Evaluation of Security Solutions in the SCADA Environment

Robert D. Larkin
Air Force Institute of Technology

Juan Lopez Jr.
Air Force Institute of Technology

Jonathan W. Butts
Air Force Institute of Technology

Michael R. Grimaila
Air Force Institute of Technology

Abstract

Supervisory Control and Data Acquisition (SCADA) systems control and monitor the electric power grid, water treatment facilities, oil and gas pipelines, railways, and other critical infrastructure assets. With the advent of greater connectivity via the Internet, organizations that own and operate these systems have increasingly interconnected them with their enterprise network to take advantage of cost savings and operational benefits. Now, these once isolated systems are susceptible to a wider range of threats resulting from new pathways into the network that previously did not exist. Recommendations for safeguarding SCADA systems include employment of traditional information technology (IT) security solutions; however, mitigation strategies designed for IT systems must first be evaluated prior to deployment on a SCADA system to quantify and to minimize the risk of adverse operational impacts. This article examines the employment of traditional IT security mechanisms in the SCADA environment. We provide considerations that should be evaluated prior to deploying security controls to mitigate negative impacts on operations. A case study is provided that evaluates a host-based intrusion detection system and a petrochemical fuels management SCADA system.

Keywords: Critical Infrastructure Protection, SCADA security, Host-Based IDS.

ACM Categories: C.2, C.2.0, C.3, C.4

General Terms: Security; Experimentation; Supervisory Control and Data Acquisition (SCADA); Critical Infrastructure Protection

Introduction

Virtually all organizations have embedded Information and Communication Technologies (ICT) into their core organizational processes as a means to increase operational efficiency, improve decision making quality, reduce delays, and/or maximize profit. However, this dependence can place the organization mission and safety at risk when an event causing the loss, corruption, or degradation of, or access to, a critical information resource occurs. Our society as a whole is dependent upon Supervisory Control and Data Acquisition (SCADA) devices, which control and monitor critical infrastructure systems. Yet, the number of associated devices connected to the Internet and vulnerable to attack is alarmingly high. In a recent study, Leverett identified 3,920 SCADA devices within the United States that were accessible via the Internet (Leverett, 2011). Because of the accessibility, SCADA devices are subject to not only targeted attacks, but

Disclaimer

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

attacks that inadvertently propagate to the control systems. For example, in 2003, the Slammer worm infected a computer network at the Davis-Besse nuclear power plant in Oak Harbor, Ohio (Dacey, 2004). The worm targeted a Structured Query Language (SQL) vulnerability commonly found on traditional Information Technology (IT) networks. Even though Slammer did not specifically target the SCADA system, the infection resulted in the malfunction of the plant's process computer, disabling the safety monitoring system for nearly five hours, and generating traffic that degraded network communications at five other utilities. Further, Slammer's increased network traffic also degraded other physical systems to include automatic teller machines and airline reservation systems (Chen, 2010).

More recently, the sophisticated Stuxnet worm represents a targeted cyber attack against SCADA systems. It has been described as "the most technologically sophisticated malicious program developed for a targeted attack" (Matrosov, et al., 2010). According to security experts, Stuxnet is believed to have targeted Iran's nuclear program impacting both the Bushehr nuclear plant and the Natanz uranium enrichment facility. The worm targeted control systems running a Siemens Programmable Logic Controller (PLC), and utilized four different Windows "zero-day" exploits to gain access to computers and search for the Siemens' PLC software (Chen, 2010). A "zero-day" exploit occurs when a threat exploits a computer application vulnerability that is unknown or is yet undiscovered by the system developer.

The deployment of IT security mechanisms can offer SCADA systems a level of protection against attacks. The majority of security guidelines (Cai, et al., 2008; Igure et al., 2006; Katzke et al., 2006; Stouffer, et al., 2013) recommend employment of firewalls, proxies and intrusion detection systems. Although such strategies may not mitigate targeted attacks implemented by motivated actors as in Stuxnet, they can be effective in preventing incidents similar to the Slammer virus noted above that impacted a nuclear power plant. Unfortunately, many SCADA devices and subnets are exempt from security protections primarily because the impact to operations is largely unknown. Determining the effects that a security solution may have is often difficult due to the expense or impracticality of replicating the production system along with the inability to take the system off-line to evaluate the solution. Replicating a SCADA system for the purpose of testing security solutions is significantly problematic for critical infrastructure due to sector interdependencies, customized system configurations, and high density of proprietary protocols still in use. Furthermore, popular automated software tools used to scan for open ports or vulnerabilities, which pose minimal risk to business enterprise networks, can cripple a SCADA network (Smith, 2006). Verba and Milvich (2008) posit that current IDS sensors also have difficulty working within a SCADA environment. All this makes for more sophisticated SCADA systems tied closer to Internet networks, making them more vulnerable to security issues (Thilmany, 2012).

In this article, we examine the employment of traditional IT security mechanisms in a SCADA environment. We identify considerations that should be evaluated prior to employment to ensure no negative impact occurs in operations. A case study is provided that uses the considerations presented to evaluate a host-based intrusion detection system integrated into a petrochemical fuels management SCADA system. In addition, implications for researchers in SCADA security are also discussed. Conceptual differences between SCADA and ICT which potentially constrain cybersecurity technical solutions are also explored. Findings demonstrate that the research approach is cost effective and provides a reasonable approach to compliment current risk management processes for SCADA system security.

Background

SCADA Overview

Control system history is rooted in early rocket telemetry and railway systems (Boyer, 2009). Rocket tests required a method to collect data and transmit it to the ground before the rocket exploded. In railways, central offices used wired communications to monitor train position and the status of switches. The benefits of remote capabilities were soon realized and transitioned to other applications. As technology progressed, the methods of communication transitioned from radio, to leased phone lines and modems, to networking technologies. Today, modern control systems often employ TCP/IP for device communications, mainly to leverage the flexibility and cost of commodity LAN and WAN technologies.

SCADA systems are industrial control systems (ICS) that manage, direct and monitor the behavior of large-scale, distributed systems in the critical infrastructure sectors. Common SCADA networks include water treatment facilities, oil and gas pipelines, railways and

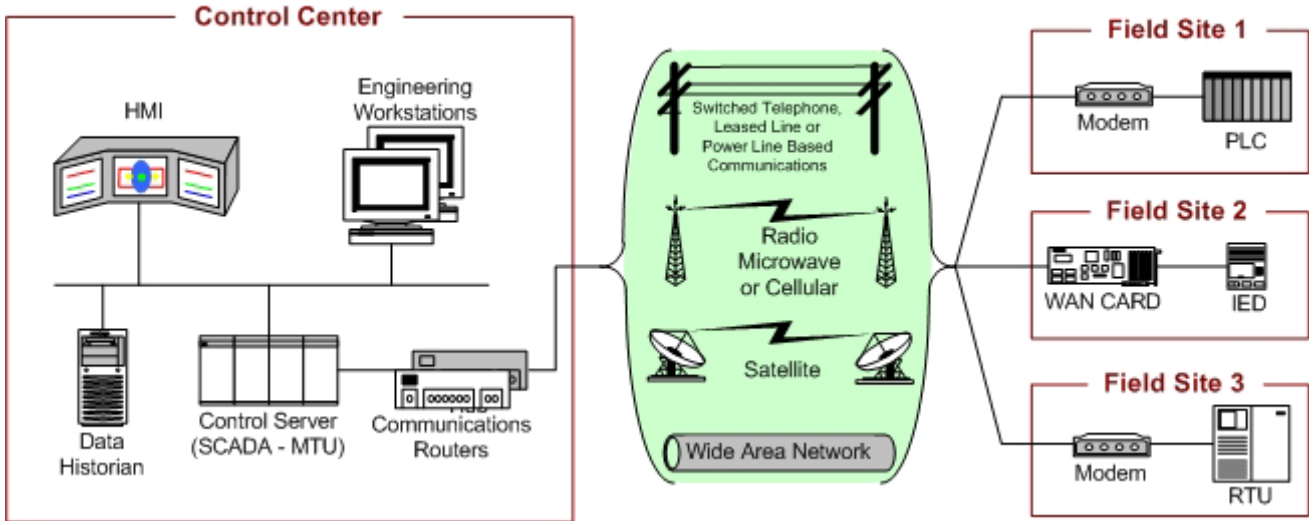

Figure 1. SCADA System General Layout (Stouffer et al., 2013)

the electric power grid (Stouffer, et al., 2013). Figure 1 presents a simple SCADA system representation.

SCADA systems use central control centers, typically with a human machine interface (HMI) for an operator in the loop to control and monitor remote processes. Remote terminal units (RTUs), programmable logic controllers (PLCs) and intelligent electronic devices (IEDs) are example field devices that communicate with the monitoring stations and convert digital control messages into physical actions such as opening and closing valves and circuit breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

The communication architecture for industrial control systems uses a hierarchical, request-response paradigm for message transmission between controller devices and remote field devices. The controller sends request messages to the outlying field device to gather operating data or to specify control actions. The field device collects discrete and analog sensor data and maintains actuator settings specified by the controller. Response messages are generated by the field device after direct requests from the controller. Additionally, the field device may notify the master when alarm conditions are detected. Devices common to SCADA networks include both mechanical and computerized devices that must adhere to strict safety, availability, and reliability requirements. For example, the NERC (North America Electric Reliability Corporation) CIP (Critical Infrastructure Protection) standards CIP-001 through CIP-009 provide a cybersecurity framework for identification and protection of critical cyber assets to support reliable operation of the bulk electric system (NERC, 2012). The banking and finance; communications; energy; health care and public health; information technology; nuclear reactors, material, and waste; and water have similar guidance tailored to business needs of entities or provides methods to address unique risks or operations.

Even though DHS and other lead agencies for these sectors have disseminated and promoted cybersecurity guidance, the GAO (2011) discovered that they have not identified key cybersecurity guidance applicable to or widely used in each of their respective critical infrastructure sectors.

Differences between SCADA and IT Networks

Due to the critical nature of the processes controlled and monitored by SCADA systems, it is vital that they operating continuously with little to no downtime or delay in transmitting control signals and process data. These systems were designed to meet performance, reliability, safety, and flexibility requirements (Stoufffer et al., 2013). Moreover, the impact to systems has been shown to cost millions of dollars, depending on the length of downtime (Miller, 2005). Furthermore, a simple port scan, which is of minimal risk to a corporate network environment, can wreak havoc on a SCADA network thus causing numerous system malfunctions (Smith, 2006). Such issues demand scrutiny of the differences between SCADA and IT. An approach to compare the differences between SCADA and IT systems is through comparison of the protection goals of each system.

Assurance for IT systems is generally evaluated according to the confidentiality, integrity and availability triad. Confidentiality ensures there is no disclosure of information or data to unauthorized individuals or systems. Integrity ensures that a system performs in the manner it was intended with no alteration or manipulation of information or functionality. Availability ensures system services and data are not disrupted and are accessible when required.

Traditional IT security goals, on average, are prioritized as (1) confidentiality, (2) integrity, and (3) availability whereas ICS security goals are inversely focused on (1) availability, (2) integrity, and (3) confidentiality (Weiss, 2010). The lack of focus on confidentiality is not surprising for three plausible reasons (1) value of information, (2) processing overhead, and (3) protocol supportability. First, telemetry data has a rapid decay rate with regard to the usefulness of real-time information for a process. ICS data typically has low informational content value (e.g. current device position, temperature, or pressure) unlike sensitive corporate documents or privacy information (e.g. personally identifiable information) found in corporate IT networks. An exception in critical infrastructure is the current privacy issue with regard to smart meters (Smart Grid Interoperability Panel, 2010). Secondly, SCADA system cryptography for integrity and authentication is also minimal because of the overhead associated with key management, the limited processing power of many field devices, and the requirement that various control system implementations must fail-safe (i.e. safety-instrumented systems). Since these systems are required to run in a deterministic environment, any change to the SCADA systems that could slow the systems down, induce latency in communications, or bring the systems offline is not permissible (Krutz, 2006). Finally, the communication protocols for control systems are often simply layered on top of existing and unsecured internet protocols for network-based communications. One reason for the lack of supportability is many SCADA protocols are proprietary, often undocumented and ported from insecure serial protocols to an IP network stack (Verba and Milvich, 2008). Most ICS protocols do not have rudimentary authentication or encryption options and even those that can theoretically be securely configured (e.g., Modbus and ICCP) require substantial effort to secure (Weiss, 2010). Additionally, traditional IT networks undergo near constant change due to the installation of new applications that produce unpredictable traffic patterns. Compared to traditional IT networks, SCADA networks have dedicated applications running services that must be available continuously for long periods.

From an assurance perspective, availability is typically the main concern for SCADA systems due to the critical nature of the operations they control. Often, SCADA systems are left unpatched because they cannot afford downtime or because updates can bring down the system (Byres, Leversage & Kube, 2007). Current SCADA system operations do not typically allocate managed downtime to implement patches or system upgrades like their counterpart business enterprise IT networks. In other cases, security patches may actually violate the certification of control systems (Krebs, 2008).

In addition to the differences discussed, ICS have additional characteristics that differ from traditional IT systems. They have different risks and priorities, performance and reliability requirements, and use of operating systems and applications that may be considered unconventional to typical IT support personnel. Additionally, safety and efficiency can sometimes conflict with security in the design and operation of control systems. For example, requiring password authentication and authorization should not hamper or interfere with emergency actions for ICS. As outlined in Table 1, Wei et al. (2010) and Stouffer et al. (2013) summarize a variety of salient differences between SCADA and IT systems. Indeed, these attributes emphasize operational, reliability, and safety concerns associated with implementing any security solution that may affect operations. As such, the control systems operational community has been reluctant to employ security solutions to the SCADA environment. With the trend to interconnect SCADA devices via networks and the manifestation of recent threats, however, leaving systems unprotected is no longer a viable option.

Table 1. Differences Between SCADA and IT (Wei et al., 2010[1]; Stouffer et al., 2013[2])

Item	SCADA Networks	IT Networks
Objectives[1]	Concerned with system availability and reliability	Concerned with data integrity and confidentiality
Architectures[1]	Use control servers, RTUs, PLCs, field devices, and HMIs	Utilize traditional IT assets like computers, servers, routers, firewalls, and proxies
Technology Bases[1]	Use many different communication protocols (e.g. DNP 3.0, ICCP, IEC61850) which are very difficult to develop common Host-Based or Network-Based security solutions	Technology base includes Windows, Unix, Linux, and IP-based protocols
Quality of Service[1]	Must function uninterrupted without error for long periods of time	QoS requirements are usually not time sensitive, do not always require real time monitoring, and can be rebooted or shutdown
Performance Requirements[2]	Real-time Response is time-critical Modest throughput is acceptable High delay and/or jitter is not acceptable	Non-real-time Response must be consistent High throughput is demanded High delay and jitter may be acceptable

Table 2 (Continued). Differences Between SCADA and IT (Wei et al., 2010[1]; Stouffer et al., 2013[2])		
Item	**SCADA Networks**	**IT Networks**
Availability Requirements[2]	Acceptable because of process availability requirements Availability requirements may necessitate redundant systems Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing	Responses such as rebooting are acceptable Availability deficiencies can often be tolerated, depending on the system's operational requirements
Risk Management Requirements[2]	Human safety is paramount, followed by protection of the process Fault tolerance is essential, even momentary downtime may not be acceptable Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production	Data confidentiality and integrity is paramount Fault tolerance is less important – momentary downtime is not a major risk Major risk impact is delay of business operations
Architecture Security Focus[2]	Primary goal is to protect edge clients (e.g., field devices such as process controllers) Protection of central server is also important	Primary focus is protecting the IT assets, and the information stored on or transmitted among these assets. Central server may require more protection
Unintended Consequences[2]	Security tools must be tested (e.g., off-line on a comparable ICS) to ensure that they do not compromise normal ICS operation	Security solutions are designed around typical IT systems
System Operation[2]	Differing and possibly proprietary operating systems, often without security capabilities built in Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved	Systems are designed for use with typical operating systems Upgrades are straightforward with the availability of automated deployment tools
Resource Constraints[2]	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities	Systems are specified with enough resources to support the addition of third-party applications such as security solutions
Time-Critical Interaction[2]	Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction	Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary for security
Communications[2]	Many proprietary and standard communication protocols Several types of communications media used including dedicated wire and wireless (radio and satellite) Networks are complex and sometimes require the expertise of control engineers	Standard communications protocols Primarily wired networks with some localized wireless capabilities Typical IT networking practices
Change Management[2]	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days/weeks in advance. ICS may use OSs that are no longer supported	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.
Managed Support[2]	Service support is usually via a single vendor	Allow for diversified support styles
Component Lifetime[2]	Lifetime on the order of 15-20 years	Lifetime on the order of 3-5 years
Access to Components[2]	Components can be isolated, remote, and require extensive physical effort to gain access to them	Components are usually local and easy to access

Identified differences between SCADA networks and IT networks warrant further discussion to appropriately frame various existing constraints potentially limiting momentum in SCADA security research. From an assessment perspective, the heavy utilization of proprietary protocols in SCADA networks and lack of appropriate protocol dissectors limit the ability to identify network communications (Hahn & Govindarasu, 2011). Most SCADA protocols were designed for serial communications and lack security or integrity mechanisms. The American Gas Association's AGA-12 standard, now known as the IEEE 1711-2010 Trial-Use standard (2011), defines a cryptographic protocol called Serial SCADA Protection Protocol (SSPP) to provide integrity, and optionally confidentiality, for cybersecurity of substation serial links. According to the standard, the "bump-in-the-wire" SSPP operates by encapsulating each SCADA or application message in a cryptographic envelope that adds minimal overhead to the message. This type of protection mechanism provides a solution that has not received widespread adoption due to (1) most SCADA security guidelines are voluntary (exception is electricity sector), and (2) the effects on system operation are unknown. The variety of differences is substantial enough to present additional challenges in security policy development and audit consistency with regard to cybersecurity mitigation strategies.

Challenges in Assessing Critical Infrastructure

Merrell, Moore, and Stevens (2010) present four challenges that governments face in assessing the risks of CI and are equally applicable to SCADA networks. They typically have limited access or insight into the capabilities of the CI owners, and have difficulty in examining evidence that an organization may present to demonstrate cybersecurity activities and appropriately evaluating that evidence within the context of national security objectives. Additionally, cybersecurity activities related to heterogeneous technologies and practices across different industries are difficult to compare to each other, and assessments are generally performed against a reference model of some sort. Merrell et al. (2010) recognize the limitations of a lack of cybersecurity standards that apply to a nation's entire CI and that align with national security goals. Interdependencies across various critical infrastructure sectors also compound the assessment problem. From a corporate social responsibility perspective, Ridley (2011) offers an approach worthy of research to explore opportunities to improve the resilience of critical infrastructure.

Threats

Given their operational characteristics, SCADA systems offer unique security challenges (Kuipers and Fabro, 2006). A primary benefit of SCADA systems is that remote and isolated locations can be monitored centrally without the need for onsite personnel. From a security standpoint, this provides entry points into the system that have minimal physical safeguards. Indeed, the trend to interconnect devices using networking technologies introduces additional entry points into the control system, often via the Internet. Network control and automation will continue to play a key role in enbaling network owners to adapt to the changing situation and opportunites to achieve their business goals while ensuring an adequate return for shareholders (Northcote-Green and Wilson, 2007). The benefits of automation in other sectors of critical infrastructure will similarly continue to be a driving factor to improve service, reliability, safety, and revenues.

Stouffer et al. (2103) identified a list of potential incidents relating to ICS and associated SCADA systems:

- Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation
- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, or endanger human life
- Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects
- ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects
- Interference with the operation of safety systems, which could endanger human life

Stouffer's list highlights potential goals of an attacker once system access is obtained. In the past, attackers had fewer system access points and would have to rely primarily on physical access; network isolation was the primary security feature (Cai, et al., 2008; Gold, 2009). More recently, however, businesses have begun connecting segregated SCADA networks to business enterprise networks to leverage cost saving benefits and to increase operational efficiency (e.g., customer billing).

The interconnection of SCADA networks with business networks creates a host of access points, often via the Internet (Cheung, et al., 2007). Once an attacker breaches the outer perimeter of a business network, they commonly pivot from one network to the next to exploit the inherent trust relationships. Note that business networks and the Internet are not the only access points to SCADA devices. Trusted

vendors may also have remote access connections to assist in maintenance and troubleshooting. Engineers often use portable workstations (e.g., laptops) to program devices and perform diagnostics and configuration changes.

The critical issue for the discussion here is that once an attacker gains access to the internal SCADA network, there are minimal safeguards in place. Such access typically provides unfettered control to issue rogue commands that can result in devastating effects such as catastrophic oil spills, poisoning a water supply, or the shutdown of an electrical grid.

Attacks

The limitations in control system security have resulted in numerous failures, including some induced by cyber attacks. In 2003, the Sobig virus infected computers at the Amtrak dispatching headquarters, causing signaling systems to shut down and halt ten trains between Pennsylvania and South Carolina (Niland, 2003). The Slammer worm penetrated a computer at the Davis-Besse, Ohio nuclear plant in 2003 resulted in the disabling of the safety monitoring system for nearly five hours (Dacey, 2004). At the Browns Ferry nuclear power plant in 2006, a "Data Storm" spike in traffic caused a PLC to crash, resulting in the failure of recirculation pumps and forcing a manual reactor shutdown (NERC, 2009).

These incidents provide examples that demonstrate the potential for malware to inadvertently propagate and adversely affect networked SCADA systems. More critically, attackers have also demonstrated the ability to launch targeted attacks specifically against SCADA systems. For example, in 2001, a disgruntled former employee launched a wireless attack on a sewage-treatment facility in Australia, which released millions of gallons of raw sewage into parks and rivers (Slay and Miller, 2008). The attacker relied on extensive insider knowledge of the system and permissions that were never revoked.

Perhaps the most notable targeted attack is the recent Stuxnet worm. Stuxnet delivered a targeted cyber attack on SCADA systems and had multiple ways of infecting systems via network shares and thumb drives (Matrosov, et al., 2010), included command and control communications seen in many botnets, resisted anti-virus detection, maintained stealth by installing a root-kit, and intentionally reduced its propagation rate to avoid detection (Chen, 2010).

Security Solutions for SCADA Systems

Past incidents highlight the need to develop and implement more robust security protections. Recommendations for safeguarding SCADA systems include implementing intrusion detection software, anti-virus software, and file integrity checking software (Stouffer, et al., 2013). However, organizations are reluctant to implement the security solutions primarily because of the potential impact they may have on operations. The following subsections discuss various security strategies and mitigation techniques recommended for safeguarding SCADA systems.

Firewalls and Network Segregation

Two of the most rapidly adopted recommendation guides are the NIST Guide to ICS Security (Stouffer, et al., 2013) and the 21 Steps to Improve the Cyber Security of SCADA Networks jointly published by the Presidents Critical Infrastructure Protection Board and US Department of Energy (n.d.). They recommend integrating security into network architectures using network segregation practices and disconnecting unnecessary connections to the SCADA network. The system should—to the maximum extent possible—should be closed-looped or air-gapped, and only connect the SCADA network if necessary. However, research suggests that many SCADA networks are connected to the Internet, sometimes without the SCADA network owner's approval or knowledge (Leverett, 2011). If the network must be connected to the Internet, Stouffer et al. (2013) provides multiple firewall architecture configurations to achieve network segregation.

Beechey (2010) presents a whitelisting application to mitigate attacks that circumvent firewalls and dupe users into executing malware. A whitelist denies the execution of all applications except for those applications explicitly identified. This concept is the converse to traditional security blacklist techniques that allow the execution of all applications except for those applications explicitly identified (e.g., antivirus signatures). The attacks examined in Beechey's research include: binders, installing fake/rogue anti-virus, dynamic link library hijacking, drive-by-downloads, and web application attacks through cross site scripting. Beechey explains how many of these attacks can be performed by script kiddies, or unsophisticated individuals who simply download and run executable files from the Internet. The primary concern with whitelisting for SCADA systems is the inflexibility for system alterations (e.g., configuration changes, upgrades and specification changes).

Remote Forensics on SCADA Networks

Chavez et al. (2008) demonstrated that Encase Enterprise can be used to perform forensics remotely on SCADA systems. Although forensics is typically performed on a system after it has been compromised, Chavez demonstrates the utility of extending a traditional IT security solution to SCADA networks without negatively affecting operations.

Intrusion Detection

By employing the characteristics of SCADA networks, behavior-based rules and signatures can be developed to detect abnormal network behavior such as the initiation of a ping sweep, three diagnostic commands issued rapidly in succession, or issuing invalid commands. Moreover, the implementation of an intrusion detection system provides network security personnel with audit logs and monitoring capabilities, an issue raised by Stouffer et al. (2013). Intrusion and anomaly detection systems can be implemented at the network and/or host layers.

In an example using a case study, Campbell and Rrushi (2011) present research on an anomaly detection model for nuclear power plants. The methodology examines detection of a potential attack that attempts to send erroneous data from a field device to the HMI. The work demonstrates the ability to extend anomaly detection models to the SCADA environment.

Message Authentication

Encryption techniques offer capabilities to ensure message authenticity and confidentiality. In the SCADA environment, however, operating parameters require the system to fail safe, or in a well defined mode that permits continued safe operations (e.g., a traffic system reverting to flashing red lights in the event of a failure). This requirement typically is counter to the fail secure principle enforced by encryption techniques which typically prevent any further operations. Some efforts, however, have examined bump-in-the-wire devices for data integrity and confidentiality. Solomakhin et al. (2010) examined bump-in-the-wire devices for message encoding and authentication between two nodes in the electric power grid. It was identified that aspects of message integrity may be more important than confidentiality because the attacker can learn the state of the system from the physical world (e.g., attacker knows an open dam spillway message was sent when they observe the spillway is open). Note that bump-in-the-wire solutions require an additional device that must be purchased, configured, and maintained by network security personnel. Furthermore, their scalability is questionable at this juncture.

SCADA Assessments

Many organizations employ penetration teams to identify vulnerabilities in their network. Teams may be internal employees or contracted to perform security auditing services. The teams validate tactics used by attackers to find and exploit SCADA networks. Attackers breach network defenses, gain access to the organization's intranet, escalate their privileges, and use administrator or system credentials to pivot from one network to the next. Findings from assessments reveal that most SCADA networks have at least one system that is dual-homed. Penetration testers have proven vital in identifying network vulnerabilities and companies now exist that focus on security auditing specifically for the SCADA environment (SpearPoint, 2012).

When penetration testers discover vulnerabilities, they identify security measures to mitigate the weaknesses. While penetration testers do not intend harm to networks, past events show that tools used by penetration testers can have detrimental impacts to SCADA systems. Consider the following examples where routine security evaluations negatively impacted SCADA System operations (Stouffer, et al., 2013):

- During a ping sweep, a common method of identifying systems within a Local Area Network (LAN) using ICMP status messages, on an active SCADA network, a 9-foot robotic arm that was in standby mode became active and swung around 180 degrees.
- While a ping sweep was being performed on an ICS network to identify all of the hosts attached to the network, the ping sweep caused a system controlling the creation of integrated circuits in a fabrication plant to lock-up. The ping sweep resulted in the destruction of $50,000 worth of integrated circuit wafers.
- A natural gas utility hired an IT security consulting organization to conduct penetration testing on its corporate network. The consulting organization carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system and the utility company was not able to send gas through its pipelines for four hours, resulting in four hours loss of service to its customers.

These examples highlight the concerns associated with implementing security solutions for SCADA systems.

Evaluation Considerations

Evaluating security solutions for the SCADA environment requires consideration of the potential impact to operational functionality and safety. Indeed, when evaluating a solution that has proven effective in the IT environment, it is more important to demonstrate that the security solution itself will not negatively impact the SCADA system functionality. The main considerations for evaluating security solutions in the SCADA environment are summarized in the list below:

1. Identify desired security goals
2. Outline SCADA services critical to operations
3. Identify SCADA components that may be effected
4. Define the average, above average, and maximal workload associated with the SCADA system
5. Determine system parameters and performance metrics for evaluation
6. Establish evaluation environment

Identifying the desired security goals helps the asset owner to determine if firewalls, VLAN's, Host-Based IDSs, or other security solutions are appropriate for the SCADA system. Because active security techniques may not be appropriate for the operational environment, passive monitoring techniques may be more applicable.

SCADA systems ensure continual monitoring and control of critical processes. Outlining the specific services critical for operations helps focus the evaluation to ensure the appropriate SCADA functionality is observed and safety thresholds are not exceeded. Additionally, introduction of a security solution should not negatively impact critical services.

While it is expensive to replicate an entire SCADA system for testing purposes, components that may be affected must be identified. Can the security solution affect the human machine interface (HMI), engineering workstations, and every Programmable Logic Controller (PLC) or Remote terminal Unit (RTU)? Are there plans to upgrade any components and will the security solution be compatible with those upgrades? It is important that the scope of the evaluation efforts is not too narrowly focused. Key considerations identified for the performance analysis presented in this work are workload, system parameters, and performance metrics.

A workload should be platform agnostic and characterized appropriately for the system under test. This is especially critical for SCADA systems since benchmarks are scant. The workload represents a set of requests that place varying demands on system resources. Average, above average, and maximum workloads are used to provide a range of evaluation scenarios. The average workload represents the SCADA system under normal operating conditions. An above average workload stresses the system to ensure that the security solution does not impact operations under heightened conditions. The maximum workload stresses the system well beyond expected operating conditions. Because of the strict availability, reliability, and safety requirements of SCADA systems, a maximum workload affords the best opportunity to identify potential negative impacts or inconsistent system behavior due to the security solution. The security solution must not deny or degrade the functionality beyond acceptable operating parameters.

System parameters are the properties and attributes of a SCADA system that determine their functionality. System parameters can include message protocols, system operating characteristics and communication infrastructure. The system parameters of concern are determined based on the security goals, critical services and components. Performance metrics identify aspects which are measured and analyzed during evaluation. The metrics determine the levels of degradation the system can tolerate without negative impact to functional operations.

The final aspect is to establish a representative evaluation environment. Devices can be replicated using real hardware and/or emulated in a simulated environment. The selected environment must be indicative of operational conditions to the extent that warrants confidence in the findings. The testing protocol should be designed to ensure that the evaluation environment incorporates the various configurations (e.g., Ethernet, wireless, and serial communications).

Case Study

This case study evaluated a host-based intrusion detection system and a fuels management SCADA system using the specified considerations. The example is intended to demonstrate a cost effective and viable option to effectively evaluate the feasibility of introducing a security solution into a SCADA environment.

Host Based Security System

The Host Based Security System (HBSS) consists of a suite of software applications used to monitor, detect and counter attacks against computer systems. HBSS is the official name given to the Department of Defense (DOD) commercial-off-the-shelf (COTS) suite of software applications (i.e. McAfee, Inc.) used within the DOD to monitor, detect and counter attacks against computer networks and systems. Figure 2 illustrates the various applications incorporated with HBSS. The HBSS framework leverages a client-server architecture that consists of an ePolicy Orchestrator (ePO) server and client workstations containing host security agents. HBSS security agents include the Rogue System Detector (RSD), Asset Baseline Monitor (ABM), and Host Intrusion Prevention System (HIPS). When deployed, HBSS security agents interact with the end-point workstation according to defined rule sets hosted on the ePO server. Each security agent generates and sends reports to the ePO server. The ePO server consolidates reports and

provides security personnel with enterprise-wide situational awareness.

This evaluation focused on the HIPS security agent. The three modules within the HIPS security agent include: the HIPS intrusion prevention system (HIPS:IPS); the HIPS firewall (HIPS:FW); and the HIPS application blocker (HIPS:AB). The first module, the HIPS:IPS, is an intrusion prevention system (IPS) with signatures specifically tailored for a host workstation or group of workstations. The second module, HIPS:FW, is similar to other software-based firewalls. The HIPS:FW can be configured to limit the connections to the server and raise an alarm for malicious activity (e.g., ping sweep or Nmap scan). The HIPS:AB module is used to blacklist or whitelist executable applications.

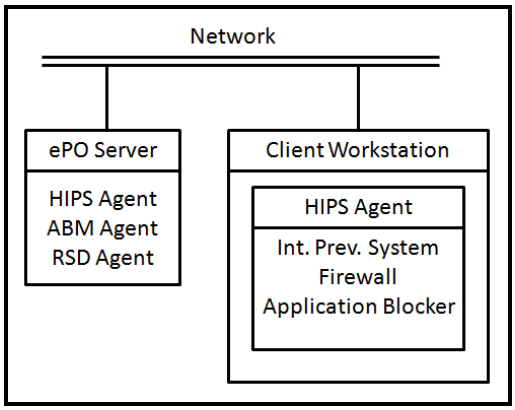

Figure 2. Overview of HBSS

Fuels Management System

Varec is a commercial entity that provides solutions for liquid petroleum asset management across bulk storage facilities, marketing terminals, refineries, petrochemical plants and military fuel facilities (Varec, 2011). The Varec fuels management system automates the control and measurement of bulk liquids during processing, transportation, and storage. Fuel operators can access data and trace the movement of fuel at all points along the refueling chain, from arrival at the fuel farm storage facility to delivery onboard a waiting aircraft. Currently, The Varec fuels management system consists of the Fuels Manager Defense (FMD) software and the remote terminal unit model 8130 (RTU 8130).

Varec's FMD solution is designed for air, ground, and naval fueling. FMD manages and controls all bulk liquid assets in a fuels facility, including transaction and inventory management, tank gauging, dispatch and automated data capture (Varec, 2011). Fuel operators utilize the FMD software to record and monitor the day-to-day operations associated with bulk fuel management. The FMD software provides fuel operators centralized monitoring, tracking, and response to fuel requests and system alarms.

Figure 3 depicts a functional diagram of the Varec fuels management system. The fuels management system consists of automated SCADA field devices including fuel tanks, gas stations, valves, and pumps that report their status (e.g., level, density, and temperature) to the RTU 8130. The RTU 8130 collects the information, processes the data, and reports it to the FMD Server. Both fuel environmental data and transaction data (e.g., dispensing or replenishing of fuel tanks) are tracked by the FMD software application. Moreover, everything that aids in the fuel process on a local business site can be tracked with the FMD software. The software application consists of several modules including Dispatch, Equipment Status, Maintenance, Personnel, Quality Control, Training, Scheduler, Accounting, and Tank Inventory. Fuel operators access the FMD Server physically or remotely via client workstations. The FMD Server consolidates interactions and provides fuel operators with complete site-wide situational awareness on all fuel-related activities.

Fuels Network Architectures

The fuels management system consists of two different types of network architectures. In one architecture, the RTU connects directly to the FMD Server using an RS232 serial connection. Installations use this configuration when the SCADA control center is near the RTU(s), usually within 150 feet. The second architecture uses RS232 over IP to connect the RTU to the FMD Server. Installations use this architecture when fuel assets are further than 150 feet from the SCADA control center and network drops are readily available.

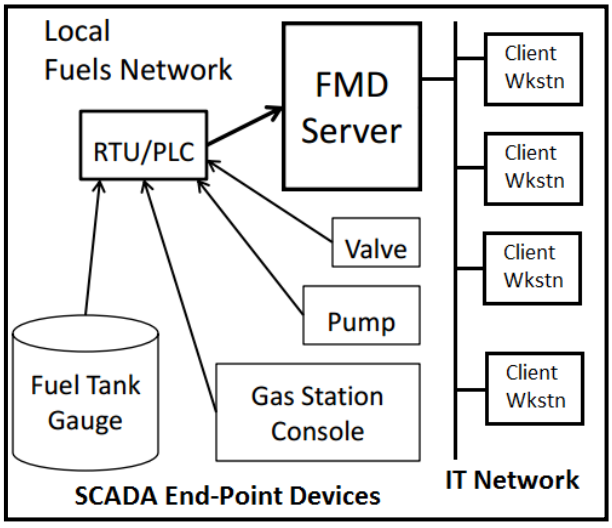

Figure 3. Varec Fuels Management System

Security Goals

This case study determines if a Host-based IDS is suitable to protect a SCADA fuels management network. It examines the interoperability of the HBSS HIPS security agent when installed on the FMD Server.

The FMD Server is connected to both the SCADA network and traditional IT network. Both FMD architectures are evaluated. It is believed the HIPS security agent has very little impact to the RS232 direct connect architecture since the HIPS security agent does not intercept RS232 communications.

The HIPS security agent executes three different modules to protect the FMD Server and prevent various cyber attacks. The evaluation aims to determine if the HIPS security agent interferes with the normal operations of the FMD Server and connected SCADA system. The HIPS security agent must not interfere with: (1) the FMD Server's communications with the SCADA network and (2) the FMD software resident on the FMD Server. Furthermore, analysis of the selected performance measurements can reveal if the addition of a HIPS security agent will negatively impact the availability, reliability, or safety requirements of the SCADA system.

SCADA Services

The FMD Server provides real time monitoring and control of various devices found in the SCADA fuels network. An operator can physically sit at the FMD server, or more commonly, connect to the FMD Server via a client workstation. The operator interacts with the FMD Server that monitors SCADA field devices and issues commands (e.g., shut off a pump or open a valve) via the Tank Inventory module within the FMD software application. Tampering with these devices can result in dangerous physical consequences associated with the fuels system. Additionally, fuel measurements are collected from SCADA devices so appropriate billing data can be aggregated. Altering the collected data can result in inaccurate billing transactions.

The HIPS security agent includes the ability to restrict programs that are able to execute (i.e., application whitelisting), limit directories where executables may be placed, and block unauthorized connections. The HIPS security agent monitors the FMD Server and reports anomalies found in the SCADA network to network security personnel.

The outcome of a properly functioning system with the HIPS security agent installed requires the FMD Server communicating within normal operating parameters to SCADA network devices and the HIPS security agent reporting malicious network activity to security personnel. Moreover, the system must adhere to reliability and safety requirements.

SCADA Components

The SCADA components involved in the evaluation included the FMD Server, the RTU 8130 and the communication infrastructure. For robustness, the four different FMD Server hardware configurations listed in Table 2 were evaluated in the case study. The PHYS configuration is comprised of the standard implementation scheme. The virtual machines are included to evaluate the potential for virtualization of the FMD Server. The basic hardware and software specifications for the PHYS FMD Server are as follows:

- 3.2 GHz processor
- 4 GB of RAM
- Hard disk drive with 160 GB of storage
- Available communication ports
- Standard Network Interface Card
- Windows 32 bit Server 2003 Enterprise OS
- IIS Web Services
- SQL Server 2000 Express software
- Default applications

The virtual machine instances are deployed on a Dell Latitude D630 Laptop running VMware Workstation 8.0. The virtual machines were evaluated using the three different system configurations that are detailed in Table 2. The three virtual machine configurations are labeled VM1, VM2, and VM3. All four system configurations are examined to determine if the HIPS security agent negatively impacts any of these system configurations, including virtual machine configurations that do not meet the minimum hardware requirements.

Table 3. FMD Server Configurations

Config	Virtual Machine	CPU Speed	CPU Cores	RAM (GB)	BIOS
VM1	YES	2.0 GHz	1	1	NO
VM2	YES	2.0 GHz	1	1	YES
VM3	YES	2.0 GHz	2	1	YES
PHYS	NO	3.2 GHz	8	4	NA

Establishing Workloads

To establish the workload, a set of operational use case scenarios were developed. The most commonly performed operation called a "Walk-Through for a Complete Fuel Transaction" comprises the majority of standard operation transactions. While the FMD software has many features, this use case is representative of the most common feature(s) utilized by fuel operators. Additionally, the Complete Fuel Transaction demonstrates one of the most resource intensive operations, making it an ideal candidate for modeling a workload on the FMD Server. For consistency during repeated measures, the workload and metric collection was implemented through the use of a batch script. The workload script simulates five fuel operators who input 60 fuel transactions each for a total of 300 fuel requests in one minute. The 300 fuel transactions were selected because it significantly exceeds the expected amount of transactions. Indeed, a typical FMD Server may only use three fuel operators who complete three fuel transactions in one minute.

Table 3. System Parameters

Parameters	PHYS	VM
CPU	2.0 GHz	3.2 GHz
RAM	4GB	1 GB
NIC	10/100/1000 Gigabit Ethernet	Virtual Ethernet Adapter
HIPS Comm Interval	1 per minute	1 per minute

Table 4. Performance Metrics

Performance	PHYS	VM
CPU Useage	<70.00%	<70.00%
Memory Usage	<256 MB	<256 MB
Memory Page Reads (Edmead & Hinsberg, 2011)	<5 @ sec	<5 @ sec
Active Network Connections	<30	<30
Response Time	RTT	RTT
Uptime	Low/Med/High	Low/Med/High

Table 5. Factor and Levels

Factor	Levels
System Configuration	VM1
	VM2
	VM3
	PHYS
HIPS Security Agent	Not Installed (Non-Active)
	Installed (Active)
Architecture	RS232 Direct Connect
	RS232 Over IP

System Parameters and Performance Metrics

The system parameters comprise properties of the fuels management system that determine functionality. Table 3 lists the parameters, table 4 lists the metrics associated with the study, and table 5 lists the factor level combinations.

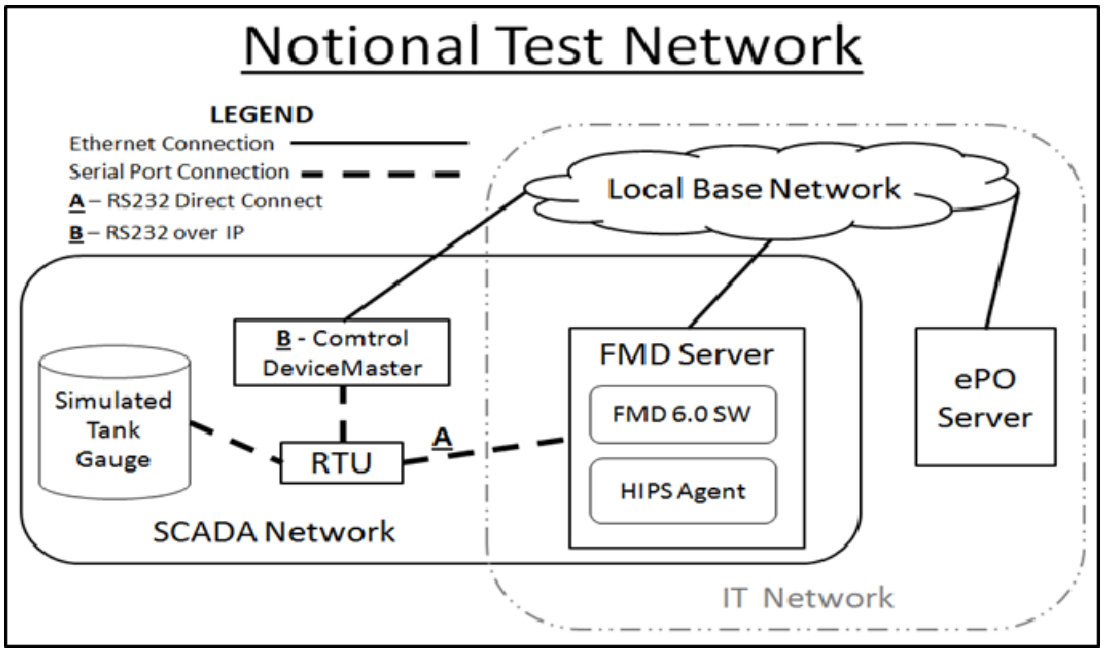

Figure 4. Notional test network for study

Table 6. Impacts to FMD Serve Configurations

Item	VM1	VM2	VM3	PHYS
CPU Usage	NO	NO	NO	NO
Mem. Usage	NO	NO	NO	NO
Mem. Paging	NO	YES	YES	NO
HBSS Comms	NO	NO	NO	NO
IIS Web Services	MIN	MIN	MIN	MIN
SCADA Comms	MIN	MIN	MIN	MIN

Evaluation Environment

The evaluation environment includes the necessary components to ensure confidence when deploying the traditional IT solution to the SCADA system. Figure 4 is a representation of the evaluation environment.

Case Study Results

Table 6 summarizes the results from the evaluation. NO indicates that no observable impacts to the system operations occurred. YES indicates that an observable degradation occurred, and MIN indicates a minor impact was observed that could be resolved with no additional impact after a configuration change.

The physical server functioned normally with the introduction of the HIPS security agent and is supported by the results from monitoring average CPU usage, average memory usage, and memory paging. Additionally, results from configuration VM1 revealed no evidence that would prevent virtualizing the FMD Server. VM1 was the most rudimentary and functioned normally with the HIPS security agent installed during the execution of the maximum workload script.

No memory paging issues were identified for VM1 or PHYS. However, configurations VM2 and VM3 both exhibited memory paging issues by exceeding the maximum five pages per second. The only notable difference between VM1 as opposed to VM2 and VM3 is the BIOS virtualization setting. The findings indicate further investigation is warranted to determine if the BIOS virtualization setting should be enabled prior to employment on a virtualized system.

Introduction of the HIPS security agent demonstrated two minor impacts to the FMD Server that were readily accommodated. The first impact effected SCADA communications associated with RS232 over IP architecture. The issue was mitigated by configuring the HIPS firewall module to permit IP communications between the FMD Server and networked RTU.

The second minor impact was the failure of FMD system services to start properly after a system reboot. The HIPS security agent interfered with the FMD Server's network communications services (i.e., the FMDataManager and FMCommManager) and the FMD Server's IIS Web Services (i.e., the IIS Admin, HTTP SSL, and WWW Publishing Service). Failure of the communication services to start resulted in the loss of communication between the FMD Server and the RTU. Failure of the IIS Web services to start resulted in prevention of remote access required to adjust fuel transactions that could result in improper reporting of fuel consumption and incorrect billing of fuel consumed.

A manual restart of system services associated with the HIPS security agent (i.e., Firesvc.exe and HIPSvc.exe) corrected the identified issues. To automate the corrective action, the FMD Server's Windows Registry was modified to force the two services to be dependent on the IIS Admin Service. Validation of the registry modification ensured proper system service startup after system reboots.

Findings associated with PHY and VM1 provide confidence that employing the HBSS solution in the FMD environment will have no negative impact on operations.

Conclusion

SCADA systems are increasingly connected to business and wide area networks. The interconnection has exposed SCADA systems to myriad threats that did not previously exist. Indeed, historical incidents have demonstrated the ability for malware to propagate to the once isolated systems and impact critical operations.

Security solutions designed for the IT environment offer protection against malware. Prior to employment in the SCADA environment, however, the security solution itself must be evaluated to ensure it does not negatively impact operations or established safety thresholds. As demonstrated in various penetration testing examples, employing security techniques without prior evaluation can lead to potential devastating and expensive consequences. This study identified a feasible approach that incorporates elements critical to SCADA system operation and the scientific rigor commensurate with performance analysis. The evaluation aids in determining whether traditional "technical" security solutions can operate concurrently without effecting critical functionality, impacting operations or compromise safety threshold levels.

A case study focused on the performance of a host-based security system integrated with a SCADA fuels management system demonstrated how technical security solutions can be evaluated prior to employment. In the case study, the evaluation identified no significant operational impact. As a result, the fuels management system inherits enhanced protection capabilities and the ability for network security personnel to monitor the system. SCADA systems are typically customized to meet stringent operational and safety requirements making evaluation of security solutions a challenge across multiple critical infrastructure sectors. The approach presented in this study provides a feasible and consistent method for researchers to conduct performance analyses and report findings that practitioners can evaluate in a consistent manner.

The implications for security research are numerous. A successful technical evaluation or performance analysis does not suggest acceptance by the SCADA community at large. The security culture of this community is very different from IT dominant organizations. As suggested by Dhillon (2006), addressing both the technical and human side of security will aid in understanding the broad range of implementation issues related to the operational impacts to information systems. Additionally, SCADA systems are highly customized implementations that exhibit subtle differences in operational environments. Results should be scrutinized sufficiently to ensure acceptable performance for each instance profiled. The assumptions for generalizability of results to a wider population of SCADA systems can be expected to be violated and deserves caution at this juncture.

References

Beechey, J. (2010) "Application Whitelisting: Panacea or Propaganda," SANS Reading Room. [online] http://www.sans.org/reading_room/whitepapers/application/application-whitelisting-panacea-propaganda_33599. Retrieved on January 26, 2012.

Boyer, S. A. (2009). Supervisory Control and Data Acquisition, 4th ed. North Carolina: ISA publishing.

Byres, E., Leversage, D., & Kube, N. (2007). Security incidents and trends in SCADA and process industries. Industrial Ethernet Book, 39(2), 12-20.

Cai, N., Wang, J. and Yu, X. (2008). "SCADA system security: Complexity, history and new developments". *6th IEEE International Conference on Industrial Informatics.* pp. 569-574.

Campbell, R. and Rrushi, J. (2011) "Detecting Cyber Attacks On Nuclear Power Plants". *IFIP Advances in Information and Communication Technology (AICT)*, Vol. 290 No. 290 pp. 1-54.

Chavez, A., Cassidy, R. F., Trent, J. and Urrea, J. (2008) "Remote Forensic Analysis of Process Control Systems". *Critical Infrastructure Protection*, Vol 253, pp. 223-235.

Chen, T. M. (2010). "Stuxnet, the real start of cyber warfare? [Editor's Note]". *Network, IEEE*, Vol 24., No. 6, pp. 2-3

Cheung, S., Dutertre, B., Fong, M., Lindqvist, U., Skinner, K. and Valdes, A. (2007) "Using model-based intrusion detection for SCADA networks". *Proceedings of the SCADA Security Scientific Symposium*, pp. 127-134.

Dacey, R. F. (2004). "Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems: GAO-04-628T". *GAO Reports*.

Department of Energy (n.d.). “21 Steps to improve cyber security of SCADA networks”. [online] http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

Dhillon, G. (2006). Principles of information systems security: Text and cases. Hoboken: Wiley & Sons.

Edmead, M. T. and Hinsberg, P. (2011). "Performance Monitor Counters"

GAO (2011). Critical infrastructure protection:

Cybersecurity guidance is available, but more can be done to promote its use. (GAO-12-92). U.S. Government Accountability Office report to congressional requesters.

Gold, S. (2009) "The SCADA challenge: securing critical infrastructure". *Network Security*, Vol 2009., No. 8., pp. 18-20.

Hahn, A. and Govindarasu, M. (2011). “An evaluation of cybersecurity assessment tools on a SCADA environment”. *IEEE Power and Energy Society General Meeting*, pp. 1-6.

IEEE Standards Association (2011). IEEE trail-use standard for cryptographic protocol for cybersecurity of substation serial links. IEEE std 1711-2010, IEEE: New York.

Igure, V. M., Laughter, S.A., and Williams, R.D. (2006). “Security issues in SCADA networks.” *Computers & Security.* Vol. 25. No. 7. pp. 498-506.

Katzke, S., Stuart, K., Abrams, M., Norton, D. and Weiss, J. (2006). "Applying NIST SP 800-53 to Industrial Control Systems". Houston, TX.

Kuipers, D. and Fabro, M. (2006). “Control Systems Cyber Security: Defense In Depth Strategies.” External Report INL/EXT-06-11478, Idaho Falls, Idaho.

Krebs, B. (2008). Cyber incident blamed for nuclear power plant shutdown, June 4. [online] http://articles.washingtonpost.com/2008-06-04/news/36929595_1_systems-computer-nuclear-regulatory-commission

Krutz, R.L. (2006). *Securing SCADA systems*. Indianapolis: Wiley Publishing, Inc.

Leverett, E.P. (2011) "Quantitatively Assessing and Visualising Industrial System Attack Surfaces".

Matrosov, A., Rodionov, E., Harley, D. and Malcho, J. (2010). "Stuxnet Under the Microscope Revision 1.31." ESET.

Merrell, S.A., Moore, A.P., and Stevens, J.F. (2010). "Goal-based Assessment for the Cybersecurity of Critical Infrastructure," *2010 IEEE International Conference on Technologies for Homeland Security*. Pp. 84-88.

Miller, A. (2005). "Trends in process control systems security". *Security & Privacy, IEEE*, Vol. 3, No. 5, pp. 57-60.

NERC. (2012) "Critical Infrastructure Protection (CIP) Standards", North American Electric Reliability Corporation, 2012. [online] http://www.nerc.com/page.php?cid=2%7C20.

NERC. (2009) "Reliability Functional Model: Function Definitions and Functional Entities, Version 5", North American Electric Reliability Corporation, Princeton, New Jersey.

Niland, M. (2003). "Computer virus brings down train signals." *InformationWeek*.

Northcote-Green, J., and Wilson, R. (2007). *Control and automation of electrical power distribution systems*. Boca Raton: Taylor & Francis.

Ridley, G. (2011). National Security as a Corporate Social responsibility: Critical Infrastructure Resilience". *Journal of Business Ethics,* Vol. 103, No. 1, pp. 111-125.

Slay, J. and Miller, M. (2008). "Lessons learned from the Maroochy water breach." International Federation for Information Processing. Boston Massachusetts: Springer.

Smart Grid Interoperability Panel (2010). "Guidelines for smart grid cyber security: Vol.2, Privacy and the smart grid," NIST: Gaithersburg.

Smith, S.S. (2006). "The SCADA security challenge: The race is on." [online] http://www.infosecwriters.com/text_resources/pdf/SSmith_SCADA.pdf

Solomakhin, R., Tsang, P. and Smith, S. (2010). "High Security with Low Latency in Legacy SCADA Systems". Critical Infrastructure Protection IV, pp. 63-79.

SpearPoint Security Services (2012). [online] http://spearpoint security.com.

Stouffer, K., Falco, J. and Scarfone, K. (2013) "Guide to industrial control systems (ICS) security". *NIST Special Publication 800-82, Rev 1*.

Thilmany, J. (2012). "SCADA Security? [Cover Story]". *Mechanical Engineering,* Vol.134, No. 6, pp. 26-31.

Varec. (2011) "FuelsManager Oil & Gas: Terminal Automation," [online] http://www.varec.com/.

Verba, J., and Milvich, M. (2008). "Idaho National Laboratory Supervisory Control and Data Acquisition Intrusion Detection System (SCADA IDS)."

Wei, D., Lu, Y., Jafari, M., Skare, P. and Rohde, K. (2010) "An integrated security system of protecting Smart Grid against cyber attacks". *Innovative Smart Grid Technologies (ISGT*). pp.1-7

Weiss, J. (2010). "Protecting industrial control systems from electronic threats". New York: Momentum Press.

About the Authors

Mr. Robert Larkin holds an MS in Cyber Operations from the Air Force Institute of Technology. He received his BS in Computer Science and Computer Engineering Technology from Central Washington University in 2006. In 2006, Robert earned his commission and entered the United States Air Force. His first assignment was to the Air Force Information Operations Center in San Antonio, TX. He performed operational test and evaluation for cybersecurity solutions, ensuring the surety of Air Force and Department of Defense network capabilities. Robert is an active duty Captain currently assigned as Deputy Flight Commander at Joint Base Langley-Eustis, VA.

Mr. Juan Lopez Jr. (CISSP) is a research engineer with the Center for Cyberspace Research located at the Air Force Institute of Technology, Wright-Patterson AFB. He conducts research in Critical Infrastructure Protection, Supervisory Control and Data Acquisition (SCADA) systems, Radio Frequency Identification (RFID), and Electromagnetic Interference (EMI) modeling of 4G wireless systems. Mr. Lopez is currently pursuing a Ph.D. in Computer Science at the Air Force Institute of Technology. His academic resume includes a BS from the University of Maryland, an MS from Capitol College, and an MS from the Air Force Institute of Technology under the Information Assurance Scholarship Program. He is an IEEE senior member, and a Certified Information Systems Security Professional (CISSP).

Dr. Jonathan Butts is an assistant professor of computer science at the Air Force Institute of Technology. He received his PhD in Computer Science from the University of Tulsa in 2010, an MS in Information Assurance from the Air Force Institute of Technology in 2006, and a BS in Computer Science from Chapman University in 2001. Jonathan is an active duty Major in the United States Air Force with 16 years of service. He is a Fellow of the National Board of Information Security Examiners and Committee Chair for the International Federation for Information Processing Working Group on Critical Infrastructure Protection. He has performed research and worked extensively with the Department of Defense, Department of Homeland Security, Department of

Energy, National Security Agency, Central Intelligence Agency and U.S. Secret Service.

Dr. Michael R. Grimaila (BSEE, MSEE, PhD, Texas A&M University) is an Associate Professor of Systems Engineering and a member of the Center for Cyberspace Research (CCR) at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio USA. He is a Certified Information Security Manager (CISM) and a Certified Information Systems Security Professional (CISSP). Dr. Grimaila's research interests include mission assurance, network management and security, quantum cryptography, and systems engineering. He is a member of the ACM, a Senior Member of the IEEE, and a Fellow of the ISSA.