Cyber-security in Industrial Control Systems

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

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?

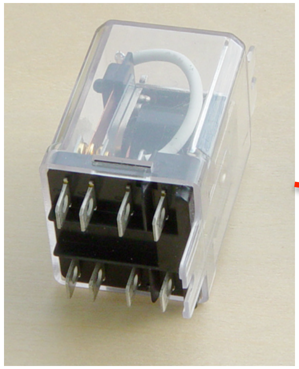
- A brief history of ICS
- ICS architecture
- Real-time process control and the industrial environment
- Communications protocols

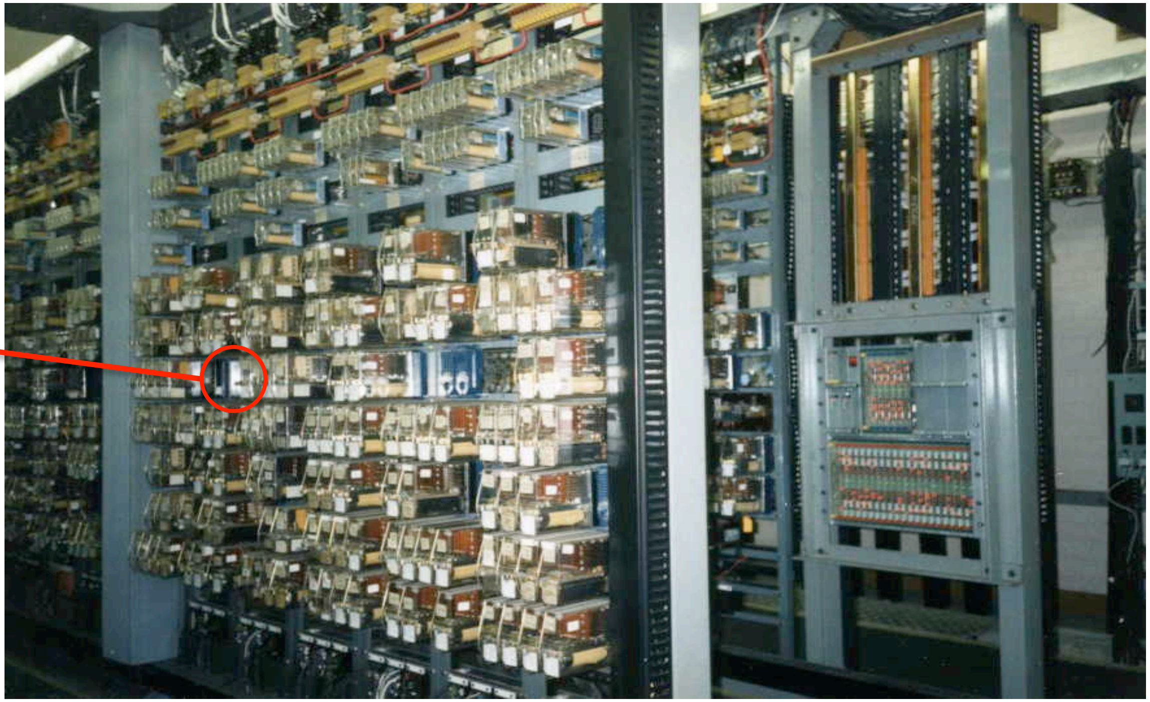
Why do we have ICS?

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

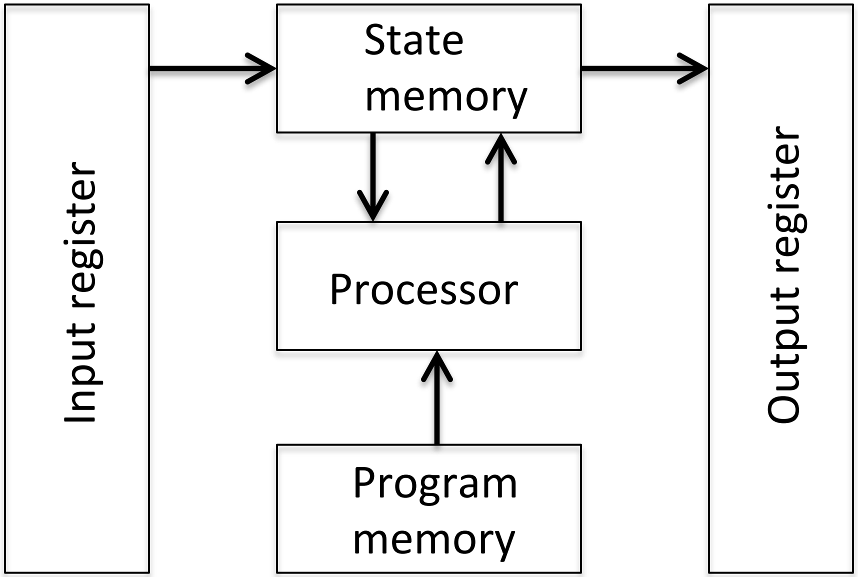
- A PLC is often used to control relatively small processes, such as one leg of an assembly line or other process with a few components. From a few up to a few hundred Input/Output (I/O) points each.
- Supervisory Control And Data Acquisition (SCADA) refers to multiple PLCs networked together for control 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.

Inputs from field sensors or manual controls that direct process control.



Input register

State memory

Processor

Program memory

Output register

Outputs to field actuators such as indicator lights, motors, and valves that operate on the process equipment.

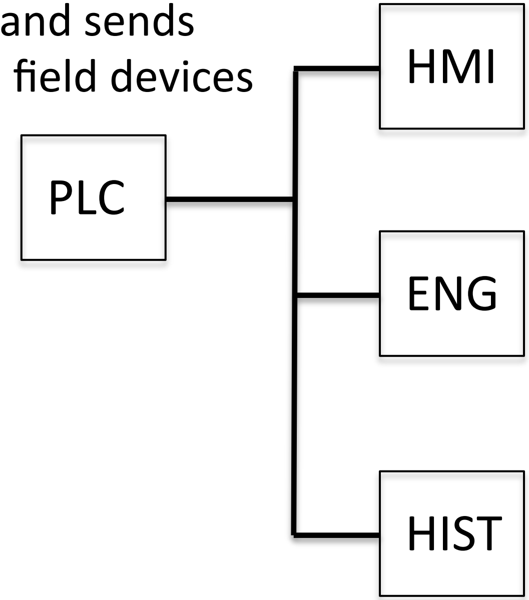
The program memory is where the control logic is stored.

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



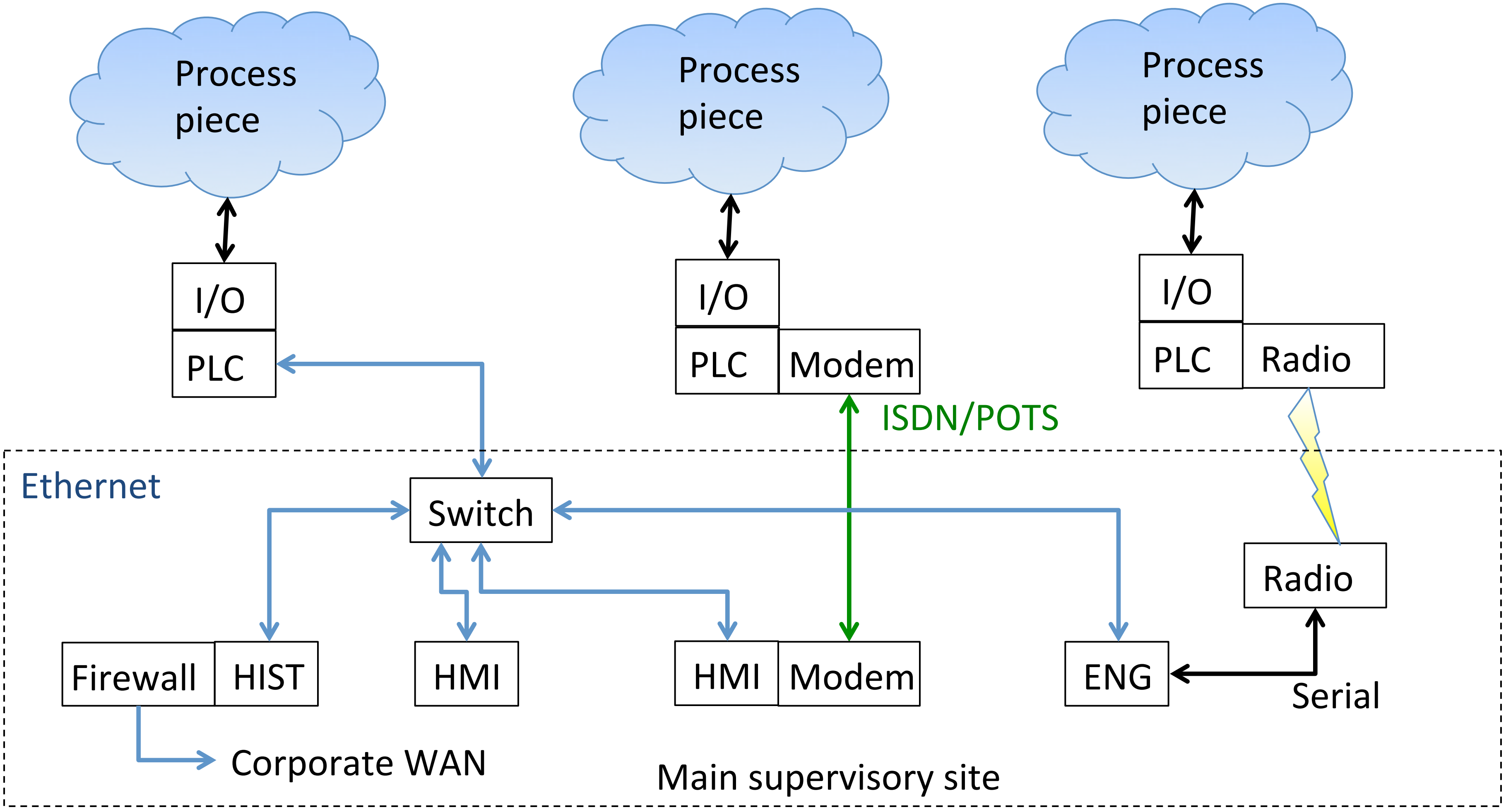
The operator operates the process through the HMI workstation.

The engineer maintains the ICS through and engineering workstation.

A historian workstation collects process data in an archive for future analysis and troubleshooting.

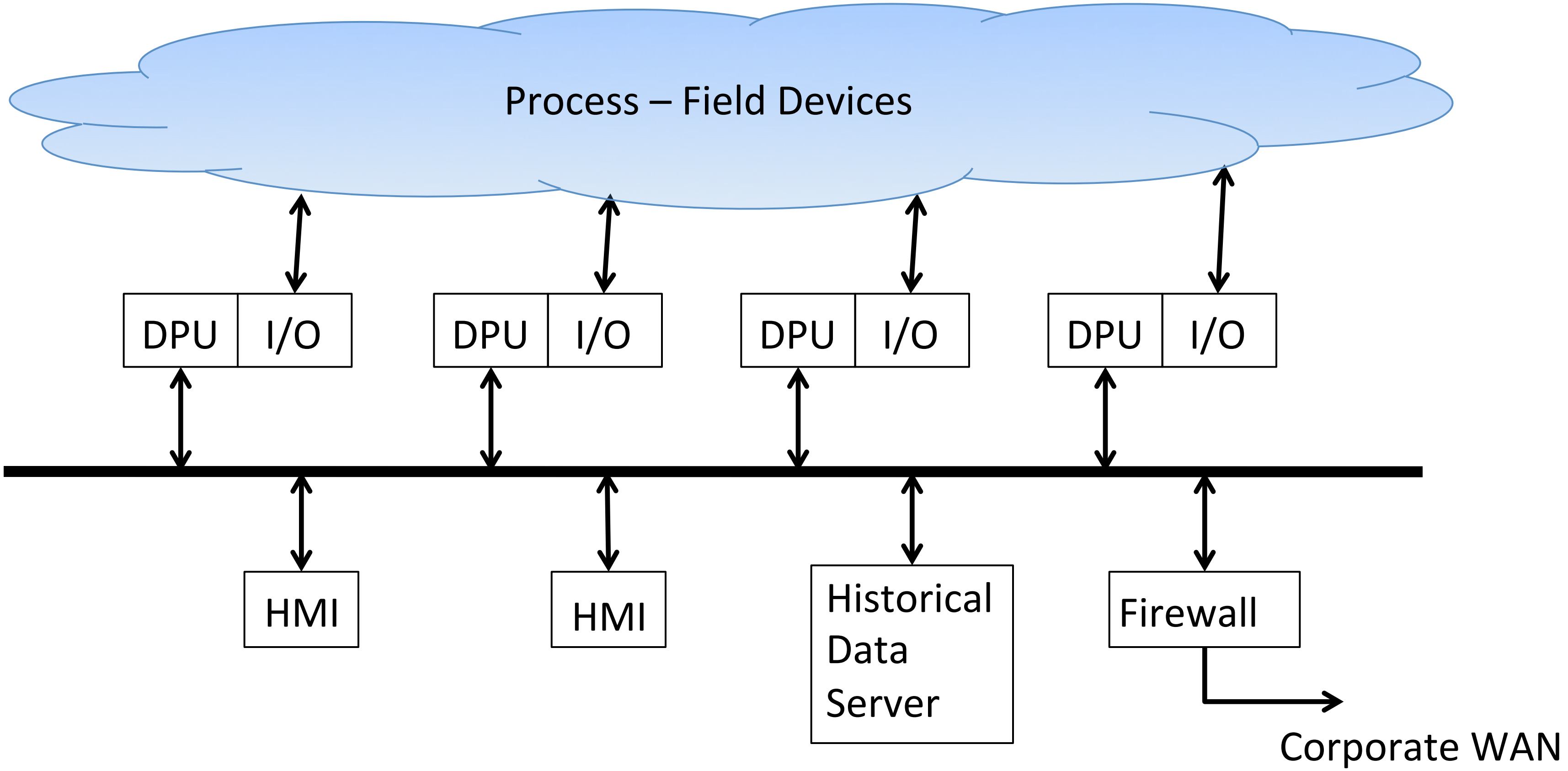
Typical ICS configurations

For geographically distributed processes at remote sites, typical SCADA



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.

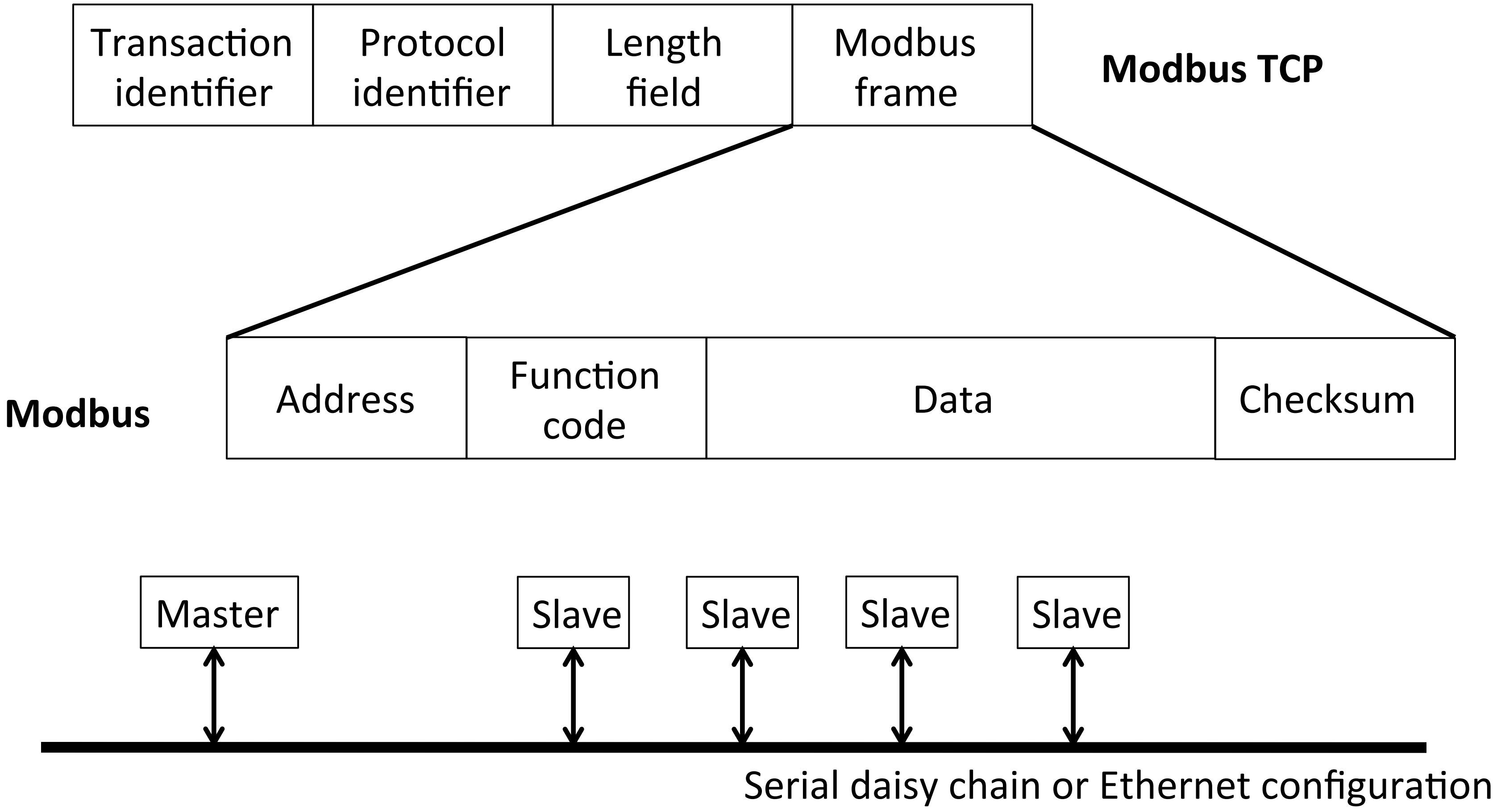
Network media used in ICS

- 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



Transaction identifier	Protocol identifier	Length field	Modbus frame

Modbus TCP

Address	Function code	Data	Checksum

Modbus

Serial daisy chain or Ethernet configuration

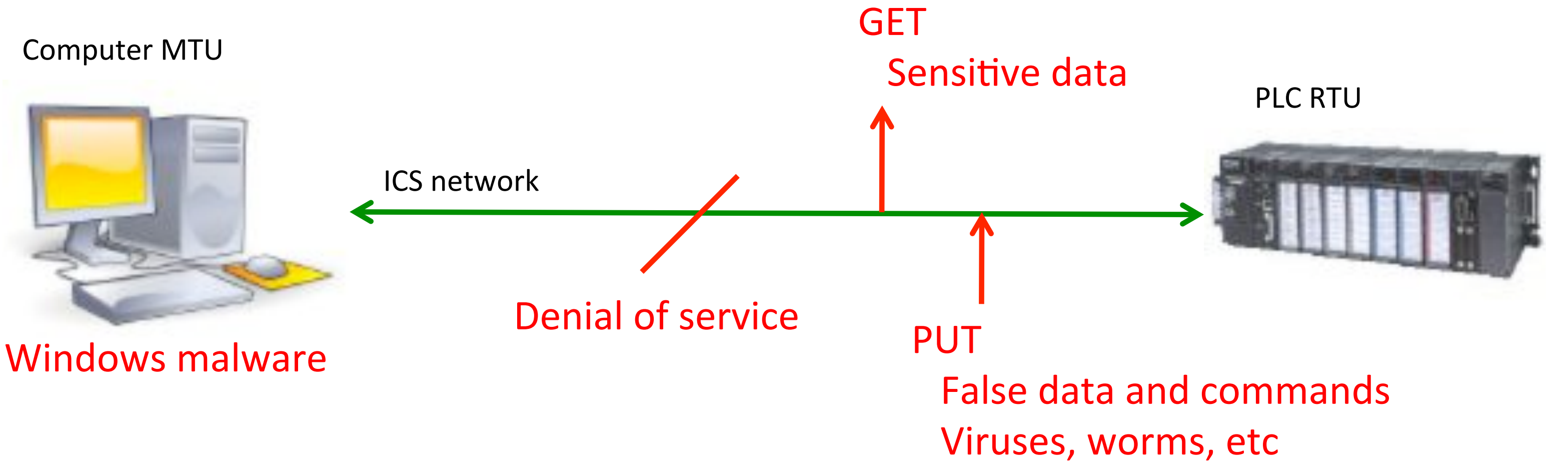
Other network protocols used in ICS

- Token passing networks, https://en.wikipedia.org/wiki/Token_ring
  - 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

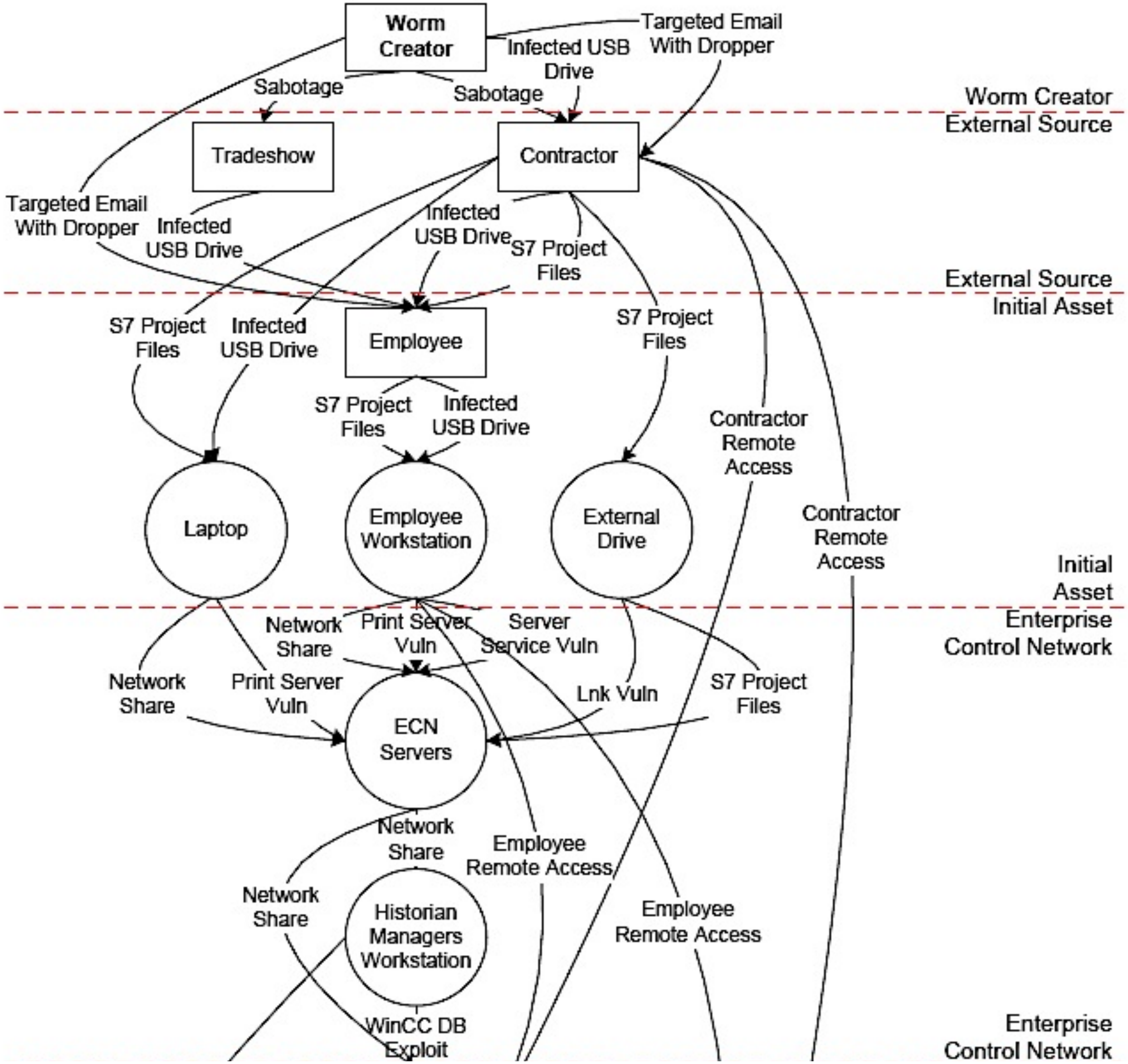
- A direct attack by taking advantage of a weak corporate security policy. At this time, ICS cyber-security was not being taken seriously.
- Location: Queensland, Australia, Feb-Apr 2000
- Target: ICS with radio controlled sewage equipment
- Culprit: Disgruntled ex-contractor
- Method:
  - Issued a series 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

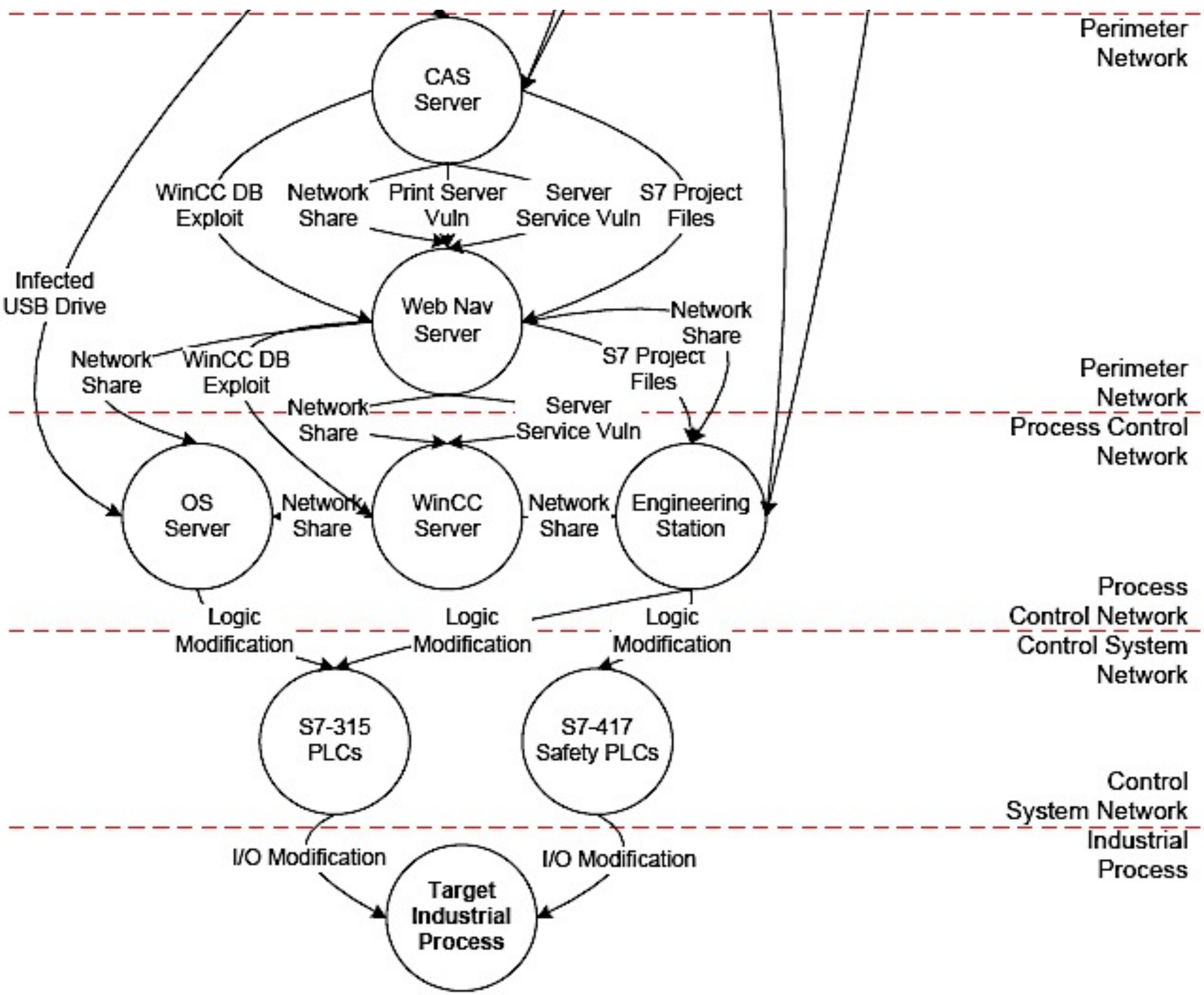
The Stuxnet worm – Path to infection



White paper

Tofino Security | Abterra Technologies | ScadaHacker.com

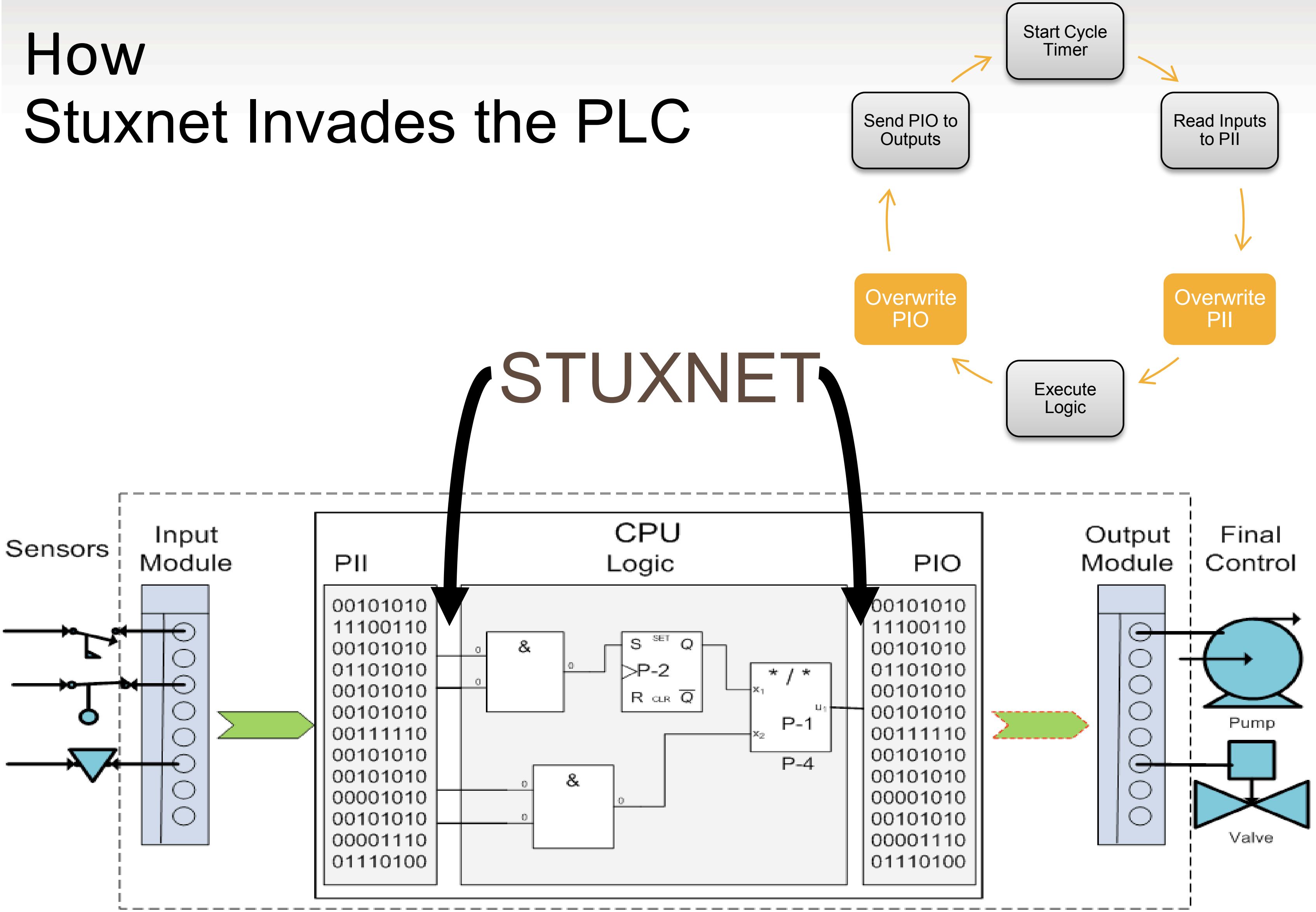
The Stuxnet worm – Path to infection



White paper

Tofino Security | Abterra Technologies | ScadaHacker.com

How Stuxnet Invades the PLC



PII

00101010
11100110
00101010
01101010
00101010
00101010
00111110
00101010
00101010
00001010
00101010
00001110
01110100

PIO

00101010
11100110
00101010
01101010
00101010
00101010
00111110
00101010
00101010
00001010
00101010
00001110
01110100

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. Indentifies 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
- Between17 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

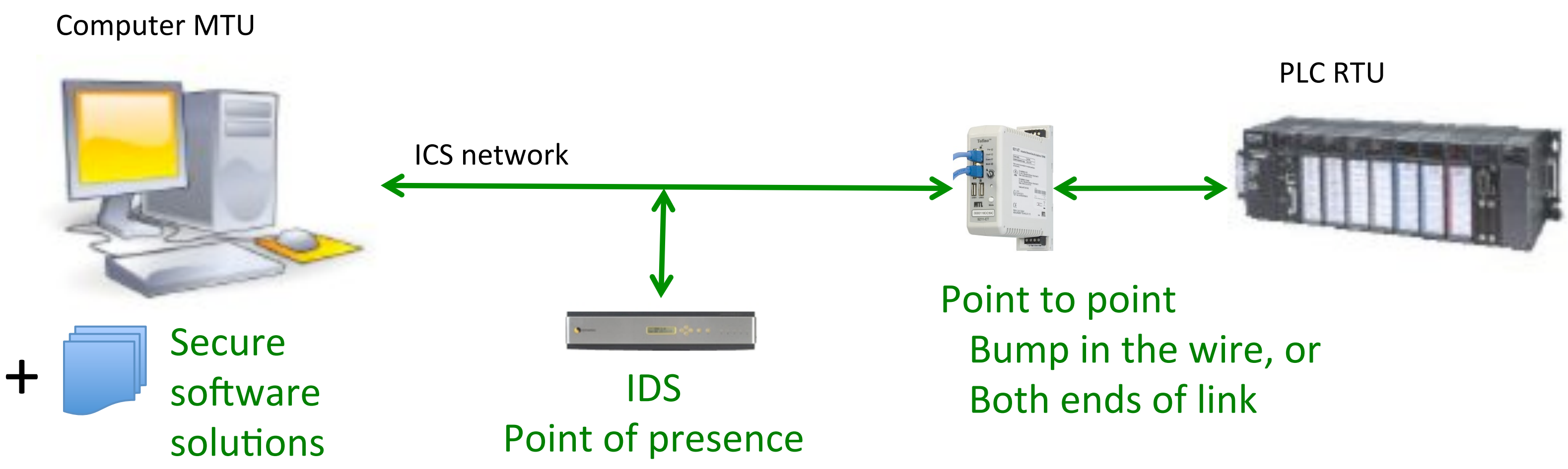
Stuxnet – Lessons learned

- 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.



Computer MTU

ICS network

PLC RTU

+ Secure software solutions

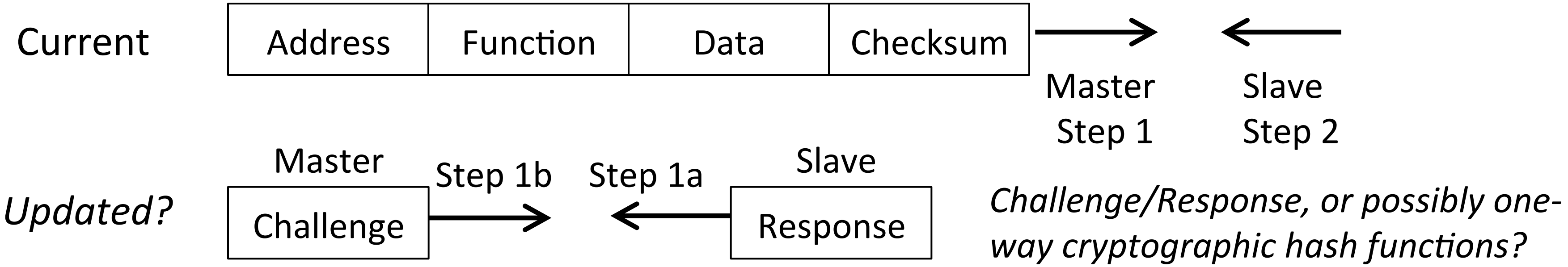
IDS
Point of presence

Point to point
Bump in the wire, or
Both ends of link

Authentication in ICS

Problems with existing protocols

- Authentication in protocols, remember Modbus?



Current

Address	Function	Data	Checksum

→ Master Step 1

← Slave Step 2

Updated?

Master: Challenge → Step 1b

Step 1a ← Slave: Response

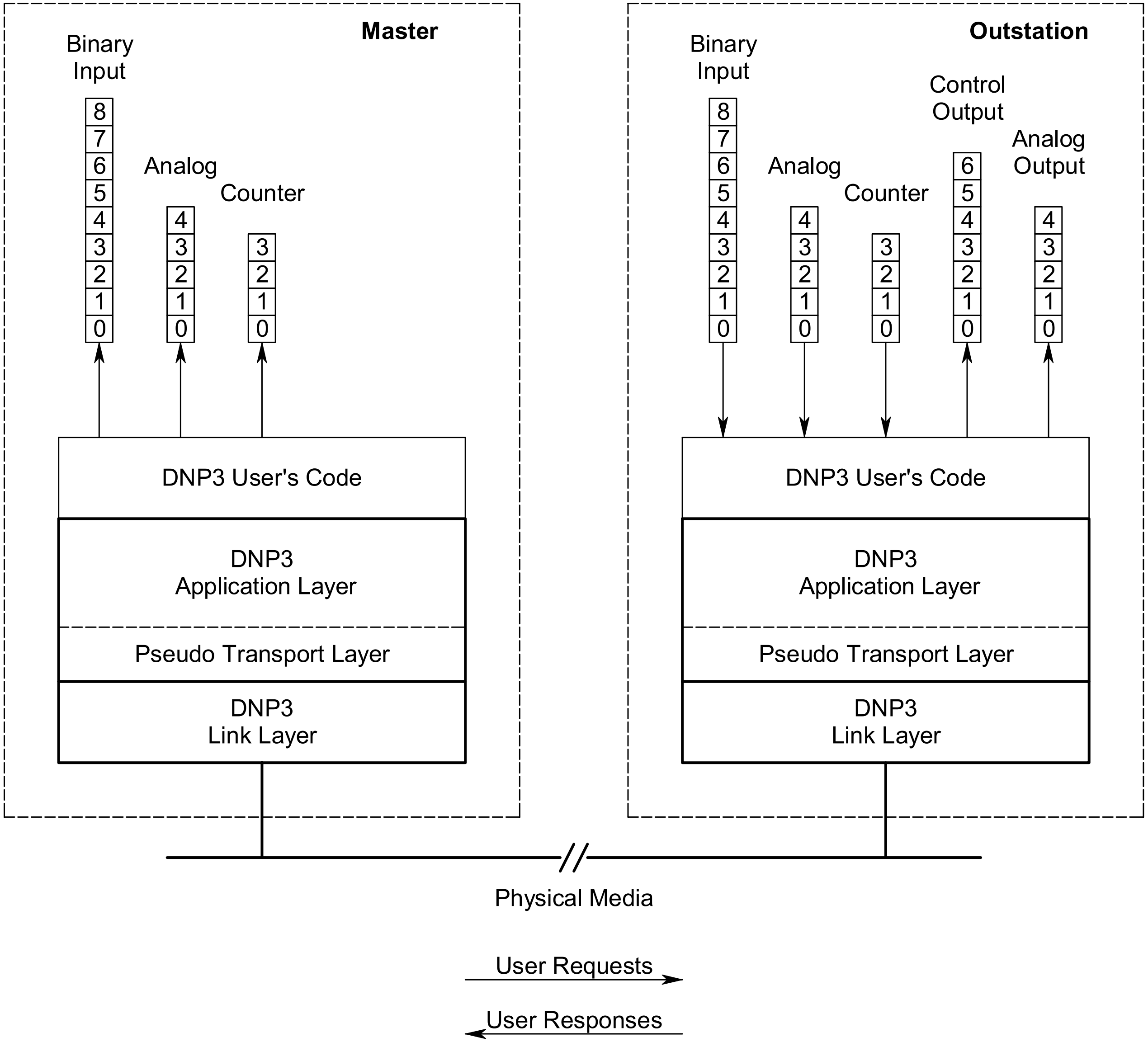
Challenge/Response, or possibly one-way cryptographic hash functions?

- 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, http://www.dnp.org/
  - 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.

Network protocols – DNP3



Authentication in DNP3

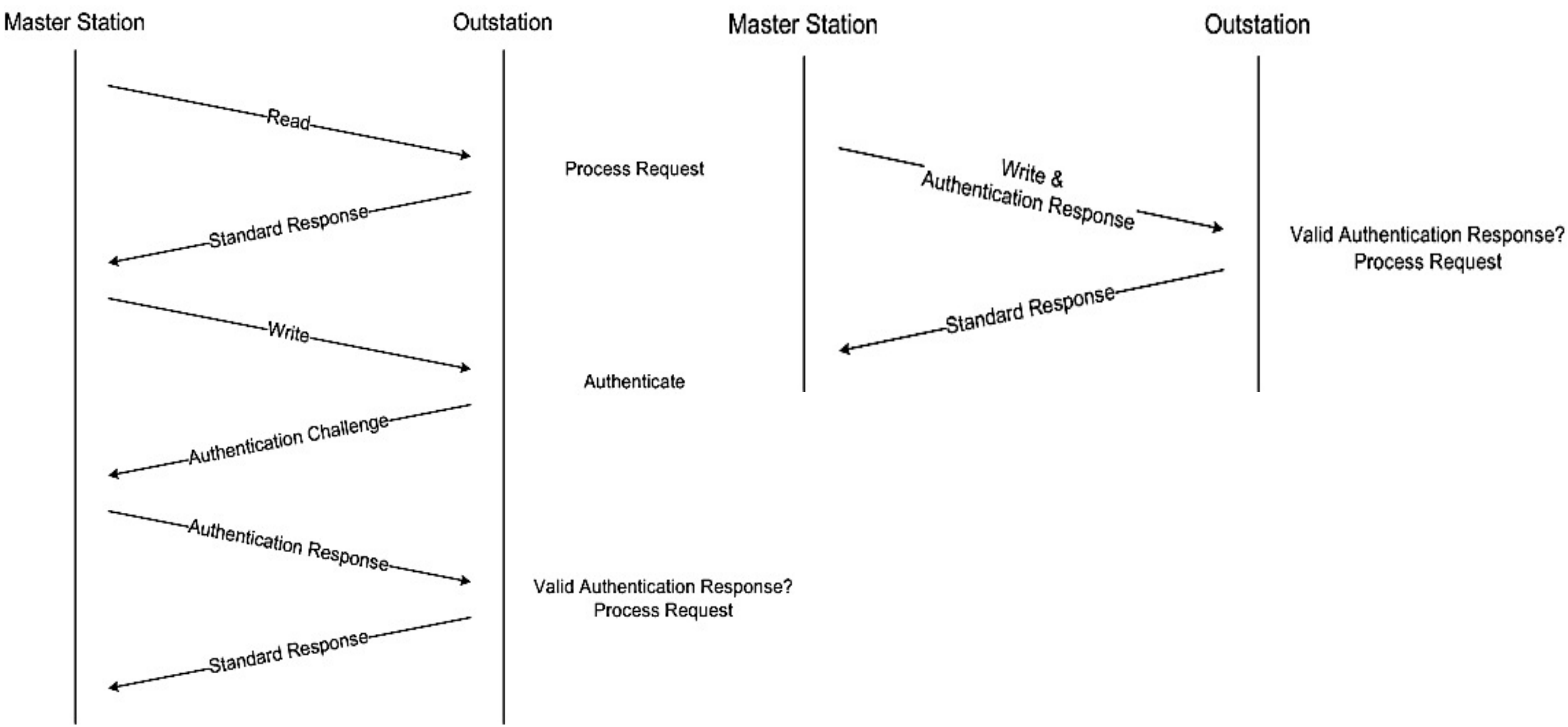
1. Initialization: When a master station initiates a DNP3 session with an outstation, Secure DNP3 will authenticate both the master station and outstation. A unique session key is generated and exchanged using pre-shared keys during this initialization.
2. Periodic: The master station and outstation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

Aggressive mode



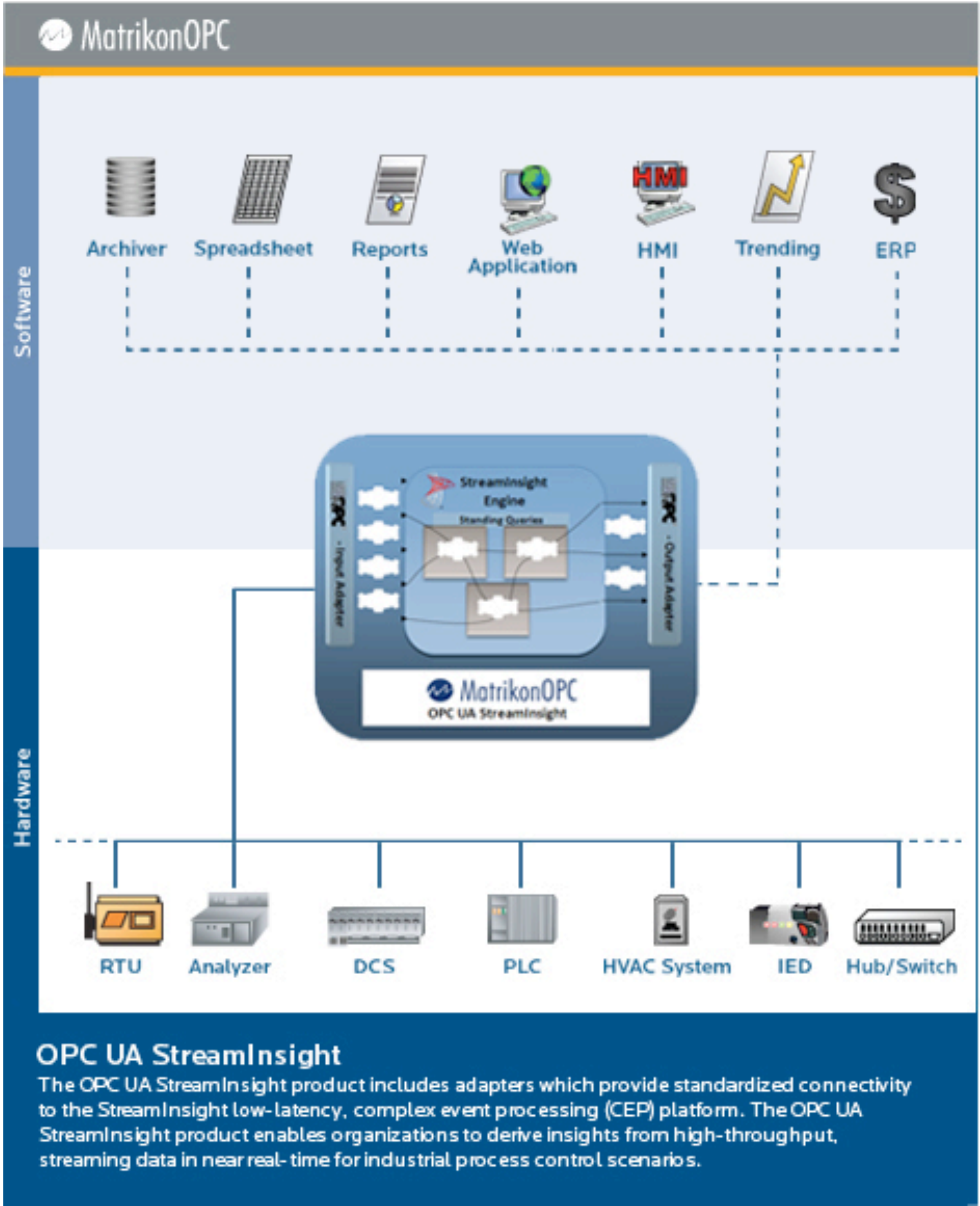
New Network Protocol – OPC

- 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.

See http://opcfoundation.org/ and
http://www.digitalbond.com/scadapedia/protocols/opc-ua/

Network Protocols
OPC UA

Widely used in ICS with drivers for almost all vendors and components today. Intended as an open standard.

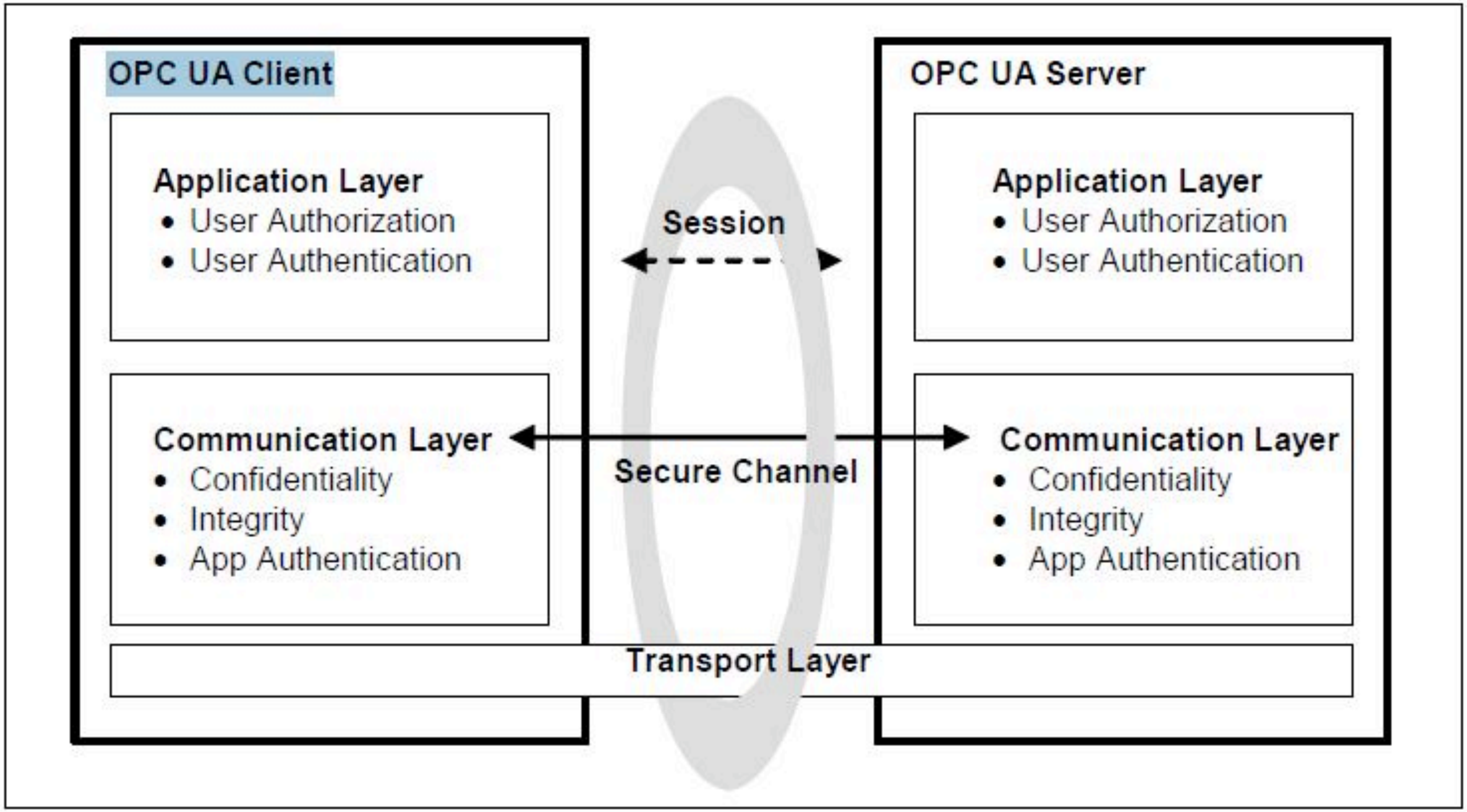


OPC UA StreamInsight

The OPC UA StreamInsight product includes adapters which provide standardized connectivity to the StreamInsight low-latency, complex event processing (CEP) platform. The OPC UA StreamInsight product enables organizations to derive insights from high-throughput, streaming data in near real-time for industrial process control scenarios.

Network Protocols – OPC UA

OPC now includes cyber-security and authentication measures.



Authentication in OPC UA

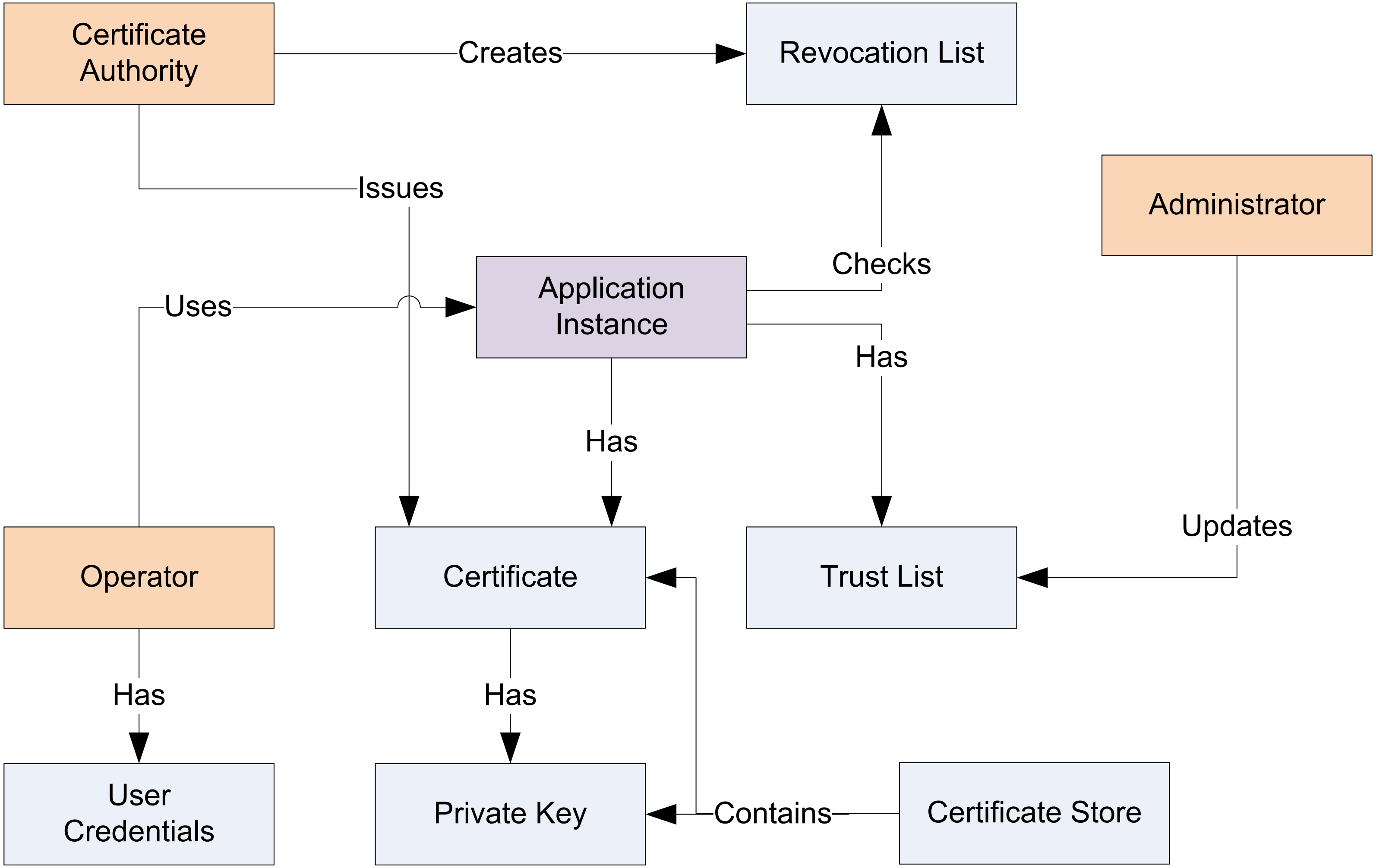


Figure 1 - Security Term and Interactions

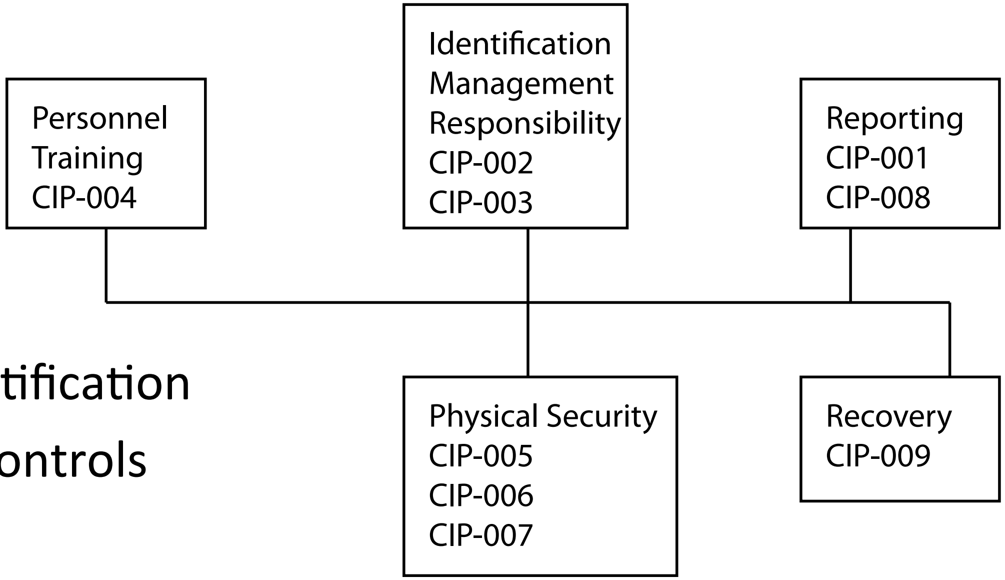
Policies developed for ICS cyber-security

- 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
  - Department of Homeland Security Catalog of Control Systems Security: Recommendations for Standards Developers
- 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
  - International Society of Automation ISA-99: **Manufacturing** and Control Systems Security, part 1 “Security for Industrial Automation and Control Systems: Concepts, Terminology and Models”

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.



Personnel
Training
CIP-004

Identification
Management
Responsibility
CIP-002
CIP-003

Reporting
CIP-001
CIP-008

Physical Security
CIP-005
CIP-006
CIP-007

Recovery
CIP-009

- 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,

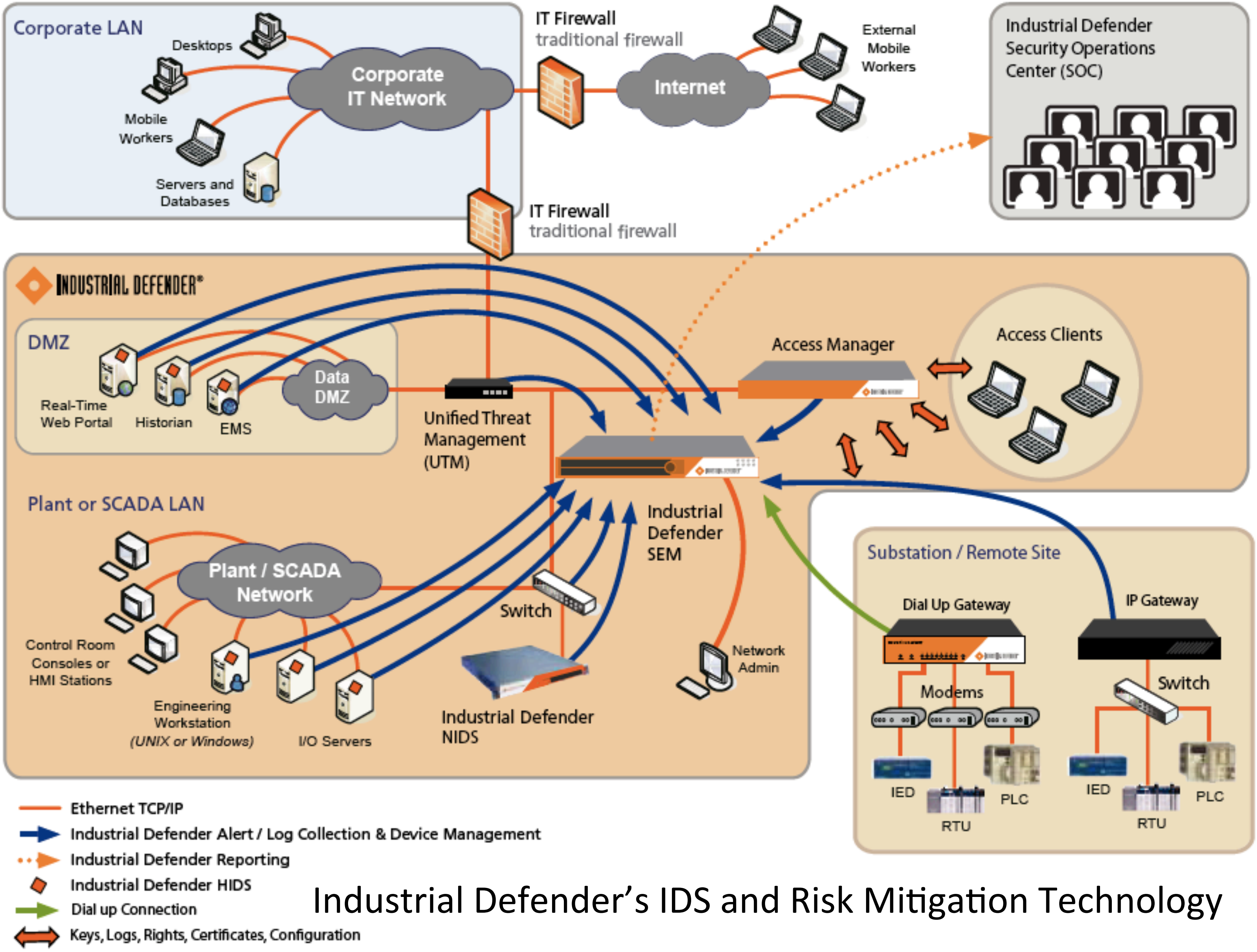
http://id.lockheedmartin.com/solutions/cybersecurity

- 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, http://id.lockheedmartin.com/industrial-defender-introduces-the-first-software-platform-for-a-unified-approach-to-security-compliance-and-change-management-in-industrial-control-systems

Automation System Manager Software Capabilities

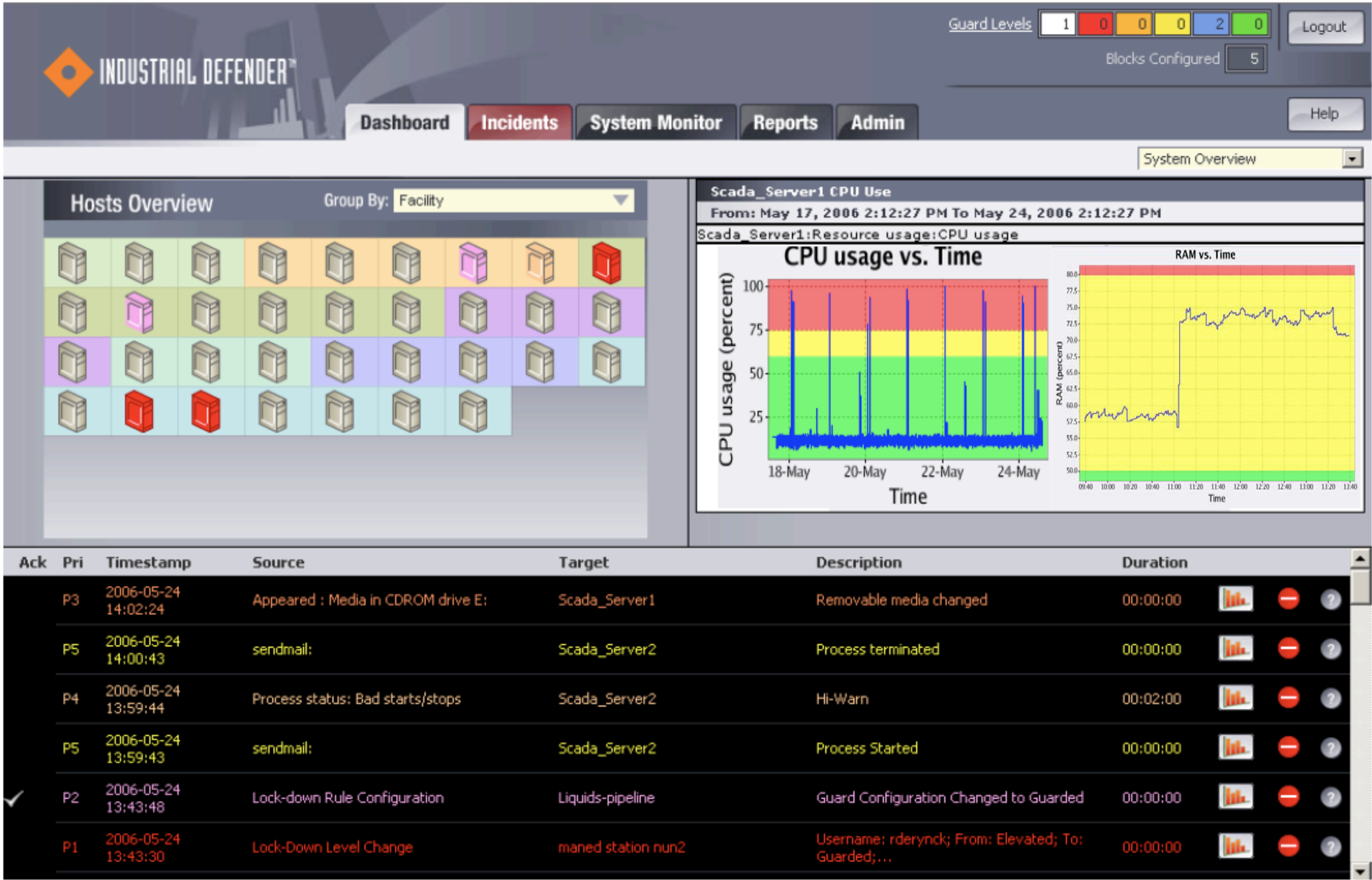
Industrial Defender

	Monitor	Manage	Protect
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 IDS and Risk Mitigation Technology

Industrial Defender’s Risk Mitigation Technology SEM



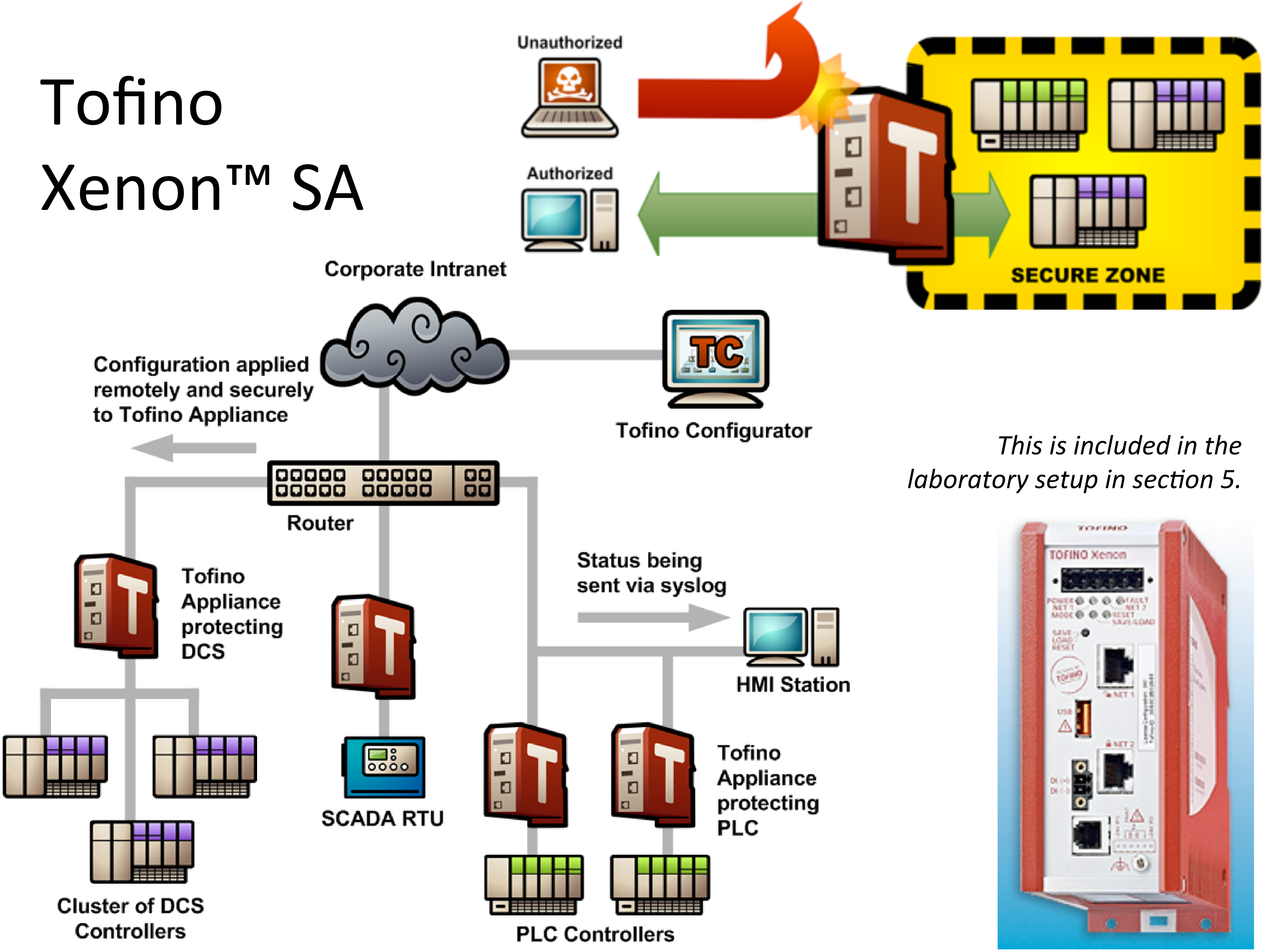
Ack	Pri	Timestamp	Source	Target	Description	Duration
	P3	2006-05-24 14:02:24	Appeared : Media in CDROM drive E:	Scada_Server1	Removable media changed	00:00:00
	P5	2006-05-24 14:00:43	sendmail:	Scada_Server2	Process terminated	00:00:00
	P4	2006-05-24 13:59:44	Process status: Bad starts/stops	Scada_Server2	Hi-Warn	00:02:00
	P5	2006-05-24 13:59:43	sendmail:	Scada_Server2	Process Started	00:00:00
✓	P2	2006-05-24 13:43:48	Lock-down Rule Configuration	Liquids-pipeline	Guard Configuration Changed to Guarded	00:00:00
	P1	2006-05-24 13:43:30	Lock-Down Level Change	maned station nun2	Username: rderynck; From: Elevated; To: Guarded;…	00:00:00

Tofino Security's Xenon™

https://www.tofinosecurity.com/products/tofino-xenon-security-appliance

- 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


Unauthorized
Authorized
SECURE ZONE
Corporate Intranet
Configuration applied remotely and securely to Tofino Appliance
TC
Tofino Configurator
Router
Tofino Appliance protecting DCS
Status being sent via syslog
HMI Station
Cluster of DCS Controllers
SCADA RTU
Tofino Appliance protecting PLC
PLC Controllers
TOFINO
TOFINO Xenon

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.
- Fact sheet, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf

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

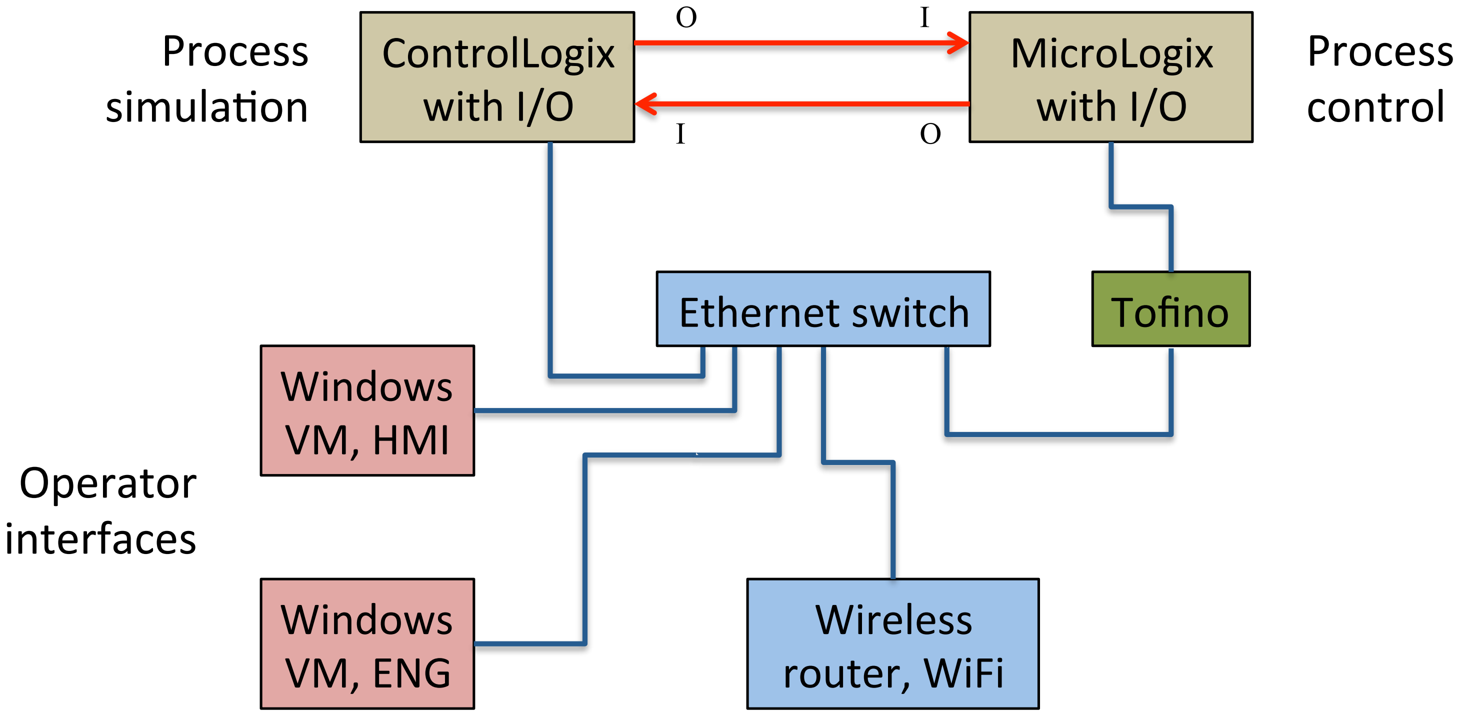
- Cyber-security is even more important in ICS as the process impacts the physical world exposing personnel and communities to severe physical harm during attacks.
- We depend on ICS to run much of our critical infrastructure, such as electricity, water, telecommunications, etc. See…
  - Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience*
  - Homeland Security Presidential Directive 7: *Critical Infrastructure Identification, Prioritization, and Protection*
- 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.



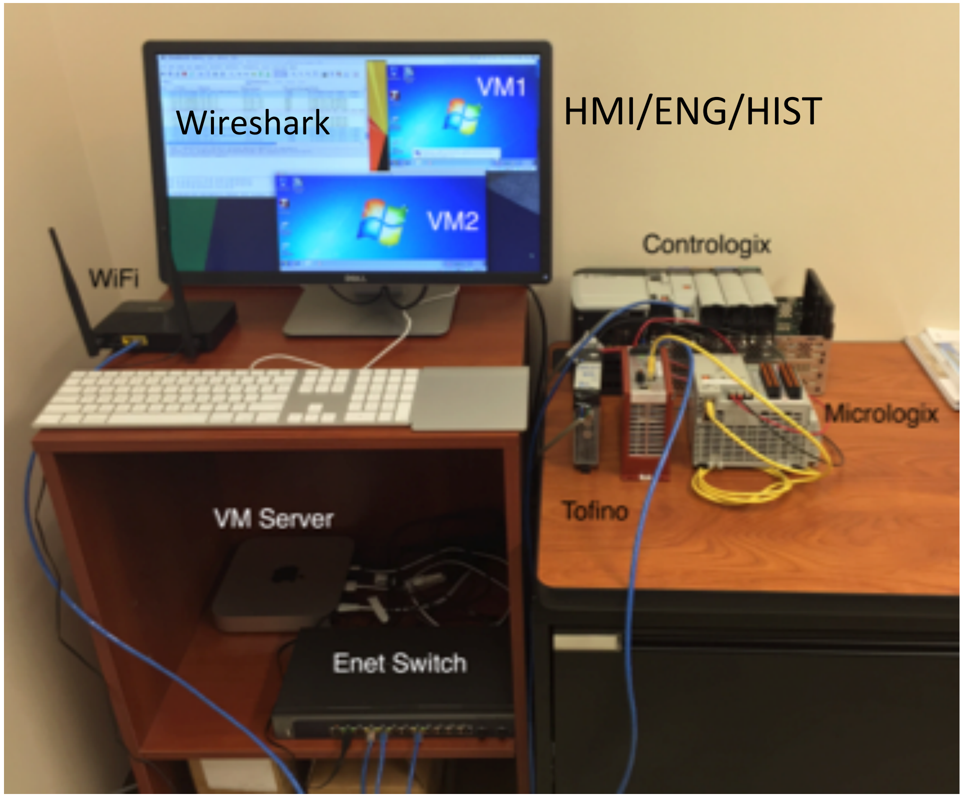
Laboratory parts list

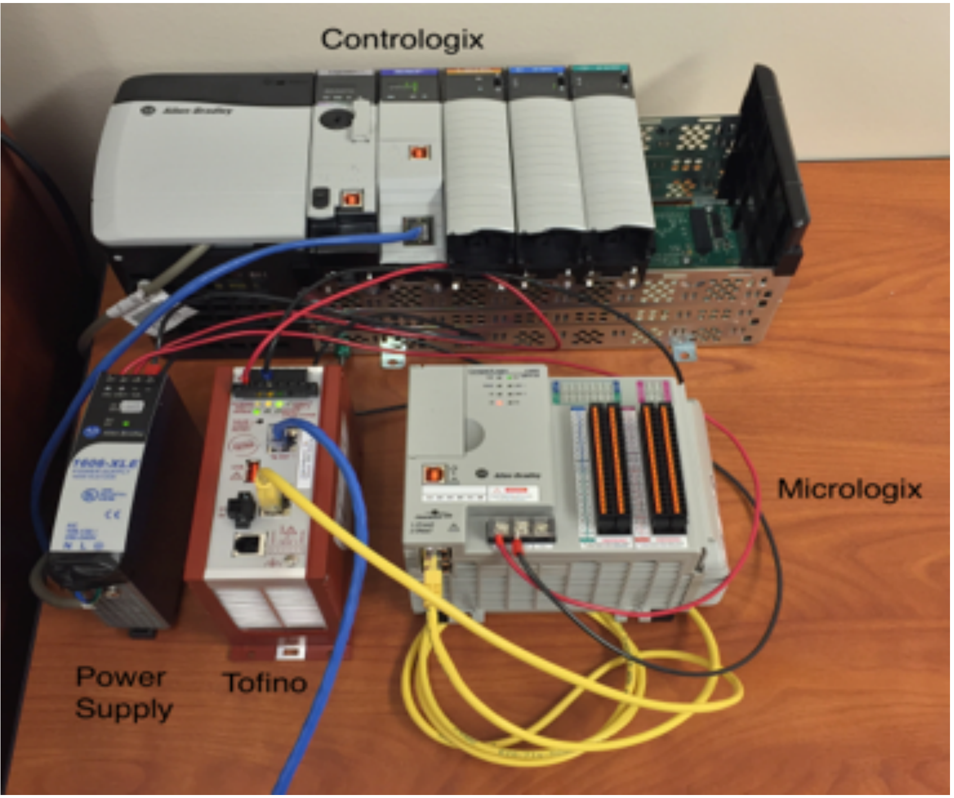
- PLCs – The use of two PLCs allows communications between PLCs to be explored. One PLC can simulate a process and the second PLC can control that process through hardwire I/O. Allen Bradley ControlLogix® and MicroLogix®.
- PCs – The Windows PCs can serve as the HMI, Engineering workstation, historical 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 - Photos

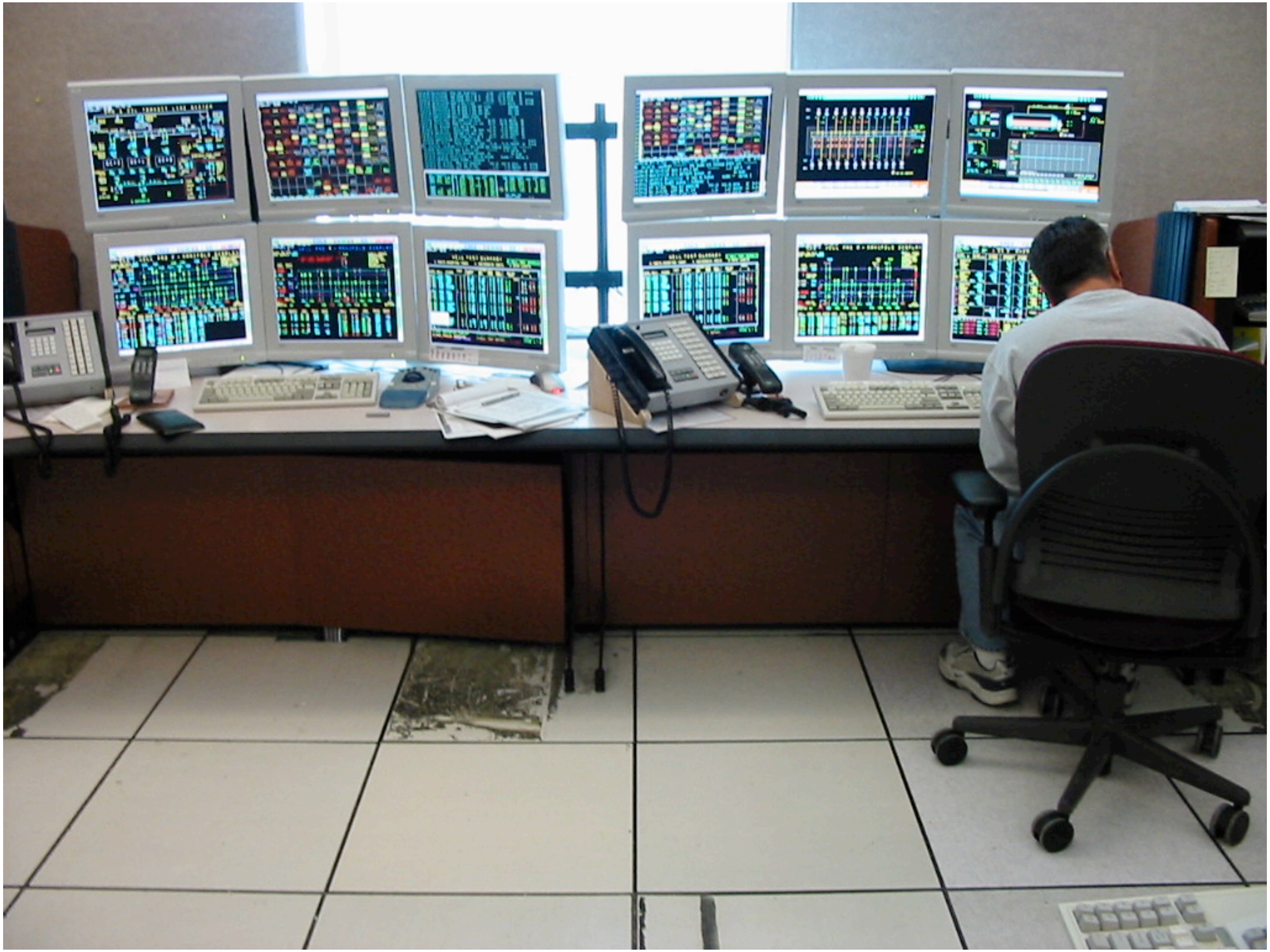
A simple laboratory setup for experiments. Students access a live ICS through the WiFi access point and attempt to hack/crack the system or play *capture-the-flag* games.

Hardwired I/O between PLCs for process simulation and control, *I/O wiring not shown.*

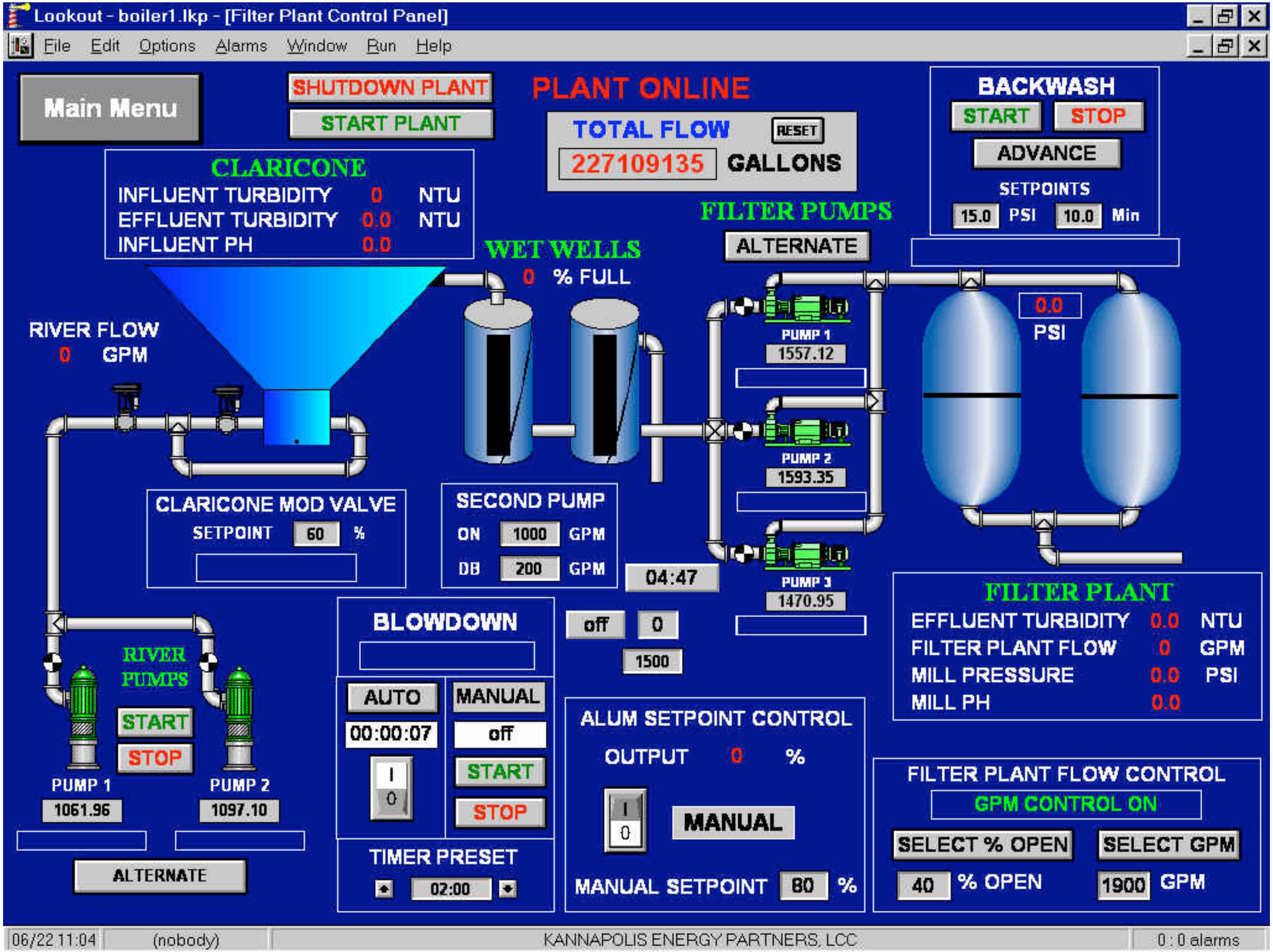




6. Modern HMI and operator



Typical HMI screen



Lookout - boiler1.lkp - [Filter Plant Control Panel]

PLANT ONLINE

TOTAL FLOW 227109135 GALLONS

CLARICONE
INFLUENT TURBIDITY 0 NTU
EFFLUENT TURBIDITY 0.0 NTU
INFLUENT PH 0.0

RIVER FLOW 0 GPM

WET WELLS 0 % FULL

BACKWASH SETPOINTS 15.0 PSI 10.0 Min

0.0 PSI

PUMP 1 1557.12
PUMP 2 1593.35
PUMP 3 1470.95

CLARICONE MOD VALVE SETPOINT 60 %

SECOND PUMP
ON 1000 GPM
DB 200 GPM

04:47

off 0
1500

BLOWDOWN
00:00:07
off
TIMER PRESET 02:00

ALUM SETPOINT CONTROL
OUTPUT 0 %
MANUAL SETPOINT 80 %

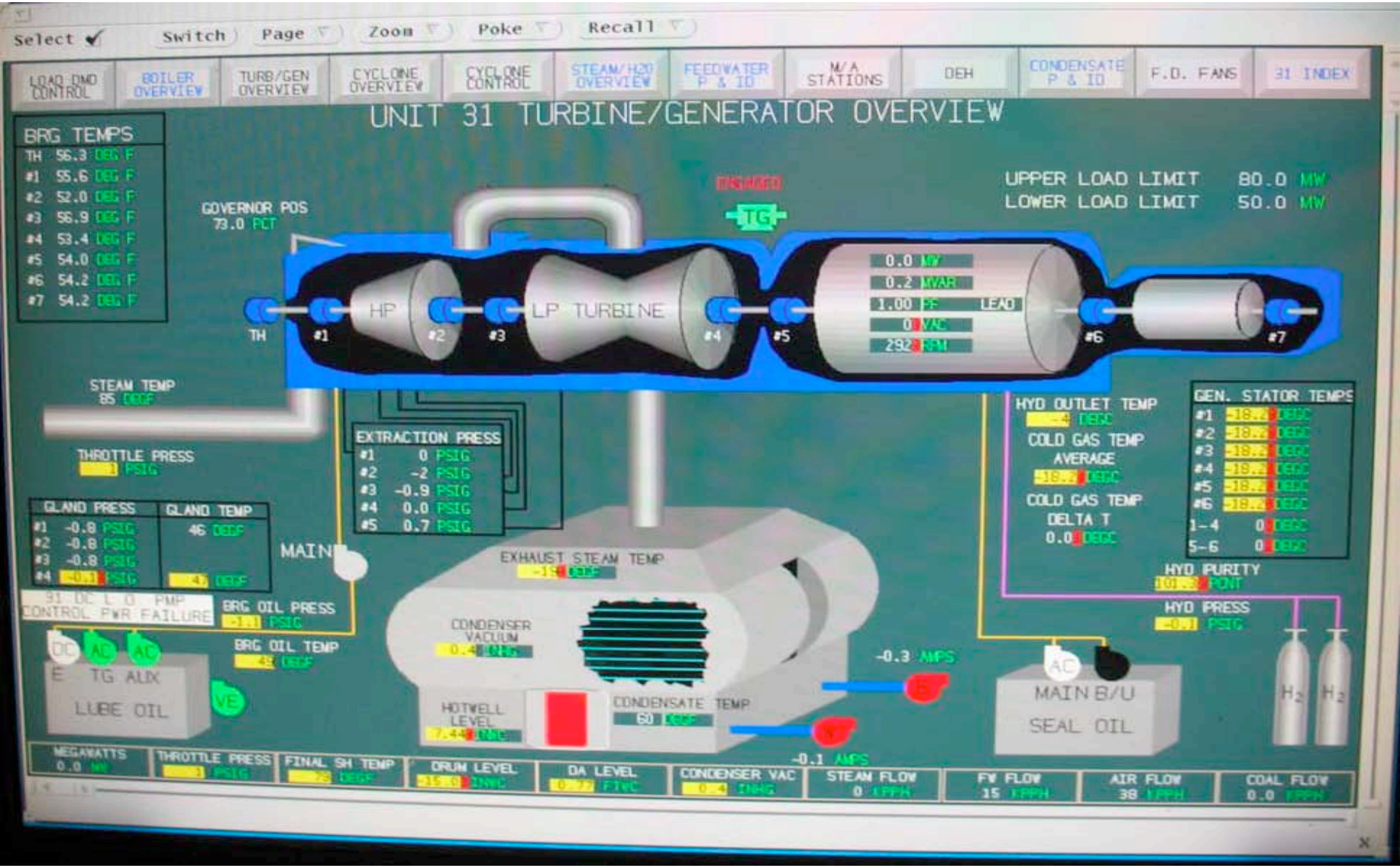
FILTER PLANT
EFFLUENT TURBIDITY 0.0 NTU
FILTER PLANT FLOW 0 GPM
MILL PRESSURE 0.0 PSI
MILL PH 0.0

FILTER PLANT FLOW CONTROL
GPM CONTROL ON
40 % OPEN
1900 GPM

RIVER PUMPS
PUMP 1 1061.96
PUMP 2 1097.10

06/22 11:04 (nobody) KANNAPOLIS ENERGY PARTNERS, LCC 0 : 0 alarms

Typical HMI screen



UNIT 31 TURBINE/GENERATOR OVERVIEW

BRG TEMPS		
TH	56.3	DEG F
#1	55.6	DEG F
#2	52.0	DEG F
#3	56.9	DEG F
#4	53.4	DEG F
#5	54.0	DEG F
#6	54.2	DEG F
#7	54.2	DEG F

GOVERNOR POS 73.0 PCT

UPPER LOAD LIMIT 80.0 MW
LOWER LOAD LIMIT 50.0 MW

0.0 MW
0.2 MVAR
1.00 PF
0 VAC
292 RPM

STEAM TEMP 85 DEGF

THROTTLE PRESS 1 PSIG

EXTRACTION PRESS		
#1	0	PSIG
#2	-2	PSIG
#3	-0.9	PSIG
#4	0.0	PSIG
#5	0.7	PSIG

GLAND PRESS			GLAND TEMP
#1	-0.8	PSIG	46 DEGF
#2	-0.8	PSIG	
#3	-0.8	PSIG	
#4	-0.1	PSIG	47 DEGF

91 DC L O PMP CONTROL PWR FAILURE

BRG OIL PRESS -1.1 PSIG

BRG OIL TEMP 49 DEGF

EXHAUST STEAM TEMP -19 DEGF

CONDENSER VACUUM 0.4 INHG

HOTWELL LEVEL 7.44 INWC

CONDENSATE TEMP 60 DEGF

-0.3 AMPS

-0.1 AMPS

HYD OUTLET TEMP -4 DEGC

COLD GAS TEMP AVERAGE -18.2 DEGC

COLD GAS TEMP DELTA T 0.0 DEGC

GEN. STATOR TEMPS		
#1	-18.2	DEGC
#2	-18.2	DEGC
#3	-18.2	DEGC
#4	-18.2	DEGC
#5	-18.2	DEGC
#6	-18.2	DEGC
1-4	0	DEGC
5-6	0	DEGC

HYD PURITY 101.3 PCNT

HYD PRESS -0.1 PSIG

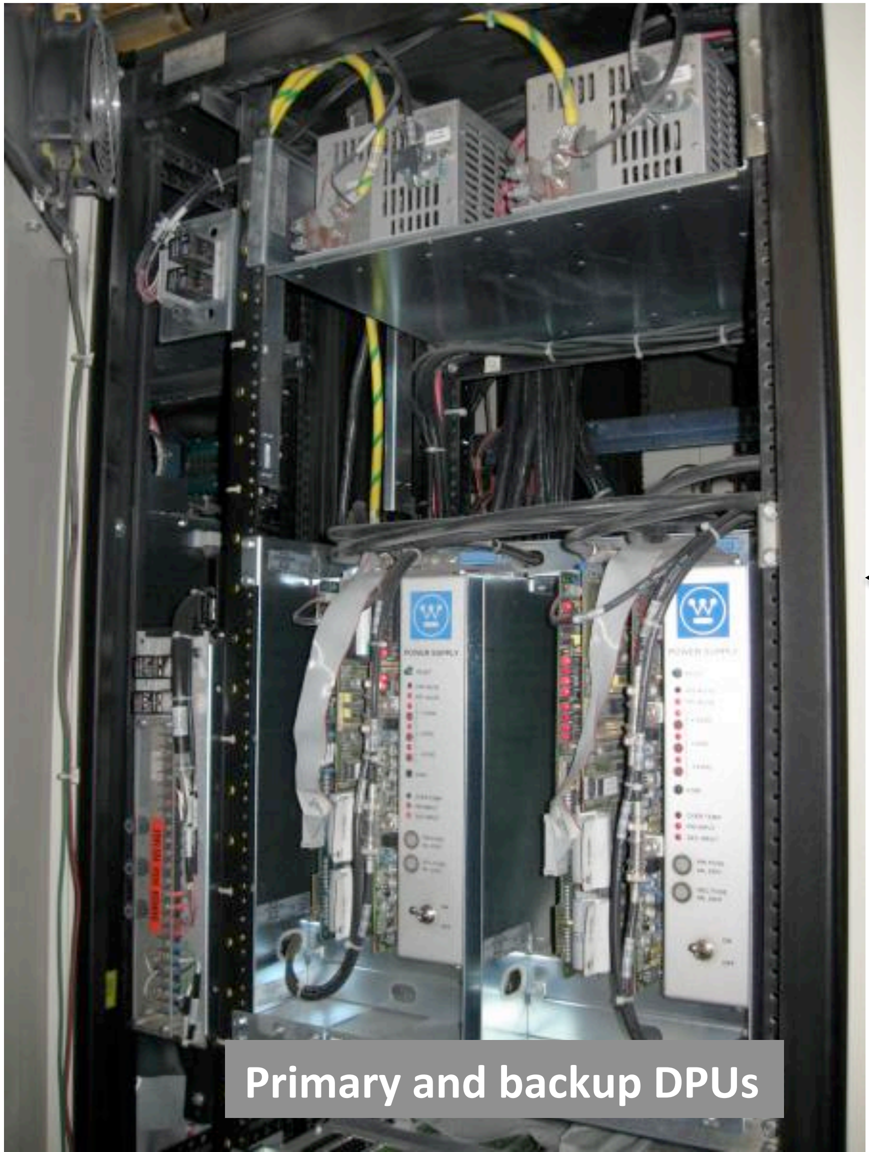
MEGAWATTS	THROTTLE PRESS	FINAL SH TEMP	DRUM LEVEL	DA LEVEL	CONDENSER VAC	STEAM FLOW	FW FLOW	AIR FLOW	COAL FLOW
0.0 MW	1 PSIG	79 DEGF	-15.0 INWC	0.77 FTWC	0.4 INHG	0 KPPH	15 KPPH	38 KPPH	0.0 KPPH

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)



Primary and backup DPUs

↔

One of many I/O racks

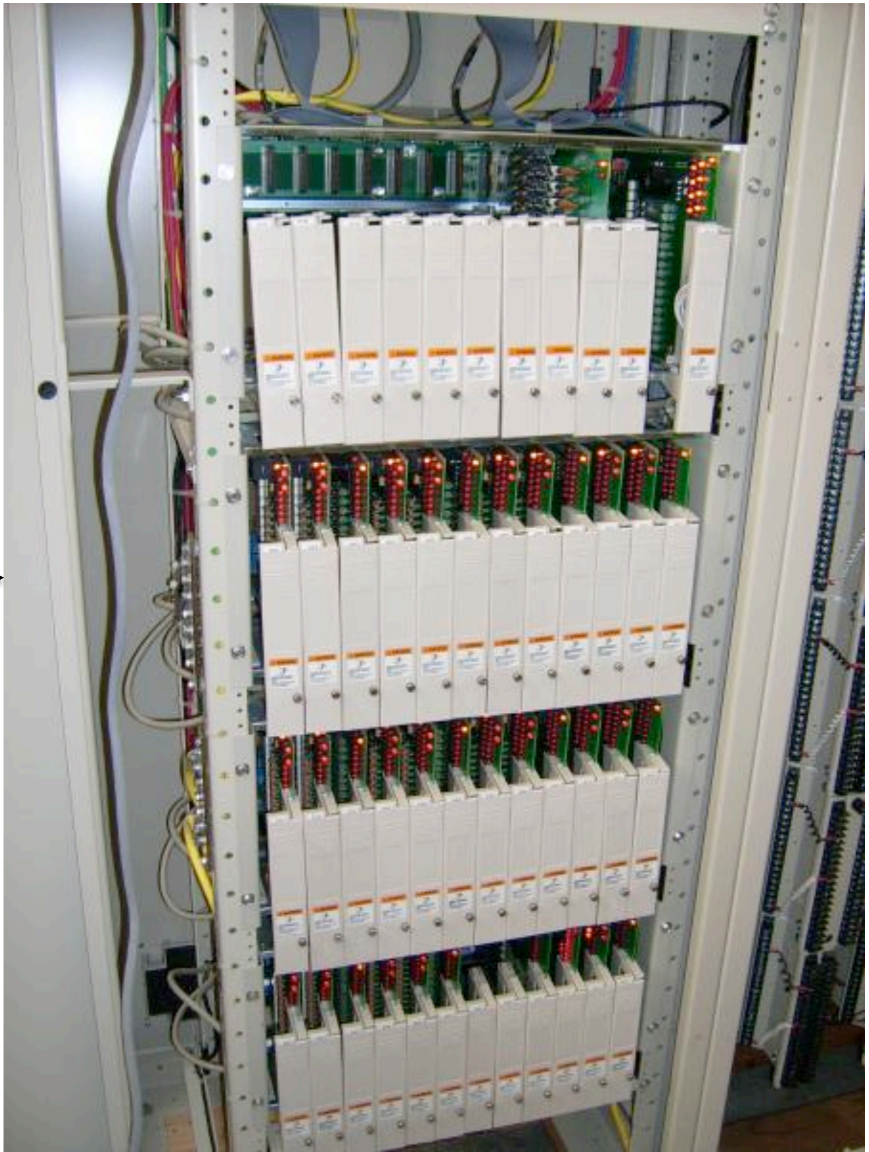
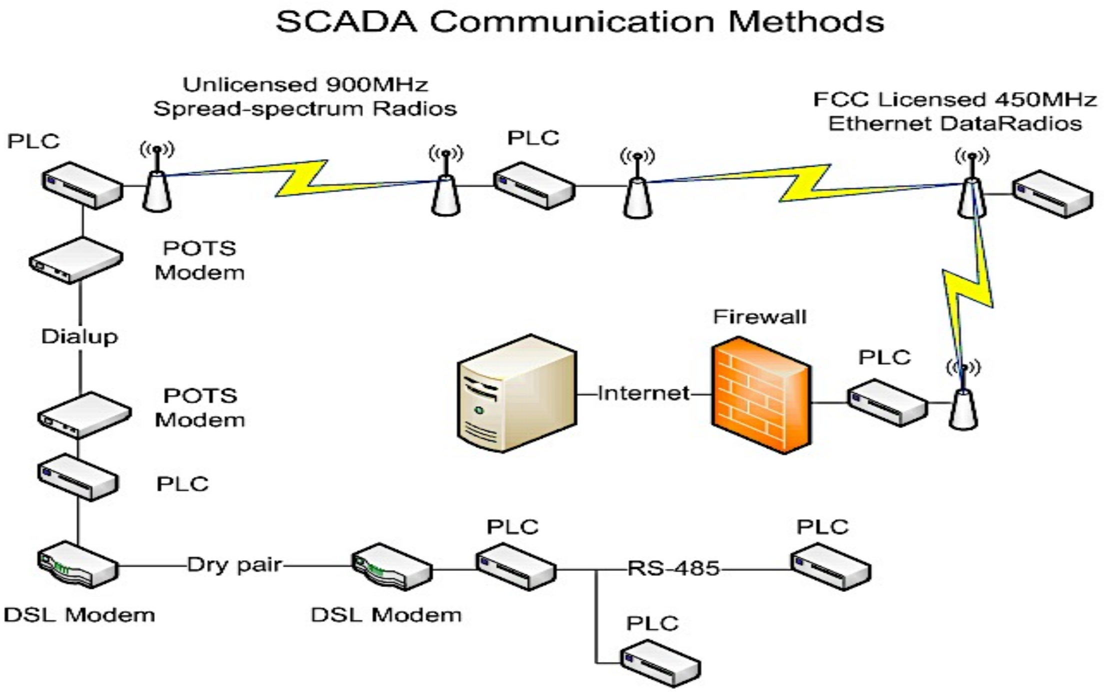
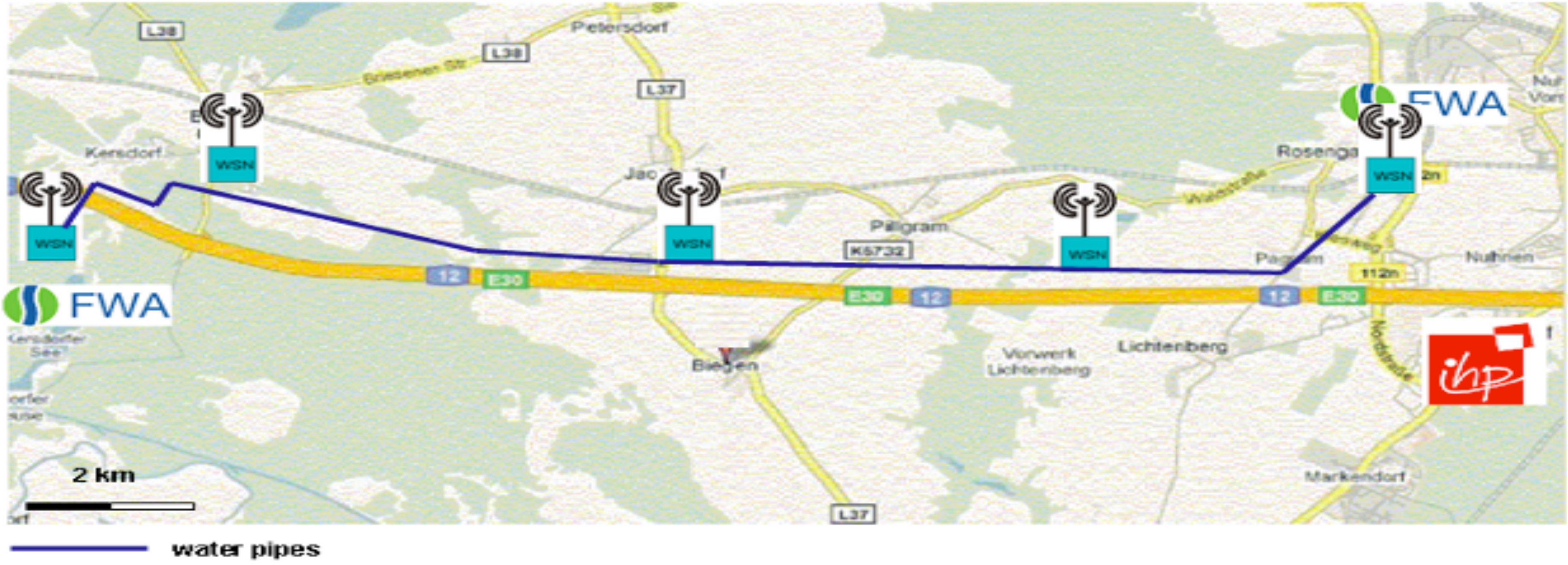


ABB substation automation racks

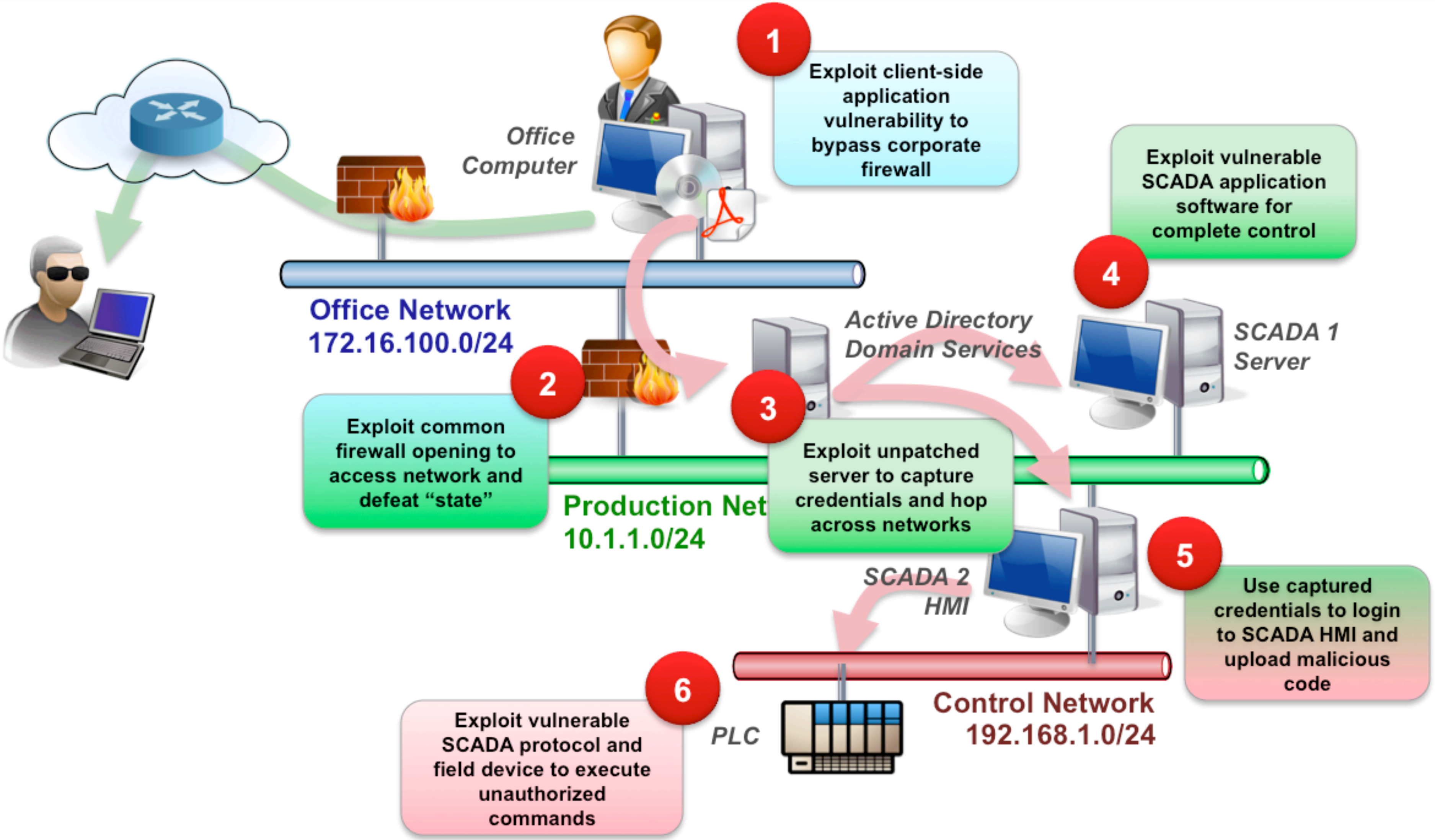
A DCS has to live in a hostile environment and control a large and complex process.

SCADA often has to spread out over larger distances and across many network types.


SCADA Communication Methods
Unlicensed 900MHz Spread-spectrum Radios
FCC Licensed 450MHz Ethernet DataRadios
PLC
PLC
POTS Modem
Dialup
POTS Modem
PLC
Firewall
Internet
PLC
DSL Modem
Dry pair
DSL Modem
PLC
RS-485
PLC
PLC



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