

Building Intrinsically Secure Control and Safety Systems

**Using ANSI/ISA-99 Security Standards for Improved
Security and Reliability**

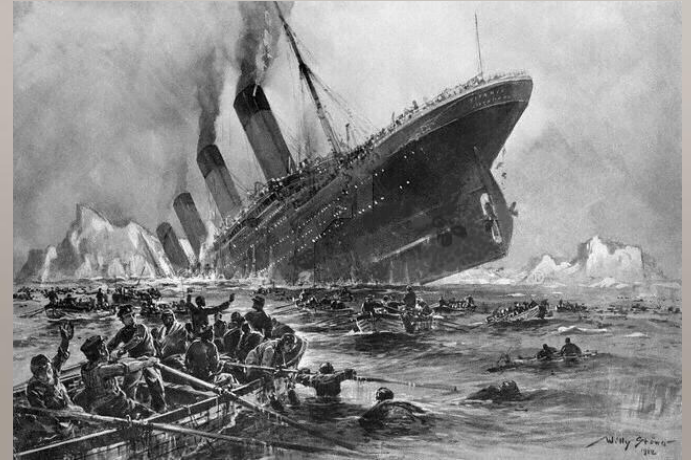
May 2009

Eric Byres, Chief Technology Officer,
Byres Security Inc.

TOFINO™

The Sinking of the Titanic

- On the night of 14 April 1912, Titanic struck an iceberg and sank two hours and forty minutes later.
- One of the contributing factors was that the bulkheads on *Titanic* 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’. The facility remained offline for 2 days.
 - Redundant drives controlling the recirculating water system failed due to “excessive traffic” on the control systems network.
 - Traffic between two different vendors’ control products was likely the cause.

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 with a PC on one of the primary **control networks**.
 - The software update was designed to **synchronize data on both systems**.
 - When the updated business computer rebooted, it reset the data on the control system computer.
 - Safety systems interpreted the lack of data as a drop in water reservoirs that cool the plant's nuclear fuel rods, and triggered a shutdown.

Lodz Tram System Security Incident

- **January 8, 2008** – Teenage boy ‘hacks’ into the track control system of the Lodz city tram system, derailing four vehicles.
 - He had adapted a television remote control so it could change track switches.
- Notice that the “Internet” is not involved...



What does the Titanic and these Control System Events have in Common?

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

The Nuclear Regulatory Commission's View...

- *“The August 19, 2006, Brown’s Ferry 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

What Makes a System Unsafe and Unreliable?

- A failure to contain communications in appropriate areas or sub-systems.
- Issues in one area can migrate to another area due to poor (or non-existent) separation strategy.
- Not Unusual... The North American Electrical Reliability Council (NERC) lists their #2 vulnerability in control systems as:
 - “*Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms*”
- The solution is the use of ***security zones***.

Addressing Flawed Design: Using ANSI/ISA-99 Standards

- Understand Zones and Conduits
- Security Levels

ANSI/ISA-99: Dividing Up The Control System

- A core concept in the new ANSI/ISA-99 security standard is “Zones and Conduits”
- Offers a level of segmentation and traffic control inside the control system.
- Control networks divided into layers or zones based on control function.
- Multiple separated zones help to provide “***defense in depth***”.

ANSI/ISA-99: Connecting the Zones

- Connections between the zones are called conduits, and these must have security controls to:
 - Control access to zones
 - Resist Denial of Service (DoS) attacks or the transfer of malware
 - Shield other network systems
 - Protect the integrity and confidentiality of network traffic
- It is important to understand and manage all your conduits between zones, not just the obvious ones.

Security Zone Definition

- “Security zone: grouping of logical or physical assets that share common security requirements”.
[ANSI/ISA-99.01.01–2007- 3.2.116]
 - A zone has a clearly defined border (either logical or physical), which is the boundary between included and excluded elements.



HMI Zone

Controller Zone

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

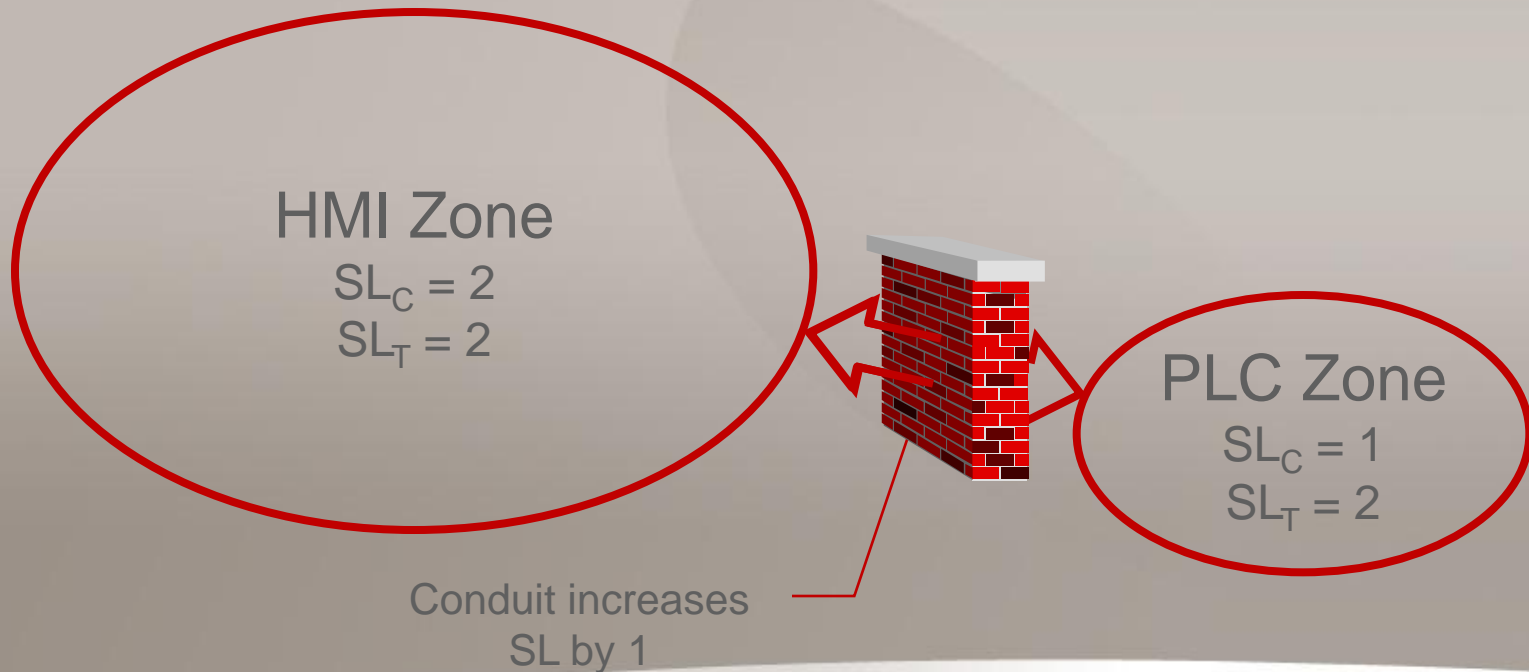
- A zone will require a Security Level Target (SL_T) based on factors such as criticality and consequence.
- Equipment in a zone will have a Security Level Capability (SL_C).
- If they are not equal you need to add security technology and/or policy to make them equal.

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.



Addressing Flawed Configurations

- **Oops – I forgot that dash**

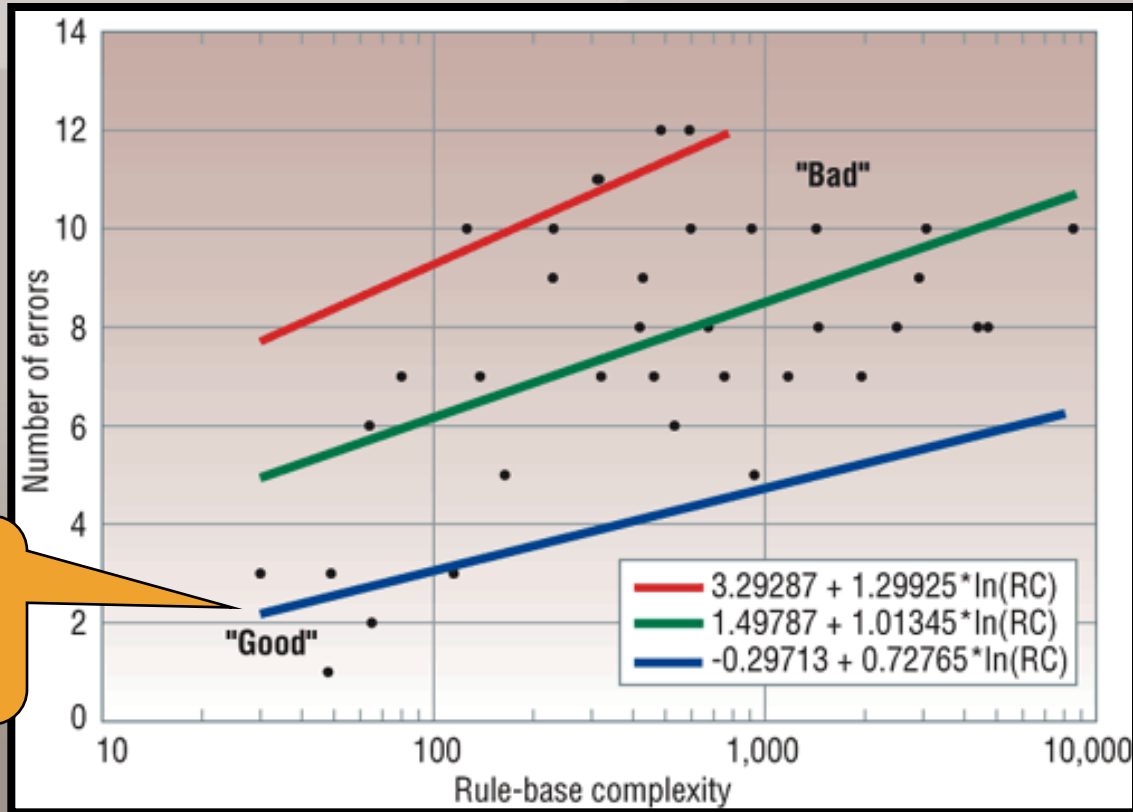
A Few Incorrectly Configured Firewalls...

- Study of 37 firewalls from financial, energy, telecommunications, media, automotive, and security firms...

“Almost 80 percent of firewalls allow both the “Any” service on inbound rules and insecure access to the firewalls. These are gross mistakes by any account.”

A quantitative study of firewall configuration errors“
Avishai Wool, " IEEE Computer Magazine,
IEEE Computer Society, June 2004

A Few Incorrectly Configured Firewalls...



Only 5 out of 37 Good Firewalls?

The Firewalls are just fine but...

- Commands for creating firewall rules are too complex. For example:

```
acl 201 permit tcp any eq 80 10.20.30.0 0.0.0.255 gt 1023  
established
```

(Cisco PIX)

```
$IPT -A PCN_DMZ -p tcp --dport ! $DH_PORT -j  
LOG_PCN_DMZ
```

(Linux iptables)

- This leads to security mistakes

More Firewall Rules

- Even an ACL for a “simple” home router is complex:

TRENDnet 54Mbps 802.11g Wireless Router
TEW-432BRP

Firewall Rule [HELP](#)

Enable Enable Disabled

Name

Action Allow Deny

	Interface	IP Range Start	IP Range End	Protocol
Source	LAN	<input type="text"/>	<input type="text"/>	TCP
Destination	LAN	<input type="text"/>	<input type="text"/>	<input type="text"/>

Action	Name	Source	Destination	Protocol
<input checked="" type="checkbox"/> Allow	MsnMsgr (192.168.1.100:7207) 60381	LAN,192.168.1.100	WAN,*	UDP,7207-60381
<input checked="" type="checkbox"/> Allow	Virtual Server FTP	WAN,*	LAN,192.168.1.1	TCP,21
<input checked="" type="checkbox"/> Allow	Modbus	WAN,*	LAN,192.168.1.1	TCP,502
<input checked="" type="checkbox"/> Allow	Port 8080	WAN,*	LAN,192.168.1.1	TCP,8080
<input checked="" type="checkbox"/> Allow	Allow to Ping WAN port	WAN,*	WAN,*	ICMP,

Requirements in the Controls World

- *"Certainly controls engineers and operators need to be security aware, but they should not all need to be security experts."*
- *"The only way this is going to happen is if we rework IT security technologies and concepts into something that makes sense to our world of industrial control."*
- *"We have to make this [security] something a plant superintendent, engineer, or senior operator can do in their spare time, or it will flop."*

ISA-S99 Discussion Forum

Solution: Making Field Deployment Simple

- Zero Configuration Field Deployment Model
- Field technician should do no more than:
 - Attach the firewall to the DIN Rail
 - Attach instrument power
 - Plug in network cables
 - Walk away...
- Firewall should be completely transparent to the process network on startup.

Solution: Control Engineer Friendly

- When needed, rule creation must be intuitive

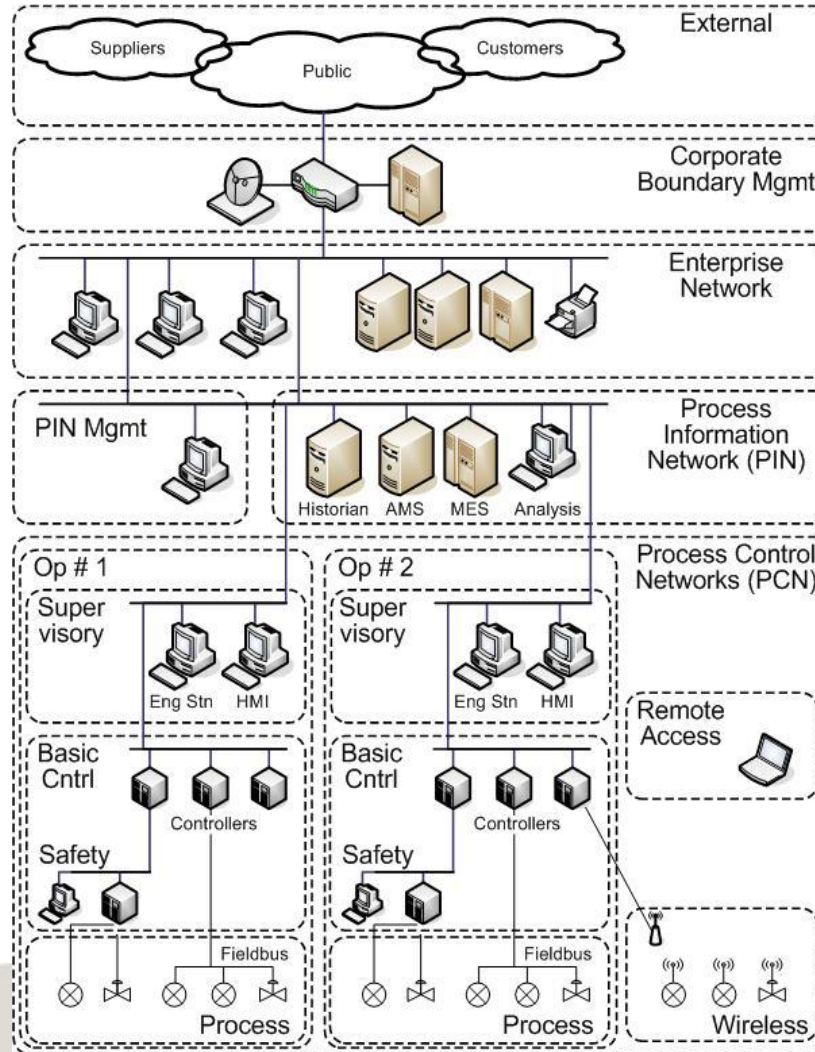
The screenshot shows the 'Network Editor' window for 'FS-PLC-0001' with the 'Firewall' tab selected. The status is 'OPERATIONAL'. A tree view on the left shows 'Communicating Devices' expanded to 'FS-HMI-0001', which has sub-items for 'ICMP PING' and 'MODBUS - TCP'. A table in the center lists these items with their respective rules and directions. A red callout box points to the 'FS-HMI-0001' entry in the tree view.

Attributes	Rule	Direction
Special Rules		
Global Overrides		
ICMP PING	CONDITIONAL	BIDIRECTIONAL
MODBUS - TCP	CONDITIONAL	INCOMING
Communicating Devices		
FS-HMI-0001	CONDITIONAL	BIDIRECTIONAL
ICMP PING	DENY	BIDIRECTIONAL
MODBUS - TCP	ALLOW	INCOMING

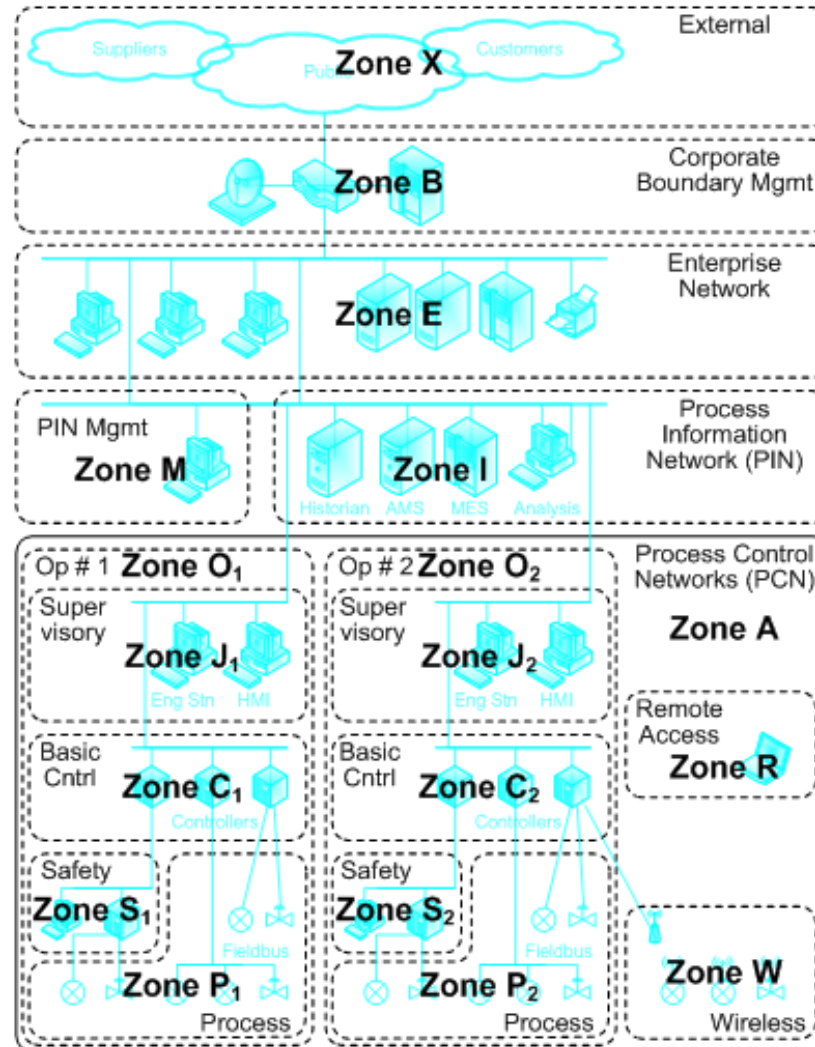
List of devices that can "talk" to a protected device and allowed protocols

Case History: Creating Intrinsically a Secure Safety System

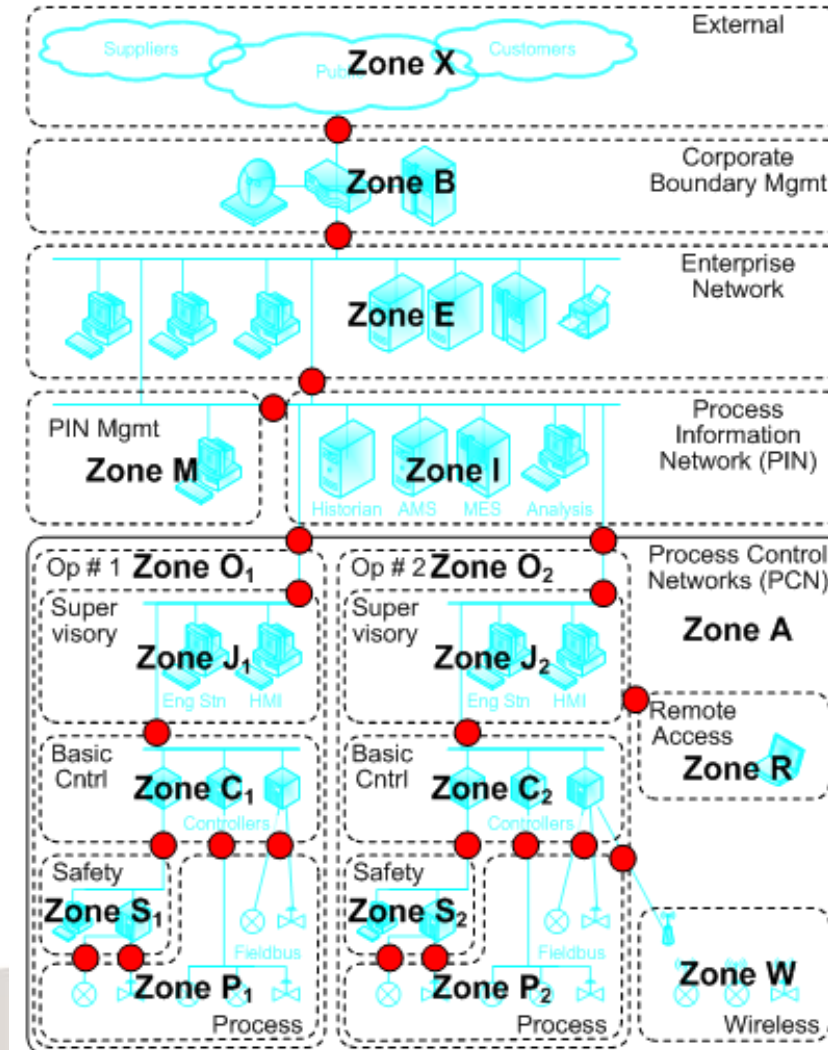
Using Zones: A Refinery Example



Specifying the Zones



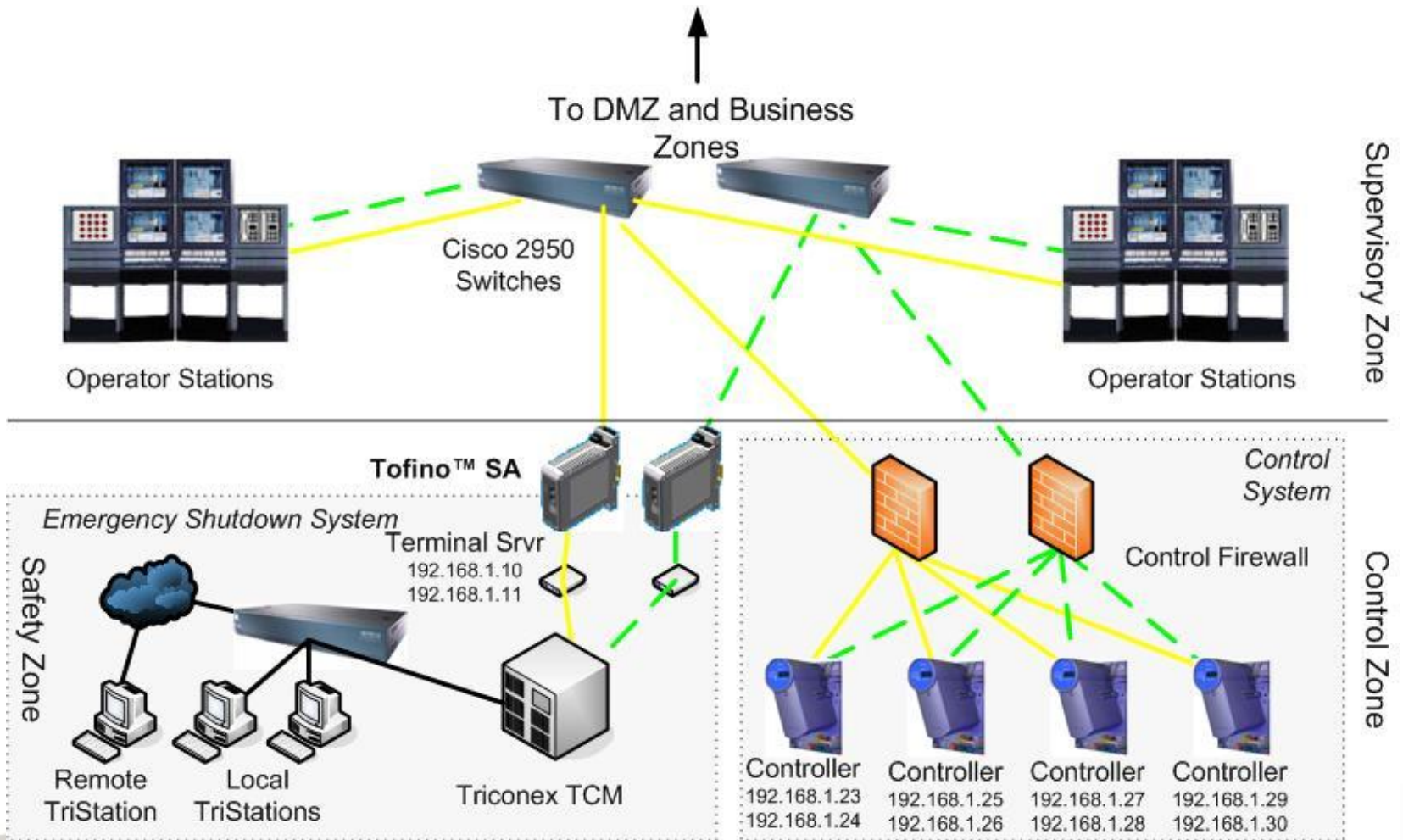
Adding the Conduits



The Need for a Protected SIS Zone

- Risk analysis indicated that there was the potential for common-mode network failures to migrate between the DCS and the Safety Integrated System
- The solution was to:
 - Separate a safety zone from the process control system zone.
 - Define an approved “conduit” between the two zones.
 - Use a Tofino Modbus-TCP Enforcer industrial firewall between the two zones to enforce inter-zone traffic controls.

The Protected SIS Zone Architecture

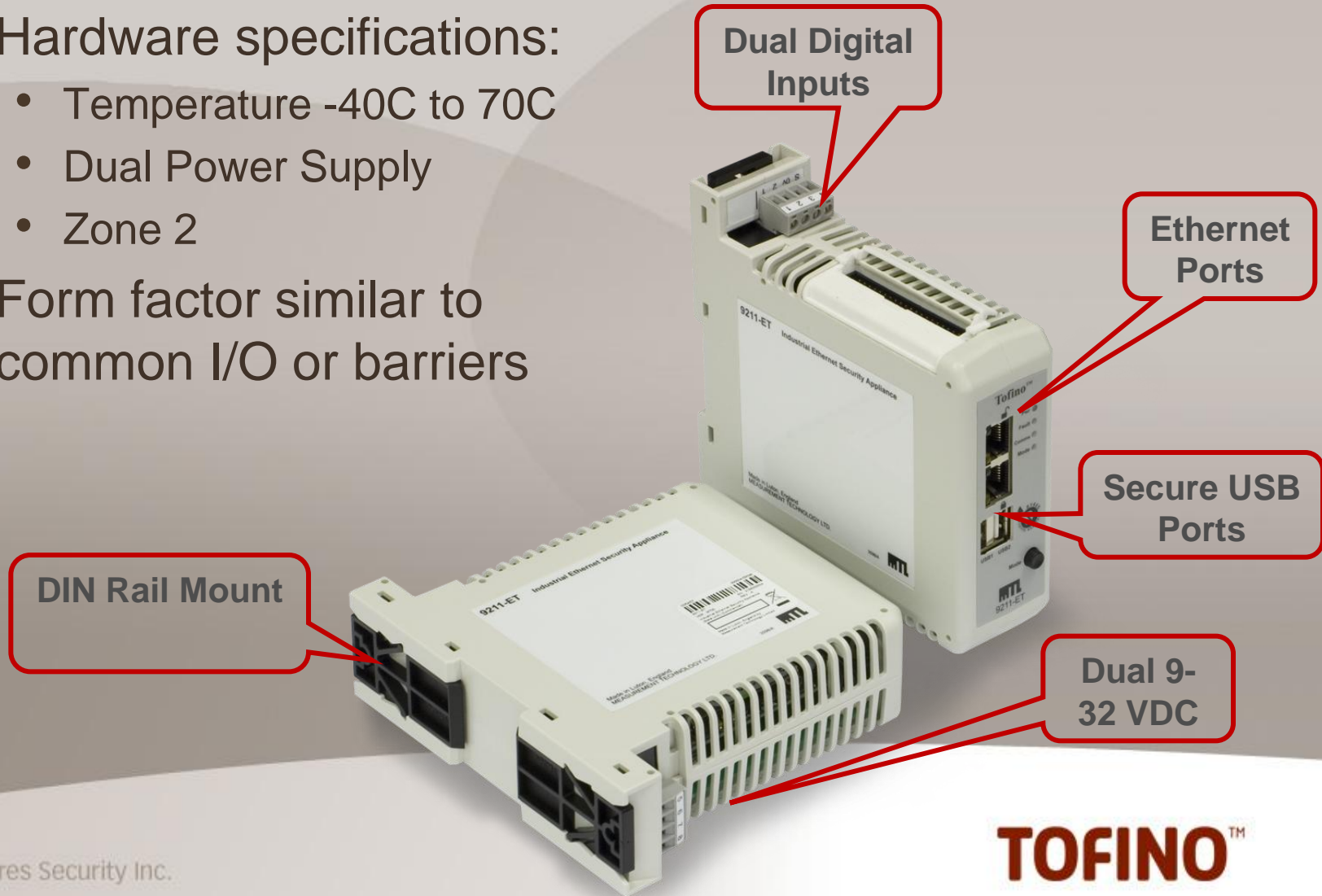


Configuration Specifics - Redundancy

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

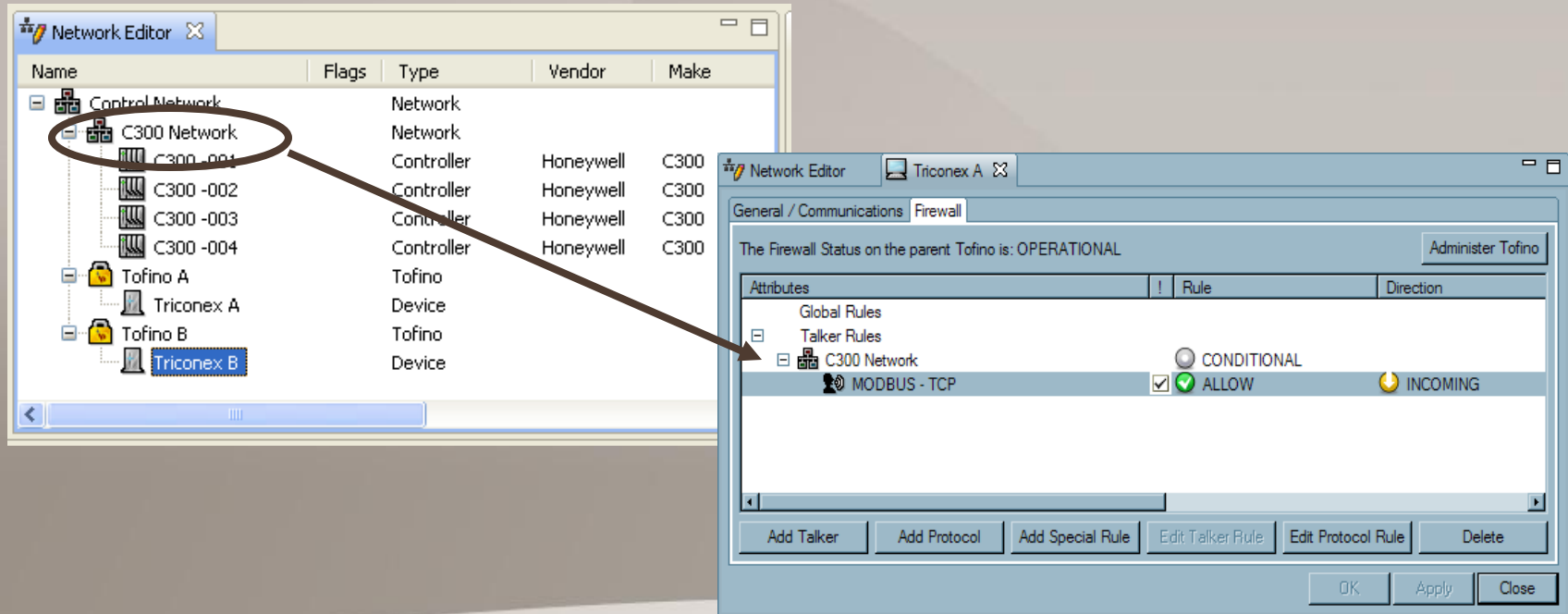
Tofino Security Appliance

- Hardware specifications:
 - Temperature -40C to 70C
 - Dual Power Supply
 - Zone 2
- Form factor similar to common I/O or barriers




Simplifying Multiple Device Rule Sets

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



Managing Multicast Nuisance Traffic

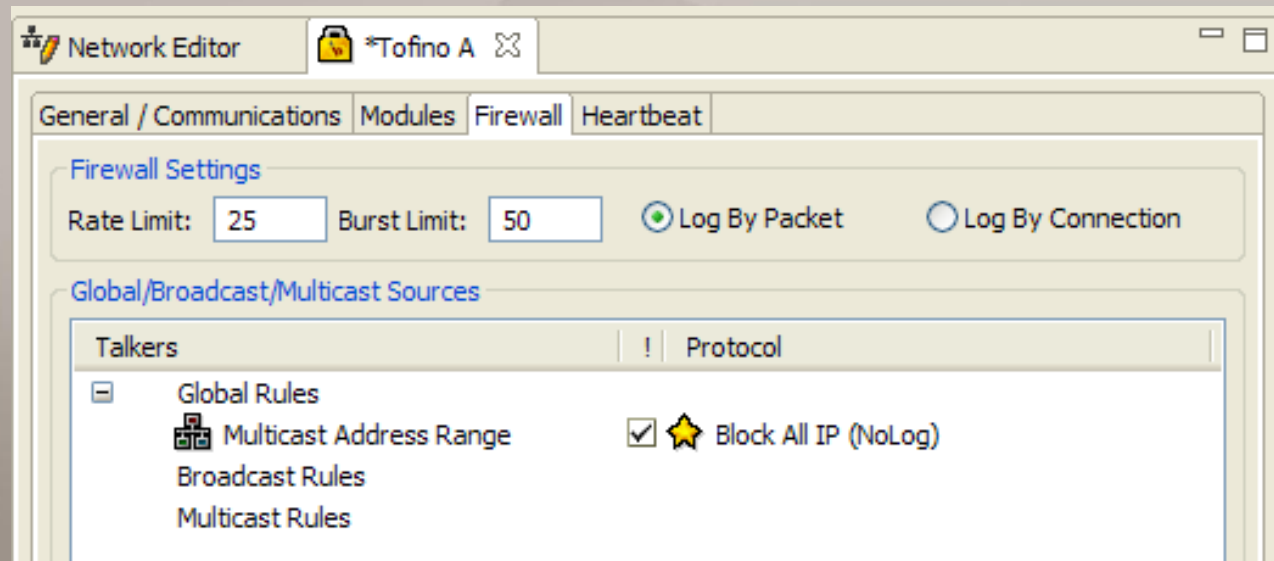
- Tofino Test mode indicated that Windows' "multicast" traffic created a significant amount of nuisance traffic on the safety networks.
- Messages like these were a significant factor in the Brown's Ferry incident.
- Needed to be silently dropped from the network.



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 Multicasts Nuisance Alarms

- Tofino's Assisted Rule Generation (ARG) feature proposed a block rule to drop these messages.



Summary

- Internet-based hackers are the tip of the iceberg of security concerns for industry.
- Easy to focus on stories of hackers and terrorists and miss the real risks posed by lax security design and policy.
- Security is maintaining the reliability and safety of control systems (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.

TOFINOTM

tofinosecurity.com