Industrial Control System Security - Existing Infrastructure and New Designs

2018 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure
Phil Salkie, Jenariah Industrial Automation - phil@jenariah.com - 301-859-0500

Reading Period
What's ICS/SCADA, and why should I care?

ICS - Industrial Control Systems
ICS is a catch-all term meaning any automated system which controls physical functions by manipulating mechanical equipment. It can mean the robots which assemble automobiles, or the heating system in a building, or the chillers at a data center. As building systems become more complex and management of plant and equipment gets more automated, more and more ICS equipment is being placed into service in new ways throughout our scientific and technical facilities. This equipment is often not designed with a robust security model in mind, designs are not implemented by engineers skilled in threat analysis, and sophisticated computer systems and communications networks are installed without the input or knowledge of the IT staff.

PLC - Programmable Logic Controller
PLCs are rugged, dedicated-purpose computing systems which use specialized programming languages and industrial-grade interface hardware to directly control physical devices and machinery.

OIT/HMI - Operator Interface Terminal / Human Machine Interface
HMIs are ruggedized display panels with embedded CPUs and multiple communications ports, designed to display data that resides in PLCs and to allow machine operators to make changes to that data. They are generally programmed using separate GUI software from that used for the PLC, and they tend to have a shorter working lifespan than PLCs due to their exposure to human interaction and their use of components like backlit displays and membrane keys. Note that there are vendors producing combination HMI/PLC devices which may present advantages or disadvantages depending on the exact usage situation.

DCS - Distributed Control System
DCS generally refers to systems where the processor is far removed from the points of control, and all input and output signals are transmitted via some form of networking back to the processor. These control systems are most often found in large "Process" control applications - think large tanks in fields, vats in buildings, pumps and sensors, all connected by miles of piping. The programming for these systems is most often a graphical representation of data flow, much like a data flow diagram from the realm of software engineering, or a programming flowchart.

SCADA - Supervisory Control And Data Acquisition
SCADA is a term which is used differently in the computer security field than it is in the controls industry. Security specialists often use "SCADA" to refer to any ICS equipment which isn't a standard commercially-available computer component like a destop PC or a laptop. In the controls industry, it specifically refers to hardware and software of any sort which is not directly involved in controlling the equipment - but rather controls the PLCs which control the equipment. That "Supervisory Control" can mean simple monitoring
via web pages, downloading of recipes, collection of log data, or all of the above and more.

Sensors
A sensor is any device which translates real world information into signals that a controller can work with. That can be a simple switch saying that a door is closed, a transmitter which reports the temperature of a liquid or the pressure inside a pipe, or complex equipment measuring the optical clarity of a stream of treated water or reporting on radio-frequency emissions from a system under automated test.

Operators
Could refer to the user of a control system, or a simple operating device like a pushbutton or a selector switch (such things are collectively referred to as "panel operators")

Actuators
Any hardware which a control system uses to mechanically move something. This could be a motor, an air-operated rod cylinder, or a mechanical gripper, just to name a few.

Telemetry
Remote measuring systems - a telemetry device allows a control system to obtain information from something far away, for example letting a water pumping system know the current level of a distant storage tank.

Custom Hardware
Embedded Controls
Ways to refer to controls hardware which doesn't use a pre-packaged solution like a PLC or HMI. Often these systems were first prototyped using off-the-shelf controls hardware, then once the requirements were fully determined, a custom hardware and software solution was produced for volume sales. These are the trade-offs involved in producing one-off custom solutions (like the control system for a building or a packaging line) versus large volume solutions like the controls for a dishwasher or a laboratory chiller.

In one-off systems, the engineering time involved in making things work is significant in proportion to the cost of the controls - so it makes sense to spend money on controls hardware which minimizes the time required to build the system. Systems such as these often become difficult to support over time, as component availability, access to specialized accessory hardware and software, and even the closing of the original machine builder may become difficult issues to surmount.

In volume produced systems, engineering time is amortized across the large number of devices that are sold - possibly only equating to pennies per unit. Therefore, investing engineering time up front to make the per-unit cost as low as possible is a definite win over the lifecycle of the product. Systems such as these tend not to allow much site-specific customization, the software which is resident in them is usually a closely-guarded trade secret, and if replacement electronics components are no longer available, it is often necessary to completely replace entire equipment rather than just replacing the controls.

Fun Fact: There were programmable controllers before there were desktop computers. ("PC" meant "Programmable Controller" before it meant "Personal Computer", then was changed to "PLC" for "Programmable Logic Controller" after the IBM-PC came out.)

Not-So-Fun Fact: Some of those controllers are still out there and running.
They may have been programmed on dedicated hand-helds, with their programs stored on cassette tape, or hand-written on paper with pre-printed boxes for entering the data. These paper documents may be the only existing copy of the operating logic.

Fun Fact: There were PLCs before there were communications network standards.

Not-So-Fun Fact: Some of those controllers are still out there, running on dozens of different networking hardware layers and hundreds of software communications protocols.
Names you may run into are: Modbus, CANBus, ProfiBus, FieldBus, InterBUS, CC-Link, DeviceNET, HART, CIP, Ethernet/IP, DF-1, DH-485, MELSECNet, BACnet, LON, ZigBee, SRTP, and many, many more.

Some of these protocols allow an external host to read and write anything stored in the controller's data memory, some allow an external host to read and write the controller's password or the logic program, some allow an external host to flash new firmware into the controller's operating system memory. Some protocols have undocumented functions and features which could be exploited.

Fun Fact: Desktop PC systems are designed with a four year product lifecycle.
One often sees PCs which are ten years old, and occasionally encounters a system that's over 20 years old. (Win98 SE, anyone?)

Not-So-Fun Fact: Controls systems are designed to be installed in capital equipment hardware which is amortized over twenty or thirty years. It is common to see controllers which were installed thirty or forty years ago, and one can occasionally see operating machinery with controls built before integrated circuits were common.

Fun Fact: The advent of the Desktop PC forced standardization of communications systems, including connectors, hardware layers, and higher level protocols.

Not-So-Fun Fact: Controls systems have used a bewildering variety of connectors, pinouts, standards, and protocols - often making changes to existing designs seemingly solely to break compatibility with existing systems. You may require specialized cables, programming interface boxes, or plug-in cards for your computer - you may even find that modern computing hardware is incapable of communicating with a given system, and you'll need to find a ten-year-old laptop with a built-in RS-232 port or a PCMCIA card slot.

Fun Fact: Modern PC motherboards support PCIe 2.0 X1, PCIe 2.0 X16, PCIe, and (possibly) PCI busses. They also support USB 2.0, USB 3.0, and (possibly) USB 3.1, USB-C, Lightning, and Firewire.

Not-So-Fun Fact: Control systems have used S-100, VME, STDbus (8,16, and 32), ISA-8, ISA-16, PC/104, PC/104-16, PCI, PCIe, and a host of other proprietary busses either based on existing standards of the time or developed entirely in isolation.
Programmable Controllers generally do not use standardized busses, but have proprietary data paths and connector sets. Dozens of bus architectures are currently in use in controls systems worldwide today.
If Desktop PCs are part of a control project, it is more than possible that they are using a bus architecture which is not available on new motherboards, and are using plug-in cards which cannot be purchased new (and may even be difficult to get repaired.)

Fun Fact: Modern computer systems use flash memory for long-term storage of data which is read more than it is written. (BIOS, etc.)

Not-So-Fun Fact: Programmable controllers may store firmware in mask-programmed ROM, UV-EPROM, or EEPROM/Flash Memory. They may store user programs and data in battery-backed SRAM, capacitor-backed SRAM, EEPROM/Flash Memory, UV-EPROM, or some combination of these. If vulnerabilities are known, patching may not be possible.

Many control systems have some sort of replaceable lithium battery to hold up SRAM data storage, or run a real time clock. While the shelf life of these batteries is 10+ years, when they are actually being used to support the memory (i.e. when sitting on a shelf as a spare part) they can deplete in less than a year. Also, batteries aren't just for CPUs - often there are special-purpose communications or motion control modules which have their own batteries which need to be tracked and changed.

The retention times of flash memory and EEPROM varies widely based on temperature and the amount of time since it was last powered - and, since the time frames we are dealing with are long in comparison to the existence of the components, largely theoretical at this juncture.
As some of these parts have been sitting for upwards of a decade, we have started seeing failures due to flash memory "bit rot".

Fun Fact: Your facility almost certainly has multiple industrial control systems which are running building infrastructure like chillers, water pumps, and emergency power generation.

Not-So-Fun Fact: There's probably no central inventory of those systems, no backup and recovery plan, no preventative maintenance, and no budget to make any of that happen.

DHS ICS-CERT Training, available for free in Idaho Falls, ID
(I attended, and found it interesting - the red/blue exercise is some serious business.)

https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT#workshop
Hands-On Format - Technical Level

ICS Cybersecurity (301) - 5 days

This event will provide hands-on training in discovering who and what is on the network, identifying vulnerabilities, learning how those vulnerabilities may be exploited, and learning defensive and mitigation strategies for control system networks. The week includes a Red Team / Blue Team exercise that takes place within an actual control systems environment. The training provides the opportunity to network and collaborate with other colleagues involved in operating and protecting control system networks.

Note that this course is not a deep dive into training on specific tools, control system protocols, control system vulnerability details or exploits against control system devices.
This event consists of industrial control systems cybersecurity training and a Red Team / Blue Team exercise:

- Day 1 - Welcome, overview of the DHS Control Systems Security Program, a brief review of cybersecurity for Industrial Control Systems, a demonstration showing how a control system can be attacked from the internet, and hands-on classroom training on Network Discovery techniques and practices.

- Day 2 - Hands-On classroom training on Network Discovery, using Metasploit, and separating into Red and Blue Teams.

- Day 3 - Hands-On classroom training on Network Exploitation, Network Defense techniques and practices, and Red and Blue Team strategy meetings.

- Day 4 - 8-hour exercise where participants are either attacking (Red Team) or defending (Blue Team). The Blue Team is tasked with providing the cyber defense for a corporate environment, and with maintaining operations to a batch mixing plant, and an electrical distribution SCADA system.

- Day 5 - Red Team/Blue Team exercise lessons learned and round-table discussion.

- Prerequisites: Each attendee should have an understanding of ICS networks and IT network details. **Every student attending this course should bring a laptop computer (with a DVD drive).** The user must be able to boot the laptop to an operating system from the DVD. If using a DVD is not an option the user may run the operating system in a VM such as VMware Player, VMware Fusion or Oracle VirtualBox.

- This course is presented at a facility in Idaho Falls, Idaho, USA configured specifically for the aspects of the course. A Certificate of Completion will be provided at the conclusion of the course. Refer to the ICS-CERT calendar for a schedule of this training option.