SCADA Technologies and Vulnerabilities

David J. Kalbfleisch

david.kalbfleisch@tufts.edu[1]
http://www.purdone.com/dave/contact.php

Mentor: Ming Chow

13 December 2013

ABSTRACT

Supervisory control and data acquisition (SCADA) systems, LonWorks networking hardware, and their associated protocols are ubiquitous in industry. Many countries, including the United States and China, have codified the protocols as national standards. These systems often link with internet connected devices, and such links expose industrial control infrastructures to internet-based attacks. Furthermore, control hardware often has poor physical security. In at least one very high profile case, the Stuxnet virus attack on Iran's Natanz nuclear enrichment facility, attackers specifically targeted SCADA components to cause catastrophic system failure. This document discusses SCADA system architectures, some of their flaws, and the present state of SCADA vulnerability research.

1 Use this e-mail address through May 2014. Thereafter, use the contact form.

INTRODUCTION

What do nuclear generating stations, electrical grids, sewage treatment facilities, building management systems, train routing systems, oil pipelines, traffic signal management systems, and manufacturing facilities have in common? The answer is "SCADA," a complex aggregation of industrial automation hardware and software with more than one-hundred-million installations around the world.[i]

Supervisory control and data acquisition (SCADA) systems, a subset of industrial control systems (ICS), allow a relatively small group of operators to view and remotely control critical process parameters and to start and stop equipment. Malfunction or intentional misuse of a SCADA system can result in a condition as benign as building inhabitants being uncomfortable or as severe as the loss of a pump used to cool a nuclear reactor. SCADA vulnerabilities facilitate tangible damage, including loss of life, but infrastructure providers are only beginning to take seriously this threat.

Frequently, SCADA systems interact with internet-connected TCP-IP local networks to allow administrative and management employees to view data relevant to business concerns.[2] This is of particular concern from a security point of view because it implies that many SCADA systems indirectly connect to the internet. Thus, many SCADA systems are vulnerable to IP/TCP-based attacks. Compounding the problem, system owners often do not realize the extent to which their SCADA system is exposed to the internet. Consider as an example a laptop computer used on an industrial site. An employee might connect the laptop to SCADA hardware using an Ethernet cable while the laptop is also connected to the internet via the local Wi-Fi. Scenarios like this, which occur daily in industry, demonstrate the impracticality of maintaining an "air gap" between the SCADA network and the internet. Protecting vital infrastructures must rely on other means.

---

2 These networks are commonly denoted, "business networks."

OPEN STANDARDS

Modern SCADA systems commonly use open protocols created within the last twenty-five years. Although automation dates from the 1930s, modern implementations rely heavily on the work of San Jose, CA-based Echelon Corporation, creator of the LonWorks technology platform, which commenced operations in 1988. For investment purposes, Echelon is a "small cap growth" company[ii] dwarfed by larger competitors, such as Cisco Systems, but LonWorks forms the basis for international standards and the national standards of many nations, including the United States and China. Some of these standards are:

I. "Control Networks" defined by ISO/IEC 14908.1 through 14908.4
II. "Control Networks" published as ISO/IEC JTC 1/SC 6 (LonTalk)
III. United States of America
   A. ANSI/CEA 709.1-C-2010 – Control Networking Protocol Specification
   B. IEEE 1473-2010 – Communications Protocol Aboard Passenger Trains
   C. NIST 800-82, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security"
IV. China – GB/Z 20177.1-2006 – Control networking and building controls

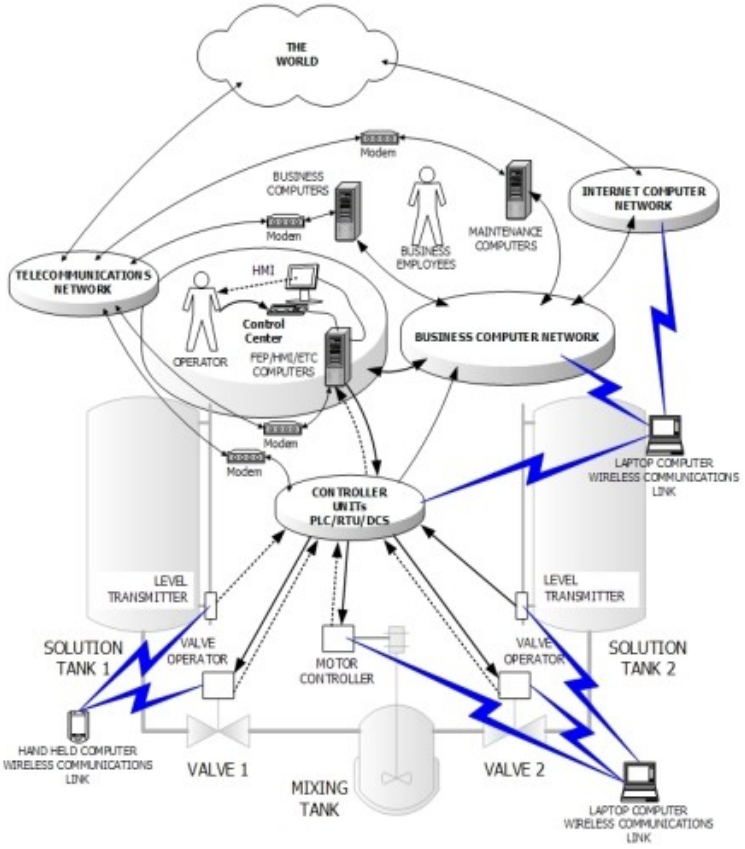
LonWorks differs from TCP-IP in that LonWorks provides services at all seven layers of the OSI model,[iii] whereas TCP-IP address only the transport and network layers. LonWorks protocols also differ from TCP-IP implementations in that LonWorks protocols optimize according to metrics relevant for control systems, including latency.[3]

More recently, Echelon is moving away from LonWorks to favor of pushing IPv6 technologies[iv] —the so-called "Internet of Things," most likely to facilitate in-home implementations at costs accessible to the mass market. For example, technology already exists to control the lights in your house via the internet.

3 If an oil pipeline develops a leak, we want the isolation values to shut fast!

SCADA COMPONENTS

Image courtesy of ICS-Cert. The author believes this constitutes fair use for educational purposes.



Three communication layers form the structure of most SCADA systems, and each layer has associated hardware and communications protocols.[v]

The lowest layer includes hardware, such as programmable logic controllers (PLCs), which connects directly with the machinery under control. PLCs take process and safety inputs and can directly affect equipment without operator intervention. For example start a backup pump.

Low-level communications protocols include DNP3, the Distributed Network Protocol. Sending commands from a master/control station to process machinery will probably use DNP3 at some point along the path. SCADA systems predate the internet, and system security historically relied on physical security. As such, low-level protocols, including DNP3, used in ICS commonly do not include any security precautions; there is no authentication or authorization. A "DNP3 Secure Authentication" protocol exists but is not yet widely implemented. In general, most system owners still rely on physical security and firewalls to isolate controlled machinery from the corporate/business network and internet.

The second communication layer generally aggregates data from the first layer and transmits the

bulk data to applications on the third layer. Implementations vary, but most hardware at this layer works with the Inter-Control Center Communications Protocol (ICCP), an international standard for transmitting data between wide-area networks. The hardware can be standard routers or hardware custom designed to handle specific protocols.

The third communication layers includes business and control applications running on standard office hardware, such as PCs and, increasingly, mobile devices. Master commands (i.e. “start” and “stop”) to remotely controlled (slave) equipment generally originate at this layer. The third layer commonly has a “data logger” that periodically stores some or all measured parameters in a database which operators can access for business analysis and trending. The dominant protocol at this level is likely to be a member of the Object Linking and Embedding for Process Control (OPC) family.[vi]

SCADA SYTEM SECURITY

Tangential to these three layers are remote terminal units (RTUs). In many implementations, an operator standing next to an automated machine does not directly operate the machine. Instead, he or she uses controls on a RTU to relay commands to a master station which might subsequently relay the commands to the machine the operator wishes to control. This centralized approach adds latency, but it has the benefit of streamlining the flow of information, which in turn reduces costs of ownership.[4] Additionally, the master station, or peripherals, can log all commands issued.

However, this operation is not without security problems, particularly because security played little role in the development of the commonly used protocols. As mentioned earlier, the DNP3 protocol, which plays a prominent role in the delivery of commands to equipment in some industries,

4 Consider that the major logistics carriers commonly route all or substantial portions of their traffic through hubs. A package shipped from Chicago to Minneapolis by UPS is likely to pass through Louisville, KY, which is hundreds of miles south of both cities. The overall gain in the efficiency of the system exceeds the local costs.

has no native security. There is neither authentication nor authorization, but this isn't necessarily undesirable. If a pump catches on fire, do we want local operators to have to login before they can stop the pump?[5] Do we want one operator not to be able to use an RTU because somebody else didn't log out?

In more recent SCADA implementations, the master station authenticates the identity of the RTU itself, rather than the operator, when it receives a command. If the master station cannot authenticate, it should not forward the command to the automated equipment. However, if an attacker can gain access to the master control station, he can issue any command; the RTUs become non-players.

Historically corporations have attempted to secure their networks using“firewall” software. In SCADA systems, PLC subsystems and local operating stations at the first layer might be firewalled from the second layer, which contains the master control station. The master control station might be firewalled from the third layer, which is firewalled from the internet. This approach has avoided the cost of patching the underlying software vulnerabilities and flawed protocols, but it doesn't fix the underlying problems. It is analogous to jacking up a deck built on a sinking foundation; the problems are only going to get worse with time.

For reasons already discussed, the master control station is almost guaranteed to connect, directly or indirectly, to the business network, which in turn connects to the internet. All known methods to subvert TCP-IP networks then become relevant for attacking SCADA systems. An attacker might be able to scan “through” firewalls using packet segmentation to get the IP and MAC addresses of relevant hardware, overflow a buffer to execute code that installs a root kit, and begin issuing commands from the master control station.

With the advent of modern, network-based cyberwarfare and cybercrime, SCADA systems are

5 Of course, this assumes that a local power switch is not accessible.

under increasing scrutiny. In 2010, the year the public learned about Stuxnet, there were 15 published SCADA vulnerabilities; in 2011, there were 129 published vulnerabilities. While this is a significant increase, a lone researcher from Malta, Luigi Auriemma, discovered almost all of the new vulnerabilities.[vii] One man's contribution, while a brilliant personal achievement, seems small in the wake of the reality that government agencies with ten-digit budgets are now actively working to undermine SCADA systems. The United States government created the Industrial Control Systems Cyber Emergency Response Team (ICS-Cert) "to reduce risks within and across all critical infrastructure sectors. . . ."[viii] ICS-Cert, part of the Department of Homeland Security, publishes alerts when it learns of new SCADA system vulnerabilities after first giving vendors the opportunity to implement patches. However, ICS-Cert does not seem to be conducting active research to improve the national infrastructures' fundamental security problems. They are enhancing the efficiency of the outdated patchwork repairs paradigm.

TO THE COMMUNITY

SCADA systems quietly underpin modern technological societies. They are part of the invisible fabric of our existence. Everybody has a stake in the reliable operation of generating stations, electrical grids, and water treatment facilities.

These concerns are likely to become highly personal with the rise of the "Internet of Things." In the not-so-distant future, "getting hacked" might include the manipulation of machines in your home and subsequent corporal injury. There is also a risk that corporations and nation-states will abuse the "Internet of Things" to conduct mass surveillance of people's homes. Consider the comments former NSA Director David Patraeus made in 2012:

> "Items of interest will be located, identified, monitored, and remotely controlled through technologies such as

radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters — all connected to the next-generation internet using abundant, low-cost, and high-power computing, the latter now going to cloud computing, in many areas greater and greater supercomputing, and, ultimately, heading to quantum computing."[ix]

In the wake of the Snowden revelations, this author considers to be implausible any denial that the "democratic" governments would engage in such activity. The people who create these technologies should be aware of the risks and include security by design.

DEFENSES

These are a few things that might help protect a SCADA network:

- Defense in depth: Secure the business network!
- Install or upgrade to secure versions of common SCADA protocols, such as DNP3 Secure Authentication.
- Ensure SCADA hardware is physically secure. For example, utility providers should ensure that substation facilities are locked.
- To the maximum extent practical, corporations should not post job listings the reference specific automation hardware and software.[6]
- Do not permit portable devices to connect to the network purely for convenience. (Note that Stuxnet got into Iran's Natanz enrichment facility through USB drives.)

CONCLUSION

SCADA systems are a fascinating technology that does wonderful things for society. However, like all technology, it has inherent risks. Let's work to ensure that we can all count on the lights staying on, the lake staying behind the dam, and the oil remaining in the pipeline!

---

6 This author has personally worked at a large biotechnology company that violates this tenant. Examples are easy to find. Just search any job site for "scada" or "automation."

i http://www.echelon.com/company/
ii Morningstar.com profile for Echelon Corporation (ELON)
iii http://www.echelon.com/technology/lonworks/lonworks-protocol.htm
iv IP-all-the-way is the way to go. Varun Nagaraj, Senior V.P. at Echelon Corporation. 23 July 2013.
v SCADA Security and Terrorism: We're not crying wolf. D. Maynor and R. Graham. Presented at Blackhat 2006.
vi OPC Foundation
vii https://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=scada_vulnerabilities
http://aluigi.altervista.org/
viii https://ics-cert.us-cert.gov/
ix CIA Chief: We'll Spy on You Through Your Dishwasher. Written by Spencer Ackerman. Published by Wired Magazine on 15 March 2012.