Mark Lewis
13 April 2015

# Cybersecurity for Industrial Control System Networks

Industrial control systems (ICS) help run a large part of our nation's critical infrastructure and industrial processes. The compromise of ICSs can have substantial negative impacts on our nation's security, health, environment, and economy. Although we have been using ICSs in industrial processes for decades, securing these systems has become more important than ever. Over the past several years we have seen increases in both the number and sophistication of cyberattacks on industrial systems. In large part this can be attributed to the fact that many organizations have been increasingly connecting their ICS networks to their corporate networks, opening new doors for attackers to get in. This paper will explore the importance of protecting ICS networks and some best practices for connecting ICS networks to less secure corporate networks.

The term industrial control system actually encompasses many different types of control systems that are used throughout various industries, including SCADA systems and Programmable Logic Controllers (PLCs). These systems can be found in energy, transportation, manufacturing, water treatment, pharmaceutical, food and beverage, and just about any other sector or industry (Stouffer, Falco and Scarfone 2-1). ICSs monitor, control, and perform industrial processes which often are physical in nature. For example, control systems could be responsible for measuring chemical levels in the water and adjusting them to maintain proper balance.

The security of our industrial control systems should be taken seriously. Because of the processes they operate and the integral functions they perform, the compromise of an ICS can have significant consequences. Some of these consequences include irreparable damage to the

control systems themselves, physical harm to the surrounding environment, significant financial issues associated with production loss, negative impacts on the economy, and potential risks to the health and safety of people (Stouffer, Falco and Scarfone 3-1). Although the idea of a cyberattack causing death and physical destruction seems like science fiction, the possibility is all too real.

When thinking about cyberattacks on ICSs, it is important to consider the risks associated with a successful compromise. Attackers will usually try to accomplish at least one of the following five things: loss of view, manipulation of view, denial of control, manipulation of control, and loss of control (Gilsinn 43). Loss of view is where information is not received, such as if operators at a water treatment plant were unable to see chemical levels in the water. Manipulation of view is when the information has been manipulated by the attacker; the system reads that the water chemical levels are normal when they are actually not. Denial of control is when operators are denied control over certain functions, like adjusting the chemical levels. Manipulation of control is where the attackers can successfully change the control signals. This could result in attackers improperly adjusting the chemical levels themselves. Finally, loss of control is a combination of the above attacks and is basically a complete loss of the control system. The attacker can adjust chemical levels and send false level information to the operators so that they will not notice.

The Stuxnet worm is perhaps the most well-known example of a cyberattack that targeted ICSs. Stuxnet was discovered in 2010, and security researchers were amazed at its sophistication. Although there is still some uncertainty about Stuxnet and its purpose, the general agreement is that the worm was developed to attack Iran's nuclear enrichment program. Stuxnet combined several of the above methods to damage centrifuges that are necessary for nuclear enrichment.

By modifying some of the Siemens PLCs and targeting the human machine interfaces, Stuxnet was able to control how fast the centrifuges were spinning—manipulation of control. At the same time, Stuxnet was able to mask the changes from operators by modifying the speed information sent to them—manipulation of view. Because the operators did not know anything had changed, Stuxnet was able to damage the centrifuges by adjusted their speeds beyond their designed limits (Byres 27).

Over the past few years we have seen an increase in the number of cyberattacks on ICSs. Kaspersky Lab reported that "targeted attacks on computer industrial control systems are the biggest threat to critical national infrastructure and take place on a regular basis." Kaspersky Lab saw 400 successful unauthorized logins to its decoy ICS in a single month, with one hacker actually reprogramming a PLC (Ashford 1-4). The Industrial Control Systems Cyber Emergency Response Team responded to 245 incidents concerning industrial control networks in 2014. These were only the reported incidents; the actually numbers would be much higher (ICS-CERT 1-2).

Organizations have been increasingly interconnecting their ICS networks using common communication protocols. By connecting their control systems to the network, organizations can help to increase productivity, reduce costs, collect more information, and increase the integration of their control systems (Recommended Practice 1). In this age of connectivity that we live in, being able to share and access information in real time has become increasingly important. These factors put tremendous pressure on organizations to provide more robust networks for their control systems (Byres 26).

Although this increase in connectivity has its benefits, it has also attributed to the increase in cyberattacks. Control system networks are now beginning to look more like IT

networks, and this means they are becoming vulnerable to the same types of attacks (Byres 26-27). When control system networks are connected to corporate networks, they instantly become at risk to a multitude of attacks, including probing and unauthorized access. As part of its report on 2014 control system incidents, ICS-CERT found that attackers often attempted unauthorized access to internet facing ICSs, performed network scanning and probing on ICS networks, attempted lateral movement between network zones, and used other remote attack techniques (ICS-CERT 1-2). In a paper published by Kaspersky, their sources showed that 35% of malicious code penetrates industrial networks via corporate networks, 26% via remote access, 9% via the internet, and 5% via Wi-Fi (Kaspersky Lab 2).

Organizations need to understand the risks when connecting control systems to the larger corporate network. Despite the fact that control networks are beginning to look more like IT networks, there are still some significant differences. These differences are what make control network breaches so dangerous and what makes stopping these breaches hard. In a control network, availability has priority over confidentiality and integrity (Recommended Practice 5). This relationship of availability, safety, efficiency, and performance can therefore hamper or conflict with security goals. Many control systems must be able to operate and communicate with little delay or jitter, otherwise negative consequences could result. Control systems also need to be available for operators to control in emergency situations (Stouffer, Falco and Scarfone 3:1-2). For example, in the case of a nuclear meltdown, operators would need to be able to shut down the reactor and initiate safety procedures quickly. If the operators have to jump through a multitude of security hoops, they might not be able to react in time and might even risk being locked out.

Besides availability and performance concerns, other factors affect security of control systems compared to IT systems. The "NIST Guide to Industrial Control Systems (ICS) Security" listed in the references does a good job of comparing ICS and IT systems. Perhaps the most important differences though involve system lifetimes and change management. IT systems can generally be replaced every 3-5 years, which could mean significant technological and security improvements over the older systems. Control systems, on the other hand, are often developed with specific purposes in mind and easily go 15 to 20 years without replacement. When we connect these older systems to our network, they often are not designed for the modern network environment and are vulnerable to many attacks. It is also difficult to patch or update these systems, as changes need to be thoroughly tested and approved. IT systems can generally be patched quickly if a significant vulnerability is found; however, it can take weeks or months to schedule changes for certain control systems (Stouffer, Falco and Scarfone 3:1-5).

Many government and security firms have researched best practices for securing control system networks. There is currently a lack of control network specific technologies available, which can make the process of securing the network a little more complex. However, organizations can still implement many of the technologies used in IT networks in their control networks (Recommended Practice 13). Organizations need to be careful though that these security technologies do not interfere with the operation of the control network (Stouffer, Falco and Scarfone 3:1). The following paragraphs will present some of the most common and recommended best practices for securing control networks.

Proper network segmentation is one of the most important components of securing control system networks, as it forms the foundation of a good security design (Ferguson 2). Network segmentation involves dividing the network up into zones. Zones can be defined as "a

grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence" (Byres 28). In other words, our network should be divided up according to function and criticality. The more important and critical zones should have extra layers of protection about them, and the protections should be tailored for the zone's function. The ISA-99 standards use the term "conduits" to describe communication between zones. We should have these conduits between our zones clearly mapped out, knowing how information is passed between them. It is usually more cost effective to implement security controls on the conduits to analyze traffic before it reaches the designated zone (Byres 28).

Firewalls and demilitarized zones (DMZ) are the preferred tools and techniques to implement network segmentation. Control zones should have their own network perimeter; simply relying on the firewall at the perimeter of our corporate network is not enough protection. Traffic should never be allowed to directly pass between the corporate and control network. Instead, the DMZ should act as a buffer between them (Ferguson 3). With firewalls between our corporate and control networks, we can permit only the traffic necessary into and out of our control network. The firewall rules should be as specific as possible, and the default for unknown traffic should be to deny. This goes for both inbound and outbound directions (Recommended Practice 18-22). Because the applications and traffic on our control network should be known, the firewall rules should be very restrictive to suite our environment. In specialized and high security situations it may be effective to use a unidirectional firewall or "digital diode." This is a specialized firewall that only allows traffic to pass in one direction through the use of an optical transmitter on one end and a receiver on the other (Ferguson 4). Using a unidirectional firewall, an organization could know that traffic cannot enter the control zone. If the firewalls and DMZs are implemented properly, the security of our control network will be significantly improved.

Intrusion Detection Systems (IDS) are a great way to monitor the network for unauthorized activity. In its list of common ICS network security weaknesses, the DHS cites lack of IDSs and poor monitoring of IDSs as common weaknesses found in control networks. They recommend network-based IDSs be deployed between the network zones, and host-based IDSs be deployed on applicable systems in the control zone—like Windows workstations (Common Cybersecurity Vulnerabilities 48). It is also recommended to use both signature-based IDSs and heuristics-based IDSs. Many signature-based IDSs still lack specific signatures for control networks, but increasing awareness of industrial cybersecurity is helping to make more signature databases available for ICS networks. Heuristics-based IDSs can do a particularly good job in a control network if tuned properly. Just as we were able to set strict rules with the firewall, we should be able to tune our IDS thresholds to catch unusual activity. Once again, this is due to the fact that we should know what is on the network. The control network should not fluctuate as much as a normal business IT network. The control network should only carry control traffic, nothing else (Recommended Practice 22-24).

Application white-listing can also be implemented in a control network. White-listing helps to prevent unauthorized programs from running and potentially opening up vulnerabilities. With white-listing enabled, only approved software can run on a system (Ferguson 5). White-listing is not common in the IT environment because software regularly changes, and it is a hassle to keep the approval list up-to-date. However, once again, control system environments shouldn't change much, and we should always know what is running in our control network. It should be relatively easy to update the application white-list as software updates go through the rigorous change process required for control networks (Gilsinn 47).

Many other tools and best practices exist to help secure control networks. To find more information regarding best practices for securing these networks, check out the references listed at the end of this paper or visit the ICS-CERT website (https://ics-cert.us-cert.gov). The exact security measures an organization will choose depends on its needs and resources. Because organizations do not have unlimited resources, it is important for them to prioritize their countermeasures to achieve the best security they can (Gilsinn 44). Many assessment tools have been created to help organizations assess their security and identify vulnerabilities. The NSA's Systems and Network Analysis Center has published a framework that can be used by industrial organizations to prioritize their countermeasures and focus on securing the most vulnerable areas of their networks. The four major components include network connectivity assessment, loss assessment, threat assessment, and prioritizing defensive efforts. By using this framework, organizations can focus their resources on the most critical areas (Systems and Network Analysis Center). The DHS and ICS-CERT have also created a tool called the Cyber Security Evaluation Tool, abbreviated CSET. CSET is actually a software based tool that can help industrial organizations assess their security controls and compare them to industry standards (Cyber Security Evaluation Tool).

Securing our industrial control systems should be a top priority. Control systems play an important role in our nation's critical infrastructure and industries. They perform important functions that if compromised can lead to serious consequences; in some cases compromised systems might even risk human lives. One of the first places to start when securing industrial control systems is to secure the control network. Although connecting ICSs to larger networks provides many benefits, it also brings many security risks. Industrial organizations should implement the proper security controls on their networks to ensure attackers cannot reach the

control systems. The U.S. government and many security firms offer best practice guidelines for securing control system networks, and organizations should make sure they meet these guidelines. The government also provides assessment tools to help industrial organizations assess their current security infrastructure. We should start building up our cybersecurity defenses now before a major incident occurs.

# Works Cited

Ashford, Warwick. "Industrial control systems increasingly under attack, says Kaspersky." *Computer Weekly* 01 July 2014. Web. <http://www.computerweekly.com/news/2240223685/Industrial-control-systems-increasingly-under-attack-says-Kaspersky>.

Byres, Eric. "Revealing network threats, fears." *InTech Magazine* January/February 2011: 26-31. Web. <https://www.isa.org/link/networkthreats/>.

Ferguson, Paul. *Toward a More Secure Posture for Industrial Control System Networks*. Research Paper. Cupertino: Trend Micro Incorporated, 2012. Web. <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/rp_toward-a-more-secure-posture-for-industrial-control-system-networks.pdf>.

Gilsinn, Jiim. "Managing industrial control system cybersecurity." *InTech Magazine* September/October 2014: 42-47. Web. <https://www.isa.org/intech/20141006/>.

ICS-CERT. "Incident Response/Vulnerability Coordination in 2014." *ICS-CERT Monitor* March 2015: 1-3. Web. <https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf>.

Kaspersky Lab. *Cyberthreats to ICS Systems*. N.p., 2014. Web. <http://media.kaspersky.com/en/business-security/critical-infrastructure-protection/Cyber_A4_Leaflet_eng_web.pdf>.

National Cyber Security Division. *Common Cybersecurity Vulnerabilities in Industrial Control Systems*. N.p.: U.S. Department of Homeland Security, 2011. Web. <https://ics-cert.us-cert.gov/sites/default/files/documents/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf>.

—. *Cyber Security Evaluation Tool*. N.p.: U.S. Department of Homeland Security, n.d. Web. <https://ics-cert.us-cert.gov/sites/default/files/documents/DHS_CyberSecurity_CSSP-CSET-v4.pdf>.

—. *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Stategies*. N.p.: U.S. Department of Homeland Security, 2009. Web. <https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf>. *

Stouffer, Keith, Joe Falco and Karen Scarfone. *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication. Maryland: National Institute of Standards and Technology, 2013. Web. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf>. *

Systems and Network Analysis Center. *A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)*. NSA Publication. N.p.: National Security Agency, 2010. Web. <https://www.nsa.gov/ia/_files/ics/ics_fact_sheet.pdf>.