Survey of Industrial Control Systems Security

Jayne Caswell, jcaswell@wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download 

Abstract

Industrial Control Systems (ICS) that monitor and operate critical industrial infrastructure worldwide are subject to an increasing frequency of cyber attacks. Evolution of the ICS environment to include standard operating system (OS) platforms and connectivity to corporate LANs and the world-wide-web occurred in ICS environments that were insulated from the outside world by a closed, trusted network. The result is legacy systems and component devices exposed to modern external threats with weak or non-existent security mechanisms in place. The risk to ICS is gradually being addressed, but not nearly fast enough to protect from easily devised cyber attacks.

Keywords

Industrial Control Systems, ICS, SCADA, Supervisory Control And Data Acquisition, critical infrastructure, control system security, industrial control, computer security, network security, cyber attacks, control system security, cyber security, risk management, control network security

Table of Contents

Acronyms

1. Introduction

Industrial Control Systems (ICS) monitor and operate critical industrial infrastructures continuously worldwide. Vital systems and services of modern society controlled by ICS processes include electrical energy generation and delivery; petroleum and gas refining and pipelines; water distribution and treatment; chemical processing and production; pharmaceutical, food and beverage production; railway transportation and air traffic control; and discrete manufacturing [Stouffer11] [Weiss10] [Hentea08]. Closer to home, "Smart Grid" devices are currently being integrated into energy delivery ICS. These new devices directly control utility meters that allow energy flow into our homes and track individual household energy consumption. ICS operate hospital systems and commonly used high-tech medical equipment.

As cyber threats have steadily increased, modernization of ICS design and implementation practices have increased security vulnerabilities. [Stouffer11] [Weiss10][DHS09] [Hentea08] Growing concern about cyber risk of critical infrastructure has focused the attention of government agencies, scientific research, and industry associations on developing and instituting security solutions designed for the ICS environment. Whether security breaches are directed maliciously or occur unintentionally due to human error, the potential for severe or even deadly consequences is substantial when ICS safety systems are compromised.

This paper first explores the components that comprise control systems in general and reviews Supervisory Control And Data Acquisition (SCADA) systems. Then wide-spread security flaws that exist in many, if not most, ICS environments are examined in detail. A few recent exploitations of these vulnerabilities are described to illuminate the reality of ICS insecurity consequences. Finally, current recommendations for securing ICS environments are described and the direction of research presented.

2. Definitions and Background

Industrial Control Systems is a generalized term referring to a system of electronic components that control the physical operations of machines. Automated or operator-entered commands can be issued to machines, either locally in-plant or remote station control devices, often referred to as field devices. The machines may transmit sensor data back to the controller for monitoring and automated operational functions.

2.1. Industrial Control Systems General Concepts

Typical control systems are a collection of control loops with sensors and actuators interacting with the physical world, Human-Machine Interfaces (HMIs), and remote diagnostics and maintenance utilities.

The HMI allows human operators to monitor the state of a control process and issue commands to change the control objective or manually override automatic controls in emergency situations. The control loop includes hardware such as Programmable Logic Controllers which interpret signals from sensors, set variables based on those signals, transmit the variables to controllers, and physically actuatey components such as switches, breakers, and motors. Remote diagnostics and maintenance utilities "prevent, identify or recover from abnormal operations or failure." Figure 1 shows a very simple ICS configuration of components and its logic control loop. [Stouffer11]

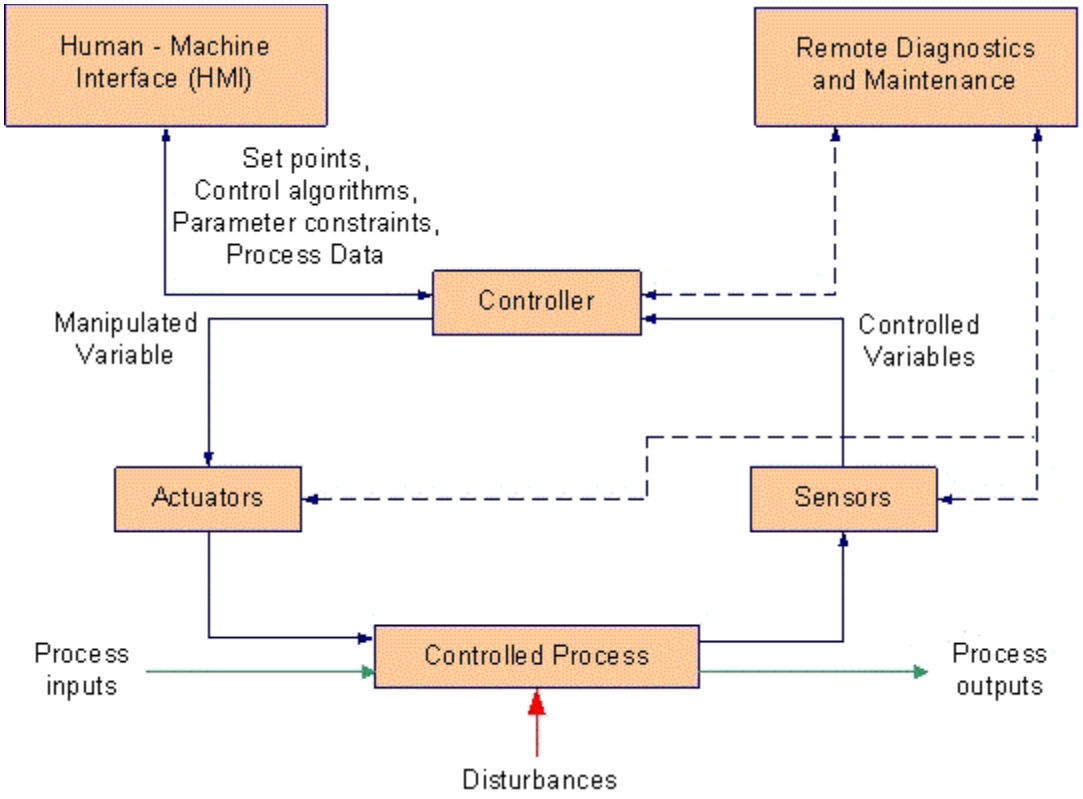

Figure 1. ICS Operation[Stouffer11]

Source: Stouffer, Falco, Scarfone, "Guide to Industrial Control Systems (ICS) Security", NIST SP 800-82, 2011, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

2.2. Control Components

In addition to the basic HMI, control loop and remote diagnostics and maintenance utilities, there are a number of other typical components that may be included in a control system configuration. These are:

- Distributed Control Systems (DCS): which is an architecture containing multiple, geographically dispersed subsystem controllers;
- Programmable Logic Controllers (PLC): industrial process control computers, heavily used in DCS and SCADA systems. Remote PLCs are often referred to as "field devices";
- Supervisory Control and Data Acquisition Systems (SCADA): highly distributed systems controlling geographically dispersed equipment. SCADA depends on centralized data acquisition and control functions to automate critical functions. SCADA systems are implemented with a variety of hardware and software components. For example, the electric transmission and distribution grid relies on SCADA operations;
- Control Server: server which hosts the DCS or PLC supervisory control software;
- Master Terminal Unit (MTU): a control unit which acts as the master in a SCADA system;
- Remote Terminal Unit (RTU): a control unit designed to support SCADA remote stations;
- Intelligent Electronic Devices (IED): a "smart" sensor or actuator containing operational intelligence for automatic control at the local level;
- Data Historian: the database where all process information is logged;
- Input/Output (IO) Server: a server which collects, buffers, and provides access to process information, and may also interface with other components. [Stouffer11]

2.3. Supervisory Control and Data Acquisition Systems (SCADA)

SCADA systems operate widely dispersed control systems and acquire system data for monitoring and control at the central server, or MTU. The data acquisition process is integral to system functions, the acquired data critical to operational integrity. SCADA systems control crucial infrastructure, including the power grid, oil and gas pipelines, railway traffic, water distribution, and waste treatment plants. Any significant disruption to a critical SCADA system could directly threaten public health and safety. SCADA may include some or all of the components defined above, plus additional specialized components not described here. Figure 2 shows an example of a typical SCADA system layout. [Stouffer11]

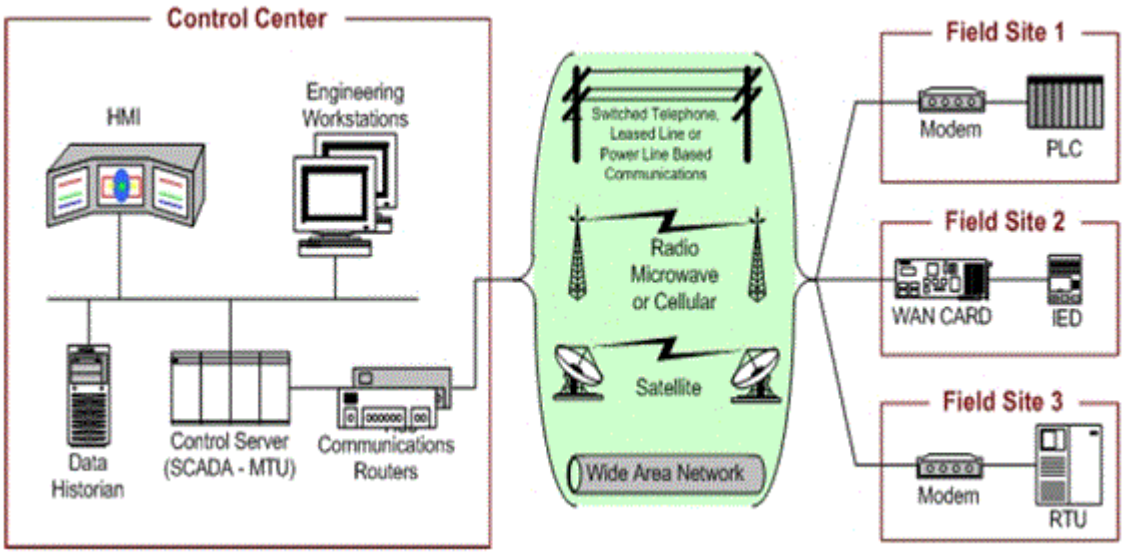

Figure 2. General SCADA Layout[Stouffer11]

Source: Stouffer, Falco, Scarfone, "Guide to Industrial Control Systems (ICS) Security", NIST SP 800-82, 2011, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

2.4. Control Network Components

The control network configuration provides the communications links tying together the control system devices and software. An ICS network can be quite small and local to a manufacturing plant floor. It can be somewhat larger and cover a metropolitan area in support of regional infrastructure such as water distribution and waste treatment plants. In the most complex configurations, an ICS network is very wide-flung geographically with a large number of components integral to operating infrastructure such as the electric grid. These networks are built with a variety of components, which are described here briefly in preparation for examining the vulnerabilities discussed in section 3.

- Fieldbus Network: Sensors and other devices, such as actuators and valve controls, are linked to their controller over the fieldbus network. Network protocols in use vary widely depending on the configuration, but many of these protocols are specifically for fieldbus communications. It is notable that fieldbus protocols began to be standardized in the mid- 1980's, but have been around since the 1970's. This was a time before internet connectivity with no need for ICS security beyond physical access control.
- Control Network: Provides connectivity between the supervisory and lower-level control devices.
- Communications Routers and Switches: Route traffic through to different network segments in a LAN and provide connectivity to WAN and long-distance communications networks.
- Modems: Convert serial digital data to a telephone signal and vice versa, allowing long- distance connectivity between MTUs and field devices. They are also used for remote access by support

personnel for maintenance and operations intervention.
- Remote Access Points: Points of entry to the control network used to perform remote maintenance or operations and configuration activities.
- Firewall: A device configured to monitor and control network traffic, implementing security policies limiting access to internal systems.

Each link in the chain of communications is susceptible to cyber interception by one method or another, and here lies the Achilles heel of cyber-security for ICS. In the next section, some of the most common vulnerabilities of control systems and control networks in particular are examined in detail.

3. Security Vulnerabilities of Industrial Control Systems

Security flaws resulting from legacy devices and software exist in many ICS environments. The difficulty and expense of comprehensively addressing ICS security has delayed security improvements and system upgrades in critical infrastructure ICS environments. A subset of these challenges is discussed here in some detail. [Stouffer11]

3.1. External Network Connectivity

Modern ICS utilize Internet Protocol (IP), connectivity to corporate LANs are often required to allow business systems access to ICS data, and ICS may be web-enabled to permit remote access of vendors and support personnel. These access paths into ICS create many opportunities to breach security. Some specific areas of weakness are examined here. Additional vulnerabilities discovered or maliciously exploited are increasing in frequency.

Denial of Service (DoS) attacks
ICS are vulnerable to commonly known TCP/IP DoS attacks such as SYN flooding, low-rate DoS (LDoS) attacks exploiting TCP's retransmission time-out mechanisms, or buffer-overflow scenarios. More directly, DoS can be achieved by simply sending reset, halt, or reboot commands. Even mainstream IT security mechanisms such as block encryption or port-scanning can "freeze up" or significantly slow down control systems, resulting in DoS. [Stouffer11] [Weiss10] [Solum09]

Insecure protocols are customarily utilized
Outdated, inherently insecure protocols such as FTP and Telnet are generally used for ICS operations. Passwords may be sent in the clear. One standard protocol for data communication between control devices, Object Linking and Embedding for Process Control (OPC), must run without authentication. SCADA and ICS communication protocols for control devices, such as Modbus/TCP, Ethernet/IP and DNP3, do not typically require any authentication to remotely execute commands on a control device, and no encryption options available. [Maynor06] [Ning08]

Basic access control cannot be enforced
Most devices lack even the most basic access control separating system software mode vs. application program mode. Server and terminal authentication is often non-existent or completely ineffective. Differentiation of access privileges between administrators and end users is generally unavailable or not implemented. [Weiss10]

Man-In-The-Middle Attacks
Lack of encryption and mutual authentication expose ICS to alteration of in-transmission instructions, commands, or alarms by network intruders. Replay attacks can trigger automatic system responses resulting in unpredictable malfunctions. Spoofing attacks can cause inaccurate monitoring data could be presented to system operators, prompting inappropriate and potentially dangerous human intervention. Network sniffing

may expose confidential data to invisible interception for governmental or industrial espionage, terrorist attacks, or criminal pursuits. [Stouffer11] [Maynor06] [Solum09]

Control System Device Corruption
Control logic software is not protected and can be easily altered. Corrupted devices could result in system damage, disruption, or safety risks. As pointed out by Martin Solum, "control logic can be pulled, edited, and pushed back to devices at will...even simply changing a few fail- open to fail-close outputs and vice versa could cause significant damage or impact personnel safety." Firmware is not protected, making it possible to alter configuration settings or push malevolent code over Ethernet in many cases. Subsequent device failure or unpredictable functionality may result in DoS incidents. [Weiss10] [Maynor06] [Solum09]

3.2 Modern ICS Configuration Flaws

ICS may now be implemented with industry standard hardware and operating systems (OS), leaving them vulnerable to the same security exposures that plague business IT systems yet often implemented with minimal security technologies and practices. A couple of the most common exposures are default services and outdated software. [Stouffer11] [Weiss10] [DHS09]

Unneeded services allowed to run by default
General purpose OS platforms provide numerous processor and network services that automatically run by default. The result is unmonitored open ports vulnerable to network exploits and actively executing code that may be subject to attacks such as buffer-overflows. Leaving these services active provides unnecessary attack vectors that can potentially be exploited. [Stouffer11]

Operating system, malware protection software, or security patches outdated
Due to the nature of ICS, high or constant availability and critical response-time requirements necessitate exhaustive testing of software and security updates. All such activities must scheduled far in advance and are generally permitted on a very infrequent basis. In addition, ICS components may not tolerate security software due to critical timing requirements. Control system components are often so processor-constrained that running security software itself creates unacceptably high delays in response, threatening system stability. The result is outdated OS levels and outdated or no malware protection software. Even if anti-virus software is up-to-date and configured for proper execution, ICS built on standard platforms are vulnerable to newly discovered malware threats that once again cannot be patched in a timely fashion. [Stouffer11] [Falco06]

Intrusion Detection Software, Port Scanning Applications, and Encryption Services
Retrofitting standard IT security tools into a control system with legacy equipment elongates network response time. The network delay may cause operational errors in the system, or cause the system to freeze or fail altogether. Software installation or modifications may not be allowed by contract with the control system vendor unless the vendor has pre-approved the change. At the very least, any introduction of ad hoc security techniques into ICS environments must be subjected to extensive performance testing to guarantee real-time performance requirements are met. [Weiss10] [Ning08]

3.3 Missing or Inadequate Audit and Control Procedures

Historically, ICS operations occurred in an isolated environment and all communications were trusted. The priorities of ICS operations were safety, availability and response. Online security administration or procedures, audit processes, or computer forensic data were not necessary.

Cyber forensic data is unavailable or insufficient
Many ICS devices have poor or no logging capabilities. Logging capabilities that do exist may not be configured properly or monitored for anomalies. [Weiss10] [DHS09]

Security policies inadequate
With today's wide-spread external connectivity, ICS systems are susceptible to security attacks inconceivable when the systems were originally designed. Development of security policies for the ICS arena has lagged behind the growing exposure to cyber threats. [DHS09] [Sommestad10]

Incidents not detected
Real-time monitoring tools are unavailable or not configured adequately. Logs that are available may be neglected due to lack of standard monitoring procedures. [Stouffer11]

4. Recent Examples of ICS Security Breaches

It has been suggested from some quarters that the concern over cyber security breaches is over-stated. [Shiels11] [Brito11] A few recent examples reported in the public domain news media are presented here to emphasize the seriousness and frequency of ICS security exploits. The ease of obtaining access to ICS systems was demonstrated in August at a Black Hat conference, underscoring the insecurity of many infrastructure ICS. [Mills11]

4.1. "Electricity Grid in U.S. Penetrated By Spies", April 2009

Cyberspies penetrated the U.S. electric grid and deposited software tools that could be used to damage or disrupt the grid. National Security forensics indicate that the spies came from China, Russia, and other countries. Pervasive attempts to map our infrastructure have been made by the Chinese and Russians, although both deny any involvement with cyberattacks. The difficulty of tracking identity in cyberspace prevents full knowledge of who is responsible or what their motivations are, however electronic trails of stolen data have been tracked to China and Russia. "Over the past several years, we have seen cyberattacks against critical infrastructures abroad, and many of our own infrastructures are as vulnerable as their foreign counterparts," Director of National Intelligence Dennis Blair recently told lawmakers. "A number of nations, including Russia and China, can disrupt elements of the U.S. information infrastructure." [Gorman09]

4.2. "Siemens: Stuxnet worm hit industrial systems", September 2010

"A sophisticated worm designed to steal industrial secrets and disrupt operations has infected at least 14 plants, according to Siemens." Stuxnet is believed to have targeted Iran's nuclear enrichment facilities. Although the author of Stuxnet is unconfirmed, sixty percent of reported infections were inside Iran. A previously unknown Windows vulnerability was exploited to spread the worm, often from USB sticks. The worm attacks Siemens ICS utilizing default passwords. . [McMillan10]

4.3. "Conficker infected critical hospital equipment", April 2009

"The Conficker worm infected several hundred machines including critical medical equipment in an undisclosed number of U.S. hospitals." Conficker is known to spread through infected Windows machines, however it is not understood how the control systems such as heart monitors and MRI machines were infected. [ElecForum09]

4.4. "Computer Virus Hits U.S. Drone Fleet", October 2011

"A computer virus has infected the cockpits of America's Predator and Reaper drones, logging pilots' every keystroke as they remotely fly missions over Afghanistan and other warzones." It is unknown where this latest virus originated or its intended function. Other security flaws of the drone systems were already known to have been exploited by hostile parties, for example many drones do not encrypt video transmissions.

[Schachtman11]

4.5. "Attack Code for SCADA Vulnerabilities Released Online", March 2011

Security researcher Luigi Auriemma posted SCADA attack code to a security mailing list in March 2011. Seven vulnerabilities were targeted in SCADA systems that are commonly used in oil and gas facilities, water-management systems, and factories. Among the 34 exploits published, tests demonstrated successful exploitation of buff-overflow vulnerabilities, denial-of-service attacks, foreign file insertion onto systems, altered data displayed to operators monitoring system operations, and enablement of remote execution for malicious code. The researcher stated that he knew nothing about the SCADA systems before beginning his tests with software and documentation easily obtained by anyone, highlighting SCADA security weaknesses. [Zetter11]

4.6. "Researchers Warn of SCADA Equipment Discoverable via Google", 2011

A Black Hat conference demonstration using a Google search engine identified the address of a remote terminal unit (RTU) controlling a pump station. [Mills11] Search engines used to identify and directly access controllers and industrial software applications are freely available, such as SHODAN, ERIPP, and Google. Coupled with the ease of obtaining documentation for common ICS protocols, security exploits can be designed fairly quickly. [ICS-CERT11]

As highlighted by the above cases of ICS infiltration, intruders are able to breach ICS on an all-too-frequent basis. Given that many ICS are largely unsecured, a continued rise in the rate of new cyber threats to critical infrastructure is quite likely.

5. Recommendations to Improve ICS Security

Multiple government agencies, industry organizations and computer security professionals have invested a great deal of effort analyzing the vulnerabilities of ICS and SCADA systems over the past 15 years. After much consideration, recommendations for building multiple layers of security were issued by the Department of Homeland Security in 2009 [DHS09], and followed in 2011 by comprehensive guidelines from the National Institute of Standards and Technology [Stouffer11]. Portions of these guidelines are gradually becoming legal requirements, strengthening the cyber defenses of our critical infrastructure. [Gorman09]

To be effective, the ICS security architecture must encompass every link in the chain from the external points of entry down to the control logic and critical data required for safe and reliable operations. The security approaches recommended here address typical vulnerabilities at a high level. Comprehensively detailed recommendations can be found in the NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security". [Stouffer11]

5.1. Utilize "Defense-In-Depth" Strategies

The Defense-In-Depth strategic framework comprehensively addresses the security architecture. A multi-layered approach to security, Defense-In-Depth is accomplished by identifying vulnerabilities across operational, network and host platforms. Countermeasures are deployed at each level to provide security encompassing the entire ICS architecture. All facets of creating a secure environment are delineated. This includes management controls such as security policy and procedures, audit and vulnerability assessment, system acquisitions, and program management. Operational control policies including personnel, configuration and maintenance practices, contingency planning, and media protection must be defined and become standard procedure. All users in an organization must receive training on system security awareness

and procedures. Incident response plans are predetermined to ensure quick response minimizing damage in a cyber attack event. [Stouffer11] [DHS09] .

Network Level Security

A primary method of denying system access to external attackers is the use of network security zones to protect functional areas. An example of network architecture with zones of system access controlled by firewalls, depicted as orange rectangles, is shown in Figure 3. This configuration implements firewalls at the network, session and application layers. Multiple perimeter networks, also known as Demilitarized Zones (DMZs), separate functional areas and control levels of access.

NOTE: Details of Figure 3 elements can be viewed by visiting the website noted here and clicking on individual elements of the graph:
http://www.us-cert.gov/control_systems/practices/Secure_Architecture_Design.html#nogo.
"This link is provided for informational purposes only and does not represent an endorsement by or affiliation with the Department of Homeland Security (DHS)."

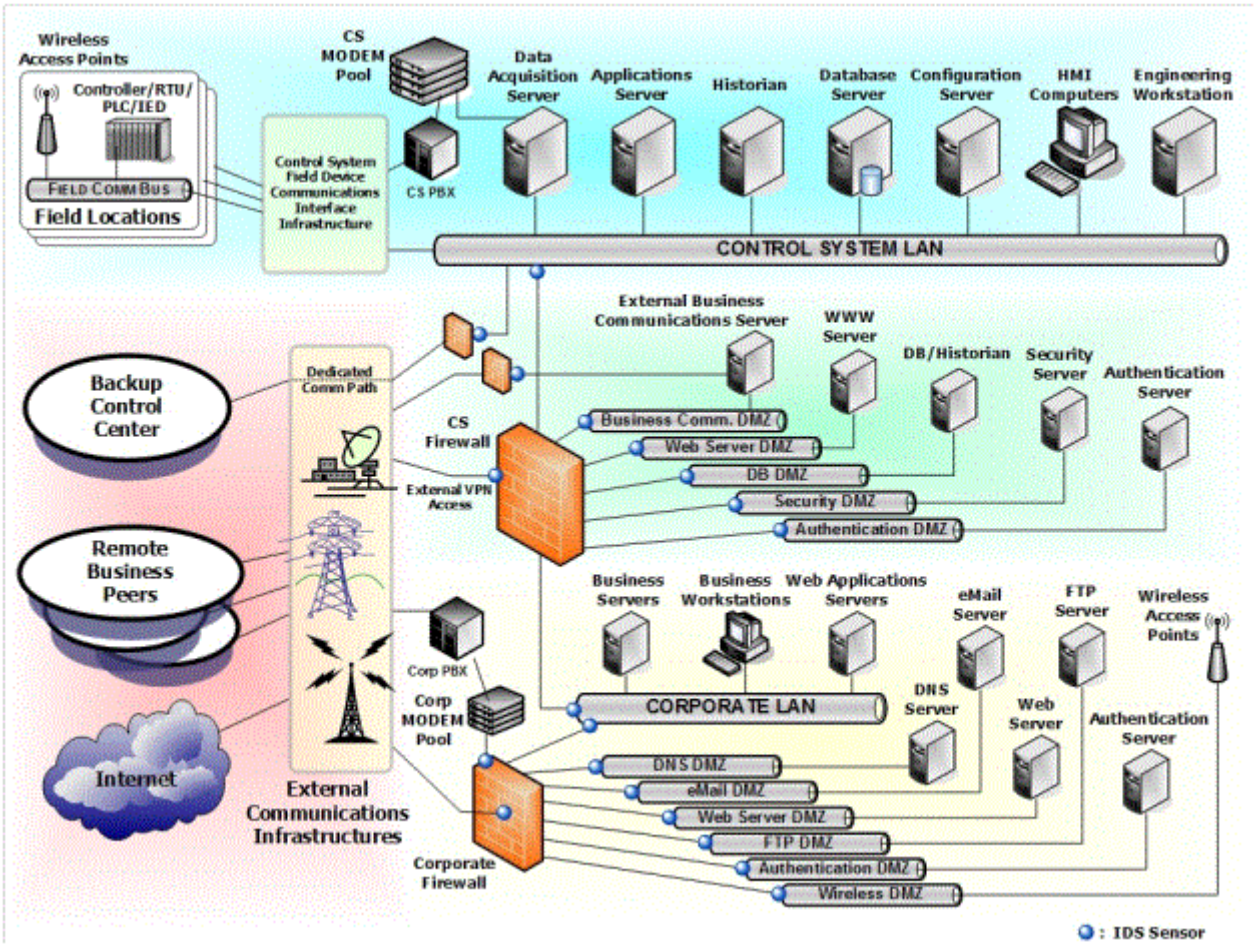

Figure 3: Recommended CSSP Architecture for Defense-In-Depth[DHS09]

Source: Dept. of Homeland Security; "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies", Control Systems Security Program, National Cyber Security Division, October 2009, , http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf

Man-in-the-Middle attacks can be averted by securing field device communications with the deployment of field level firewalls designed for PLCs, IEDs, and SCADA RTUs. Alternatively, port security can be applied by MAC address locking at the network switch level.

Network monitoring to ensure awareness of unusual or unauthorized activity is necessary. Intrusion Detection Systems (IDS) that have quite sophisticated functionality for managing security zones are frequently used for this purpose. *Security Information and Event Management (SIEM) technologies* provide crucial operational alarms when a security incursion event may be in-progress. SIEM tools are also needed to manage and interpret the massive stream of security audit data that accumulates from disparate system components. By providing visibility of aggregated security data, incident response time and capabilities can be improved. [Stouffer11] [DHS09]

5.2. Improve Software Management Practices

Employ System Hardening techniques. Disable unneeded services and close unused open ports to eliminate hostile use as an easy attack vector. Remove installed software that is not used or inappropriate for the intended use of a particular workstation. For example, HMI terminals intended for system operational control do not need to include standard corporate software packages such as word processing, spreadsheets, and email clients. [Creery07]

Implement standardized system configuration techniques, such as creating a workstation "gold disk" to be used as the master system maintenance image. This disk should contain only required software and be configured with appropriate security settings. The startup configuration should include only needed services and ports. Audit logging is enabled and mechanisms to collect historical logs and transmit them to central security monitoring processes are in place.

Implement scheduled software upgrade and patch management procedures at routine intervals. Development of procedures to incorporate security patches promptly and current software recommendations on a regular basis can substantially limit opportunities for hostile parties to target newly discovered vulnerabilities, which are widely publicized immediately. Organizations should institute practices to protect themselves without granting ample time for would-be intruders to apply the new knowledge against critical systems. [Stouffer11]

5.3. Continue research and development of ICS security improvements

Incorporate encryption and authentication techniques in future systems. Many ICS systems and devices were designed without encryption or authentication and may not function at all or may crash due to delays incurred by incorporating other methods of encryption or authentication. Future designs of ICS software should incorporate these security mechanisms. [Stouffer11] [Weiss10] [Solum09]

Develop specialized integrity monitoring tools for industrial control components. PLCs are precluded from incorporating on-board security features due to size and functionality requirements. Low-level logic controllers cannot by their nature include additional functions to provide security. Tools to monitor access are scarce. Vendor development of specialized tools to supplement the protection provided by firewalls is required to fully secure control system hardware. [Johnson10]

Develop automated response and recovery actions where possible. [Khurana11] Continue research with the integrated security framework proposed and tested at the Idaho National Lab as part of the "Protecting Intelligent Distributed Power Grids against Cyber Attacks" project for the Department of Energy. This conceptual framework integrates power, automation, and control process layers with a layer providing security functions. Successful proof-of-concept testing shows promise for future development. [Wei10]

These recommendations are a partial list of improvements-in-progress and future possibilities. Intensive efforts are continuing to provide cyber defenses before an infrastructure failure of severe consequence occurs.

6. Summary

Review of the Industrial Control Systems (ICS) upon which our critical industrial infrastructure relies has revealed numerous security vulnerabilities which can, and are, being exploited on an increasingly regular basis. The most prominent concern is legacy ICS with no security mechanisms in place connected to the world-wide-web. This is a dangerous combination of old and new control system configurations which can easily be exploited by a moderately computer- savvy hacker.

Safe and reliable operation of critical infrastructure relies on substantially insecure ICS configurations in an environment of escalating cyber threats from many sources. A NIST Risk Management Framework has been defined and industry guidelines for ICS security have been established. However these practices have not yet been comprehensively integrated into the industrial infrastructure. Private sector recognition that ICS security vulnerabilities directly risk the safety and reliability of systems operation is necessary to support the business case for increasing security expenditures.

References

[Stouffer11] Stouffer, Falco, Scarfone; "Guide to Industrial Control Systems (ICS) Security", NIST SP 800-82, 2011, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[DHS09] Dept. of Homeland Security; "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies", Control Systems Security Program, National Cyber Security Division, October 2009, http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf

[Weiss10] Weiss, Joseph, "Protecting Industrial Control Systems from Electronic Threats", Momentum Press, 2010, ISBN:1606501976 9781606501979.

[Khurana11] Khurana, Himanshu; "Moving beyond defense-in-depth to strategic resilience for critical control systems," Power and Energy Society General Meeting, 2011 IEEE , vol., no.,pp.1-3, 24-29 July 2011,doi: 10.1109/PES.2011.6039873. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6039873&isnumber=6038815

[Sommestad10] Sommestad, T.; Ericsson, G.N.; Nordlander, J.; , "SCADA system cyber security - A comparison of standards," Power and Energy Society General Meeting, 2010 IEEE , vol.,no., pp.1-8, 25-29 July 2010,doi: 10.1109/PES.2010.5590215. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5590215&isnumber=5588047

[Zetter10] Zetter, Kim, "SCADA System's Hard-Coded Password Circulated Online for Years",July 19, 2010, http://www.wired.com/threatlevel/2010/07/siemens-scada/

[Zetter11] Zetter, Kim, "Attack Code for SCADA Vulnerabilities Released Online", March 22,2011, http://www.wired.com/threatlevel/2011/03/scada-vulnerabilities/

[Hentea08] Hentea, Mariana, "Improving Security for SCADA Control Systems", Interdisciplinary Journal of Information, Knowledge, and Management, Volume 3, 2008, http://ijikm.org/Volume3/IJIKMv3p073-086Hentea361.pdf

[Mills11] Mills, Elinor, "Researchers Warn of SCADA Equipment Discoverable via Google", CNET News, August 2, 2011, http://news.cnet.com/8301-27080_3-20087201-245/researchers-warn-of-scada-equipment-discoverable-via-google/

[Shiels11] Shiels, Maggie; "Cyber War Threat Exaggerated Claims Security Expert", BBCTechnology News, February 2011, http://www.bbc.co.uk/news/technology-12473809

[Brito11] Brito, Jeremy, Watkins, Tate; "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy", Mercatus Center, George Mason University, April2011, http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy

[Johnson10] Johnson, R.E.; , "Survey of SCADA security challenges and potential attack vectors," Internet Technology and Secured Transactions (ICITST), 2010 International Conference for, vol., no., pp.1-5, 8-11 Nov. 2010. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5678102&isnumber=5678008

[Kiuchi] Kiuchi, M.; Serizawa, Y.; , "Security technologies, usage and guidelines in SCADA system networks," ICCAS-SICE, 2009 , vol., no., pp.4607-4612, 18-21 Aug. 2009. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5333009&isnumber=5332438

[ElecForum09] "Conficker infected critical hospital equipment", April 2009, http://www.electricityforum.com/news/apr09/ConfickerinfectedcriticalequipmentHtml

[Falco06] Falco, Joe, et al., "Using Host-based Anti-virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts", NIST SP 1058, 2006. http://www.uscert.gov/control_systems/practices/pcsf/groups/d/1177076007-nist_sp1058.pdf

[Maynor06] D. Maynor and R. Graham. "SCADA Security and Terrorism: We're Not Crying Wolf",2006, http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

[McMillan10] McMillan, Robert, "Siemens: Stuxnet worm hit industrial systems", ComputerWorld, September 14, 2010. http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142

[ICS-CERT11] U.S. Dept. of Homeland Security, "SCADA Hacking Using Internet Search Engines", * Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) Monthly Monitor, October 2011, http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Oct2011.pdf

[Solum09] Solum, Martin, "Quickdraw Retrospective, Part #1," Digital Bond, November 17, 2009, http://www.digitalbond.com/2009/11/17/quickdraw-retrospective-part-1/; "Quickdraw Retrospective, Part #2," Digital Bond, November 19, 2009, http://www.digitalbond.com/2009/11/19/quickdraw-retrospective-part-2/;

[Gorman09] Gorman, Siobhan, "Electricity Grid in U.S. Penetrated By Spies", Wall Street Journal, Technology, 04 April 2009, http://online.wsj.com/article/SB123914805204099085.html

[Ning08] Ning Cai; Jidong Wang; Xinghuo Yu; , "SCADA system security: Complexity, history and new developments", Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on , vol., no., pp.569-574, 13-16 July 2008, doi: 10.1109/INDIN.2008.4618165. http://ieeexplore.ieee.org.libproxy.wustl.edu/stamp/stamp.jsp?tp=&arnumber=4618165

[Wei10] Dong Wei; Yan Lu; Jafari, M.; Skare, P.; Rohde, K.; , "An integrated security system of protecting Smart Grid against cyber attacks, Innovative Smart Grid Technologies (ISGT), 2010 , vol., no., pp.1-7, 19-21 Jan. 2010,doi: 10.1109/ISGT.2010.5434767. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5434767&isnumber=5434721

[Creery07] Creery, A.A.; Byres, E.J.; "Industrial cybersecurity for a power system and SCADA networks - Be secure", Industry Applications Magazine, IEEE, vol.13, no.4.pp.49-55, July-Aug. 2007. doi: 10.1109/MIA.2007.4283509. http://ieeexplore.ieee.org.libproxy.wustl.edu/stamp/stamp.jsp?tp=&arnumber=4283509&isnumber=4283495

[Schachtman11] Schachtman, Noah, "Exclusive: Computer Virus Hits U.S. Drone Fleet", October 7,2011, http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

Acronyms

DCOM.....Distributed Common Object Model
DCS.....Distributed Control Systems
DHS.....U.S. Department of Homeland Security
DMZ.....Demilitarized Zone
DNP.....Distributed Network Protocol

DoS.....Denial-of-Service attack
HMI.....Human Machine Interface
ICS.....Industrial Control Systems
ICS-CERT....Industrial Control Systems Cyber Emergency Response Team
IDS.....Intrusion Detection Systems
IED.....Intelligent Electronic Devices
IP .....Internet Protocol
IT .....Information Technology
LAN.....Local Area Network
LDoS.....Low-rate Denial-of-Service attack
NIST.....National Institute of Standards and Technology
OPC.....Object Linking and Embedding for Process Control
PLC.....Programmable Logic Controllers
RTU.....Remote Terminal Unit
SCADA.....Supervisory Control and Data Acquisition Systems
SIEM.....Security Information and Event Management

Date Last Modified: 12/08/2011
This and other papers on latest advances in network security are available on line at: http://www1.cse.wustl.edu/~jain/cse571-11/index.html
Back to Raj Jain's Home Page