WHITE PAPER

Industrial Control Systems + Cyber Security

April 5

2013

This white paper presented by SDV INTERNATIONAL explains the importance appropriate U.S. cybersecurity policy to protect Industrial Control Systems (ICS) and Critical Infrastructure (CI). It is important that American governmental and industrial information systems be protected with a high level of assurance through sound security measures, practices, procedures, and enterprise architecture policies. Author: Jason Roys

.:. SDV INTERNATIONAL, LLC .:.
.:. Phone: (202) 455-6554 .:.
.:. Email: info@SDVInternational.com .:.
.:. Website: www.SDVInternational.com .:.

INTRODUCTION

This White Paper analyzes cybersecurity and Industrial Control Systems (ICS), which relate to critical infrastructure and national security. The report focuses attention on ICS vulnerabilities and threats, and probabilities of vulnerability occurrence.

Further, this report identifies selected organizations that have experienced exploitation and non-adversarial incidents related ICS vulnerabilities, and explores how policy and procedures can be effectively implemented to manage risks. An analysis of vulnerabilities, threats, policy, and procedures is made from the point of view of the cybersecurity practitioner. Further, from the perspective of a cybersecurity policymaker, such as a Chief Executive Officer with the responsibly to operate organizations like those examined herein, the report analyzes critical issues related to system safety and customer satisfaction.

Keywords: cybersecurity, industrial control systems, ICS, supervisory control and data acquisition systems, SCADA, distributed control systems, DCS, programmable language controllers, PLC

Industrial Control Systems (ICS):

Effective Organizational Cybersecurity Standards & Policies

In March of 2013, the United States (US) Director of National Intelligence (DNI), James Clapper, stated that cyberattacks are now America's greatest threat to critical infrastructure and standard of living. These statements are relevant to cybersecurity professionals because critical infrastructure, such as civil utilities, is dependent upon ICS that are vulnerable to cyberattacks.

Therefore, it is critical to design effective organizational cybersecurity standards and policies that apply to ICS. While the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the NSA can help defend American interests against cybercriminals and cyber terrorists, the private sector plays its own vital role in providing information systems security.

ICS include, but are not limited to, Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) systems, as well as other control components such as Programmable Logic Controllers (PLC) that are found in critical infrastructures. ICS are typically using industrial settings, such as power plants, water treatment facilities, natural gas facilities, chemical manufacturing facilities, transportation networks, pharmaceutical companies, food processing facilities, and durable goods manufacturing facilities.

Many of these systems are interconnected and interdependent. In the United States, more than 90% of critical infrastructure is owned by the private sector. The US federal government also operates critical infrastructure. For example, the US Postal Service uses ICS to automate and process mail handling. As another example, the US Federal Aviation Administration uses ICS to route air traffic.

A SCADA system is capable of acquiring and processing data, as well as applying system controls over long distances (i.e. hundreds of miles). Examples of SCADA systems include power transmission systems, and railway systems. SCADA systems are designed to address unique

signal challenges, including delays in transmission, posed by utilization of various transmission systems.

A DCS functions by controlling infrastructure that is distributed throughout the process being controlled, rather than by a centrally located control unit. DCS are used to control industrial processes such as electrical power generation, wastewater treatment, and automotive production.

There are several *major control components* in ICS. Major control components include control servers, master terminal units (MTU), remote terminal units (RTU), programmable logic controllers (PLC), intelligent electrical devices (IED), human-machine interfaces (HMI), data historians, and input-output (IO) servers. As an example of one of these control components, PLCs are solid-state control systems that store instructions for the purpose of implementing specific functions such as on and off controls, timing, counting, communication, arithmetic, and data processing. PLCs are utilized, at a component level, in almost all industrial processes.

There are different network characteristics in various layers of ICS. Network topologies vary from organization to organization, with modern systems using Internet-based information system infrastructure. In contrast to previous decades, ICS now merge with corporate networks to enable engineers to monitor and control system assets from outside the control system network, and to allow stakeholders to access data in real time from anywhere.

Common manufacturers of ICS systems include Wonderware, GE Fanuc Intellution, Siemens, Rockwell, CiTech. ICS are vulnerable to attacks, and cybersecurity professionals must understand how to protect critical infrastructure.

Vulnerabilities, Threats, and Potential Severity of Impact on Service or Users

In order to secure an ICS, cybersecurity professionals must understand inherent vulnerabilities, associated threats and the potential severity of impact on stakeholders. ICS vulnerabilities may be viewed in the following categories: *policy and procedure; platform configuration, and; network configuration*.

Policy and Procedure Vulnerabilities

Policy and procedure vulnerabilities include inadequate security policy, inadequately documented security procedures, lack of security training and awareness, deficiencies in equipment implementation guidelines, lack of security enforcement, lack of security audits, lack of continuity of operations or disaster recovery plans, and lack of configuration change management procedures.

Platform Configuration Vulnerabilities

Platform configuration vulnerabilities include elapsed time between operating system (OS) vulnerability detection and subsequent software patching, improper OS patch management, OS patch implementation without testing, use of default platform configurations, lack of configuration backup, poor password policy, inadequate access controls, and unprotected portable data storage devices. There are also a number of specific software and hardware platform vulnerabilities that may put ICS at risk.

Network Configuration Vulnerabilities

Network configuration vulnerabilities include inadequate network security architecture, lack of data flow controls, poorly configured security equipment, unsaved network device configurations, poor password policy, poor access controls, network configuration vulnerabilities, network hardware, network segmentation, network monitoring and logging, network communication, and wireless network connections.

Threats

There are various threats associated with each of these vulnerabilities. There may be both non-adversarial and adversarial threats. Non-adversarial threats include natural disasters, human errors and accidents, and equipment failures. Adversarial threats include cyber criminals, terrorists, hostile governments, and industrial spies. Threat agents carry out adversarial attacks. Threat agents include criminal groups, foreign intelligence services, hackers, industrial spies, insiders, and terrorists.

Severity of Impact on Service and Users

Each of these threats poses potential impact on services or users. The Federal Information Processing Standards (FIPS), a key publication from the Federal Information Security Management Act (FISMA) of 2002, provides guidance on how to categorize security standards through its publication number 199. FIPS categorizes potential impact on users under three security objectives: confidentiality, integrity, and availability. In each security objective, FIPS assigns a potential impact level of low, moderate or high. In general, a low impact would likely lead to a *limited* adverse effect on confidentiality, integrity or availability. In contrast, a moderate impact would likely lead to *serious* adverse effects. Finally, a high impact would likely lead to *severe or catastrophic* adverse effects.

In this recent well-publicized case, Saudi Aramco, a major oil refiner, was a victim of a cyberattack whereby attackers erased data on hundreds of computers and made machines unavailable to users, while freezing monitor screens displaying an image of a burning American flag. The Saudi Aramco case is an example of a moderate impact effect of an intact on the company's information system integrity and availability.

As another example of a cyberattack on an ICS that produced a high impact, one may consider the case in which a teenager in Worcester, Massachusetts disabled airport communications, runway lights, phone services, the airport fire department, and the airport weather system. This is a case of high impact because the cyberattack might have caused aircraft collision and death.

Probabilities of an Occurrence for Each Vulnerability (High, Medium or Low)

There is no method to measure the exact probability of an occurrence for each of the ICS vulnerabilities mentioned above, primarily because threat vectors change over time. Adversarial threats, such as hackers and Advanced Persistent Threats (APT), develop new weapons and evolve over time. Non-adversarial threats may be somewhat more predictable and defensible, by way of consideration paid to geographic locations and general environmental analysis. It is possible, however, to assign general probabilities to occurrences of vulnerabilities, such as: *High, Medium, or Low.*

Analyzing the ICS vulnerability categories described above (i.e. *policy and procedure, platform configuration, and network configuration*), cybersecurity professionals may analyze historical information to better understand these probabilities.

Probability of Policy and Procedure Vulnerability Occurrences (HIGH)

As may be gleaned from the explanation of this ICS vulnerability category description above, policies and procedures focus on how people act within an environment that utilized an ICS (e.g., training, implementation of guidelines and procedures, enforcement). The insider threat (i.e. employees, subcontractors, consultants, or service providers) is the most impactful threat source for ICS. Moreover, the insider threat is the most common threat source because insiders are allowed direct contact with an ICS.

As an example of an ICS inside attack, one may consider the case in which a former employee of a manufacturing software company was rejected for a job from an Australian municipal utility. In this case, the attacker used his knowledge of industrial software to attack the municipal ICS, and ultimately caused 264,000 gallons of raw sewage to be released into waterways. Overall, the probability of the occurrence of a vulnerability in this category is high.

Probability of Platform Configuration Vulnerability Occurrences (LOW)

ICS components often remain operative for more than 30 years. As a result, platform configuration vulnerabilities are less likely to be a problem. For example, older ICS operating systems and ICS control components have been in operation long enough for security professionals to identify and patch vulnerabilities that might be exploited by adversarial actors. While there are new networked ICS that introduce new vulnerabilities, the majority of ICS continue to utilize older platform configurations.

There are examples of non-adversarial threats to the older ICS. For example, components in older systems may fail and cause blocking and deadlock of production systems. In the case of the widely publicized failure of the Taum Saik Water Storage Dam in 2005, a catastrophic ICS failure caused billions of gallons of water to spill.

While the probability of an occurrence of a vulnerability in this category may be higher in ICS that utilize new technologies, or in an old ICS that is not properly maintained, the overall probability of a vulnerability occurrence in this ICS category remains low.

Probability of Network Configuration Vulnerability Occurrences (MEDIUM)

ICS network configurations have become more complex in the past decade as organizations have begun to utilize the internet to integrate elements of corporate IT with ICS. As a result, network configuration vulnerabilities have increased in such industrial systems. While there are security practices that can help secure an ICS that is connected to a corporate IT system, such as by way of a Demilitarized Zone (DMZ), adversarial actors have more tools than ever before to attack network vulnerabilities. For example, vulnerability assessment and penetration testing tools offer users hundreds of methods to scan and evaluate network information on potential targets for penetration testing, and provide information about how to mitigate discovered vulnerabilities. For example, the BackTrack Linux distribution is a very strong platform that may be utilized to run various vulnerability scanning tools to assess hosts and host attributes (e.g., open ports, applications, operating systems). Other common network vulnerability scanners include FireWalk, MetaSploit, Hydra, NMAP and Snort. Many of these tools are becoming easier to use, with graphical user interfaces rather than command line interfaces, and even novice attackers pose some threat to poorly secured networks.

Consider the case of the Zotob Worm that affected DaimlerChrysler automotive manufacturing plants by infecting Windows 2000 and Windows XP machines, leading to shutting down manufacturing plants across the country. In this case, a weak network configuration allowed an outsider to penetrate the network and hack the DaimlerChrysler ICS. Despite this ICS vulnerability category having a higher probability of occurrence than most platform configuration vulnerabilities, the risk level of this category is medium because strong security architecture can mitigate network vulnerabilities.

Policies and Procedures to Efficiently Manage Risk

Sound policies and procedures are required to efficiently manage risk in ICS. It is worth noting that ICS security policies and IT security policies differ. ICS security controls policy should address: Management Controls (e.g., risk assessment, personnel security, incident response); Business Continuity Planning and Disaster Recover Planning; Configuration Management; Intrusion Detection and Prevention Systems; Patch Management; Awareness and Training; Access Controls (e.g., biometrics, role-based access control (RBAC), authentication tokens); Encryption; and Auditing and Accountability. Important procedures include approaches to separation of duty between users of ICS and users of corporate IT infrastructure, as well as a separation of the respective system infrastructures. Each of these strategies mitigate the *Policy and Procedural* threat group and the *Platform Configurati*on threat group.

To further manage risk, organizations that rely on ICS must employ defense-in-depth strategies. One defense-in-depth policy would be network separation. Another common defense-in-depth policy requires the use of a DMZ that comprises an intermediate network for systems for network components that are utilized by both the corporate network and the control network (e.g., Data Historian, Data Server). A defense-in-depth policy procedure to handle traffic coming and going to DMZ would be the use of paired firewalls between corporate and control networks. The US Department of Homeland Security provides Control Systems Security Program guidelines that describe risk management approaches, including secure control system (i.e. enterprise architecture) policies and procedures to manage risk. Sound defense-in-depth strategies mitigate network configuration vulnerabilities and many external threat groups.

Security Policy and Procedures Implementation and Customer Satisfaction

A business case must be made before any security program is established. A security program business case may include benefits, costs, potential consequences (i.e. physical impacts, economic impacts, social impact), charter and scope. Among these factors, policy makers and practitioners consider the potential impact a system might have on customer satisfaction.

In the event an ICS is improved and measurable safety improvements result, customers may be pleased with security plans. In the event an ICS security program is modified and unintended consequences occur, customer satisfaction may suffer.

As an example of the latter, take the case of a gas company that hired an IT consulting firm to conduct penetration tests on its corporate network, only to find the test crossed over into the gas company's ICS and caused gas lines to cease functioning for several hours. This is a scenario where customers suffered as a result of security policy that included improperly executed procedures. There may also be risk in scenarios where incorrectly configured firewalls cause delays in an ICS by slowing data flow between a DMZ-based component and an ICS component.

Customer satisfaction is a critical part of the business case that every industrial cybersecurity team must address, and in which potential consequences are considered.

Conclusion

General Michael Hayden (Ret.) (personal communication, March 26, 2013), the former Director of the Central Intelligence Agency (CIA) and the NSA, in a statement made to this report's author in an unclassified meeting, expressed the taxonomy of cyberattacks in two categories: cyberattacks that cause damage that is limited to the cyber domain, and; cyberattacks that cause damage that impacts other domains, such as critical infrastructure and citizens.

Everyone depends on critical infrastructure in this modern world, and critical infrastructure is dependent on Industrial Control Systems. When securing Industrial Control Systems, cybersecurity experts must be aware that their work may impact a wide range of stakeholders.

Cybersecurity practitioners must consider vulnerabilities, threats and the potential severity of impact on stakeholders. When evaluating Industrial Control Systems vulnerabilities, cybersecurity experts must consider policies and procedures, platform configuration, network configuration, as well as the probabilities of each vulnerability occurring. Establishing effective policies and procedures is critical to managing risk in an Industrial Control System ecosystem.

Ultimately, the customers of Industrial Control Systems exist throughout society, and include individuals, families, communities, and governments. It is important for cybersecurity professionals to work together to secure critical infrastructure and implement sound policy.

Sources

Anstrom, W. (2003). What SCADA System Is The Most Used In The Industry? Control.com. Retrieved from www.control.com

Aydogmus, O., & Talu, M. F. (2012). A Vision-Based Measurement Installation for Programmable Logic Controllers. *Measurement (02632241)*, *45*(5), 1098-1104. doi:10.1016/j.measurement.2012.01.031

Barrios, R. M. (2013). A Multi-Leveled Approach to Intrusion Detection and the Insider Threat. *Journal Of Information Security, 4(1), 54-65. doi:10.4236/jis.2013.41007*

Chaffin, M., & Nelson, T. (2011). Common Cybersecurity Vulnerabilities in Industrial Control Systems. Department of Homeland Security. Retrieved from www.us-cert.gov

Chew, S., Wang, S., & Lawley, M. A. (2011). Resource Failure and Blockage Control for Production Systems. *International Journal Of Computer Integrated Manufacturing*, *24*(3), 229-241. doi:10.1080/0951192X.2011.552526

CNN. (1998). Teen hacker faces federal charges. Cable News Network, Inc. (CNN). Retrieved from www.cnn.com

Ciprian, B. (2011). SCADA Security in the Context of Corporate Network Integration. *Analele Universitatii Maritime Constanta*, *12*(15), 159-164.

Efstathios, B., & Joseph H., S. (n.d). Augmenting Defense-in-Depth with the Concepts Of Observability and Diagnosability from Control Theory and Discrete Event Systems. *Reliability Engineering And System Safety*, *96*

Escudero, J., & Luque, J. (2004). Experimental Study On the Transmission of Measurements by Tolerance in SCADA Systems. *IEEE Transactions On Power Delivery*, *19*(2), 590-594.

Geers, K. (2010). The Challenge of Cyber Attack Deterrence. *Computer Law & Security Review*, *26*(3), 298-303. doi:10.1016/j.clsr.2010.03.003

Loughery, K. (2013). Averting a “Cyber Pearl Harbor” Without Sinking Corporate America: The Ramifications of Cybersecurity Regulations on the Private Sector. *Contract Management*, *53*(4), 34-39.

Michaels, J. (March 13, 2013). General's Cyberwarning: Threats 'Are Growing'. *USA Today*.

Nan, C., Eusgeld, I., & Kröger, W. (2013). Analyzing vulnerabilities between SCADA system and SUC due to interdependencies. *Reliability Engineering & System Safety*, *113*76-93. doi:10.1016/j.ress.2012.12.014

NIST. (2004). Federal Information Processing Standards Publication: Standards for Security Categorization of Federal Information and Information Systems. National Institute of Standards and Technology (NIST). Retrieved from www.nist.gov

NIST. (2008). Technical Guide to Information Security Testing and Assessment. National Institute for Standards and Technology (NIST). Retrieved from www.NIST.gov

NIST. (2011). Guide to Industrial Control Systems (ICS) Security. National Institute for Standards and Technology (NIST). Retrieved from www.NIST.gov

Kabay, M. E., & Kelley, S. (2009). Developing security policies. In Bosworth, et al., (Eds.), *Computer security handbook*. New York, NY: John Wiley & Sons.

Koski, C. (2011). Committed to Protection? Partnerships in Critical Infrastructure Protection. *Journal Of Homeland Security & Emergency Management, 8(1), 1-18. doi:10.2202/1547-7355.1860*

O'Halloran, J. (2005). Zotob and VoIP. *Network Security, 2005(9), 2-20. doi:10.1016/S1353-4858(05)70276-2*

Rahmani, B., & Markazi, A. (2012). Networked control of industrial automation systems-a new predictive method. *International Journal Of Advanced Manufacturing Technology*, *58*(5-8), 803-815. doi:10.1007/s00170-011-3416-1

Raman, K., & Beets, K. (2009). Developing classification policies for data. In Bosworth, et al., (Eds.), *Computer security handbook*. New York, NY: John Wiley & Sons.

Rogers, J., Watkins, C., & Chung, J. (2010). The 2005 Upper Taum Sauk Dam Failure: A Case History. *Environmental & Engineering Geoscience*, *16*(3), 257-289.

Sallay, H. (2011). Towards an Integrated Intrusion Detection Monitoring in High Speed Networks. *Journal Of Computer Science, 7(7), 1094-1104.*

Sang-Chin, Y., & Yi-Lu, W. (2011). System Dynamics Based Insider Threats Modeling. *International Journal of Multimedia & Its Applications, 3(3), 1-14. doi:10.5121/ijnsa.2011.3301*

The Celebrated Maroochy Water Attack. (2005). *Computing & Control Engineering*, *16*(6), 24-25.

Tufoi, M., Bizău, V., & Marta, C. (2009). Management of Industrial Processes with Programmable Logic Controller. *Analele Universitatii 'Eftimie Murgu'*, *16*(1), 254-265.

Vasilogambros, M. (2013). America's 3 Biggest Cybersecurity Vulnerabilities. *National Journal.* Retrieved from www.nationaljournal.com

Welander, P. (2010). Control system lifespan: How long is long enough?. *Plant Engineering*, *64*(3), 57-59.

Wen, S., Deng, M., Bi, S., & Wang, D. (2012). Operator-based robust nonlinear control and its realization for a multi-tank process by using a distributed control system. *Transactions Of The Institute Of Measurement & Control*, *34*(7), 891-902. doi:10.1177/0142331211424427