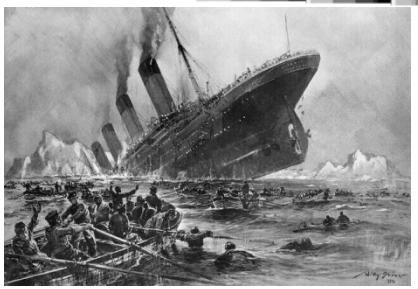
Process Control Systems
Industry Conference

Protecting Safety Instrumented Systems from Cyber Attack Using a Zone and Conduit Design

Eric Byres

Kevin Staggs

The Sinking of the Titanic



- On the night of 14 April 1912, during her maiden voyage, Titanic struck an iceberg, and sank two hours and forty minutes later.
- One of the contributing factors was that the bulkheads on *Titanic* only extended 10 feet above the waterline and did not make compartments fully watertight.
- Water from the damaged compartments was able to flood into the undamaged ones, sinking the ship.

Zotob Worm Security Incident

- **August 18, 2005:** 13 US auto plants were shut down by a simple Internet worm.
  - Despite professionally installed firewalls between the Internet the company network and the control network, the Zotob worm had made its way into the control system (probability via a laptop).
  - Once in the control system, it was able to travel from plant to plant in seconds.
- 50,000 assembly line workers to cease work during the outages.
- Estimated $14 million loss.

The Browns Ferry "Security" Incident

- **August 19, 2006:** Operators at Browns Ferry Nuclear plant had to "scram" the reactor due to a potentially dangerous 'high power, low flow condition'.
  - Redundant drives controlling the recirculating water system failed due to "excessive traffic" on the control network.
  - Traffic between two different vendors' control products was likely the cause.
- Facility remained offline for 2 days.

The Hatch Nuclear "Security" Incident

- **March 7, 2008:** Unit 2 of the Hatch nuclear plant forced into an emergency shutdown for 48 hrs.
  - An engineer installed a software update on a computer operating on the plant's business network.
  - The computer was used to monitor diagnostic data from one of the primary control systems,
  - The software update was designed to synchronize data on both systems.
  - When the updated computer rebooted, it reset the data on the control system, causing safety systems to errantly interpret the lack of data as a drop in water reservoirs that cool the plant's radioactive nuclear fuel rods, and triggering a shutdown triggering a shutdown.

What these Events and Titanic have in Common?

- Poor design of the “system”
- A lack of separation between key sub-systems
- A misunderstanding of the threat sources and the resultant risk.

The NRC's View…

- *"The August 19, 2006, transient unnecessarily challenged the plant safety systems and placed the plant in a potentially unstable high-power, low-flow condition.*
- *Careful design and control of the network architecture can mitigate the risks to plant networks from malfunctioning devices, and improper network performance, and ultimately result in safer plant operations."*

NRC INFORMATION NOTICE: 2007-15

Process Control Systems
Industry Conference

Designing for Secure and Reliable Control Networks

What Makes a System Unsafe and Unreliable?

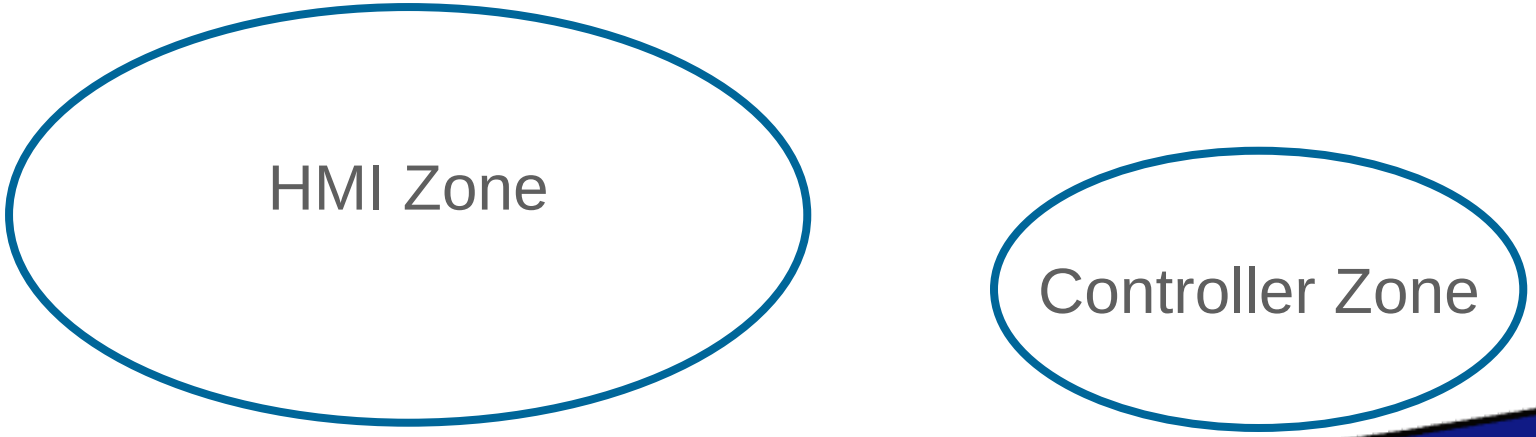
- Remember that in all these cases, there was a failure to contain communications in appropriate areas or sub-systems.
- Issues in one area were allowed to migrate to another area due to poor (or non-existent) separation strategy.
- The solution is the use of ***security zones*** *as defined in ANSI/ISA-99*

ANSI/ISA-99.02.01 Standard (Draft)

- 4.3.2.3 ELEMENT – Network Segmentation
- Objective:
  - Group and separate key IACS devices into zones with common security levels in order to manage security risks and to achieve a desired target security level for each zone.
- Requirement 4.3.2.3.1:
  - A network segmentation countermeasure strategy employing security zones shall be developed for IACS devices based upon the risk level of the IACS.

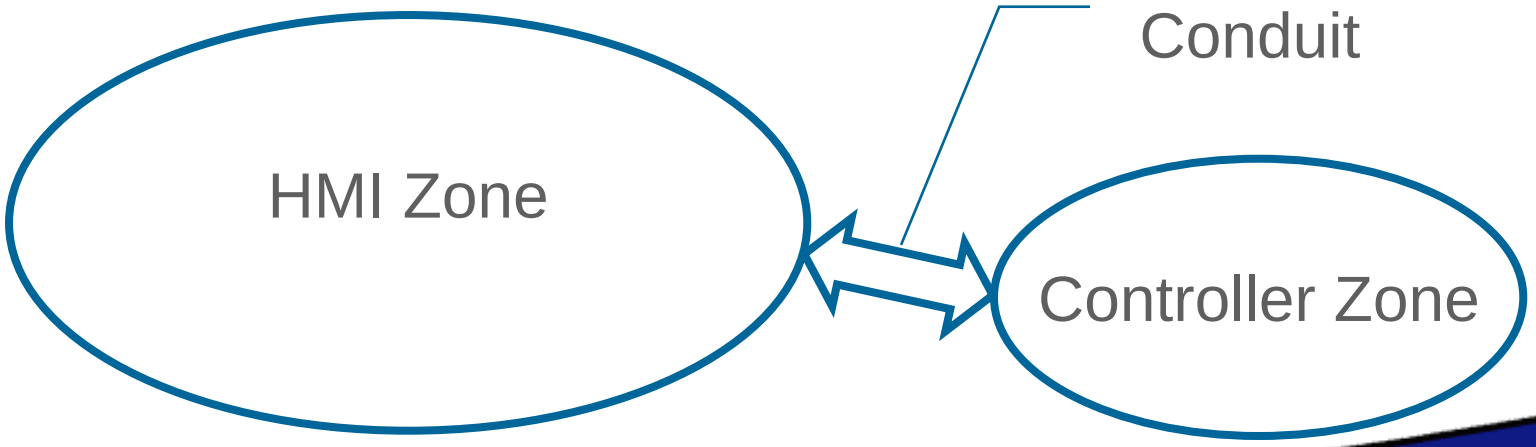
Security Zone Definition

- "Security zone: grouping of logical or physical assets that share common security requirements". [ANSI/ISA–99.00.01–2007- 3.2.116]
  - A zone has a clearly defined border (either logical or physical), which is the boundary between included and excluded elements.



Conduits

- A conduit is a path for the flow of data between two zones.
  - can provide the security functions that allow different zones to communicate securely.
  - Any communications between zone must have a conduit.



Security Levels

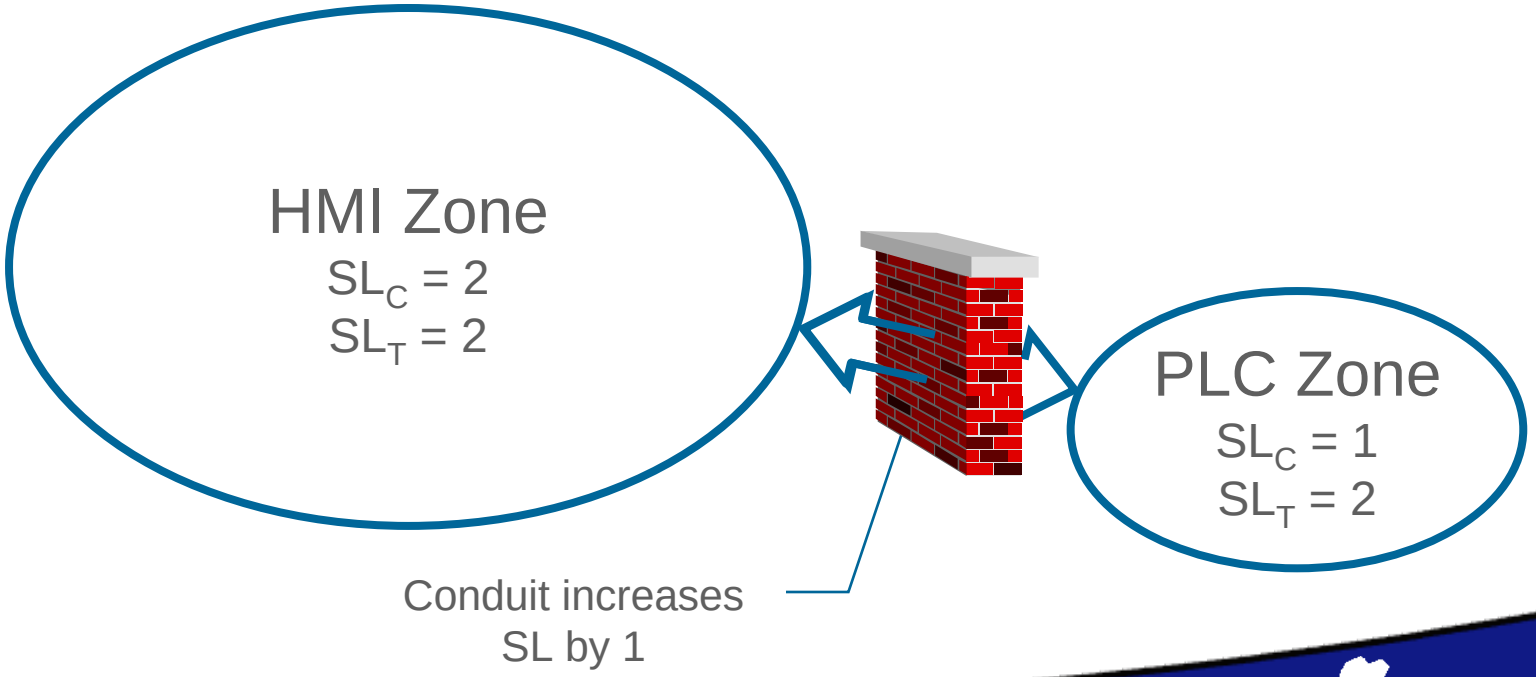
- A zone will require a **Security Level Target (SL_T)** based on factors such as criticality and consequence.
- Equipment in a zone will have a **Security Level Capability (SL_C)**
- If they are not equal you need to add security technology and/or policy to make them equal.

Security Targets vs. Capabilities

- Example: The security level capabilities (SL_C) of a zone full of Windows XP-based HMIs is typically greater than:
  - a zone of Windows NT servers
  - a zone with PLCs
- BUT they may have the same SL_T .
- Securing the whole control system to the level needed by PLCs and NT Servers can be expensive:
  - Complex process edge VPNs and firewalls…
  - Wholesale replacement…
  - Firewalls for each device…

Saving Money with Zones and Conduits

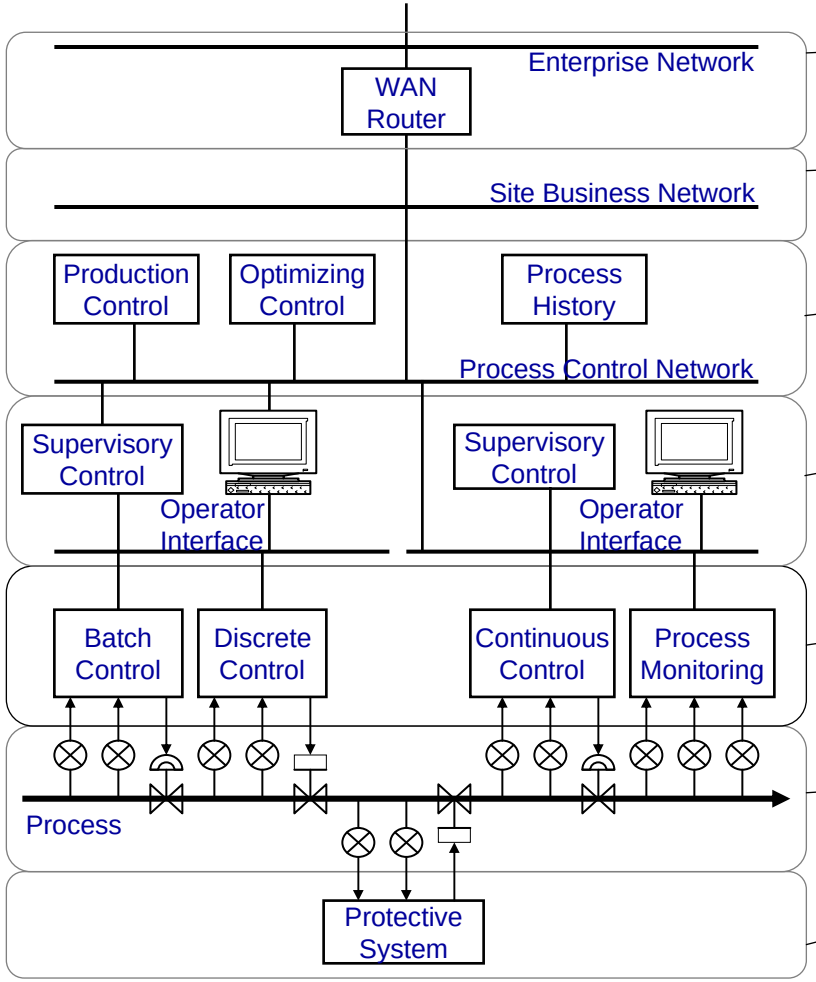
- Solution: Separate the PLCs and NT servers into their own zones and focus on securing each zone with a conduit.



Process Control Systems
Industry Conference

A Control System Security Solution

Traditional Hierarchical Model



Level 5 - Enterprise

Level 4 - Site Business Planning

Level 3 - Site Manufacturing Operations

Level 2 - Area Supervisory Control

Level 1 - Basic Process Control

Level 0 - Field Instrumentation

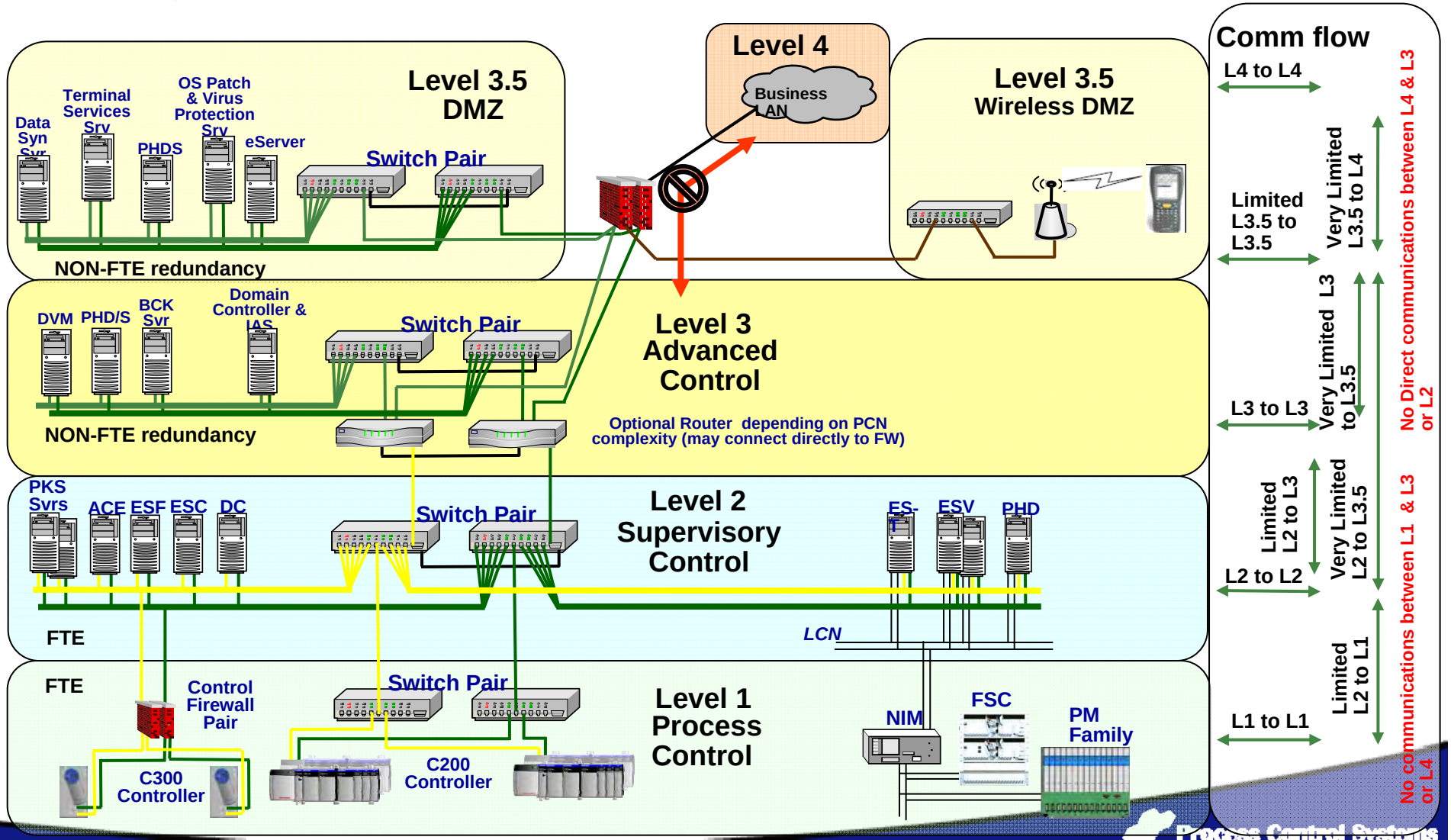
Safety-Critical
- Protective Systems
- Safety Instrumented Systems

Copyright © 2004 ISA

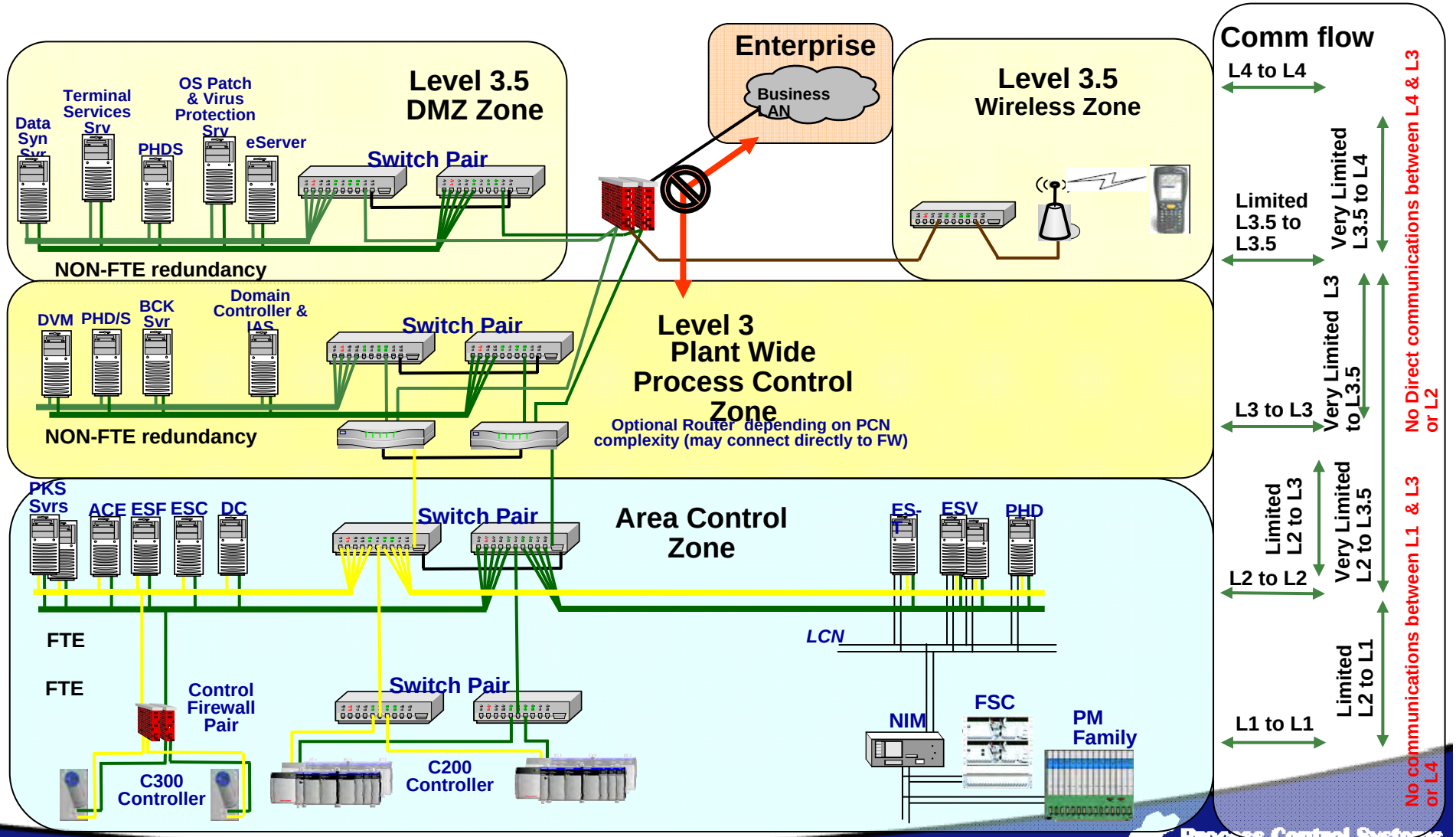
Hierarchical Network Strategy

- Layered network topology
  - Most critical layers deeper in the topology
  - Provides more layers of protection
- Compartmentalize components and data
  - Limits network traffic to where it is needed
  - Creates Security Zones and defines Conduits between those Zones
- Firewall between level 3 and level 4
  - Logical break between PCN and Enterprise Network
- DMZ between level 3 and level 4
  - Well known IT strategy

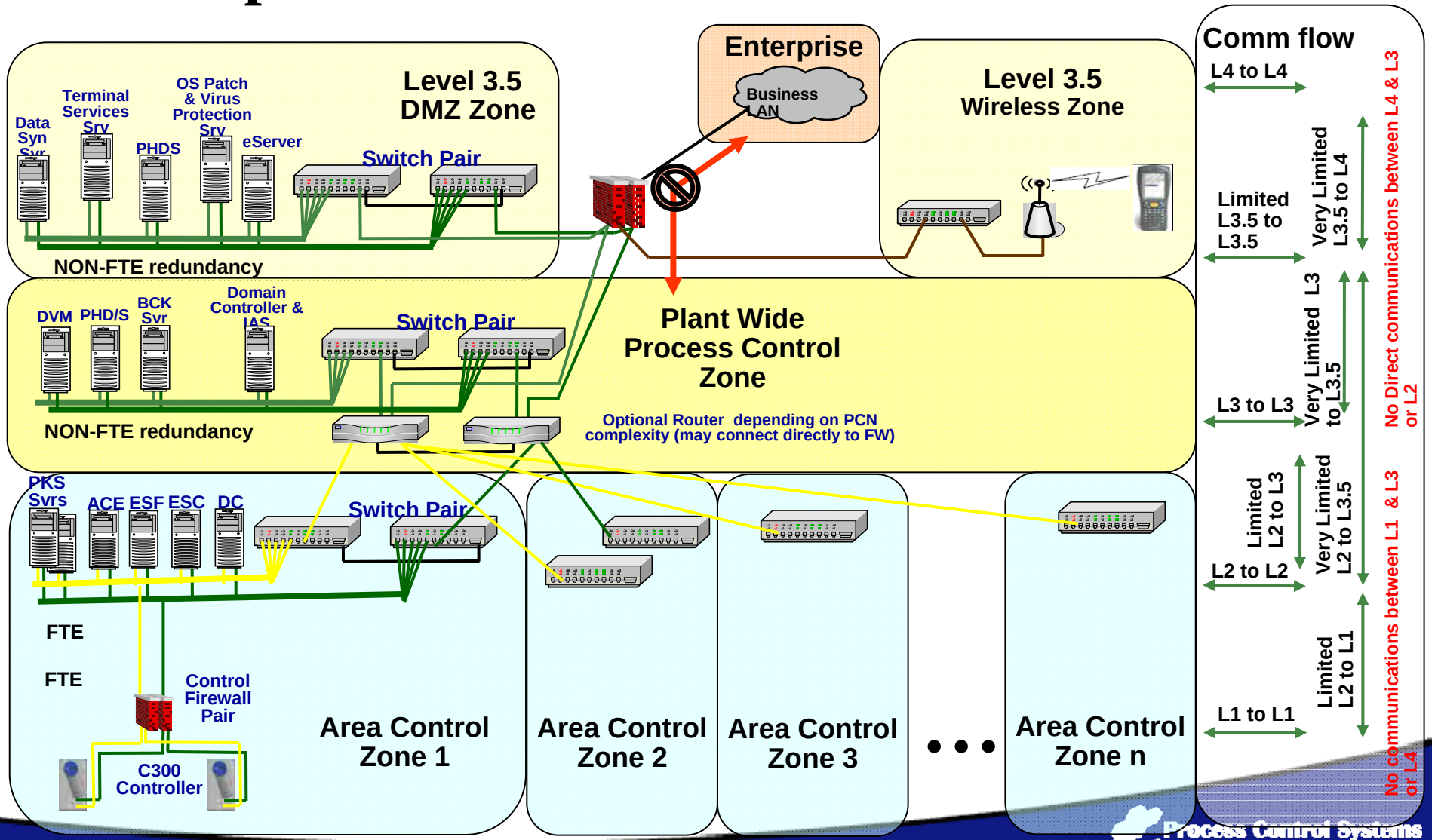
High Security Network Architecture



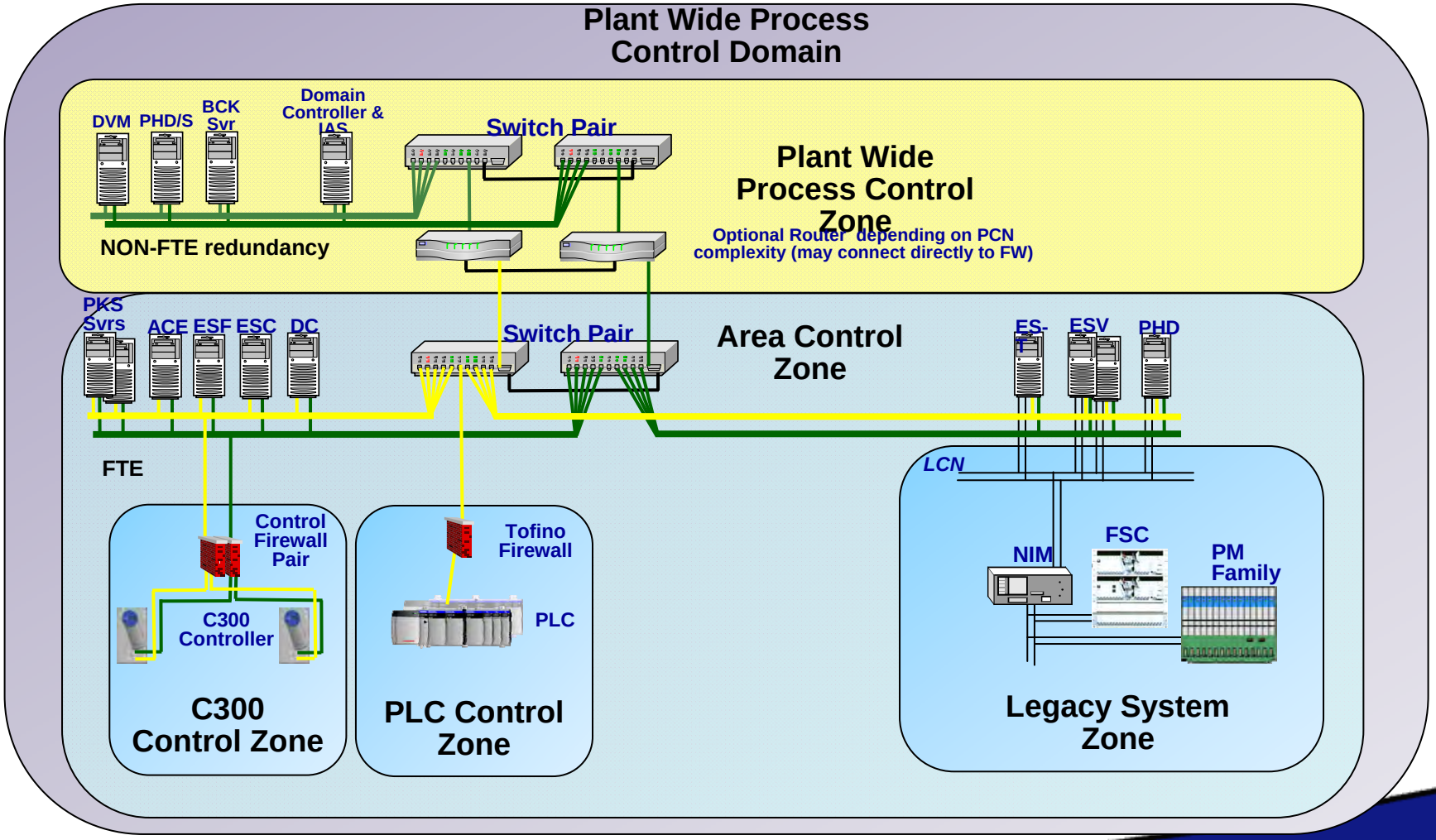
Network Architecture as Zones



Multiple Area Control Zones



Zones within Zones



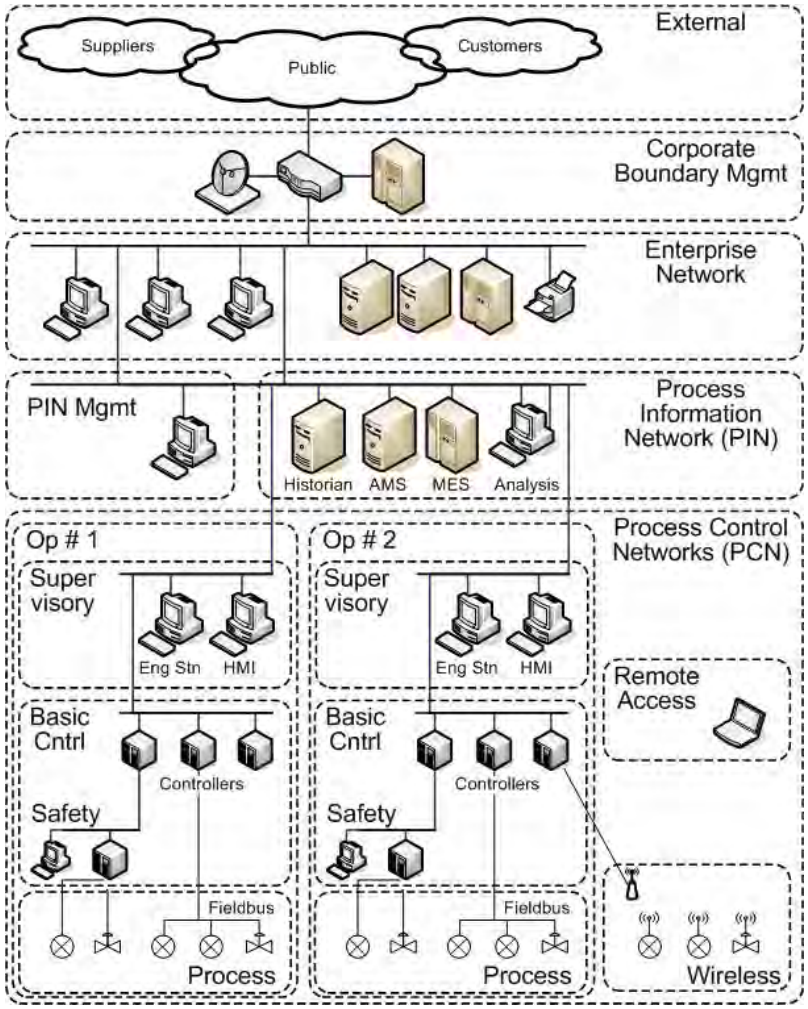
Zone Communication Rules

- **Communication traverses zones through an interface at a higher network level**
  - Example:
    - C300 zone connects at Level 2
    - PLC zone connects at Level 2
    - Area control zones connect at Level 3
    - Process Control Domain Zone connects at Level 4 firewall

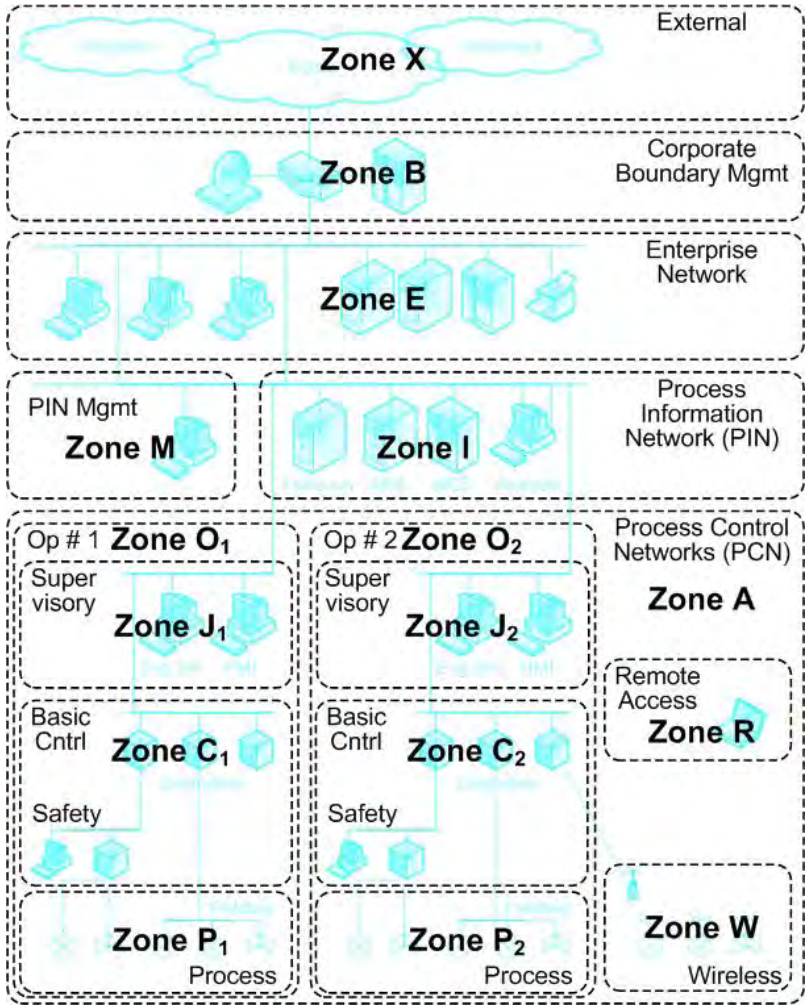
Process Control Systems
Industry Conference

A Security Case History in a Refinery

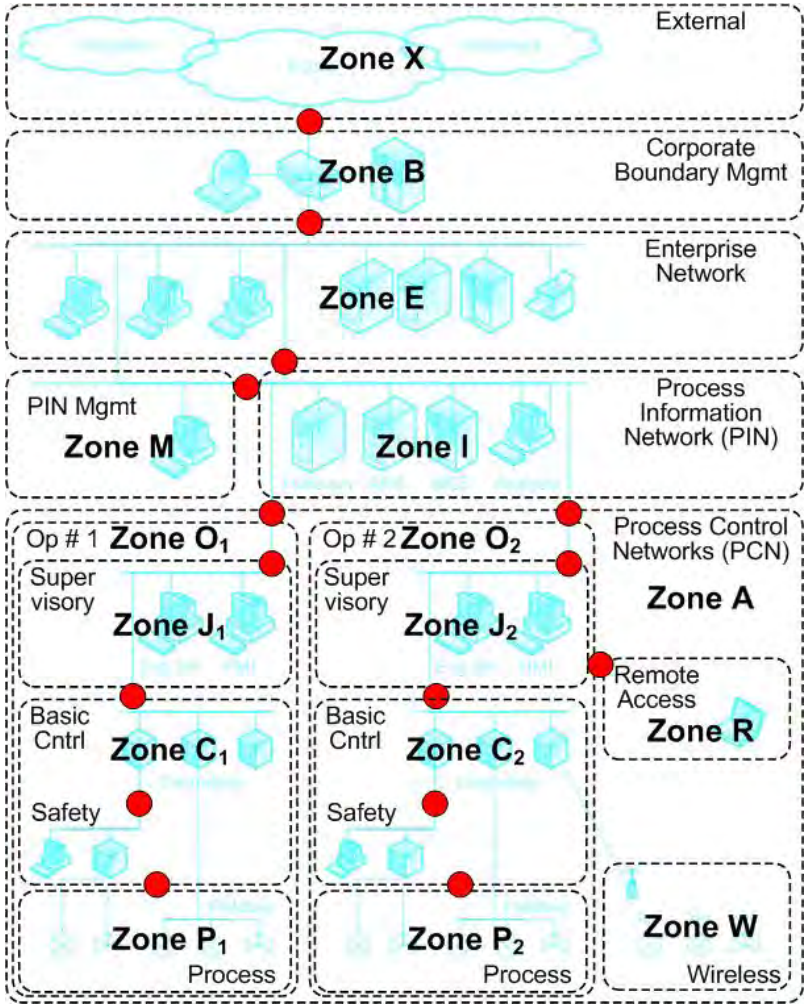
Using Zones: A Refinery Example



Specifying the Zones (1st Pass)



Adding the Conduits (1st Pass)



A Risk Analysis of the Operational Zone

Threat	Vulnerability	Possible Threat Source	Skill Level	Potential Consequence	Severity	Likelihood	Risk
Release of hazardous product	Manipulate control system	Organized Crime, Activist	Intermediate	Major Injury Complaints or Local Community Impact	Medium	Low	Low-Risk
	Disable/manipulate emergency shutdown	Terrorist, Organized Crime, Activist	High	Fatality or Major Community Incident	High	Very Low	Low-Risk
Process reactivity incident	Manipulate control system	Domestic or Foreign Terrorist, Disgruntled Employee	Intermediate	Lost Workday or Major Injury Complaints or Local Community Impact	Medium	Low	Low-Risk
	Disable/manipulate emergency shutdown	Domestic or Foreign Terrorist	High	Fatality or Major Community Incident	High	Very Low	Low-Risk
Process shutdown	Trip emergency shutdown	Malware, Novice Hacker	Low	Shutdown > 6 Hours	Medium	High	High-Risk
	Cause Loss of View of SIS	Malware, Novice Hacker	Low	Shutdown > 6 Hours	Medium	High	High-Risk
	Manipulate control system	Hacker, Disgruntled Employee	Intermediate	Shutdown > 6 Hours	Medium	Medium	Medium-Risk
	Disable PCN communications	Malware, Novice Hacker	Low	Shutdown < 6 Hours	Low	High	Medium-Risk
	Spoof operators	Hacker, Disgruntled Employee	Intermediate	Shutdown < 6 Hours	Low	Medium	Low-Risk

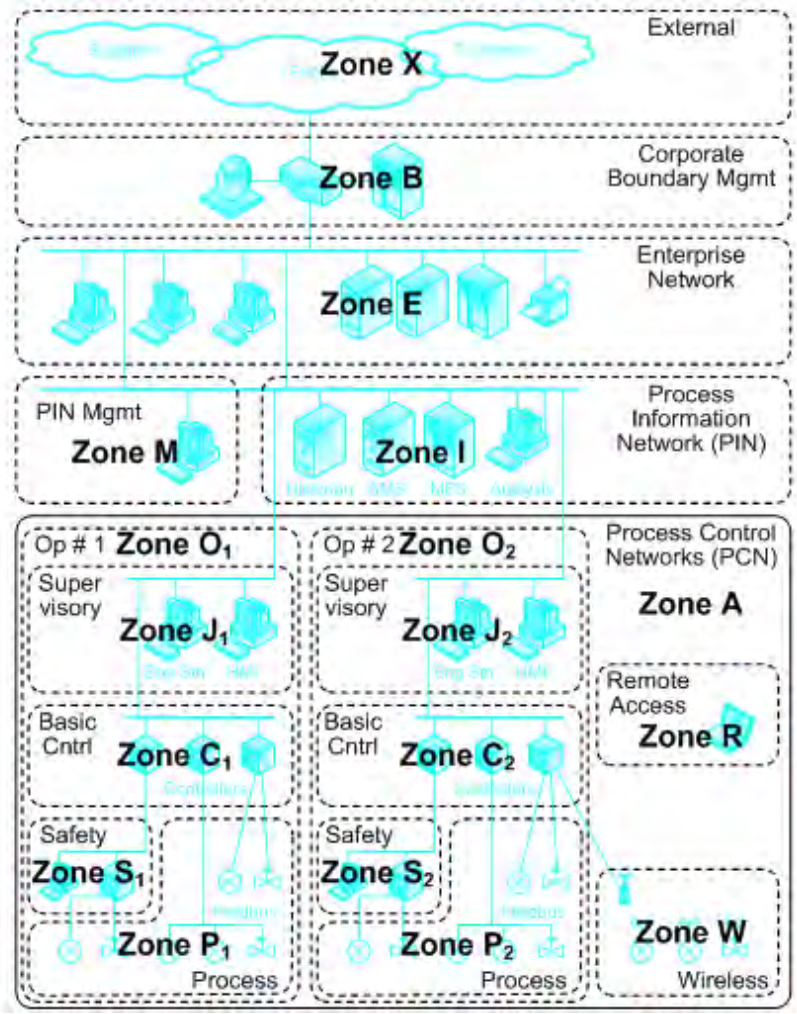
Isolating the High Risk Vulnerabilities

Threat	Vulnerability	Possible Threat Source	Skill Level	Potential Consequence	Severity	Likelihood	Risk
Release of hazardous product	Manipulate control system	Organized Crime, Activist	Intermediate	Major Injury Complaints or Local Community Impact	Medium	Low	Low-Risk
	Disable/manipulate emergency shutdown	Terrorist, Organized Crime, Activist	High	Fatality or Major Community Incident	High	Very Low	Low-Risk
Process reactivity incident	Manipulate control system	Domestic or Foreign Terrorist, Disgruntled Employee	Intermediate	Lost Workday or Major Injury Complaints or Local Community Impact	Medium	Low	Low-Risk
	Disable/manipulate emergency shutdown	Domestic or Foreign Terrorist	High	Fatality or Major Community Incident	High	Very Low	Low-Risk
Process shutdown	**Trip emergency shutdown**	**Malware, Novice Hacker**	**Low**	**Shutdown > 6 Hours**	**Medium**	**High**	**High-Risk**
	Cause Loss of View of SIS	**Malware, Novice Hacker**	**Low**	**Shutdown > 6 Hours**	**Medium**	**High**	**High-Risk**
	Manipulate control system	Hacker, Disgruntled Employee	Intermediate	Shutdown > 6 Hours	Medium	Medium	Medium-Risk
	Disable PCN communications	Malware, Novice Hacker	Low	Shutdown < 6 Hours	Low	High	Medium-Risk
	Spoof operators	Hacker, Disgruntled Employee	Intermediate	Shutdown < 6 Hours	Low	Medium	Low-Risk

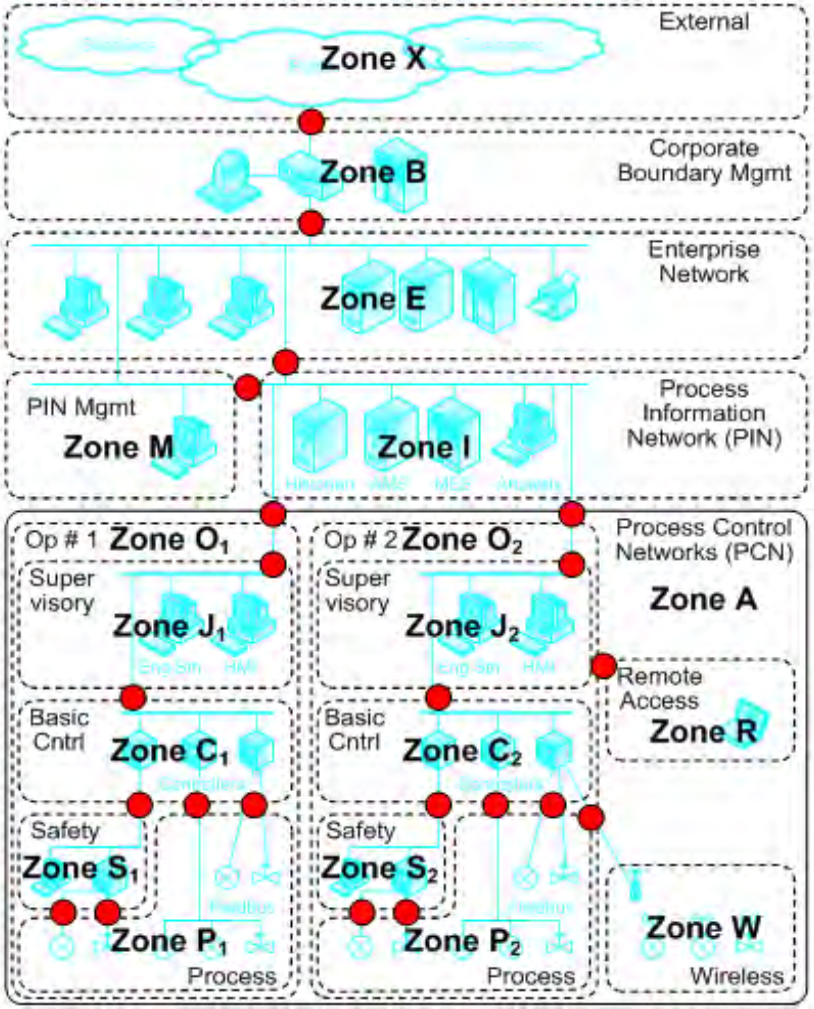
Solution: A Protected SIS Zone

- The solution was to separate Safety Integrated System (SIS) zone from the process control system zone.

Specifying the Zones (2nd Pass)



Adding the Conduits (2nd Pass)



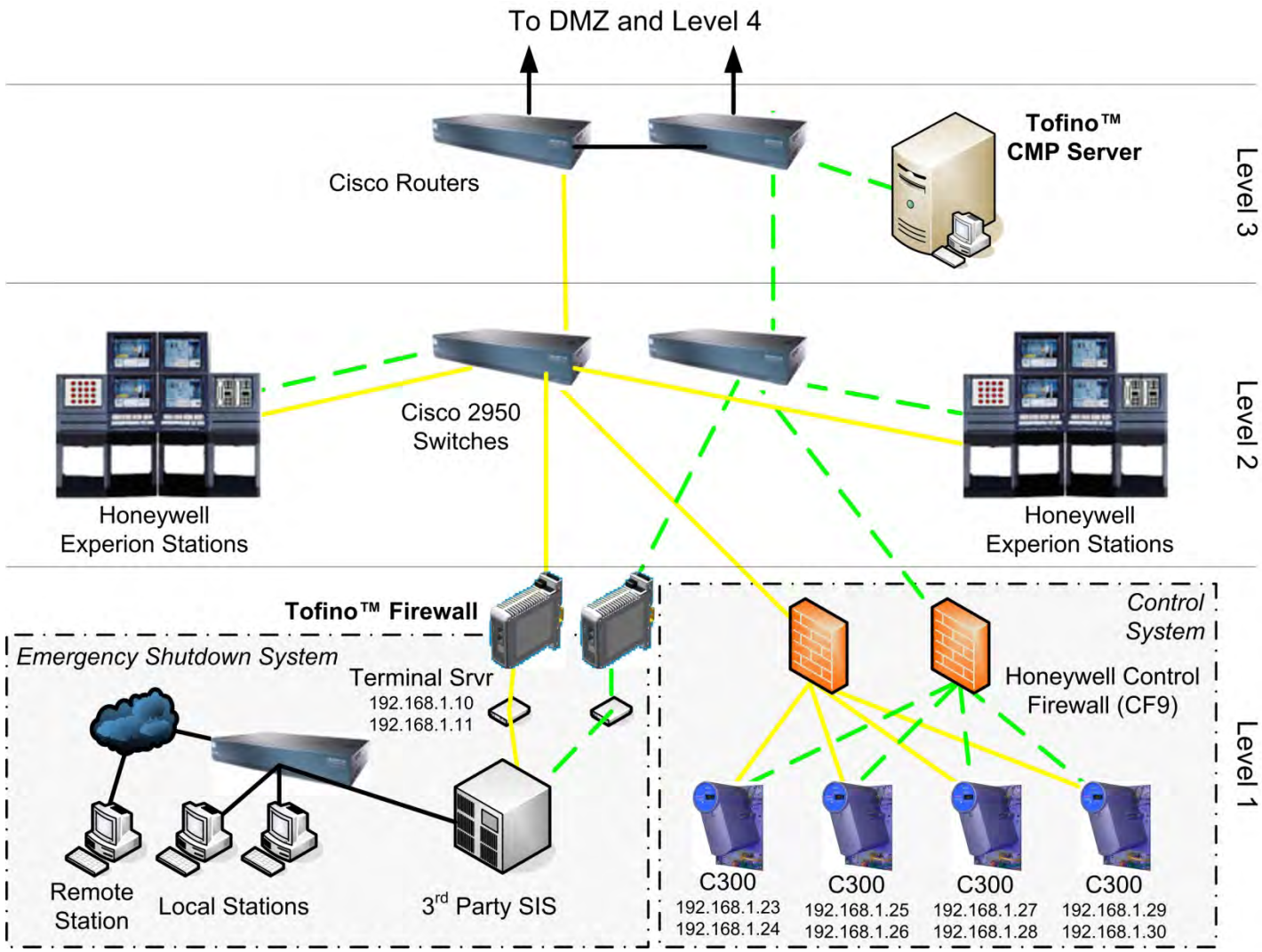
Solution: Managing the SIS Zone Conduits

- Security on the conduit between the Basic Control zone and the SIS zones was then needed.
- The solution was a MODBUS Industrial Firewall between the two zones.
- Two options available – preconfigured and configurable FW.
- In this case configurable was selected.

Why a MODBUS/TCP Industrial Firewall?

- Designed specifically for MODBUS/TCP traffic.
- Hardened for industrial environments:
  - Temperature -40C to 70C - Zone 2
  - Dual Power Supply - 27 Year MTBF
- Ease of installation - field technicians only:
  - Attach the firewall to the DIN Rail
  - Attach instrument power
  - Plug in network cables
- Completely transparent to the process network on startup and will not disrupt operations.

The Protected SIS Zone Architecture

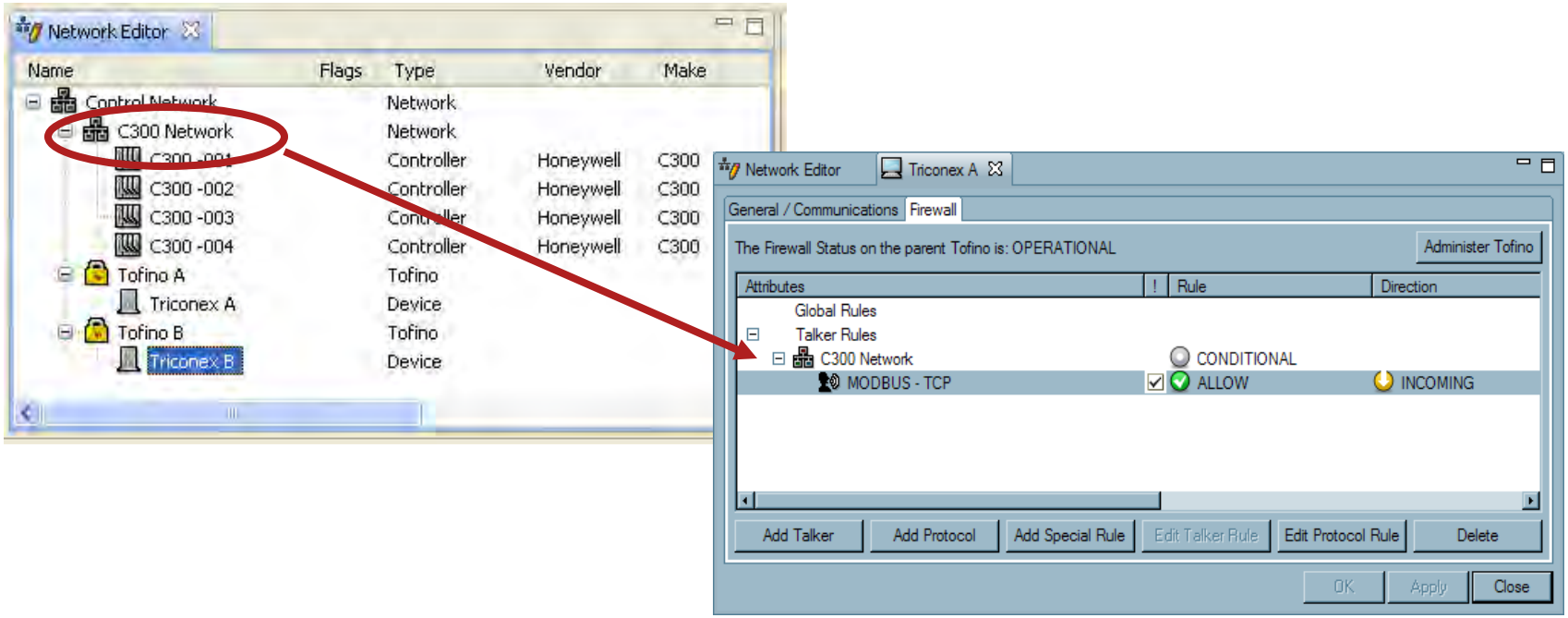


Some Configuration Specifics - Redundancy

- Two Firewalls were connected between the Triconex™ terminal servers and the Level 2 Ethernet switches, providing redundant connections between the ESD system and control system.
- The fact that the firewalls offered bridging mode rather than traditional routing simplified this configuration greatly.

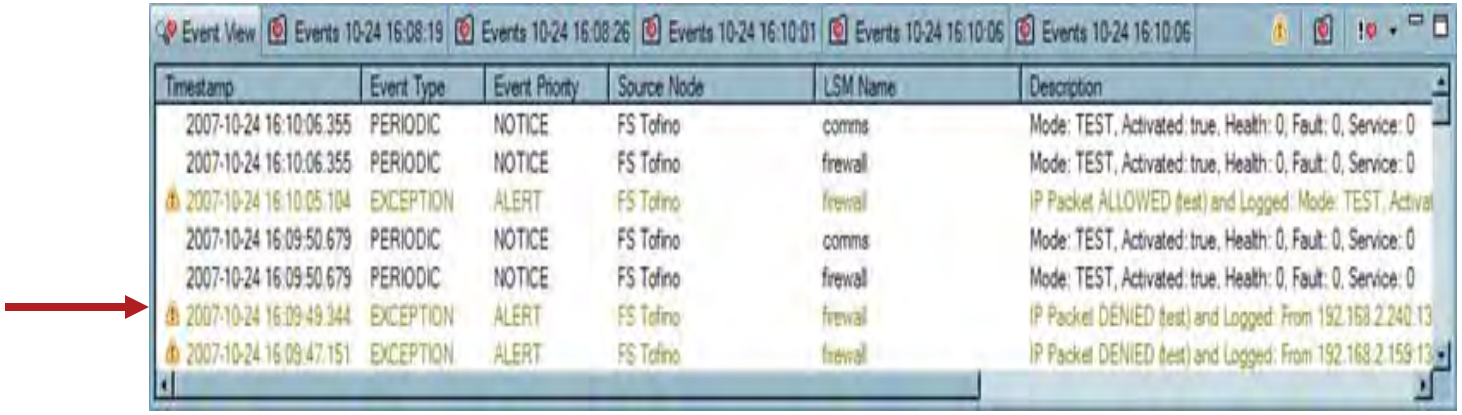
Simplifying Multiple Device Rule Sets

- Grouping of similar devices into “networks” simplified rule creation for common rule management



Managing Nuisance Alarms from Multicasts

- Windows “multicast” traffic created a significant amount of Nuisance traffic on the control network.
- These needed to be silently dropped

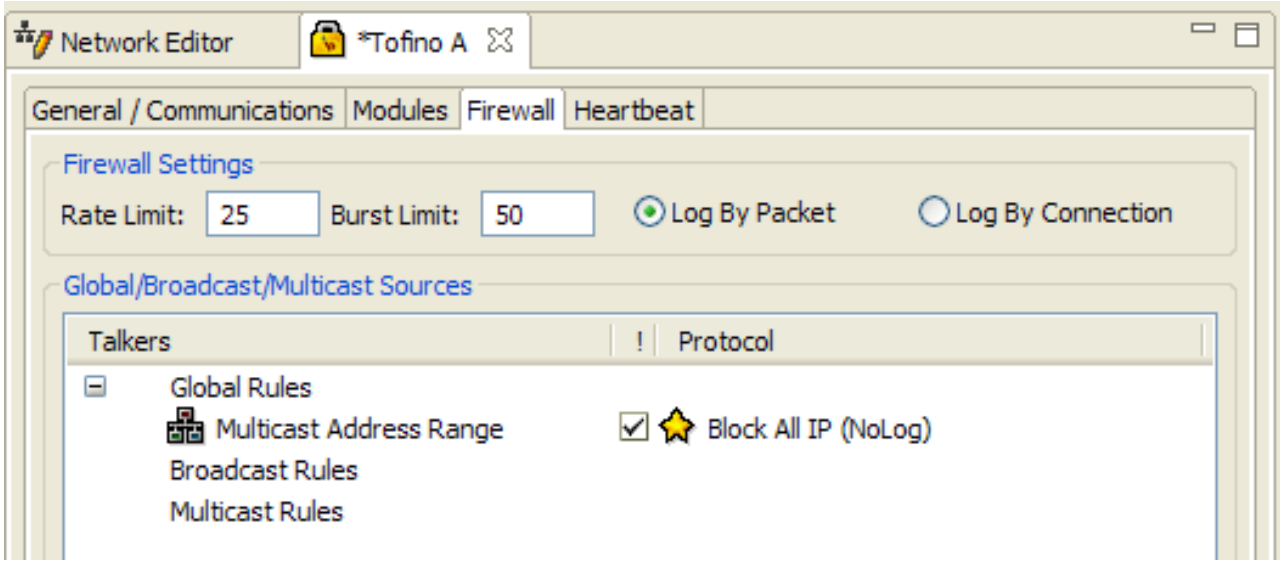


Event View | Events 10-24 16:08:19 | Events 10-24 16:08:26 | Events 10-24 16:10:01 | Events 10-24 16:10:06 | Events 10-24 16:10:06

Timestamp	Event Type	Event Priority	Source Node	LSM Name	Description
2007-10-24 16:10:06.355	PERIODIC	NOTICE	FS Tofino	comms	Mode: TEST, Activated: true, Health: 0, Fault: 0, Service: 0
2007-10-24 16:10:06.355	PERIODIC	NOTICE	FS Tofino	firewall	Mode: TEST, Activated: true, Health: 0, Fault: 0, Service: 0
2007-10-24 16:10:05.104	EXCEPTION	ALERT	FS Tofino	firewall	IP Packet ALLOWED (test) and Logged: Mode: TEST, Activat
2007-10-24 16:09:50.679	PERIODIC	NOTICE	FS Tofino	comms	Mode: TEST, Activated: true, Health: 0, Fault: 0, Service: 0
2007-10-24 16:09:50.679	PERIODIC	NOTICE	FS Tofino	firewall	Mode: TEST, Activated: true, Health: 0, Fault: 0, Service: 0
2007-10-24 16:09:49.344	EXCEPTION	ALERT	FS Tofino	firewall	IP Packet DENIED (test) and Logged: From 192.168.2.240:13
2007-10-24 16:09:47.151	EXCEPTION	ALERT	FS Tofino	firewall	IP Packet DENIED (test) and Logged: From 192.168.2.159:13

Managing Nuisance Alarms from Multicasts

- Assisted rule generation feature proposed a block rule to drop these messages.



Summary

- Security is about maintaining the reliability and safety of a control system (not just keeping hackers out).
- Separation of a process system into zones improves security AND reduces costs.
- Security of safety systems can be significantly improved at little cost with industrial firewalls.

Questions

Eric Byres, P. Eng.
Byres Security Inc.
250 390 1333
eric@byerssecurity.com
http://www.byressecurity.com

Kevin Staggs, CISSP
Engineering Fellow
Global Security Architect
Honeywell Process Solutions
kevin.p.staggs@honeywell.com