Industrial Control Systems- Security is Required

By Richard Triplett & Tushar Nandwana
Risk Control Technology Specialists
Published January 2012

Executive Summary

On August 18, 2005, 13 major U.S. auto plants were shut down for 50 minutes by a simple internet worm called "Zotob" that entered the plants' automation system—probably through an unsecured laptop—bypassing the installed firewalls between the internet and their network. 50,000 employees were forced to stop work, resulting in an estimated $14 million downtime loss.[1]

On January 8, 2008, a 14 year-old hacked into the Lodz Tram control system in Poland, using a modified television remote control and derailing four trams and injuring 12 passengers.[2]

In January 2008, the CIA reported that cyber attacks caused at least one power outage that affected numerous municipalities located outside of the United States.[3]

In July 2010, researchers found evidence of a worm called "Stuxnet" that attacked a specific type of hardware from Siemens. Although it infected hundreds of thousands of systems globally, it was specifically targeted for the control systems at the Bushehr and Natanz nuclear facilities in Iran. The primary purpose of the worm was to sabotage the centrifuges used to enrich uranium. The sophistication of the Stuxnet worm makes it one of the first weaponized pieces of malware.[4]

So, what do these four events have in common? They were all cyber attacks on Industrial Control Systems (ICS).

ICS systems can be found everywhere and are highly intertwined with our way of life. ICS control the electrical grid and electricity that you use in your home or business, the flow of oil and natural gas from the field to the consumer, processes at water/sewage treatment facilities and industrial manufacturing operations to HVAC systems in office buildings and shopping centers.

However, ICS today face greater vulnerability to cyber attacks due to the growth in their numbers and increased reliance on open/internet and wireless-based networks. Such networks facilitate easier communications and installations but also open up the system to cyber attacks. A major interruption of these critical systems could significantly impact life-safety, utilities, transportation or production processes.

What is an ICS?

An ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS) found in industrial sectors and critical infrastructure.[5] Generally, an ICS collects data from various sensors on a factory floor or from operations in remote locations, and forwards

this data to a centralized computer system for processing. It then sends a response to manage the various controller devices in the field or factory floor.

SCADA systems are used to monitor, manage and control geographically dispersed assets (over several thousand square miles), while DCS are more localized or plant centric. For example, a SCADA system would be found controlling the electrical grid, while a DCS would be found on a factory production floor.

The ICS will generally consist of the following components which collect, monitor, manage and transfer the data:[6]

- A Human Machine Interface (HMI) - The apparatus which presents process data to a human operator, and through this, the human operator monitors and controls the process.
- A supervisory (computer server) system- Gathers data on the process and sends commands (controls) to the process. Programmable Logic Controller (PLCs) or Remote Terminal Units (RTUs) connect to sensors in the process, convert sensor signals to digital data and send digital data to the supervisory system. PLCs and RTUs can be viewed as specialized, mini computers. PLCs are more flexible since they are configurable compared to RTUs which are more specialized.
- Communication infrastructure that connects the supervisory server system to the PLCs/RTUs. The infrastructure can be wired and/or wireless; wireless communications can occur over wi-fi, cellular or proprietary radio networks. The communication network can be on proprietary or TCP/IP (Ethernet/internet) based protocols. To ensure compatible communications among the disparate components in an ICS, there is greater use by vendors of TCP/IP over proprietary protocols.

ICS Operation

Let's use a very large oil field in Texas that has oil wells, pumpjacks, pipelines, valves and collection tanks as an example of ICS operations. Sensors that measure temperature, pressure, flow of the pumped crude, status of a valve (open/close) or pumpjack, etc. would generally be located throughout the field along with actuators that operate valves, pumpjacks and other components. RTUs/PLCs are connected to these sensors and actuators to collect and upload critical data to regional and centralized supervisory computer systems over wired or wireless network. The supervisory server is connected to the HMI system, which is used to graphically display information about the process being monitored, change the process operations or set points and enable alarm conditions. Human or preset instructions act on this data and submit a response (e.g. open/close valve A, manage pump B to affect pressure in pipeline C, etc.). Response is downloaded from the supervisory server to the field based PLCs/RTUs which then act on the actuators, valves, and other critical field systems. This data feedback loop continues until the desired condition is reached.

To get a better understanding of how a sample ICS operates at a water treatment facility, check out the following video at http://www.scadasystems.net/

SCADA & DCS Applications

SCADA systems are used worldwide in both private and public infrastructures including water treatment plants, municipality distribution systems, collection and treatment of waste water, power utility companies including electrical and gas/oil pipe lines and railway transportation systems. Industrial or factory production facilities utilize DCS systems to

monitor, supervise and control the production modes of operations as well as specialized process involved in critical quality control. These can be found in electrical power generation, oil refineries, manufacturing of products (chemicals, pharmaceuticals, food, beverages, automotive, others), etc. DCS enables users to obtain and review real time data to monitor conditions at many remote locations.

Exposures

ICS have evolved with each generation due to changes in technology. Proprietary networks, closed architecture and wired communications have given way to the use of TCP/IP protocols, open architecture and wireless communications.[7] These changes have increased the exposure for networked ICS to cyber attacks. Per NIST, this could include[8]:

- Direct manipulation of a PLC/RTU controlled field device – sending an unauthorized signal action to a valve or motor controlled by a PLC.
- Operator spoofing – feeding an ICS system with false [data? signals?] to trick an operator into taking an incorrect action
- Denial of service – overloading a system with junk data preventing the system from monitoring and controlling as designed.

Additionally, certain industrial users of SCADA systems have requested vendors offer specific SCADA applications which are hosted on remote, cloud based platforms.[9] A cyber attack on the ICS controlling a processing operation or failure of the cloud-based platform may result in a significant interruption of the customer's ICS. This could result in a serious interruption to our daily lives or security issues for industrial applications.

Controls – System Security

ANSI/ISA 99.02.01-2009[10], NIST 800-82[11] and NERC CIP[12] are various standards that address cyber security controls for ICS. NERC CIP focuses on minimum requirements for electrical grid systems. The key security objectives of these standards are to have the necessary measures and controls in place to maintain the availability, integrity and confidentiality of the data within the ICS. The following should be considered with establishing or reviewing an existing ICS security program:[13] [14]

- Written security policy and assessment that involves senior management
- Clear and controlled separation of the ICS network from other LAN, WAN and internet facing networks
- Separation of key and subsystems within the ICS network through the use of prudent network design, the purpose of which is to limit the number of contact points to mitigate against vulnerabilities
- Firewalls located at the network gate server that provide protection for private network from outside users
- DMZ (Demilitarized Zones) that serves as a buffer between a trusted ICS network and the corporate network or Internet
- Intrusion detection
- Security over the network and operating environment, wireless network, VPN, IP and applications
- Audit trails and logging capabilities
- Redundant control centers to ensure availability of system

- Use of authentication and encryption in network communications

Conclusion

Compliance with ISA, NIST and NERC standards should harden ICS against cyber attacks. However, there needs to be ongoing vigilance and continual review to ensure that the system protections are keeping up with the changes in technology and new attack vectors. Users utilizing ICS need to be cognizant of these issues, have a proactive risk management approach to security, and as a measure of last resort, react quickly when necessary.

Contact Us

To learn more about how OneBeacon Technology Insurance can help you manage online and other technology risks, please contact Lloyd Takata, Vice President of OneBeacon Technology Insurance at ltakata@onebeacon.com or 706.474.9003. Also, please visit our website: www.onebeacontech.com.

References

[1] http://www.eweek.com/c/a/Security/Zotob-PnP-Worms-Slam-13-DaimlerChrysler-Plants/ ; http://www.nwppa.org/web/presentations/Jan_2011_IT_Meeting/Network_Security_SCADA_and_Control_Systems_Eric_Byres.pdf

[2] http://www.theregister.co.uk/2008/01/11/tram_hack/

[3] InformationWeek, CIA Admits Cyber attacks Black Out Cities. Thomas Claburn http://www.informationweek.com/news/205901631

[4] http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all

[5] http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, page 2-1

[6] http://en.Wikipedia.org/wiki/SCADA

[7] SCADA Systems, Meme Bridge, www.scadasystems.net

[8] Ibid 5

[9] Ibid 7

[10] ANSI/ISA 99.02.01-2009 - http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243

[11] NIST 800-82 - http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[12] NERC CIP (North American Electric Reliability Council Critical Infrastructure Protection) - http://www.nerc.com/page.php?cid=2%7C20

[13] Ibid 5

[14] SCADA/Business Network Separation: Securing an Integrated SCADA System, Scott Wooldridge. http://www.automation.com/resources-tools/articles-white-papers/hmi-and-scada-software-technologies/scadabusiness-network-separation-securing-an-integrated-scada-system

January 2012.