PHOENIX CONTACT
INSPIRING INNOVATIONS

Cybersecurity for Critical Control Systems in the Power Industry

Primary Author: W. Michael Sutton, P.E., Project Sales Engineer – SE Region, Phoenix Contact
Co-Authors: Deralee Bowlin, Industry Manager – Electric Power, Phoenix Contact
Dan Schaffer, Business Development Manager – Networking & Security, Phoenix Contact

Abstract

It has become almost a weekly occurrence to read about some new cybersecurity attack, whether it is intended to obtain private information or to deliberately bring down a particular company's network. However, cybersecurity attacks are not just limited to IT networks. With the advent of Stuxnet, cybersecurity attacks on control and SCADA systems have become a reality. The threat of cybersecurity attacks on our nation's critical control systems infrastructure, which includes our power generation facilities, presents yet another challenge to utility directors and staff. We will discuss what the federal government is doing about cybersecurity and the impact of the latest Presidential Executive Order.

As part of the growing need for cybersecurity, the types of malwares and viruses that have been designed to attack SCADA systems (such as Stuxnet and Flame) will be examined. To address the need to secure our critical control systems, this paper will discuss the latest standards, regulations, and guidelines that can be applied to the power industry. The discussion will focus on the Version 5 NERC-CIP standards and the ISA99, Industrial Automation and Control Systems Security standards.

Based on the ISA99 standards and Department of Homeland Security guidelines, there are a number of best practices that engineers can employ in designing control systems networks and that end users can implement for existing systems. These include authentication and auditing, intrusion detection, and defense-in-depth strategies, including firewalls and virtual private networks (VPNs). We will focus on these best practices and how they apply to the Version 5 NERC-CIP standards.

TABLE OF CONTENTS

PHOENIX CONTACT
INSPIRING INNOVATIONS

Introduction

Increasingly, cybersecurity is a major headline in our newspapers on a daily basis. Most of these attacks are against IT networks at large companies in the hopes of obtaining private information or intellectual property (IP) information. The threat against our critical infrastructure has become an undeniable reality..

The U.S. government recognizes this threat of cyber-warfare. On January 24, 2013, the head of the Department of Homeland Security (DHS), Janet Napolitano, noted the following during a talk at the Wilson Center think tank:

"We shouldn't wait until there is a 9/11 in the cyber world. There are things we can and should be doing right now that, if not prevent, would mitigate the extent of damage."[1]

She believes that such an event could occur imminently and could cripple the country, taking down the power grid, water infrastructure, transportation networks, and financial networks.

The former Defense Secretary, Leon Panetta, expressed similar sentiments in October 2012 and in a February 2013 speech to a Georgetown University audience, noting, "There is no question, in my mind, that part and parcel of any attack on this country in the future, by any enemy, is going to include a cyber element…I believe that it is very possible the next Pearl Harbor could be a cyber-attack…[that] would have one hell of an impact on the United States of America. That is something we have to worry about and protect against."[2]

Although the Cybersecurity Act of 2012 stalled in the Senate in November 2012, President Barack Obama recognized the growing need and issued the Executive Order on Improving Critical Infrastructure Cybersecurity on February 12, 2013.[3] This executive order calls for increased information sharing between the U.S. government and critical infrastructure owners and operators so that these entities can better protect themselves from cyber-threats. The executive order also calls for the Director of the National Institute of Standards and Technology (NIST) to develop the Cybersecurity Framework, which will provide a cost-effective approach to security measures for critical infrastructure owners to use in assessing and managing cyber risk. NIST issued a Request for Information (RFI) on February 26, 2013, as a first step in developing the Cybersecurity Framework.

Thus, cybersecurity is at the forefront of everyone's mind, particularly our federal government. This paper will review the emerging threats to control systems and the potential impacts of these threats to power generation facilities. It will provide an overview of the latest NERC-CIP standards and what standards and guidelines exist that can help comply with these new standards, including the ISA99 standards and DHS guidelines for defense-in-depth strategies. We will also discuss some technologies that can be applied to secure control systems in the energy sector.

The views expressed in this paper are solely those of the authors and do not necessarily reflect the views of Phoenix Contact.

PHOENIX CONTACT
INSPIRING INNOVATIONS

Growing Concerns in the Power Industry

Under Presidential Policy Directive-21 (PPD-21), issued on February 12, 2013, the President outlined the role of the Department of Homeland Security as protecting the security and resilience of our critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7 (HSPD-7), of December 17, 2003, and identifies 16 critical sectors.[4] The energy sector is identified as one of these critical sectors, which is further divided into electricity, petroleum, and natural gas. Each sector is led by a Sector-Specific Agency (SSA) that reports to DHS and is responsible for developing and implementing a Sector-Specific Plan in accordance with the National Infrastructure Protection Plan (NIPP).[5] The energy sector includes over 6,400 power plants and covers all forms of generation, including coal and natural gas combustion, nuclear, hydroelectric, and renewables.

A key component in protecting critical infrastructure is securing the critical Programmable Logic Controller (PLC)– and Distributed Control System (DCS)–based systems used to monitor, control, and automate power generation facilities. The National Cyber Security Division (NCSD) established the Control Systems Security Program (CSSP) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to protect and secure our critical control systems and the rising threat of cyber-attacks. ICS-CERT is responsible for responding to control systems incidents, including on-site services, as well as coordinating vulnerability studies and the disclosure of this information to the public.

In their recent annual review, ICS-CERT noted that of their 198 incidents, more than 40 percent belonged to the energy sector:

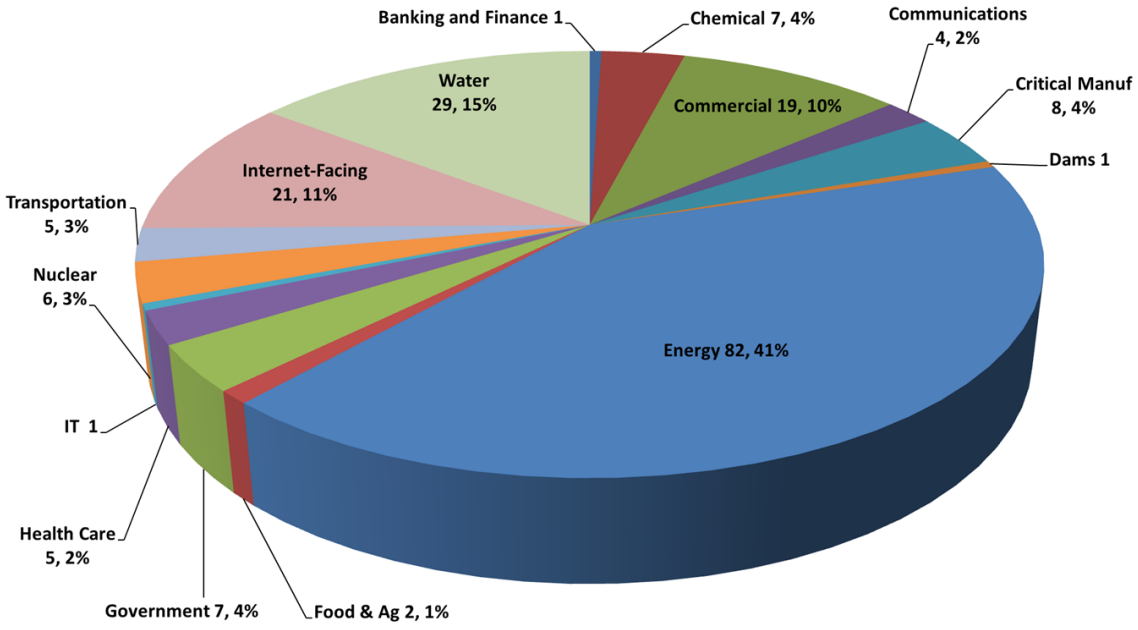

Figure 1: Incidents by Sector (+ Internet-Facing) – 198 Total in Fiscal Year 2012, ICS-CERT *Monitor*, October/ November/December 2012 [6]

PHOENIX CONTACT
INSPIRING INNOVATIONS

Growing Concerns in the Power Industry *(continued)*

In approximately half of the incidents reported in the energy sector to ICS-CERT, information regarding the ICS to gain remote unauthorized operations was targeted. Although none of these incidents has yet resulted in major headlines, it is clear that the energy sector is being probed and is open to potential serious attacks.

Cyber incidents do not have to be initiated by an Advanced Persistent Threat (APT) trying to get into a control systems network from the outside. Cyber incidents can be attributed to a number of issues, including:

Technical defects – Hardware malfunctions in control systems networks can lead to broadcast storms that can overload a control systems network, potentially crippling the network and access to the control system. For example, in August 2007, more than 17,000 international passengers were stranded at the Los Angeles International Airport due to a malfunctioning network interface card (NIC) on a desktop computer, which led to a broadcast of data that effectively crippled the airport network.[7]

Human error – Improper procedures in updating control systems programs or patching control systems software can lead to the inadvertent dissemination of malware and viruses within a control system network. In the December 2012 edition of the ICS-CERT *Monitor*, two such incidents were noted at power generation facilities.

In the first incident, an employee used his USB drive to back up configuration files for the control system. When this drive was analyzed by IT staff on a computer with up-to-date antivirus software, they found that the drive was infected with malware. Further analysis of the SCADA computers revealed that two engineering workstations had also been infected due to the USB drive.

In the second incident, a third-party technician installed software upgrades for a turbine control system using an infected USB drive. Consequently, the Mariposa virus spread to ten computers within the control systems network. The result was a delayed restart of the plant by three weeks.

Human error can be attributed to the incidents noted above with the USB drives, but the most infamous malware to date, Stuxnet, was intended to be spread via USB drives through vulnerabilities in the Windows operating systems of networked and non-networked PCs. The ultimate target of this highly sophisticated malware is the Siemens industrial control system running WinCC databases and STEP 7 PLC programming projects.[8] The Stuxnet malware has the capability of manipulating the DLL file that is responsible for the communication between the SIMATIC Manager and the S7 controllers. This enables Stuxnet to inject and hide malicious code into PLCs and prevent it from being overwritten. The infected PLC code ultimately leads to the destruction of the controlled equipment; the malware is so sophisticated that an operator sitting at the Human Machine Interface (HMI) will not notice the changes at the affected equipment.

Because of its sophistication, Stuxnet was believed to be a state-sponsored attack by the United States and Israel against Iran to destroy the centrifuges used in their nuclear enrichment program. According to a report in *The New York Times*, Stuxnet was initiated as part of a program under the Bush administration[9] and was accelerated by President Obama during the early part of his first administration. Although Stuxnet was discovered in 2010, it was clearly underway for some time prior to its discovery.

Growing Concerns in the Power Industry *(continued)*

Stuxnet was an incredible eye-opener in many ways and was deemed a "cyber weapon of mass destruction" by Ralph Langner, a German cybersecurity consultant who worked on deciphering the Stuxnet code[10]. Two important facts remain:

- It was the first reported malware to target an industrial control system. Stuxnet confirmed that industrial control systems are vulnerable and can be exploited, leading to significant damage.
- With the discovery of Stuxnet, the concern now is copycat attacks. With this code being discovered and available to the world, potential cyber-terrorists can use it as a blueprint to attack critical infrastructure in the U.S. and throughout the world.

Since the discovery of Stuxnet, two related cyber malwares have been identified, Flame and DuQu. DuQu is thought to be a Stuxnet successor operating since 2007. Flame was discovered by Kaspersky Lab in May 2012. It is a highly complex espionage tool aimed at data gathering and exfiltration that is believed to have infected over 10,000 machines throughout the Middle East and North Africa.[11] Further research into this malware reveals that it has been gathering data since at least December 2006 and has the ability to steal files, record keystrokes, and turn on the internal microphone of computers to record conversations.

NERC-CIP Cybersecurity Standards

In the United States, the energy sector has made significant strides in protecting the critical cyber assets (CCAs) at power generation facilities through the voluntary efforts of the North American Electric Reliability Corporation (NERC). A non-governmental, independent, and not-for-profit organization, NERC seeks to ensure the reliability of the bulk electric system in North America through the development and enforcement of standards. NERC is subject to oversight by the U.S. Federal Energy Regulatory Commission, but as of June 2007, NERC was given the legal authority to enforce reliability standards with all users, owners, and operators. These reliability standards include the Critical Infrastructure Protection (CIP) Standards.

In regard to cybersecurity, NERC has and continues to develop reliability standards. Generator operators and owners, or Responsible Entities (REs), were required to be compliant with the initial set of cybersecurity standards CIP-002-1 through CIP-009-1 on January 1, 2010. There have been subsequent revisions and additional standards since the initial compliance date. Major revisions to the standards were released in November 2012 and included two new standards, CIP-010-1 and CIP-011-1.[12]

CIP-010-1 provides details on configuration change management and vulnerability assessments as related to the requirements of the other CIP standards. CIP-011-1 specifies information protection requirements to protect against the compromise of Bulk Electric System (BES) Cyber Systems from instability or inappropriate operation. The entire set of CIP standards, from CIP-002 through CIP-011, is now referred to as Version 5 CIP Cyber Security Standards and shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. However, on April 18, 2013, the Federal Energy Regulatory Commission raised concerns about ambiguity in the standards, the implementation plan, and the compliance date, in their Notice of Proposed Rulemaking (NOPR) regarding

PHOENIX CONTACT
INSPIRING INNOVATIONS

NERC-CIP Cybersecurity Standards *(continued)*

the Version 5 Standards.[13] Thus, depending on the resolution from this NOPR, the compliance effective date and requirements may be modified in the final version of the standards.

One of the major modifications in the Version 5 CIP Cyber Security Standards is the shift from identifying CCAs to identifying BES Cyber Systems in CIP-002-5, Cyber Security – BES Cyber System Categorization. Essentially, a BES Cyber System is a collection of CCAs. It provides the RE a more convenient level in which to document their compliance. The CIP-002-5 further categorizes the BES Cyber Systems based on impact categories. Specific requirements in subsequent CIP standards are now applied to these impact categories. The concept of using impact categories was adapted from the NIST Risk Management Framework to more appropriately apply requirements based on the impact of the BES Cyber System.

Major modifications were also made to the primary standards for electronic security in NERC-CIP, which include CIP-005-Electronic Security Perimeter(s) (ESPs) and CIP-007 – Systems Security Management. Some of the more significant requirements and modifications to the new versions of CIP-005 and CIP-007 include the following:

- Establish, implement, and document an Electronic Security Perimeter (ESP) to protect Critical Cyber Assets (CCAs) and non-critical cyber assets within the ESP. An ESP defines the zone of protection around a BES Cyber System. Cyber assets within the ESP can be mixed in terms of impact categories, but they all must meet the requirements of the highest impact classification. An ESP must be defined for the BES Cyber System regardless of whether there is external network connectivity to cyber assets within the ESP. For communication outside of the ESP via a routable protocol such as TCP/IP, an Electronic Access Point (EAP) (such as a firewall or VPN) is necessary to limit the traffic to only that communication that is required for proper operation.
- Protection against the use of unnecessary ports has been moved to CIP-007.
- Monitoring and logging of access points to the ESP has been moved to CIP-007. Requires logging of failed access attempts, alerts for security incidents, and review of logs every 15 days minimum to identify undetected cyber incidents.
- Documenting inbound and outbound access permissions through a list of rules (firewall, access control list), and each rule has a documented reason.
- Authentication for dial-up connectivity and a documented process for how this authentication is achieved.
- Have one or more methods of malicious communication detection for ESPs and documentation of those methods. This requirement directly supports FERC Order No. 706, which discusses the concept of defense-in-depth strategies and the need for two distinct security measures so that the cyber assets do not lose all protection if one security mechanism fails. NERC is utilizing malicious traffic inspection as a method to add defense-in-depth.
- For all interactive remote access sessions, use a minimum of AES-128 encryption at an intermediate system so that there is no direct access to the cyber asset. Provide multi-factor authentication for all interactive remote access sessions. Multi-factor authentication includes the use of two or more pieces of information to authenticate the transaction, such as a password + key or password + certificate.
- Security patch management, including a process for tracking, evaluating, and installing cybersecurity patches for applicable cyber assets. Security patch management includes evaluating newly released patches every 35 days and applying these patches or developing and implementing a mitigation plan for the patches.
- Malicious code prevention, including methods to deter and prevent malicious code propagation. This could include such anti-malware techniques

NERC-CIP Cybersecurity Standards *(continued)*

as antivirus software, white-listing, and Common Internet File System (CIFS) integrity checking. CIFS is a standard way that users can share and access files across corporate intranets and the Internet. Some security devices have the ability to use CIFS integrity checking to monitor files on a network to determine if they have changed over a time period. A change could indicate a possible virus or unauthorized intervention.

- Another anti-malware mechanism is white-listing, whereby only trusted applications, i.e., those on the "white list," are allowed to run. While this may require some administration to ensure the white list is current and the proper files are allowed, it does help ensure that malicious or unwanted files can never be executed.
- System access control, including identification of individuals with authorized access, procedures for password management, routine password changing, and enforcement of stricter password protection that requires a minimum number of characters with three or more different types of characters.

DHS Guidelines and ISA99/62443 Standards

There are a number of standards and guidelines available to assist end users in meeting the requirements of the Version 5 NERC-CIP standards. These standards include guidelines from the Department of Homeland Security, ISA99 Standards, and the NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security.[14] For this paper, we will focus on the first two documents and how they can offer some valuable insight into meeting the NERC-CIP standards.

The first document of discussion was released by the Department of Homeland Security in October 2009 and is titled "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies."[15] This document is a concise and useful tool that describes potential methods of attack and security challenges within an ICS, the concept of zones within a network, and the potential defense-in-depth strategies that can be deployed within an ICS. Figure 2 shows a common ICS architecture and the zones that can be found within that network:

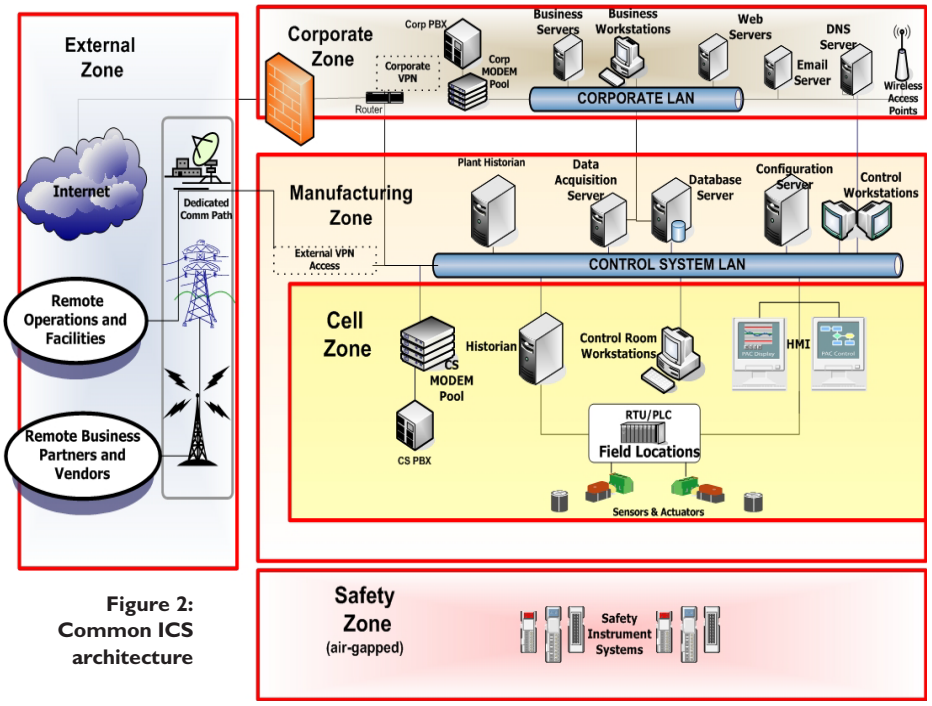

Figure 2: Common ICS architecture

PHOENIX CONTACT
INSPIRING INNOVATIONS

DHS Guidelines and ISA99/62443 Standards *(continued)*

These best practices and recommendations from the DHS document can be applied to meet the requirements of NERC-CIP-005:

Device-Level Firewalls – Deployment of layered firewalls throughout the control systems network, including field level device firewalls at the RTU/PLC/DCS level. Embedded security in controllers is gaining traction with some vendors, but it is still a future concept. To that end, protecting the process controller that may be controlling a turbine or is part of a burner management system with a device-level firewall can add significant robustness to a BES Cyber System.

Potential cons of adding this much defense in a network include additional latency, capital cost, and operational cost in managing the firewalls. However, there are cost-effective device-level firewalls on the market that provide efficient means of managing firewall configurations. These device-level firewalls have been deployed in the automotive industry on multiple manufacturing assembly lines without degradation in network performance.[14]

Multiple Firewall Manufacturers – Implementing redundant firewalls at key electronic access points between network zones from different manufacturers. The firewalls should be established with the same set of rules and configuration parameters. Using different manufacturers, increases protection against exploitation of one company's firmware security vulnerabilities and provides time to patch potential vulnerabilities.

SIEM Technologies – There are a number of Security Information and Event Management (SIEM) technologies on the market to streamline the review of logs, SNMP traps, and event management. SIEM technologies provide a central console for security personnel to review logs from Intrusion Detection Systems, firewalls, and other cybersecurity devices. These types of technology can assist in the compliance with the monitoring, logging, and review requirements of CIP-007-5.

Patch Management – Security patch management is a major component of CIP-007-5 and is a difficult task, given the legacy industrial control systems that exist at power generation facilities. DHS recommends that end users or REs ensure that a proper backup and recovery plan is in place for each cyber asset in the network. Patches should be tested in a simulation environment that replicates the operational environment as closely as possible. Once patches are tested, the RE should verify those results with the appropriate vendors as a means of double verification.

Figure 3 depicts the network architecture for a complete defense-in-depth strategy with intrusion detection systems (IDS) and SIEM technologies:

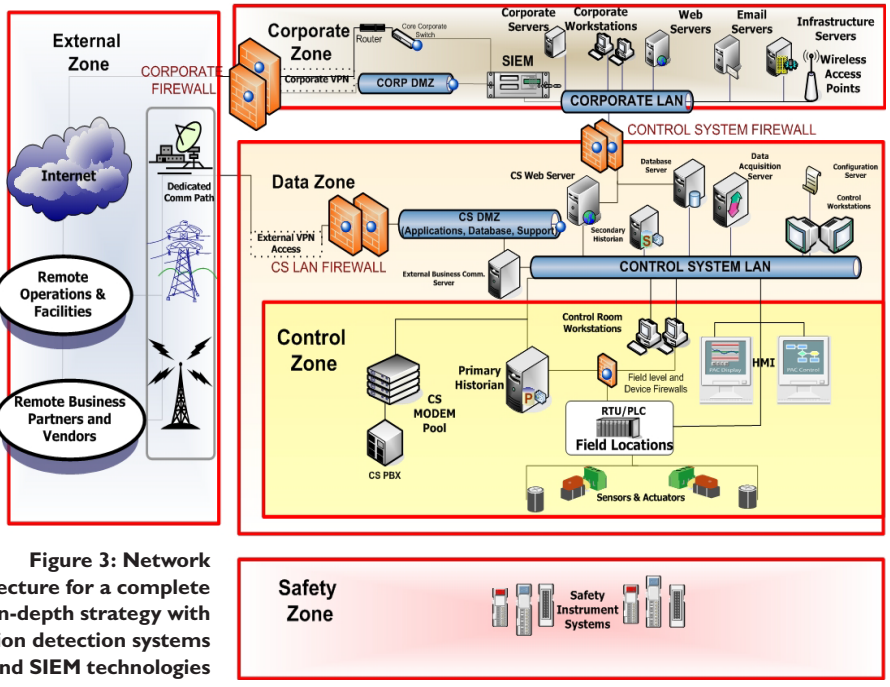

Figure 3: Network architecture for a complete defense-in-depth strategy with intrusion detection systems (IDS) and SIEM technologies

DHS Guidelines and ISA99/62443 Standards *(continued)*

In addition to the Department of Homeland Security, other organizations are developing standards for electronic and cybersecurity. The International Society for Automation (ISA) established the ISA99 Committee to produce standards, technical reports, recommended practices, and information to define procedures for securing industrial automation and control systems (IACS) and to develop security practices for assessing electronic security performance. The following table outlines the status of these standards and technical reports:[15]

The ISA99 Committee has published three main documents as American National Standards Institute (ANSI) documents, two of which are under revision and review:

- ISA-62443-1-1: Terminology, Concepts and Models[18]
- ISA-62443-2-1: Requirements for an IACS Security Management System[19]
- ISA-TR62443-3-1: Security Technologies for IACS[20]

The ISA99 standards also serve as the foundation for the International Electrotechnical Commission (IEC)

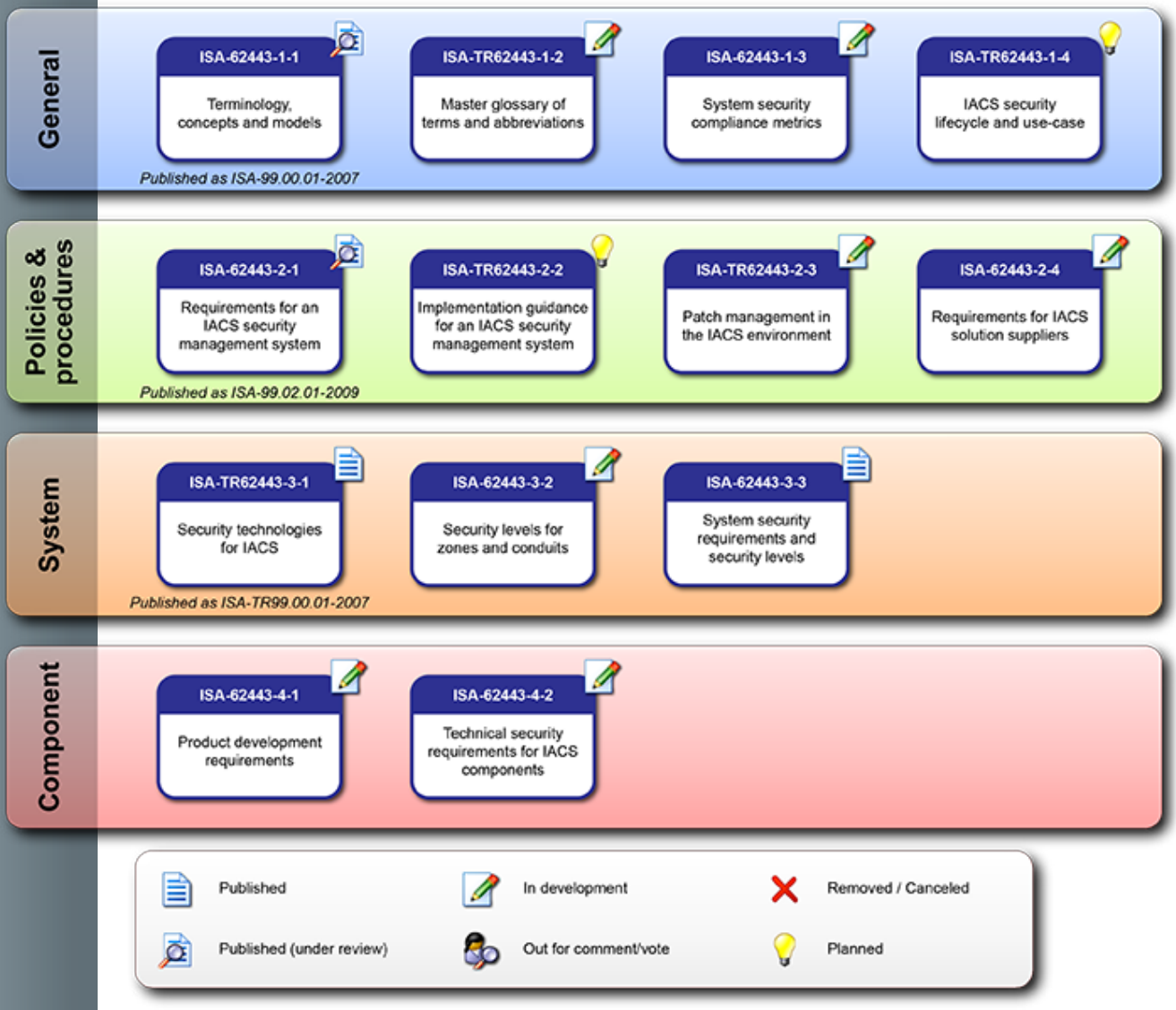

Table copyright ISA; used with permission

PHOENIX CONTACT
INSPIRING INNOVATIONS

DHS Guidelines and ISA99/62443 Standards *(continued)*

62443 series of international standards on electronic security. To align more closely with the IEC 62443, the ISA99 documents are being renumbered and will have the new numbering scheme upon release or re-release. The ISA-62443-1-1 standard is the first in the series and describes the basic terminology, concepts, and models of an IACS used and applied in subsequent standards. The ISA-62443-2-1 standard defines the elements contained in a cybersecurity management system (CSMS) and provides guidance on how to develop the elements. The elements are grouped into three main categories:

- Risk analysis
- Addressing risk with the CSMS
- Monitoring and improving the CSMS

The ISA-TR62443-3-1 is a technical report that outlines the major technologies for securing an IACS. This report discusses many technologies that can be applied to the requirements of the NERC-CIP cybersecurity standards:

Authentication and Authorization – The need for authentication is clearly called for in CIP-005 for remote access and under CIP-007 as part of security access control. The ISA report denotes a number of technologies that can be employed for access control, including:

- Role-Based Access Control – Generally, a position or role within a facility changes less than the individuals employed at that facility. Use of roles for granting access to devices versus individual user accounts simplifies account administration.
- Challenge/Response Authentication – When service is requested, the service provider will send a random string as a challenge. The service requester responds, and if the response is as expected, access is granted. This type of authentication is utilized by Remote Authentication Dial-In User Service (RADIUS) servers to grant access to devices, including remote access. Deployment of RADIUS servers can provide central authorization and authentication services as well as an accounting log of requests, which is a requirement found throughout the CIP standards. The RADIUS server can be located in either the Corporate or Data Zones.
- Physical Token/Smart Card Authentication – Similar to password authentication, this requires the requester to have something in their possession to gain access, but in this case, it is a physical device, such as a smart card or a security token.
- Biometric Authentication – Determine authenticity through a unique biological feature, such as a fingerprint or retinal scan. This technology continues to develop and can be used not only to access control systems workstations but as a means of physical access control to locations that house sensitive cyber assets. Physical tokens and smart cards can be lost, so biometrics has a potential advantage over that technology.

Filtering and Access Controls – As the DHS guidelines noted the use of firewalls in networks, the ISA99 standards also recommend their deployment in networks, particularly in the use of establishing demilitarized zones (DMZs) for computers and workstations that require interaction with the enterprise network. When selecting firewalls for use in networks, it is important to recognize that there are different varieties and each has a particular function and place within a network. The three main types of firewall include:

1. Packet Filtering – These firewalls check the address information in each packet of data against a set a criteria before forwarding the packet. They provide the lowest latency on networks and are cost-effective solutions. However, they offer the lowest level of security, and can be susceptible to common hacking techniques, such as Spoofing and Hi-Jacking.
2. Stateful Inspection – These firewalls track active sessions and use that information to determine if packets should be forwarded or blocked. They offer a high level of security, and there are industrially

PHOENIX CONTACT
INSPIRING INNOVATIONS

DHS Guidelines and ISA99/62443 Standards *(continued)*

hardened and cost-effective solutions on the market today. Despite the added functionality and security over Packet Filters, they maintain high network speed and low latency.

3. Deep Packet Inspection (DPI) – These firewalls examine each packet at the application layer (i.e., Layer 7) and provide the highest level of security. Care must be taken in deploying these firewalls in an industrial control systems network because they can add substantial latency on the network and require additional expertise to configure and maintain. Typically, they are deployed in IT networks where latency is not as critical.

Virtual LANs – Another technology that can be deployed in networks is Virtual LANs, or VLANs. VLANs physically divide networks into smaller, more logical networks to help increase performance and simplify management of the network. While designed to aid in network management and not to address network security or vulnerabilities, a properly designed VLAN can help mitigate broadcast storms that may occur from hardware failures or cyber incidents.

Data-Diodes – While not explicitly noted in the ISA99 standards, data-diodes are another access control technology that can be deployed in control systems networks. For traffic that needs be only uni-directional (e.g., operational data being sent to a backup location), a data-diode can ensure that no return traffic is allowed back into the protected system. A data-diode is a system in which a pair of devices works together; one device has only a physical transmitter while the other has only a physical receiver. Software within the system handles the generation of TCP acknowledgments that are required for many communication protocols.

Encryption Technologies – The CIP-005-5 standard requires multi-factor authentication for all remote access for High and Medium Impact BES Cyber Systems. The ISA99 standards recommend the use of VPNs to secure remote connectivity. A VPN allows private networks to communicate over a public infrastructure. It encrypts data across untrusted networks and authenticates access into trusted networks. Authentication can be achieved in a number of ways, but X.509 certificates are a more secure method than typical password authentication. An X.509 certificate is a small file that contains a very long encrypted signature that is exchanged during the authentication process.

Utilizing VPNs with X.509 certificates with a RADIUS server is one method of meeting the multi-factor authentication requirements of the CIP-005-5 standard.

Owners and operators of BES Cyber Systems will need to review their current cybersecurity posture and evaluate it against the new Version 5 standards to determine what modifications will need to be made to comply with these standards. There are a number of resources and standards, including the ones noted above, as well as new technologies that can be implemented to help meet these new standards.

PHOENIX CONTACT
INSPIRING INNOVATIONS

Where We Are Headed

Now that recent events and media coverage have pushed it to the forefront, cybersecurity in the industrial world will mature and catch up to the enterprise world. "Conveniences," such as keeping the same password on a system for 10 years, and open access to all data, will be replaced by common-sense security practices. These practices will include much more authentication and authorization – most likely with a combination of passwords, certificates, smartcards and biometric data. Accessing data, performing programming updates, and pulling diagnostic information will all result in a much larger audit trail than exists today. Information about "who did what when from where" will be logged, audited, and reviewed.

Data itself will be treated differently, with more stringent protections safeguarding it. It will be protected where it resides and encrypted when it travels, as VPNs will be put to greater use in both inter- and intra-network communications. The demands for these changes will necessitate that vendors more aggressively integrate "security" into their products. Clear text authentication and unauthenticated protocols will no longer be acceptable to the industry (or the government and compliance officers), forcing security down to a lower and more fundamental level of the system.

While these changes won't happen overnight, the transformations in the world we live in, as well as the explosion in cyber capabilities of the "bad guys," will make it necessary to maintain the security, safety, and reliability of our critical infrastructure.

Conclusion

The U.S. government recognizes that protecting our critical infrastructure from a major cyber incident is of paramount importance; this is supported by the fact that the President issued an executive order on cybersecurity earlier this year. Of the 16 critical infrastructure sectors, the power industry continues to be at the forefront of promulgating regulations and standards and adding enforcement measures to protect our bulk electric systems. In late 2012, NERC released Version 5 of the cybersecurity standards, which has increased the cybersecurity requirements for owners and operators in the power industry. We hope that some of the resources and technologies mentioned in this paper will assist owners in complying with these new standards and defending against an ever increasing frequency and range of cyber threats.

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-7388 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com

PHOENIX CONTACT
INSPIRING INNOVATIONS

References

1. Charles, Deborah. *Reuters*. "U.S. Homeland Chief: Cyber 9/11 Could Happen 'Imminently.'" January 24, 2013. http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124
2. U.S. Department of Defense. " Panetta Warns Cyber Threat Growing Quickly." February 6, 2013. http://www.defense.gov/news/newsarticle.aspx?id=119214
3. Executive Order – Improving Critical Infrastructure Cybersecurity. February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
4. Presidential Policy Directive – Critical Infrastructure Security and Resilience. February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
5. NIPP plans can be found at http://www.dhs.gov/sector-specific-plans.
6. ICS-CERT *Monitor*, Oct/Nov/Dec 2012. http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf
7. Zetter, Kim, *Wired*. "Coders Behind the Flame Malware Left Incriminating Clues on Control Servers." September 17, 2012. http://www.wired.com/threatlevel/2012/09/flame-coders-left-fingerprints/
8. NERC: Critical Infrastructure Protection – Cyber Security Standards, CIP-002 through CIP-011. http://www.nerc.com/page.php?cid=2|20
9. Abdollah, Tami. *Los Angeles Times*. "LAX Outage is Blamed on 1 Computer" August15, 2007. http://articles.latimes.com/2007/aug/15/local/me-lax15
10. Rössel, Tommen. *Innominate Security Technologies AG*. "Post-Stuxnet Industrial Security: Zero-Day Discovery and Risk Containment of Industrial Malware." December 2010.
11. NERC: 18 CFR Part 40, Version 5 CIP Reliability Standards, Notice of Proposed Rulemaking. April 18, 2013. http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=13237850
12. "National Institute of Standards and Technology. Special Publication 800-82:" Guide to Industrial Control Systems (ICS) Security. June 2011.
13. Department of Homeland Security. "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies." October 2009.
14. Costlow, Terry. *Automation World*, "Network Security Matures – Firewalls for 40 Machine Networks." May 3, 2012. http://www.automationworld.com/security/network-security-matures
15. Industrial Society of Automation (ISA). ISA99 Work Product Overview. February 2013. http://isa99.isa.org/ISA99%20Wiki/WP_Overview.aspx
16. ANSI/ISA-99.00.01-2007: Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts and Models. Approved October 29, 2007.
17. ANSI/ISA-99.02.01-2009: Security for Industrial Automation and Control Systems, Part 2: Establishing an Industrial Automation and Control Systems Security Program. Approved January 13, 2009.
18. ANSI/ISA-TR99.00.01-2007: Security Technologies for Industrial Automation and Control Systems. Approved October 29, 2007.