

Convergence of Physical & Network Cyber Vulnerabilities



Unified Port of San Diego
BITS Department
Security Section
Thomas P. Gresham
Technology Security Supervisor

07/20/2016

Briefing Outline

- Overview
- Industrial Control Systems (ICS)
 - Heating, Ventilation, and Air Conditioning (HVAC)
 - Physical Access Control System (PACS)
- Vulnerabilities
- Countermeasures



Overview



Convergence refers to the recent interconnection of General Support Information Technology (IT) systems with Industrial Control Systems (ICS). Traditionally, IT networks that carried business systems were not physically connected to control systems networks and the two systems did not communicate.

For a variety of reasons, more and more organizations have created connections to their control systems, but operators are often unaware of exposure created by these connections. The increasing connectivity of ICS is creating new avenues of access for potential cyber attackers. Awareness of this risk is vitally needed by both IT and Physical Security professionals to adequately address the risk created by the convergence of Industrial Control Systems and IT systems.

Heating, Ventilation, and Air Conditioning (HVAC)



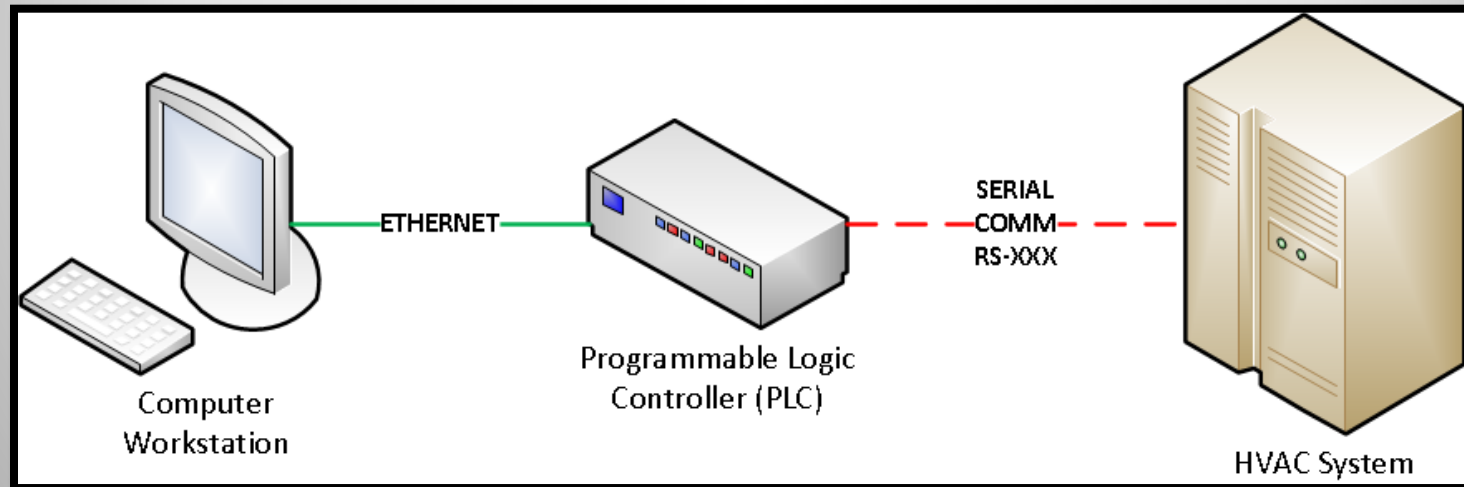
An HVAC system manages environmental conditions within a building such as heating, cooling, lighting and other functions.

Vulnerabilities:

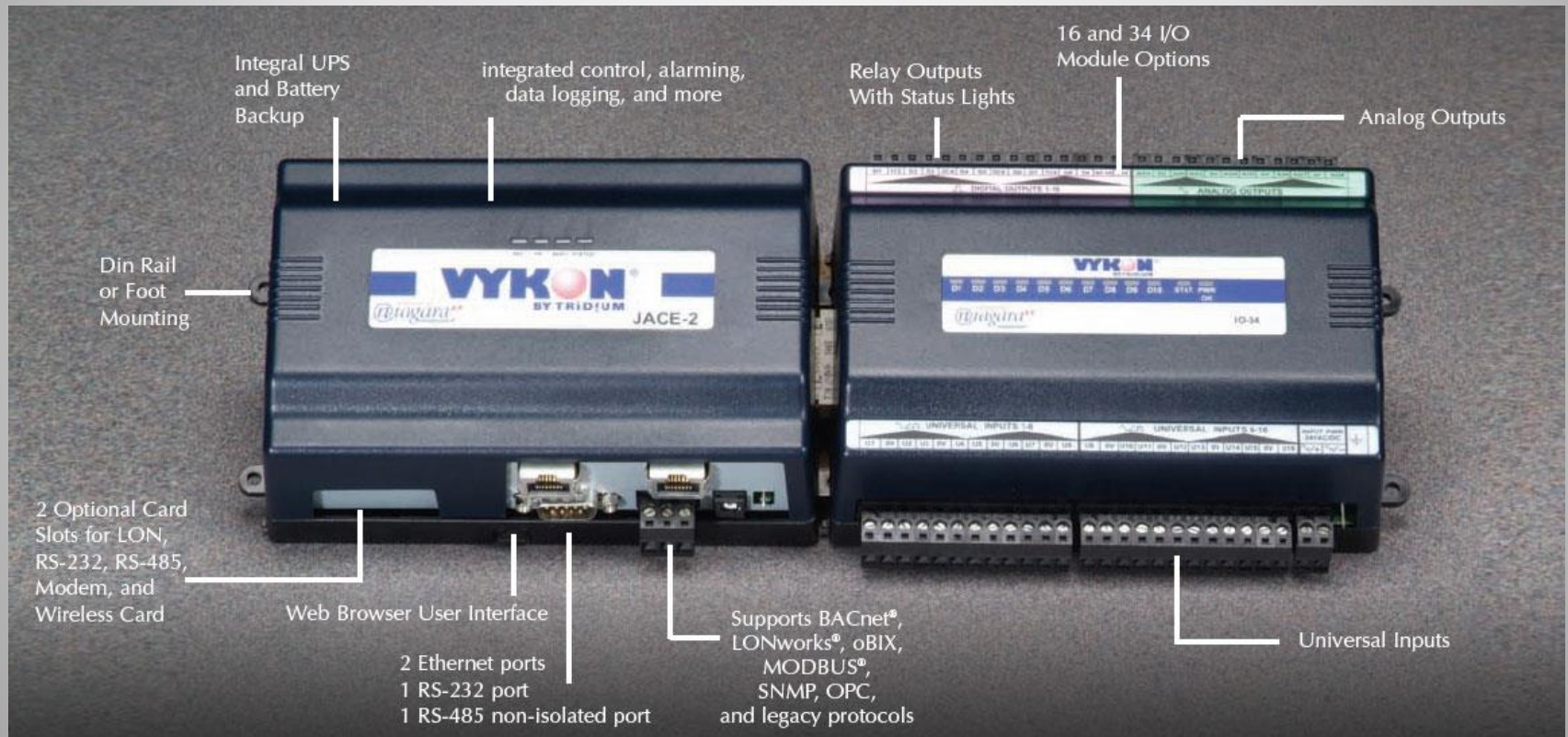
- Information Theft: The Target breach occurred when hackers broke into the network of a company that managed the company's heating, ventilation and air conditioning (HVAC) systems.
- Kinetic Effect: HVAC systems often maintain critical temperatures for server rooms, food storage, hospitals, etc. The compromise of such systems can have catastrophic results.

Heating, Ventilation, and Air Conditioning (HVAC)

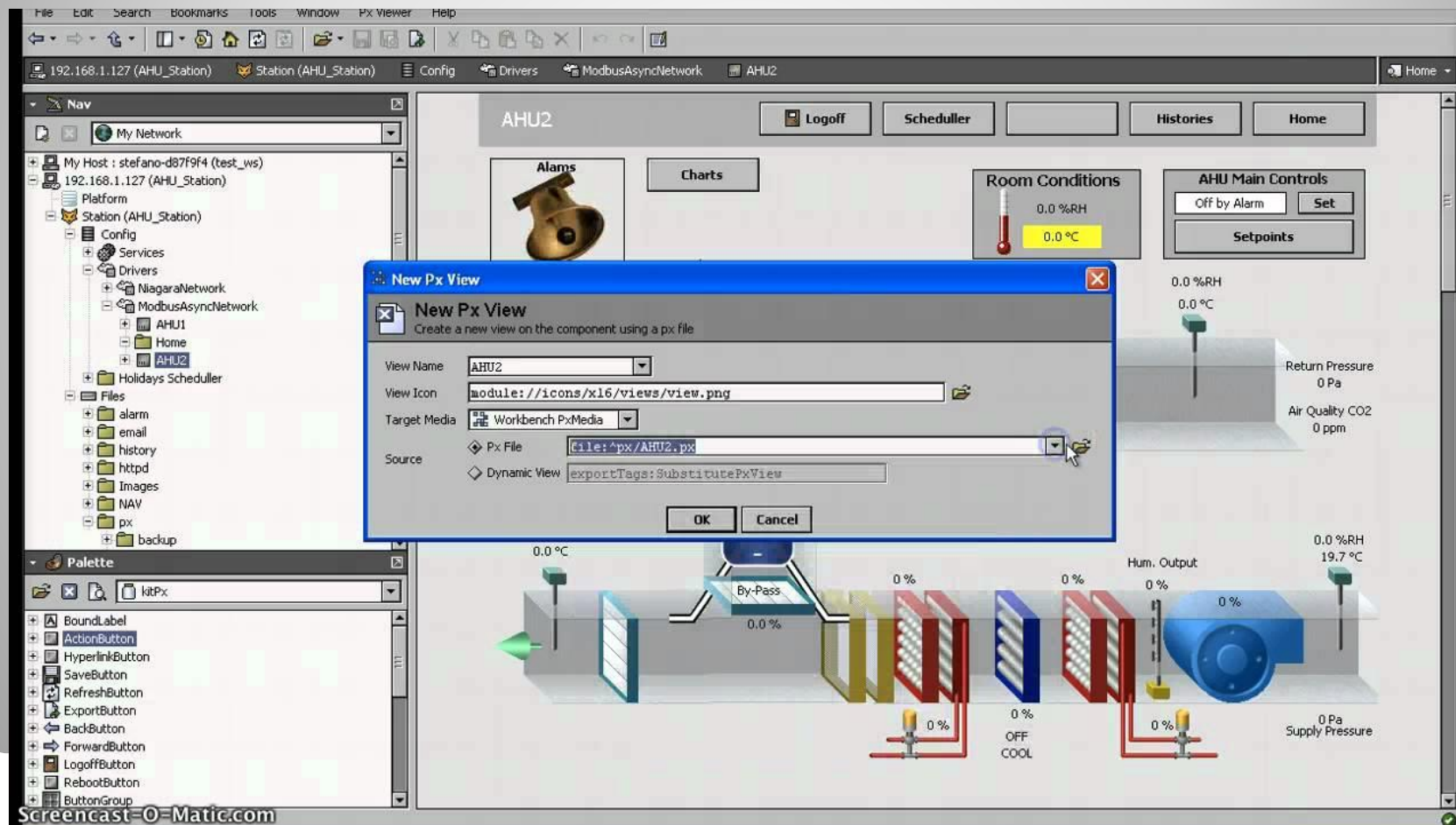
A Programmable Logic Controller (PLC) allows remote control of an ICS from a workstation.



Programmable Logic Controller (PLC)



HVAC Java Application Control Engine (JACE) Controller Interface



Physical Access Control System (PACS)



A PACS manages the physical security of a building or perimeter. Functions provided include: gate/door access and credential issuance.

Vulnerabilities:

- Credential Issuance: An attacker can elevate privileges for an existing access card or generate a new one.
- Kinetic Effect: A PACS interface allows for the possibility of an attacker to remotely physically open, close and lock doors and gates.

Physical Access Control System (PACS)

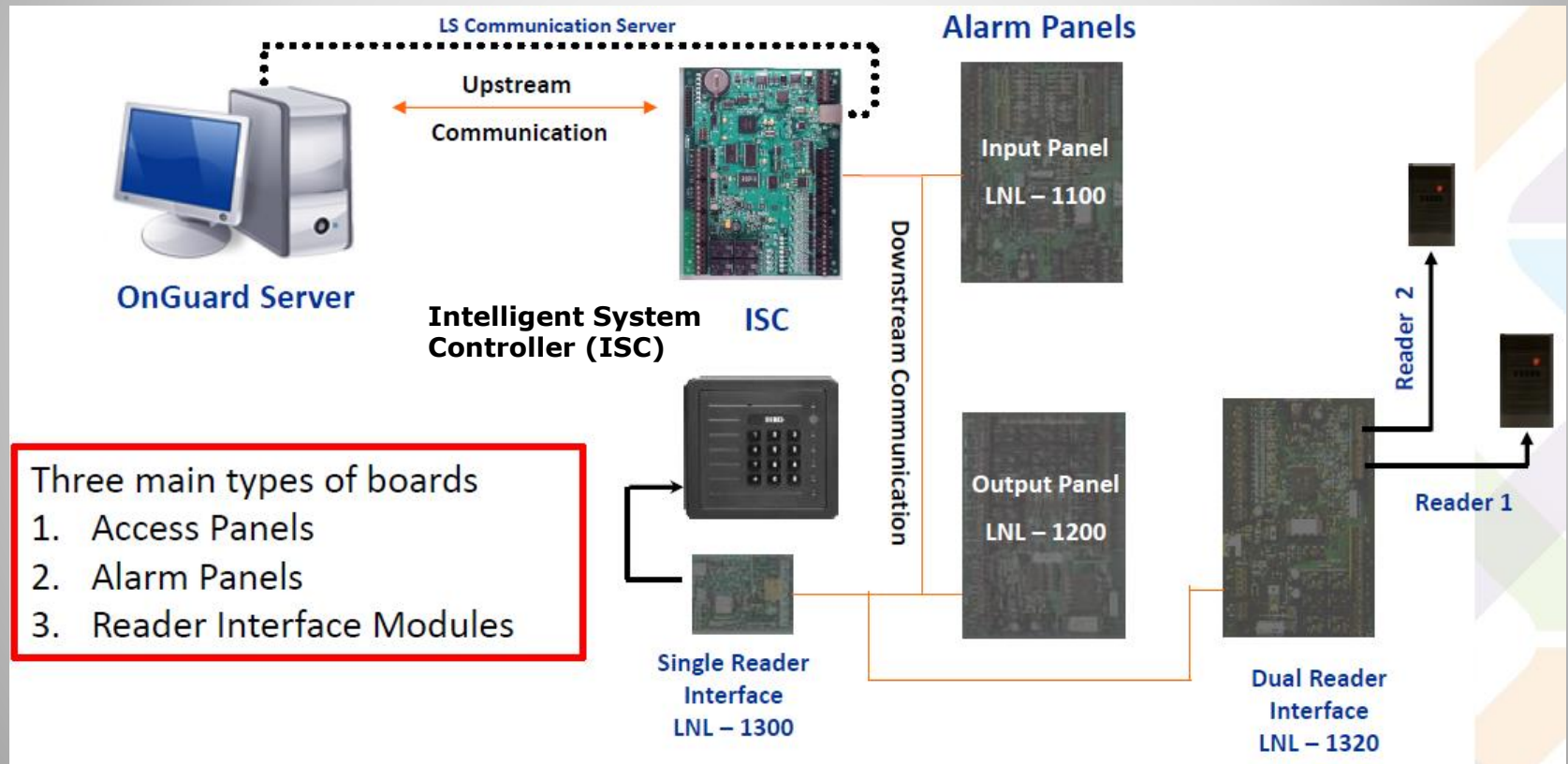
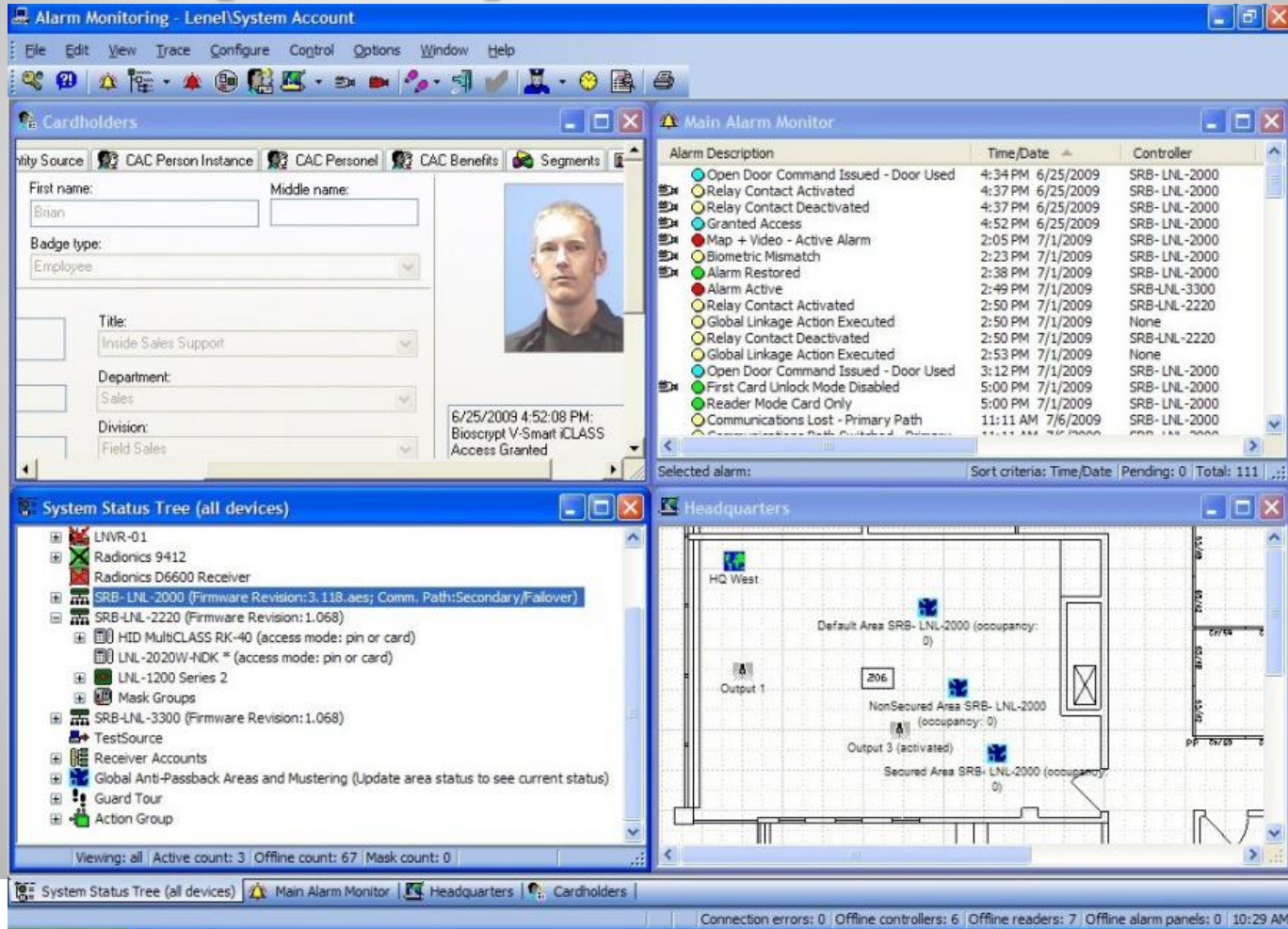


Image Courtesy of Lenel

Physical Access Control System (PACS)



The screenshot displays the Lenel System Account software interface, which is used for managing a Physical Access Control System (PACS). The interface is divided into several main sections:

- Cardholders:** This panel on the left allows for the management of individual cardholders. It includes fields for First name, Middle name, Badge type (set to Employee), Title (set to Inside Sales Support), Department (set to Sales), and Division (set to Field Sales). A photo of a man is displayed next to the cardholder information.
- Main Alarm Monitor:** This panel on the right displays a list of alarm events. The table below shows the data for these events:

Alarm Description	Time/Date	Controller
Open Door Command Issued - Door Used	4:34 PM 6/25/2009	SRB-LNL-2000
Relay Contact Activated	4:37 PM 6/25/2009	SRB-LNL-2000
Relay Contact Deactivated	4:37 PM 6/25/2009	SRB-LNL-2000
Granted Access	4:52 PM 6/25/2009	SRB-LNL-2000
Map + Video - Active Alarm	2:05 PM 7/1/2009	SRB-LNL-2000
Biometric Mismatch	2:23 PM 7/1/2009	SRB-LNL-2000
Alarm Restored	2:38 PM 7/1/2009	SRB-LNL-2000
Alarm Active	2:49 PM 7/1/2009	SRB-LNL-3300
Relay Contact Activated	2:50 PM 7/1/2009	SRB-LNL-2220
Global Linkage Action Executed	2:50 PM 7/1/2009	None
Relay Contact Deactivated	2:50 PM 7/1/2009	SRB-LNL-2220
Global Linkage Action Executed	2:53 PM 7/1/2009	None
Open Door Command Issued - Door Used	3:12 PM 7/1/2009	SRB-LNL-2000
First Card Unlock Mode Disabled	5:00 PM 7/1/2009	SRB-LNL-2000
Reader Mode Card Only	5:00 PM 7/1/2009	SRB-LNL-2000
Communications Lost - Primary Path	11:11 AM 7/6/2009	SRB-LNL-2000

- System Status Tree (all devices):** This panel on the bottom left shows a hierarchical list of all devices connected to the system. The list includes:
 - LNVR-01
 - Radionics 9412
 - Radionics D6600 Receiver
 - SRB-LNL-2000 (Firmware Revision: 3.118.aes; Comm. Path: Secondary/Failover)
 - SRB-LNL-2220 (Firmware Revision: 1.068)
 - HID MultiCLASS RK-40 (access mode: pin or card)
 - LNL-2020W-NDK * (access mode: pin or card)
 - LNL-1200 Series 2
 - Mask Groups
 - SRB-LNL-3300 (Firmware Revision: 1.068)
 - TestSource
 - Receiver Accounts
 - Global Anti-Passback Areas and Mustering (Update area status to see current status)
 - Guard Tour
 - Action Group
- Headquarters:** This panel on the bottom right displays a map of the facility. The map shows various areas and their occupancy status:
 - HQ West
 - Default Area SRB-LNL-2000 (occupancy: 0)
 - Output 1
 - 206
 - NonSecured Area SRB-LNL-2000 (occupancy: 0)
 - Output 3 (activated)
 - Secured Area SRB-LNL-2000 (occupancy: 0)

The bottom status bar of the application shows the following information: Viewing: all | Active count: 3 | Offline count: 67 | Mask count: 0 | Connection errors: 0 | Offline controllers: 6 | Offline readers: 7 | Offline alarm panels: 0 | 10:29 AM

Image Courtesy of Lenel

Countermeasures

Mitigations may be implemented to reduce the risk to both HVAC and PACS. Best practices include changing of default credentials. Default usernames and passwords are known and set by the vendor when new devices are shipped. Well-known usernames and passwords are published on the Internet.

<https://github.com/scadastrangelove/SCADAPASS>



scadapass

Countermeasures



Other mitigations may be implemented to further protect ICS systems through internal network segmentation. Internal segmentation slows down or prevents attackers from breaching higher-security systems.

Below is a list of common network segmentation approaches.

- \$ VLAN/Subnet Access Control Lists
- \$\$ Firewall Network Enclave
- \$\$\$ Data Diode
- \$\$\$ Air Gapping

VLAN/Subnet Access Control Lists (ACLs)

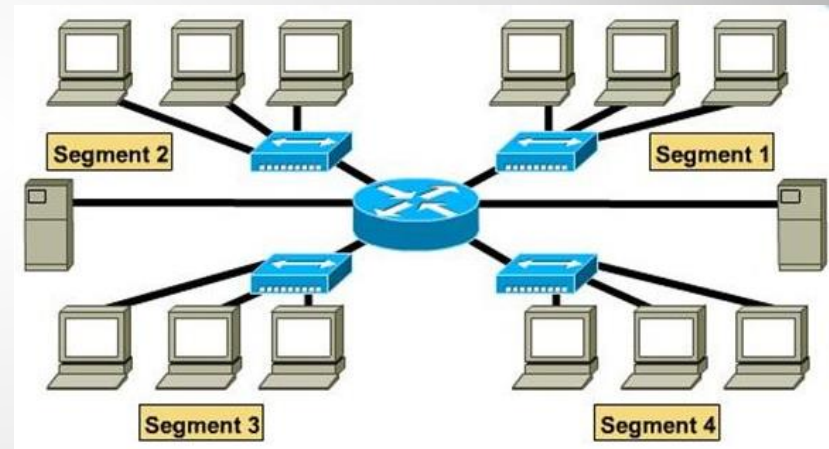
A network access control list (ACL) is a layer of security for your that acts as a control gate for network traffic in and out of one or more subnets.

Benefits:

- Inexpensive to implement
- Low skillset to maintain
- Rapid deployment

Drawbacks:

- Difficult to track / maintain
- Traffic is only controlled at a network/port level
- Low security
- Minimal event logging



Firewall Network Enclave

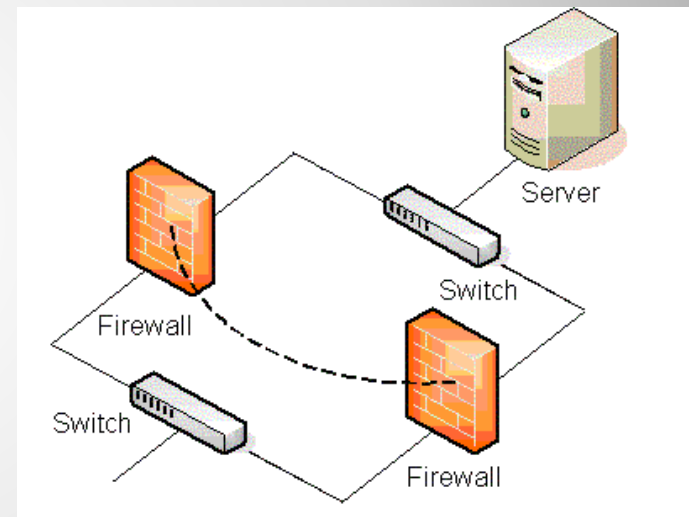
A Firewall Network Enclave is a segment of an internal network that is defined by common security policies and protected through one or more firewall devices.

Benefits:

- Networks remain connected
- Traffic controlled at all levels
- Detailed event logging

Drawbacks:

- Moderate implementation cost
- Moderate skillset required to maintain
- Potential for false positive blocks



Diode Architecture



A unidirectional network (also referred to as a unidirectional security gateway or data diode) is a network appliance or device allowing data to travel only in one direction, used in guaranteeing information security.

Benefits:

- Extremely Secure – nearly impossible to hack
- Networks are still connected for reporting

Drawbacks:

- Very expensive
- Advanced skillset required to maintain
- No remote administration of ICS

Diode Architecture

What is a Data Diode?

- Hardware based cybersecurity designed to be only One-way
- Impervious to software changes or attacks (hardware cannot change)
- Defends the perimeter of the source network
- Transfers data out of the protected network

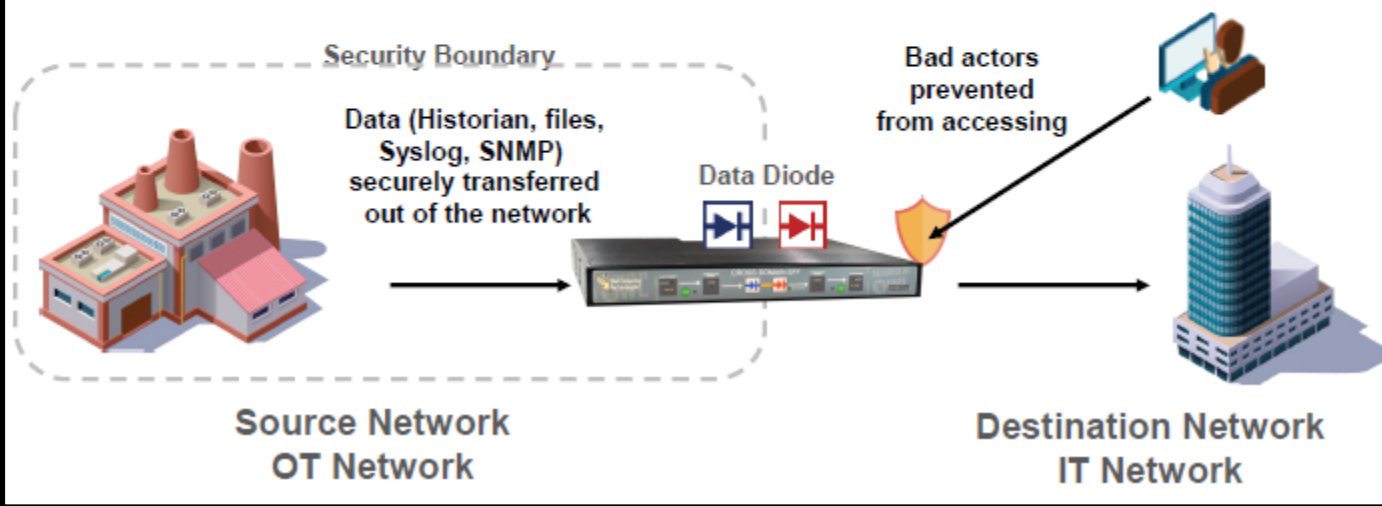


Image Courtesy of Owl Computing Technologies

Air Gapping



An air gap is a network security measure, also known as air gapping, employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks.

Benefits:

- Impossible to remotely compromise

Drawbacks:

- Very expensive – Manual inspection / maintenance
- No remote administration or communication with ICS

Closing Thoughts



- Convergence will happen
- Awareness and coordination are key among IT and Physical Security Professionals
- Vulnerabilities are real
- Countermeasures should be considered based on risk tolerance

Questions?