connection to the network, breaks the connection of the user or device under attack, then impersonates the connection to which the victim was connected. The connection is then reestablished through the attacker, and the victim's data are forwarded to the original endpoint.

Man-in-the-middle attacks exploit a lack of authentication. Once a connection is established, the attacker can control the connection, eavesdrop on data passing through, and inject false messages.

C. 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. In February 2013, ICS-CERT released a quarterly report showing a sharp increase in brute force attacks against critical infrastructure [3].

D. 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 passwords.

E. 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 attacker must first obtain information about the system.

F. Denial-of-Service Attacks

A denial-of-service (DoS) attack is launched with the intent of halting the availability of services. The attack floods a network with an abundance of requests, which saturates the network so that legitimate traffic is slowed to a halt. Electric power grid operators have been targets of DoS attacks [4]. DoS attacks are not limited to a flood of data. An alternative method exploits vulnerabilities in devices to allow an attacker to take a device such as a PLC or relay out of service. This method is not a flood of data, but it is a DoS attack.

G. War Dialing

War dialing is a technique of identifying modems. Modems are a popular target of attackers because they often connect to a company's internal network or electronic equipment. War dialing calls a range of phone numbers with the intent of discovering modems and logging their numbers for future uses, such as attempting to gain access. Once a connection is established, the attacker can obtain a command or login prompt. If a banner is included in the prompt, the attacker can glean information about the device, such as the device type, manufacturer, and location.

H. Default Passwords

Default passwords may be the greatest risk to organization systems. Many devices use default passwords, specific to the device manufacturer, that should never be assumed to be secret. One 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 for the access and control of a targeted SCADA system. Keeping default passwords in equipment poses a significant risk of unauthorized access.

I. Data Modification

Data modification is when an attacker changes data prior to reception and processing at their destination. Contrary to popular belief, the risk of data modification is not mitigated in Ethernet protocols by encryption alone. An attacker can modify an encrypted packet just as easily as if it was unencrypted, though the attacker may not know what the change will do. Encryption without authentication is inadequate to stop this type of attack. For example, if the encrypted command **DkeFA3d03** is changed to **DkFFF3do3**, the command string could trip a breaker.

Although no risk can be completely eliminated, a proper operations security implementation mitigates the threats outlined in this section. The remainder of this paper focuses on the methods to detect, counter, and mitigate these individual attack methods.

IV. Securing Internet Protocol

There are many methods, programs, and techniques to eavesdrop, sabotage, or access systems. Many of these methods are associated with Internet Protocol (IP) communications. Mitigating these types of attacks requires a basic understanding of encryption methods. This section presents a basic overview of encryption and authentication.

A. Internet Protocol Security Offers Encryption and Authentication

Internet Protocol Security (IPsec) is a standardized framework for securing IP communications over a trusted or untrusted network. IPsec provides confidentiality, integrity, and authentication. Strong encryption algorithms provide confidentiality, while integrity is provided with the use of message validation schemes known as checksums and hashes. A hash is a one-way mathematical function that transforms a string of data into a fixed-length value known as a hash value. This one-way operation means that the input data cannot be re-created from the hash value. Hash values are used as digital fingerprints. By comparing the hash value of a sent message to the hash value of a received message, the receiver can verify that the message was not tampered with.

IPsec builds a secure tunnel of communications between two endpoints, as shown in Fig. 1. The protocol exchanges secret keys between the two endpoints. Once the tunnel is established, the sender and receiver agree on the encryption algorithm to use.

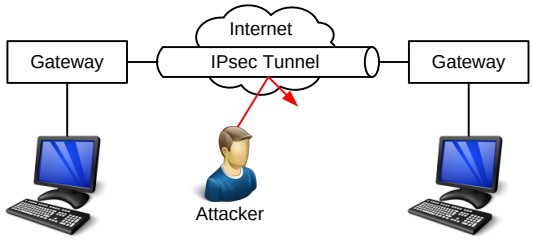

Fig. 1. IPsec secure tunnel

IPsec uses two protocols for data transfers, which are summarized in Fig. 2.

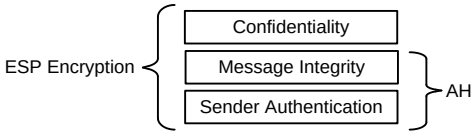

Fig. 2. ESP and AH work together

1) Authentication Header (AH)

The AH protocol authenticates IP traffic but performs no encryption. The authentication is performed by calculating hashed messages over the packet of data.

2) Encapsulating Security Payload (ESP)

The ESP protocol provides confidentiality by encrypting data. In addition to confidentiality, ESP provides authentication, integrity, and anti-replay. ESP can be used with or without the AH protocol.

Wrapping SCADA traffic in a protective IPsec stream provides secure communications between a gateway and end devices, such as PLCs or relays.

B. Advanced Encryption Standard Encryption

The Advanced Encryption Standard (AES) is a United States government-accepted and globally recognized standard for encoding data. AES operates by splitting data into blocks called matrixes 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 (i.e., an algorithm in which a single key is used for both encryption and decryption).

C. Logging and Audits

One of the 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. Stealth is the goal of the intruder.

Many attacks are built to operate silently 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 after enough 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. Many devices available today provide event logging. Logs contain information such as a history of logins and the state of a device. Syslog is a protocol used to send these events to a data collection server or security information and event management (SIEM) server. Because Syslog protocol is standardized, software packages can analyze the data to generate reports and security metrics.

A cybersecurity solution must include logging features that address the requirements of regulatory bodies and good security practices.

V. Mitigation Techniques

The objective of any security plan is to reduce risk. Previous sections of this paper discussed the numerous methods attackers use to gain access, gather intelligence, and execute malicious activities. Each form of attack has a mitigation technique.

Recall that in a replay attack an intercepted password or encrypted control command is replayed. With IPsec protocol, a sequence number is incremented for each packet sent. These sequence numbers prevent replay attacks.

A similar technique exists for man-in-the-middle attacks. Defense against such attacks is accomplished through authentication. Strong encryption with authentication provides such defense. As mentioned in Section III, encryption alone is inadequate for some types of attacks.

Defense against data modification also relies on authentication. One method of authentication is a keyed hash-based message authentication code (HMAC) used within the IPsec protocol. Using a hash function along with a key generates a message authentication code. The following is the definition of the HMAC function used to authenticate communications, per the Internet Engineering Task Force (IETF®) Network Working Group Request for Comments (RFC) 2104 [5]:

$$\mathrm{HMAC}(K, m) = H\left((K \oplus \mathrm{opad}) \mid H\left((K \oplus \mathrm{ipad}) \mid m\right)\right)$$

where:

K is a secret key.

m is the message to be authenticated.

H is a cryptographic hash function, such as SHA-1 or MD5.

$\oplus$ denotes the XOR logic function.

opad is the outer padding constant (0x5c).

| denotes concatenation (i.e., joining two character strings end-to-end).

ipad is the inner padding constant (0x36).

HMAC is used to verify both the integrity and authenticity of the data by calculating an authentication code. The authentication code uses a cryptographic hash function along with a secret cryptographic key. 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, identifying the data as nonauthentic. HMAC authentication acts like the protective seal found on bottles of pain killers. If the protective seal is broken, it should be thrown out. This is what HMAC does programmatically.

VI. Mitigation Controls

Encryption with authentication is the first step in mitigating risks to communications. Previously, the paper discussed how encryption alone does not prevent data modification or replay attacks. However, mitigation controls are required for legacy equipment, such as dial-up modems.

Dial-up modems are still widely used for remote access into engineering segments of utilities. This presents the risk of unauthorized access. War dialing software is available for an attacker to identify modems. The best practice is to disconnect any modems not in use. Some utilities require a phone call to an operations center to request access to a modem. After access is granted, the modem is physically switched into the system. If this method of switching is not a possibility, consider whitelisting inbound numbers or enabling a call-back feature.

Attacks on passwords, such as dictionary and brute force attacks, exploit weak passwords. Recent breaches into physical devices were successful because the passwords were never changed from the factory defaults. It is a fair assumption that if a manufacturer has default passwords, or backdoor passwords, a potential attacker knows them. Change the default passwords left in equipment by the manufacturer to strong passwords. A good password policy requires a minimum number of characters, one or more symbols, and a combination of uppercase and lowercase characters. For devices that cannot support the full character sets and lengths required for strong passwords, use a security gateway, which can support strong passwords and act as a proxy for the device. With a security gateway, strong passwords are used and a secure tunnel wraps the password between the user and the device.

For greater security, use a passphrase. A passphrase is a sequence of words that is typically longer than a password. Passphrases such as **Oaks Sub$tat1on Deliv3rs!** make dictionary and brute force attacks difficult. Note that transposing alphanumeric characters increases the strength of the passphrase.

DoS and distributed denial-of-service (DDoS) attacks require special attention. A DoS attack can typically be defeated by filtering and rejecting the source IP address. However, a DDoS is much more difficult and must be handled by a network team.

Firewalls are important mitigation controls. In simple terms, firewalls allow or deny traffic to relays, intelligent electronic devices (IEDs), or other devices. A firewall analyzes data packets and, based on a set of rules, determines if the data should pass to the device.

Every day new vulnerabilities are uncovered in computer systems and their operating systems. These vulnerabilities are

a serious risk because computer systems reside inside the organization and are potentially connected to critical equipment. As new vulnerabilities are discovered, firms work to issue patches. According to the National Institute of Standards and Technology (NIST), timely patching of security vulnerabilities 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 attacks [6]. Before beginning a patch and vulnerability management program, an inventory of system devices is required; an unpatched and unaccounted-for computer is at risk of exploit. Organizations should use automated patch management tools to monitor for vulnerabilities.

VII. Protecting SCADA and ICS Communications

One of the key intentions of this paper is to address the risks introduced by remote access and how to secure all engineering access points. This section brings together the previous discussions and presents the application of countermeasures. In addition, a discussion of secure communications, with examples, is presented. Mitigating risk to a system is the main goal in security, and this section outlines the requirements for accomplishing this goal.

A. Dependable Communications for Wide-Area Network Infrastructure

Reliable communications across a wide-area network (WAN) are often achieved across a synchronous optical network (SONET) ring. SONET communicates over fiber-optic rings, which provide redundant paths in case a piece of fiber breaks. This redundancy makes SONET a good choice for dependable communications in critical applications.

Linking a WAN to a local-area network (LAN) is achieved through a multiplexer. In the example in Fig. 3, four sites at different locations are linked through a SONET communications ring.

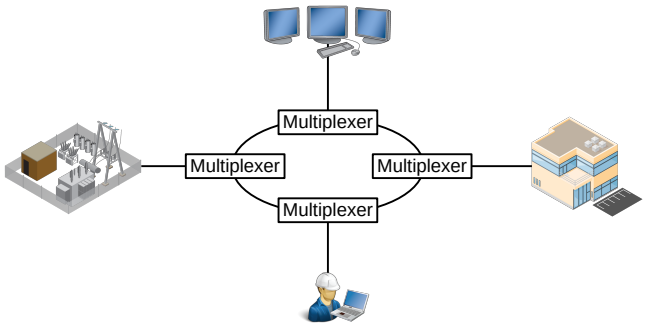

Fig. 3. A utility WAN communications example

A multiplexer should support the application of AES security on the SONET ring. Transmissions between adjacent nodes must be strongly encrypted. Some SONET multiplexers are configurable to use 128-bit or 256-bit key strengths, with negligible increases to transmission times. Authentication is provided through HMAC. Multiplexers are often specifically designed to meet the needs and latency requirements of the electrical utility industry.

The encrypted ring protects the most exposed portion of the communications channel—the fiber that forms the rings running between substations and control centers and that is not in a physical building. This encryption provides a formidable deterrent to tapping and protects the fiber medium from eavesdropping.

B. Ethernet Communications Security

The first step in establishing Ethernet security is access control. Controlling access to relays and IEDs can be accomplished by means of a security gateway, as shown in Fig. 4.

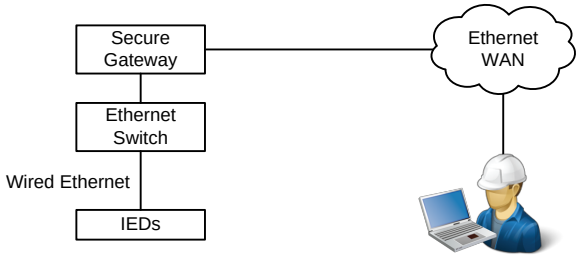

Fig. 4. Ethernet communications security concept

A security gateway should employ some method of authentication. Most organizations use Lightweight Directory Access Protocol (LDAP) as their database of authorized user accounts and passwords so that the security of the system and accounts can be managed in a centralized location. Centralized authentication improves security by providing a scalable and manageable way to perform user-based authentication on a large number of devices.

A security gateway also helps to manage the IED passwords, ensuring that password changes happen regularly and that passwords conform to complexity rules for stronger security. An authentication proxy feature provides user-based single sign-on access to several Ethernet and serial devices. Small security gateways fit in enclosures and structures where space is limited.

Encryption provides confidentiality for Ethernet communications, while authentication provides integrity. Anti-replay protections built into the protocols and encryption standards prevent attackers from effectively capturing an encrypted session with a packet capture tool and replaying it. Attackers are further thwarted from passing through the interface from the outside world to the hosts inside. Authentication prevents an attacker from injecting frames into the encrypted stream of protected packets. The attack will be foiled, as shown in Fig. 5, and any traffic will be dropped at the interface—a barrier consisting of a combination of authentication and encryption. The use of AH protocol results in an authentication failure of the forged packet, which prevents the attack.

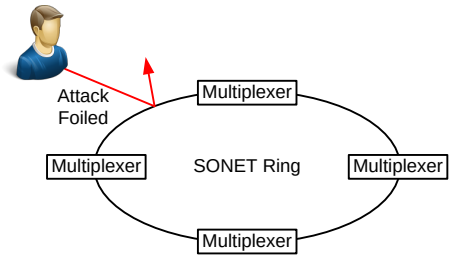

Fig. 5. Attacker foiled in forged packet attempt

Another layer in Ethernet security is access through switching. Consider Media Access Control (MAC) address security. The addresses in 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 these MAC addresses into the switch configuration on a per-port basis.

After building an Ethernet network in a substation, users may choose to implement other MAC address security features, such as count lock. Count lock enables the operator to enter the total number of MAC addresses to learn. The Ethernet switch gathers MAC addresses until the counter reaches the parameter that the operator has entered. MAC security is then locked until the operator needs to add more hosts. Another security feature is time lock. Time lock is used by entering a time period for the switch port to learn new MAC addresses. Users can use this feature to capture the endpoints during the initial commissioning of a network. MAC security is most effective when a single host is connected to a dedicated port.

All Ethernet communications devices should have monitoring and auditing enabled. Logging features 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. These data can be fed to networked intrusion detection systems (IDSs) or remote logging servers.

New technology exists for detecting Ethernet link statuses as a method of detecting vandalism. Some Ethernet security gateways now include a contact output that can be asserted in the case of a loss of link. This could occur as the result of an act of vandalism in which a cable is cut or removed. In the case of a field cabinet, such as a pole-mounted cabinet, the control center can be notified through an out-of-band communications medium, such as a dedicated radio or fiber connection.

C. Wireless Communications Security

Wireless communications are used in SCADA networks because of their convenience and flexibility in reaching remote installations where other communications cannot be established. Private wireless communications offer attractive cost savings. Even though the predominant method is point-to-point wireless connections, interception remains a concern. In the example in Fig. 6, two remote sites (a substation and a protective relay) are linked via a secure wireless scheme.

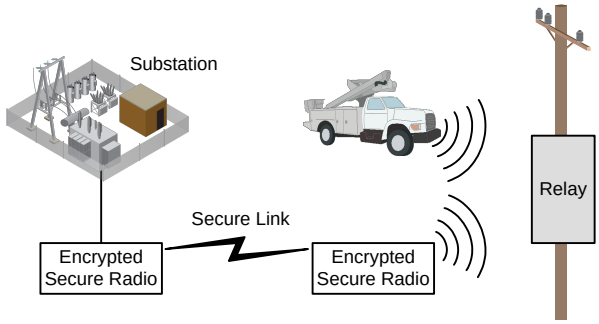

Fig. 6. Secure wireless communications

Many electric utilities use RF communications. When doing so, it is important to secure these transmissions over the air. In order to repel malicious attacks or information gathering via eavesdropping, authentication and encryption must be implemented. Serial radio transceivers should support session authentication and strong encryption, such as 256-bit AES technology.

In addition to RF, field service vehicles can also communicate with remote devices via Bluetooth. Bluetooth adapters are available for short range communications that enable field technicians to service equipment from their service vehicles. Pole-mounted equipment can be accessed for maintenance without the need for climbing or opening the enclosure. Bluetooth serial adapters should use Bluetooth v2.1 + Enhanced Data Rate (EDR) security. An extra level of security is provided by secure simple pairing (SSP). SSP ensures that only Bluetooth devices with v2.1 and EDR are able to connect to each other. This pairing of encryption and authentication makes them secure for SCADA applications.

The ability to communicate through new secure Bluetooth adapters keeps cabinet doors closed. Consider these new technologies when planning upgrades to existing installations or new system implementations.

D. Serial Communications

Serial networks are well established throughout the power and industrial control industry and are an important part of the communications infrastructure. Until recently, serial communications were vulnerable to tapping, intercepting, and replaying commands.

The introduction of serial encryption devices has solved this problem and using them closes a serious avenue of attack. Serial communications can now be placed in a secure wrapper that prevents data injection, espionage, and replay attacks. A serial encryption device protects communications over the SCADA network with AES encryption. A serial encryption device also prevents data modification and replay attacks by using HMAC authentication.

E. Precision Time

Precise time synchronization has become a critical component of modern power systems. The need for submicrosecond precision has become a requirement for some fault location applications [7]. An advantage of precise time, from a security perspective, is that it can be used for precision

logging. Precision logging is very important for security audits and for evaluating logs and time-stamped reports in reconstructing an incident. Modern clocks can provide IRIG-B and Network Time Protocol (NTP), and time information can be distributed over a SONET network.

F. Backdoor Passwords and Maintenance Accounts

A significant source of exposure for organizations is devices that have backdoor passwords and maintenance accounts, which are commonly used for equipment access. Backdoor accounts, if they exist, can give elevated access rights to whoever logs in (including malware). Insist that manufacturers disclose in writing if they have any such mechanism in place.

G. Secure Engineering Access

Remote access to SCADA and ICS networks is a mission-critical need. Reliable remote access is a must-have 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 firewalled.

Fig. 7 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 a security gateway. The gateway provides a central point of entry with user-based access control and detailed activity logs. Authentication and encryption are also provided.

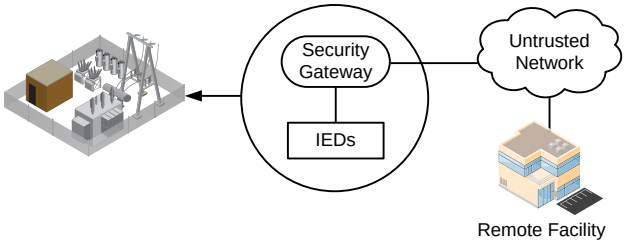

Fig. 7. Engineering access over an untrusted network

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

Take, for instance, an application of remote access via a plain old telephone service (POTS) circuit. Dial-up connections via a modem occur over an untrusted telephone circuit. An attacker can access and alter the communications by injecting malicious data. When using serial communications for remote access, it is imperative to encrypt the communications to and from the engineering workstation using serial cryptographic transceivers. These transceivers provide a secure SCADA link by authenticating and optionally encrypting the communications.

In Fig. 8, the serial encryption provided by the serial cryptographic transceiver protects the communications 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.

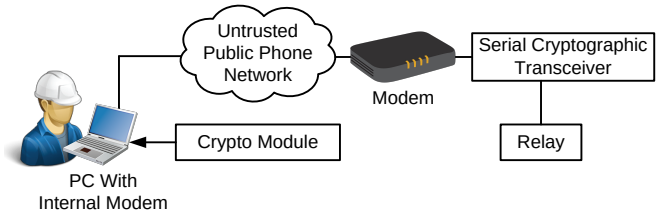

Fig. 8. Dial-up secure remote access

Finally, with remote engineering access, never forget auditing (i.e., determining who has accessed the network and devices). Analyze not only the rejected logins but also the accepted logins.

H. Authentication

Section III discussed the importance of authentication and that encryption alone does not prevent attacks that exploit a lack of authentication. In the case of an advanced persistent threat (APT), targeted attacks on a specific organization system indicate that the malware knows the system on which it is installed (i.e., it has been designed to attack that specific system design). These types of attacks can be prevented by using a method of authentication. For SCADA and ICS networks, defining which networks talk to which networks—even down to which ports and protocols—is an option for authentication. This is done by defining the range of hosts and networks that the SCADA or automation equipment can communicate with.

I. 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, along with several partners, developed new technology based on whitelist malware protection. This technology is now available in some secure gateway devices. The technology uses a secure kernel to prevent unauthorized access 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.

J. Tamper Detection

Critical communications originate from, pass through, and terminate in remote sites and field cabinets, like the one shown in Fig. 9. These communications endpoints are isolated from substations and are not manned by employees. Methods to detect intrusion attempts and vandalism can be introduced into equipment at these sites.

Fig. 9. Pole-mounted field cabinet

Pole-mounted equipment, such as recloser control cabinets, can be a target for break-in or tampering. New technology is available in some security gateway devices to notify of tampering and vandalism with the use of movement, light level, and/or binary sensors.

Some equipment contains an optical sensor to detect when a cabinet door is opened by sensing changes in light conditions. In addition to light sensors, a contact input can be used for receiving a trigger from a door contact.

Other sensors can detect a jolt or sudden movement through the use of an internal accelerometer. In such conditions, an alarm can be generated. A tilt sensor can detect if someone is physically handling a device.

When a state change occurs in the various sensors, the device generates and sends the proper notification via Syslog protocol and a Simple Network Management Protocol (SNMP) trap. It then pulses a contact output. For instance, the contact input on the device sends notifications on recloser door-open events. Requiring a combination of physical tamper indications before alarming reduces false tamper alerts. If a kinetic event and a door-open event both occur, the likelihood is higher that a serious problem has occurred. The suppression of false positives provides confidence that an alarm is definitely a tamper event.

For the event of a remote cyberattack or physical equipment manipulation, alarms can be triggered when the Ethernet cable is connected or disconnected. Using the Ethernet link status as an indicator, an alarm can be triggered via output contacts. The alarm can be sent via an out-of-band communications medium, such as a dedicated radio or fiber connection.

K. Separation

Multilayer security allows for unique security controls at each layer, as shown in Fig. 10. Critical assets are put at the most reliable and secure layer. Not only must an attacker compromise the perimeter, the security controls at each additional layer must also be compromised to reach the target asset. Reliable and rugged Ethernet switches and security gateways allow for this type of layered framework in SCADA and ICS environments.

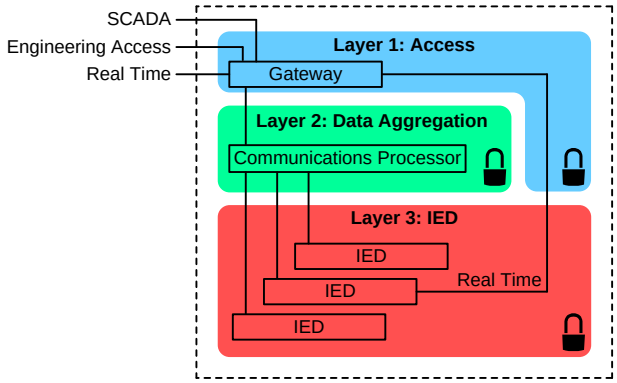

Fig. 10. Multilayer security framework

In Fig. 10, Layer 1 is the access zone where perimeter gateway security exists. The function of this zone is secure access, and it is here that password management takes place and access security is managed. The firewall and port server at this level also provide secure transport and manage traffic flows and encryption for machine-to-machine connections and human-to-machine interactions. The gateway secures the pathway between the industrial and central control networks. Also at this layer are firewall functions, virtual private network (VPN) and encryption technology, port server access, and endpoint-to-endpoint SCADA rules and logging.

Layer 2 is the intelligence zone. Data concentration, switches, and controllers are at this layer. It is here that Ethernet port security, virtual LANs (VLANs), and traffic policing occur. VLANs are used to restrict broadcast domains.

Layer 3 is the IED zone where the critical assets are located. It is here that the operator interacts with the human-machine interface (HMI). This layer is where individual devices are configured by operators and time-critical data are received and forwarded to other devices. Ethernet switches with port security are used here. This layer's network can be expressed by multiple types of topologies, such as ring or mesh, depending on the need. If there is a requirement to separate application traffic within the zone, two Ethernet channels can be built within a single-ring (or two-ring) design with a different VLAN for each.

L. 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 reliability of these computers 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. These computers withstand harsh environments and extreme temperature ranges by using new thermal designs that allow for quick heat dissipation without fans or vents. These new designs also operate 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.

M. Network Intrusion Detection

A network 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 having allowed the system to be exposed to the outside world. An IDS would have proven to be valuable in detecting 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 Fig. 11. The rule contains information on how to inspect each packet and how to alert if action is necessary.

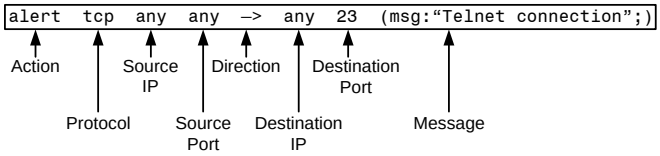

Fig. 11. Intrusion detection rule

Some threats may originate from within an organization. These threats can be discovered because an IDS also analyzes traffic between devices. In the following example, the rule is used to detect a possible buffer overflow or DoS attack. Because the maximum size of a Modbus® TCP packet is 260 bytes, the rule checks for a packet size of greater than 300 bytes. In the event that the packet in Fig. 12 is seen, a formatted log event will be generated.

```
alert tcp $MODBUS_Client any –> $MODBUS_Server \
502 (dsize:>300; msg:“Illegal Modbus TCP Packet Size”;)
```

Fig. 12. Buffer overflow rule

Deploying an IDS is accomplished by mirroring an Ethernet port with a managed switch, as shown in Fig. 13. 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.

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

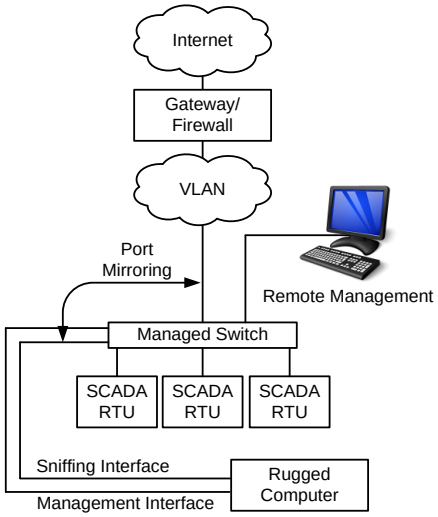

Fig. 13. Intrusion detection with port mirroring

VIII. 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 play an important role in IEC 61850 deployments. When implementing an automation system, consider including unique login accounts and profiles for role-based user authorization. Create temporary accounts for consultants and consulting engineers that will deactivate after a defined period of time. This causes consultant access to be automatically removed on a future date that the operator specifies.

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.

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

IX. Conclusion

For a SCADA protocol to be as secure as possible, it must provide end-to-end authentication, integrity, and nonrepudiation (i.e., a proof-of-integrity mechanism that

provides evidence so that the sender and receiver of a message cannot deny having participated in the exchange of communications). If the protocol cannot provide these security features, then users must provide a secure wrapper (encryption) to encapsulate the communications.

Compensating controls, such as placing an encryption wrapper around legacy serial protocols, are additional steps that must be taken to secure systems that are inherently nonsecure. They are a necessity for legacy systems. Remember, operational security practices and controls also protect SCADA systems from harm. Implementing data and user authentication and authorization with strong encryption provides networks with data integrity assurance. Getting upgrades or replacement projects on the drawing board can also help to mitigate threats from older, legacy systems by migrating to more capable and secure platforms.

Know the system. Verify that isolated engineering and control networks do not have the ability to connect to other networks. Locate and identify entry points into the network, such as remote telephone, fiber-optic, Ethernet, and radio links. Also identify wireless access points, and verify where authentication is enabled. Finally, conduct physical security surveys at periodic intervals.

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

X. References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," IETF Network Working Group Request for Comments: 2104, February 1997. Available: https://www.ietf.org/rfc/rfc2104.txt.

[6] 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?.

[7] S. T. Watt, S. Achanta, H. Abubakari, and E. Sagen, "Understanding and Applying Precision Time Protocol," proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2014.

XI. 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 $(ISC)^2$, 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 and received his first SEL patent in 2010.

20150122 • TP6678-01