Cyber-security in Industrial Control Systems

Chris Foreman, PhD CSE
Purdue University
jchrisf@purdue.edu

These slides are supported by a gift from Intel Corporation to promote cyber-security in industrial control systems. You are free to utilize and modify for the purposes of education of cyber-security in industrial control systems, no other use is granted and under no circumstances may these slides be used for profit. You should credit both Intel Corporation and myself in the development of these slides. The photos used in these slides are either created as part of this work or captioned with the source.
Overview of Modules

1. Discuss how Industrial Control Systems (ICS) are different the general computing systems.
2. Explore the cyber-security challenges that are unique to ICS.
3. Explore the cyber-threats to ICS.
4. Explore the existing approaches to mitigating risk of cyber-attack.
5. A simple laboratory setup for experiments is also presented.
6. Miscellaneous pictures.
1. How are ICS different?

• A brief history of ICS
• ICS architecture
• Real-time process control and the industrial environment
• Communications protocols
Why do we have ICS?

Before computer-based control systems, relays were used to automate equipment on assembly lines. They were manually assembled, thus they were costly, and any change in the program required labor-intensive rewiring.

Huge relay panel. Today this panel might only take a few lines of code to replicate.

Individual relay as an automatic logic switch

https://en.wikipedia.org/wiki/Relay
Programmable Logic Controllers (PLC)

In 1968, GM sought a replacement for these costly relay systems. The winning proposal came from Bedford Associates, who founded Modicon, which stood for MOdular DIgital CONtroller, to build the first PLC. This allowed cheap and rapid programming changes to be made in minutes instead of days.

A small Allen Bradley PLC with processor and I/O cards
Small to large systems

• A PLC is often used to control relatively small processes, such as one leg of an assembly line or other process with a few components. From a few up to a few hundred Input/Output (I/O) points each.

• Supervisory Control And Data Acquisition (SCADA) refers to multiple PLCs networked together for control of multiple small processes, often including small processes at remote sites.

• A Distributed Control System (DCS) is used for larger processes, such as a power generation process or other centralized plant-wide control, using Distributed Processing Units (DPU) on a dedicated network with each DPU handling thousands of points of I/O.
Industrial Control Systems (ICS)

PLC, DPU, SCADA, and DCS all fall into the category of ICS. The architecture of a PLC is theoretically similar to a DPU, so we will look at PLCs more closely as a model.

The state memory is where variables are stored. The program memory is where the control logic is stored. Inputs from field sensors or manual controls that direct process control.

Outputs to field actuators such as indicator lights, motors, and valves that operate on the process equipment.
Industrial Control Systems (ICS)

Other components that round out a complete ICS.

- HMI – Human Machine Interface
- ENG – Engineering workstation
- HIST – Process data archive

The PLC collects the process data, executes the control logic, and sends commands to field devices.

- The operator operates the process through the HMI workstation.
- The engineer maintains the ICS through and engineering workstation.
- A historian workstation collects process data in an archive for future analysis and troubleshooting.
Typical ICS configurations

For geographically distributed processes at remote sites, typical SCADA

Diagram:
- I/O
- PLC
- Process piece
- Switch
- Ethernet
- Firewall
- HIST
- HMI
- Main supervisory site
- Corporate WAN
- ISDN/POTS
- Serial
- Radio
- ENG
- Modem
- Radio
- Modem
- Modem
- PLC
- PLC
Typical ICS configurations

For large, centralized processes, typical of DCS
2. Cyber-security challenges unique to ICS

• The operating environment of ICS
  – The physical process and real-time control
  – User and organizational motivations and considerations
• Unique network configurations and protocols
The ICS operating environment

• The ICS and software control a physical process and thus, operate in a real-time environment.
  – Data can become useless (stale) in a fraction to a few seconds, resulting in lost process efficiency, damage, or shut down.
  – As a result, ICS reliability is crucial and must continue to operate even during a cyber-attack.
• ICS must function in environments that are electrically noisy, dirty, at temperature extremes, etc.
• Process inefficiencies and shut downs are often very expensive, with tens of thousands of dollars an hour or much more for large processes.
• In critical infrastructure, loss of the ICS can have significant, detrimental impacts on the health and functioning of society.
ICS users and cyber-security

• Historically, ICS were physically isolated or air-gapped from the outside world. Now systems are linked into the corporate WAN and Internet to allow process monitoring and maintenance for off-site groups.

• Control engineers, technicians, operators typically are not skilled in cyber-security. Conversely, IT professionals are not skilled in process control.
  – They have different, and sometimes conflicting, goals and management in the corporate structure.

• It is difficult to make a business case for cyber-security, though this is improving. The perception is no attacks mean no problems.
ICS cyber-security

• The focus is on keeping the process running, not cyber-security. Cyber-security can add a point of failure, disrupt the process, and make maintenance more difficult.

• In IT systems, the information is the primary focus. In ICS the information is coupled with the physical process, but it’s the physical process that is the primary focus.
  – The process data consists of temperatures, pressures, control commands, etc., and is rarely considered confidential.
  – However, the validity of the information is critical. Authentication is of high importance.

• ICS are built on proprietary hardware and software.
  – Incompatible or unknown reaction to cyber-security patches. ICS often operate with out of date software.
  – IT-based solutions, such as firewalls are not familiar with ICS communications protocols.
Network media used in ICS

• Modern systems are mostly Ethernet, 10M – 1G baud
  – While not real time or guaranteed access, this is fast enough to avoid latency issues. The commercial availability of Ethernet reduces the cost of new control systems.

• Serial link, 9600 – 57k baud
  – For point to point access
  – RS232 / RS485 low-bandwidth direct cable links
  – Modbus serial protocol, real time, guaranteed access
  – Still used for simple links to some instrumentation and legacy systems

• Proprietary, loop or daisy chain, 1 – 4M baud
  – Typically token ring
  – Time multiplexed, real time, guaranteed access
  – These configurations are being phased out, but many still remain
Network protocols used in ICS

• Ethernet TCP/IP
  – We already know this. It is used to gain the benefits of COTS components and fast enough to *emulate* real-time access.

• Modbus, Modbus TCP
  – Modbus is an early but common protocol used in serial communications developed by Modicon.
  – A master/slave network. The master node sends commands or requests data from a slave node and the slave responds. The slave node cannot initiate communications.
  – Access is done by address only. No authentication, encryption, or other security measures are incorporated in the standard.
  – TCP refers to an updated version of Modbus over Ethernet, still without security. Modbus communications are encapsulated in Ethernet packets to allow use of high speed and commercially available Ethernet solutions.
Network protocols – Modbus

Modbus TCP

Modbus

Transaction identifier | Protocol identifier | Length field | Modbus frame
---|---|---|---
Address | Function code | Data | Checksum

Master
Slave
Slave
Slave
Slave

Serial daisy chain or Ethernet configuration
Other network protocols used in ICS

  – Other protocols such as Siemens PROFIBUS, Allen Bradley Data Highway®, Westinghouse WDPF®, use some variation of a deterministic network approach by sharing and passing a virtual token to determine which node has right of way on the network.
  – While similar to a master/slave configuration, each node passes a virtual token around the network. Whoever holds the token is allowed to initiate communications. When that node’s time to hold the token has expired, it passes to the next node on a net list. This is designed to give every node a chance to communicate.
  – As we said earlier, these are being replaced with Ethernet-based protocols, such as Siemens SIMATIC NET, Allen Bradley Ethernet/IP, to allow COTS Ethernet solutions. The idea being that Ethernet is fast enough to allow every node to communicate whenever needed. Still, there is a significant penetration of these network protocols and they are still deployed in some instances.
3. ICS cyber-threats

• Previous attacks indirect and direct
• Stuxnet case study
• Discussion of critical infrastructure attacks

Attacks are now more prevalent that Windows and other COTS systems are being used in ICS. Attacks may deny access or service, get sensitive data, or even put false, malicious commands and code into the ICS.
Davis-Besse Nuclear Power Plant

• An indirect attack meant for Windows that also compromised an ICS.
• Location: Ohio, USA, January 2003
• Target: Safety Monitoring System
• Culprit: Slammer worm
• Method:
  – Entered the business network through unprotected T1 line “backdoor” then spread to plant control network disabling SPDS (Safety Parameter Display System).
• www.securityfocus.com/news/6767
CSX Railroad

- Another indirect attack meant for Windows that also compromised an ICS.
- Location: USA, August 2003
- Target: Telecommunication network supporting the signal and dispatch system
- Culprit: Worm infection
- Method:
  - Worm entered the network and infected signal and dispatch systems, halting passenger and cargo train traffic in 23 states.
Olympic Pipe Line Company

• An example of why control engineers do not want to install security patches on ICS systems. Some patches may not be compatible with the custom/proprietary hardware and software used in ICS.
• Location: Bellingham, WA, USA, June 1999
• Target: Accidental
• Contributing factor: ICS failure, software update on live ICS caused it to become unresponsive.
  – Programming error?
  – Patch application failure?
• Incident:
  – Gasoline pipeline ruptured and ignited causing 3 deaths, 8 injuries, $45MM in damages, and spilling ~237k gallons into the environment.
Maroochy Shire Council Water Breach

• A direct attack by taking advantage of a weak corporate security policy. At this time, ICS cyber-security was not being taken seriously.
• Location: Queensland, Australia, Feb-Apr 2000
• Target: ICS with radio controlled sewage equipment
• Culprit: Disgruntled ex-contractor
• Method:
  – Issued a series of control commands to disable alarms at pumping stations and spill 800k liters of raw sewage at various points.
  – Driving around control area with access to wireless ICS network using old passwords.
  – One of the first widely known intentional ICS attacks.
Case study: The Stuxnet worm

- A direct attack intended for ICS. This was a major turning point in ICS attacks where critical infrastructure became an interesting target for terrorists.
- Very sophisticated and specifically targeted. The design suggests significant resources were allocated at the national level.
- Benign on mainstream computers. Does not come alive unless utilized on ICS network with certain Siemens PLCs.
- Performs specific actions to fool operator into false impression of process. Process data and process logic representations affected.
- You can patch PCs but not most PLCs. The ICS remains vulnerable after the attack is known.

http://www.tofinosecurity.com/stuxnet-central
The Stuxnet worm – Path to infection
The Stuxnet worm – Path to infection
How
Stuxnet Invades the PLC

STUXNET

Start Cycle Timer
Read Inputs to PII
Overwrite PII
Execute Logic
Overwrite PIO
Send PIO to Outputs

STUXNET

CPU Logic

Input Module
Sensors

Output Module
Final Control
Pump
Valve
What Stuxnet Does to Its Victim

1. Locates and infects STEP 7 programming stations
2. Replaces STEP 7 DLL routines on stations (so person viewing logic would not see any changes that Stuxnet later makes to the PLC)
3. Looks for specific models of Siemens PLCs (6ES7-315-2 and 6ES7-417).
4. Identifies a victim PLC by looking for special configurations and strings
5. Injects one of three STEP 7 code “payloads” into PLC to change process operations
What Stuxnet Does to a PLC

- PLC’s PROFIBUS driver is replaced
- Main PLC program block (OB1) and the primary watchdog block (OB35) are significantly modified
- Between 17 and 32 additional function blocks and data blocks are injected into the PLC
- Payloads ‘A’ and ‘B’ change the frequencies of Variable Frequency Drives and thus motor speed
- Payload “C” designed to control a master system, possibly a safety system
Stuxnet – Lessons learned

• Stuxnet demonstrated how completely a virus could gain control of a PLC.
• No readily applicable patches for PLC logic.
• Attacks are becoming focused on specific locations by professional level attackers.
  – Attackers are no longer going after the most common systems.
  – Serves as a template for future attacks.
  – Again, ICS are used for critical infrastructure which causes much greater harm to society than financial infrastructure attacks.
  – Attackers are no longer motivated solely by money or fame. Most are sponsored by hostile nations and terrorists as acts of war.
4. Approaches to mitigating risks

- New methods of authentication and protocols
- New policies, hardware, software, approaches
- New training and systems validation

ICS with secure devices such as Intrusion Detection Systems (IDS), firewalls, etc. that reside on ICS components or on the network as either a point of presence or physical barrier to cross.
Authentication in ICS
Problems with existing protocols

• Authentication in protocols, remember Modbus?

<table>
<thead>
<tr>
<th>Updated?</th>
<th>Address</th>
<th>Function</th>
<th>Data</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Master
Step 1b
Slave
Step 1a
Step 2
Challenge/Response, or possibly one-way cryptographic hash functions?

• For example, we could try to update Modbus to make it more secure. However, this would no longer be compatible with the Modbus standard. Existing systems would no longer function.

• Remember that ICS are expected to have lifetimes on the order of twenty years. New technologies are often not compatible with such vintage systems, and interoperability across generations is important.
New network protocols for ICS

  - DNP3 is a comprehensive effort to achieve open, standards-based interoperability between field computers: PLCs, RTUs, IEDs (Intelligent Electronic Devices) and control room computers: HMI, ENG, Servers.
  - Designed to be more robust, efficient, and self compatible than older protocols such as Modbus, at the cost of somewhat higher complexity. Includes security enhancements.
The middle row in Figure 2 shows a hierarchical type system where the device in the middle is an outstation to the master at the left and is a master with respect to the outstation on the right. The middle device is often termed a sub-master.

Both lines at the bottom of Figure 2 show data concentrator applications and protocol converters. A device may gather data from multiple outstations on the right side of the figure and store this data in its database where it is retrievable by a master station on the left side of the figure. This design is often seen in substations where the data concentrator collects information from local intelligent devices for transmission to the master station.

TCP/IP

Many vendors offer products that operate using TCP/IP to transport DNP3 messages in lieu of the media discussed above. Link layer frames, which we have not talked about yet, are embedded into TCP/IP packets. This approach has enabled DNP3 to take advantage of Internet technology and permitted economical data collection and control between widely separated devices.

More On Layering

Communication circuits between the devices are often imperfect. They are susceptible to noise and signal distortion. DNP3 software is layered to provide reliable data transmission and to effect an organized approach to the transmission of data and commands. Figure 3 shows the layering that was not shown in Figure 1.

Link Layer Responsibility

The link layer has the responsibility of making the physical link reliable. It does this by providing error detection and duplicate frame detection. The link layer sends and receives packets, which in DNP3 terminology, are called frames. Sometimes transmission of more than one frame is necessary to transport all of the information from one device to another.
Authentication in DNP3

1. Initialization: When a master station initiates a DNP3 session with an outstation, Secure DNP3 will authenticate both the master station and outstation. A unique session key is generated and exchanged using pre-shared keys during this initialization.

2. Periodic: The master station and outstation will periodically re-verify to prevent hijacking and other attacks. A new session key is generated and exchanged during this periodic update.

3. Critical Function Requests: Critical requests as defined by the protocol and application.

4. Implementation Specific: Vendors and end users can also implement custom authentication requirements for other functions.
Network protocols – DNP3

- DNP3 now includes secure authentication, key management, cryptography enhancements

**Challenge/response**

Master Station → Outstation
- Read
- Standard Response
- Write
- Authentication Challenge
- Authentication Response

Outstation → Master Station
- Process Request
- Authenticate
- Valid Authentication Response?
- Standard Response

**Aggressive mode**

Outstation → Master Station
- Write & Authentication Response
- Standard Response
- Process Request

Master Station → Outstation
- Valid Authentication Response?
- Process Request
New Network Protocol – OPC

• OPC – *originally* OLE for Process Control using Microsoft’s OLE COM/DCOM.
  – Typically required a completely open DCOM configuration, allowing all. Also problems with buffer overflows, etc. Windows only.
  – The new specification, Unified Architecture (OPC UA), is based on Web Services for cross platform use and is enhanced for security and stability.
  – Client/server model implemented over Ethernet.

Network Protocols

OPC UA

Widely used in ICS with drivers for almost all vendors and components today. Intended as an open standard.
Network Protocols – OPC UA

OPC now includes cyber-security and authentication measures.
The OPC UA Security Model – 3 – Version 1.00

For Administrators

Application Instance – An OPC UA Application installed on a single machine is called an Application Instance. Each instance must have its own Certificate which it uses to identify itself when connecting to other applications. Each Application Instance has a globally unique URI which identifies it.

Administrator – An Application Instance must have an Administrator which manages the security settings for the Application.

Operator – An Operator is a person who uses the Application Instance. More than one Operator may exist for any given application. An Operator may have User Credentials which are used to determine access rights and to track activities.

Certificate Authority (CA) – A Certificate Authority (CA) is an administrator or organization which is responsible for creating Certificates. The Certificate Authority must verify that information placed in the Certificate is correct and add a digital signature to the Certificate that is used to verify that the information has not been changed. Each CA must have its own Certificate which is used to create the digital signatures.

Certificate – A Certificate is an electronic ID that can be held by an application. The ID includes information that identifies the holder, the issuer and a unique key that is used to create and verify digital signatures. The syntax of these certificates conforms to the X509 specification, as a result, these certificates are also called “X509 Certificates”. Certificates also have a Private Key associated with them.

User Credential – A User Credential is a generic term for an electronic ID which identifies an Operator. It may be passed to a Server after the Application Certificate is used to create a secure channel. It is used to determine access rights and to track activities.

Private Key – A Private Key is a secret number known only to the holder of a Certificate. This secret allows the holder to create digital signatures and decrypt data. If this secret is revealed to unauthorized parties then the associated Certificate can no longer be trusted or used.

Certificate Store – A Certificate Store is a place where Certificates and Private Keys can be stored on a file system. All Windows systems provide a registry based store called the Windows Certificate Store. All systems support a directory containing the Certificates stored in a file which is also called an OpenSSL Certificate Store.

Figure 1 - Security Term and Interactions
Policies developed for ICS cyber-security

• Government entities have created regulations and guidelines for implementing ICS security.
  – Critical Infrastructure Protection (CIP) Reliability Standards by the North American Electric Reliability Corporation under FERC and DOE for the Power industry
  – National Institute of Standards and Technology (NIST) SP 800-82 Guide to SCADA and Industrial Control Systems Security

• Industry has also created several guidelines for implementing ICS security.
  – Report 12 by the American Gas Association
  – Water Infrastructure Security Enhancements (WISE) by the American Water Works Association et al
  – American Petroleum Institute API 1164 SCADA Security document
Critical Infrastructure Protection Standards (CIP)

http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

The North American Electric Reliability Corporation (NERC) was tasked by the Federal Energy Regulatory Commission (FERC) to develop these for the power sector.

- CIP-001 Sabotage Reporting
- CIP-002 Critical Cyber Asset Identification
- CIP-003 Security Management Controls
- CIP-004 Personnel & Training
- CIP-005 Electronic Security Perimeters
- CIP-006 Physical Security of Critical Cyber Assets
- CIP-007 Systems Security Management
- CIP-008 Incident Reporting and Response Planning
- CIP-009 Recovery Plans for Critical Cyber Assets
Industrial Defender,
http://id.lockheedmartin.com/solutions/cybersecurity

• Industrial Defender provides an Automation Systems Manager™ software solution for ICS cyber-security. Configurations and capabilities are shown on the next slides.

• Software management approaches such as these provide intelligent monitoring and simplified management while being specifically aware of the unique hardware and software components utilized in ICS.

• Adoption of these approaches have been slow at first, but are becoming more prevalent as ICS cyber-attacks increase.

• See this and other articles at,
## Automation System Manager Software Capabilities

### Industrial Defender

- Event logging, correlation, and archiving
- Single unified view across disparate endpoint base
- Customizable User Interface Dashboards
- Scalable Architecture
- File Integrity
- Network traffic monitoring
- Critical process & service monitoring
- Report subscriptions
- User account change identification
- Device configuration file archiving
- Understand network & system health and performance
- Maintain central configuration policy
- Collect & report on settings, accounts, configurations
- Analyze changes across asset base & environment
- Manage hardened electronic security perimeter
- Enforce trusted change policies
- Configuration change management
- Enforce host level application policies
- Prevent rogue applications/malware
- Block unauthorized applications
- Application whitelisting
Industrial Defender’s Risk Mitigation Technology SEM
Tofino Security’s Xenon™

• Xenon is an ICS Security Appliance (SA) designed to be plug-and-play providing ICS-aware firewall and monitoring.
• Serves as a bump-in-the-wire secure point on Ethernet ICS networks.
• Uses Loadable Security Modules (LSM) to provide dynamic configuration of security.
  – Including: Firewall, Event logger, NetConnect remote configuration, Modbus TCP, OPC, and Ethernet/IP protocols.
• Includes the Tofino Configurator
  – Device and event monitoring and reporting
  – Configuration and management of multiple devices
  – Passive scanning for dynamic asset discovery and configuration
Tofino Xenon™ SA

This is included in the laboratory setup in section 5.
National SCADA test bed (NSTB)

- Idaho National Laboratory (INL), Sandia National Laboratory (SNL), and others participate to provide a national resource for ICS cyber-security and resiliency testing.
- Industry partners may validate their ICS hardware and software solutions prior to commercial deployment.
- Research organizations may conduct experiments and training with the test bed.
NSTB INL – short course topics

- SCADA Network Communications Overview
- Common Vulnerabilities of Control Systems
- Inadequate Policies and Procedures
- Poorly Designed Control System Networks
- Misconfigured or Unpatched Operating Systems and Imbedded Devices
- Inappropriate use of Wireless Communication
- Inadequate Authentication of Control System Communications
- Inadequate Identification and Control of Access to Control System
- Lack of Detection and Logging of Intrusion
- Dual use of Control System Networks
- Lack of Security checking of Control System Software/Applications
- Lack of Change Management/Change Control Procedures and Agreements
- Potential Mitigation Strategies based on multiple levels of implementation
- Cyber Security Awareness Demonstration Video
NSTB INL multi-day course topics

- General Security Observations and Pitfalls
- Control System Network Communications Overview
- Potential Control System Network Entry Points AND Defenses
- Control System Network Scanning and Vulnerability Identification
- Network Monitoring and Simple Intrusion Detection
- Dissecting Control System Protocols
- Common Programming Pitfalls
- Modern Hardware and OS Mitigation Strategies
- Incident Response Essentials for the Control System Community
- Red team / blue team competition
In Summary: Contrasts with IT systems

• In IT systems, the information is the primary focus. In ICS, the information is coupled with the external industrial process, but this process is the primary focus.
  – Real-time data for the control of physical process equipment. Physical safety concerns as well.

• Proprietary hardware and software
  – Incompatible or unknown reaction to cyber-security patches. Often running out of date.
  – Unfamiliar protocols with respect to COTS security systems and firewalls.

• The need to fail open - system must remain available during cyber attacks.
In Summary: Contrasts with IT systems

• Very few users
  – Typically a single operator at a time with all operators sharing a common account. Always on 24/7.
  – Technicians and engineers access only during troubleshooting and configuration.
  – Corporate users access the database only, read only.

• Constant small data streams
  – Large files almost never on network, instead there are continuous small data transfers between all network nodes. Updates every second with a physical device relying on each update in order.

• Authentication and reliability are critical. Secrecy is less important.
In Summary: Contrasts with IT systems

• Cyber-security is even more important in ICS as the process impacts the physical world exposing personnel and communities to severe physical harm during attacks.

• We depend on ICS to run much of our critical infrastructure, such as electricity, water, telecommunications, etc. See...

• Cyber-security has been slow to achieve in ICS, but solutions are being developed.

• The groups responsible for IT and ICS cyber-security come from different backgrounds and have different goals, but they need to work together.
Problems with cyber-security solutions

• Several products exist for IT infrastructures that can be applied to ICS, but very few ICS-specific.
• Hardware/software limitations, ICS do not readily allow complex algorithms to be implemented.
  – Legacy systems with limited processing power and small memory footprints, obscure operating systems
  – Often requires an external server, moving security off the control devices
• Communications protocols do not include security.
• Training – control engineers do not know cyber security and IT security professionals do not know process control.
5. A simple laboratory setup

This is a block diagram of a two-PLC, Ethernet-based SCADA system. Included is a Tofino security device to assist in network analysis. Such a system allows most attacks and vulnerabilities to be analyzed and represents a very common implementation.
Laboratory parts list

• PLCs – The use of two PLCs allows communications between PLCs to be explored. One PLC can simulate a process and the second PLC can control that process through hardwire I/O. Allen Bradley ControlLogix® and MicroLogix®.

• PCs – The Windows PCs can serve as the HMI, Engineering workstation, historical data server, etc. These can be explored for vulnerabilities as well.

• Tofino Xenon® – This is a firewall and IDS device that is aware of ICS protocols and hardware. It allows Snort-type rules for network anomaly detection and also allows more advanced network monitoring.

• Ethernet – This is an Ethernet switch as typical in an IT network. A managed switch allows more monitoring options and functionality.

• Wireless access point – This allows students and researchers a wireless link into the system to launch and monitor attacks. A whole class can be given access to explore (hack) the system while the instructor monitors their progress. An Internet connection is not necessary for this system.
A simple laboratory setup for experiments. Students access a live ICS through the WiFi access point and attempt to hack/crack the system or play *capture-the-flag* games.

Hardwired I/O between PLCs for process simulation and control, I/O wiring not shown.
6. Modern HMI and operator
Typical HMI screen
Typical HMI screen

http://www.exponent.com/electric_power_generator_control_system/
Manual panelboard controls

The HMI replaces these expensive manual controls and indicators with graphical user interfaces that can be easily modified and maintained.
Distributed Control System (DCS)

One of many I/O racks

Primary and backup DPUs
ABB substation automation racks
A DCS has to live in a hostile environment and control a large and complex process.
SCADA often has to spread out over larger distances and across many network types.
Attack Demonstration

1. Exploit client-side application vulnerability to bypass corporate firewall
2. Exploit common firewall opening to access network and defeat “state”
3. Exploit unpatched server to capture credentials and hop across networks
4. Exploit vulnerable SCADA application software for complete control
5. Use captured credentials to login to SCADA HMI and upload malicious code
6. Exploit vulnerable SCADA protocol and field device to execute unauthorized commands