

Making the Control System Intrinsically Secure

Eric Byres, P.Eng.

CEO

Byres Security Inc.

eric@byressecurity.com

Agenda

- 1. Who Turned Out the Lights?**
Trends in Industrial Cyber Security
- 2. Defence in Depth**
Real-world Solutions for Control Security
- 3. The Tofino Industrial Security Solution**
Creating Intrinsically Secure Control Systems
- 4. Industry Feedback / Questions & Answers**

The Incident in Harrisburg, PA

- ◆ **Oct 2006 -a foreign-based hacker (via Internet) infiltrates the laptop of an employee at the Harrisburg water system.**
- ◆ **Uses the employee's remote access as the entry point into the SCADA system.**
- ◆ **The hacker then installs malware and spyware in a SCADA HMI computer.**

But It Won't Happen to My System...

“Most public utilities rely on a highly customized SCADA system. No two are the same, so hacking them requires specific knowledge”.

Scott Berinato;

“Debunking the Threat to Water Utilities”

CIO Magazine

March 15, 2002

A Few Known Security Incidents in the Water Industry

- Salt River Project SCADA Hack
- Maroochy Shire Sewage Spill
- Software Flaw Makes MA Water Undrinkable
- Trojan/Keylogger on Ontario Water SCADA System
- Viruses Found on Auzzie SCADA Laptops
- Audit/Blaster Causes Water SCADA Crash
- DoS attack on water system via Korean telecom
- Penetration of California irrigation district wastewater treatment plant SCADA.
- SCADA system tagged with message, "I enter in your server like you in Iraq."

A Few Known Security Incidents in the Petroleum Industry

- Electronic Sabotage of Venezuela Oil Operations
- CIA Trojan Causes Siberian Gas Pipeline Explosion
- Anti-Virus Software Prevents Boiler Safety Shutdown
- Slammer Infected Laptop Shuts Down DCS
- Virus Infection of Operator Training Simulator
- Electronic Sabotage of Gas Processing Plant
- Slammer Impacts Offshore Platforms
- SQL Slammer Impacts Drill Site
- Code Red Worm Defaces Automation Web Pages
- Penetration Test Locks-Up Gas SCADA System
- Contractor Laptop Infects Control System

A Few Known Security Incidents in the Chemical Industry

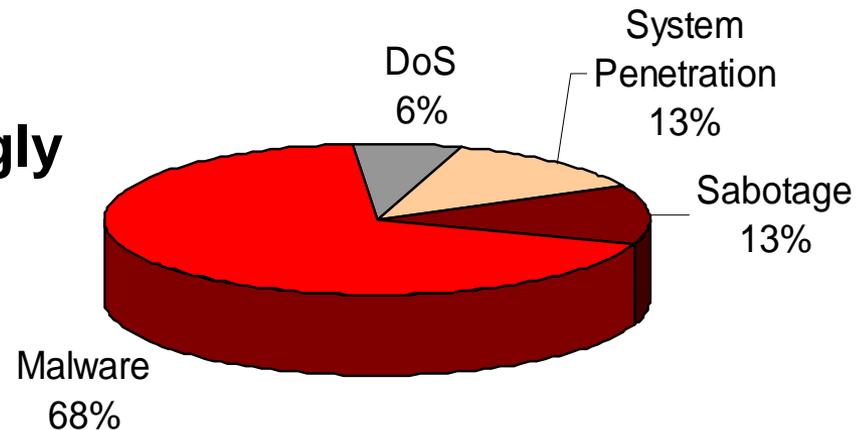
- IP Address Change Shuts Down Chemical Plant
- Hacker Changes Chemical Plant Set Points via Modem
- Nachi Worm on Advanced Process Control Servers
- SCADA Attack on Plant of Chemical Company
- Contractor Accidentally Connects to Remote PLC
- Sasser Causes Loss of View in Chemical Plant
- Infected New HMI Infects Chemical Plant DCS
- Blaster Worm Infects Chemical Plant

A Few Known Security Incidents in the Power Industry

- Slammer Infects Control Central LAN via VPN
- Slammer Causes Loss of Comms to Substations
- Slammer Infects Ohio Nuclear Plant SPDS
- Iranian Hackers Attempt to Disrupt Israel Power System
- Utility SCADA System Attacked
- Virus Attacks a European Utility
- Facility Cyber Attacks Reported by Asian Utility
- E-Tag Forgery Incident in Power PSE
- Power Plant Security Details Leaked on Internet

Incident Types 2002 - 2006

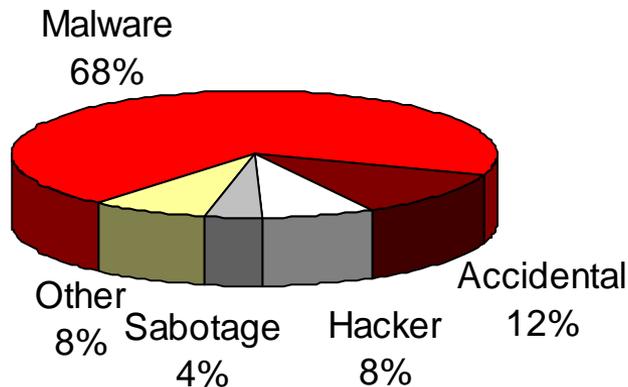
- ◆ Malware accounts for 2/3 of the external incidents on control systems.
- ◆ Appears to match IT trends.
- ◆ However there is a surprisingly large amount of sabotage.



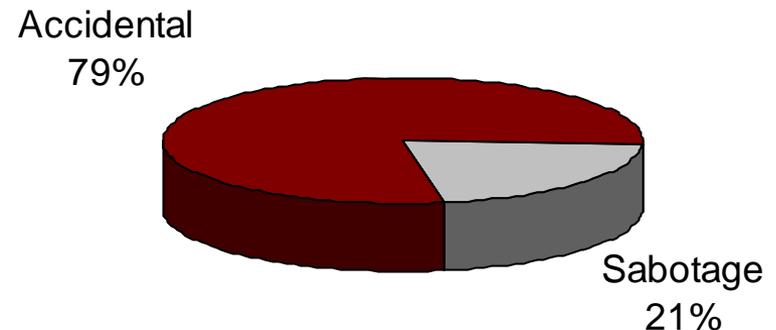
**% of Incident Types
2002 to Sept. 2006**

What Really Hurts?

- ◆ Malware incidents are the most common but aren't the most costly.
- ◆ Control systems are highly susceptible to simple network issues.



Impact < \$100,000



Impact > \$100,000

Risking It All on the Great Wall

The Bastion Model of Security

- ◆ **One possible solution is to install one big firewall between business and the control system.**
- ◆ **This is known as the Bastion Model since it depends on a single fixed point of security.**
- ◆ **Other example of the bastion model:**
 - The Great Wall of China
 - The Maginot Line

So Much for the Firewall...

- ◆ **The Slammer Worm infiltrated a:**

- Nuclear plant via a contractor's T1 line;
- Power utility SCADA system via a VPN;
- Petroleum control system via laptop;
- Paper machine HMI via dial-up modem.

- ◆ **Firewalls existed in at least three of these cases.**

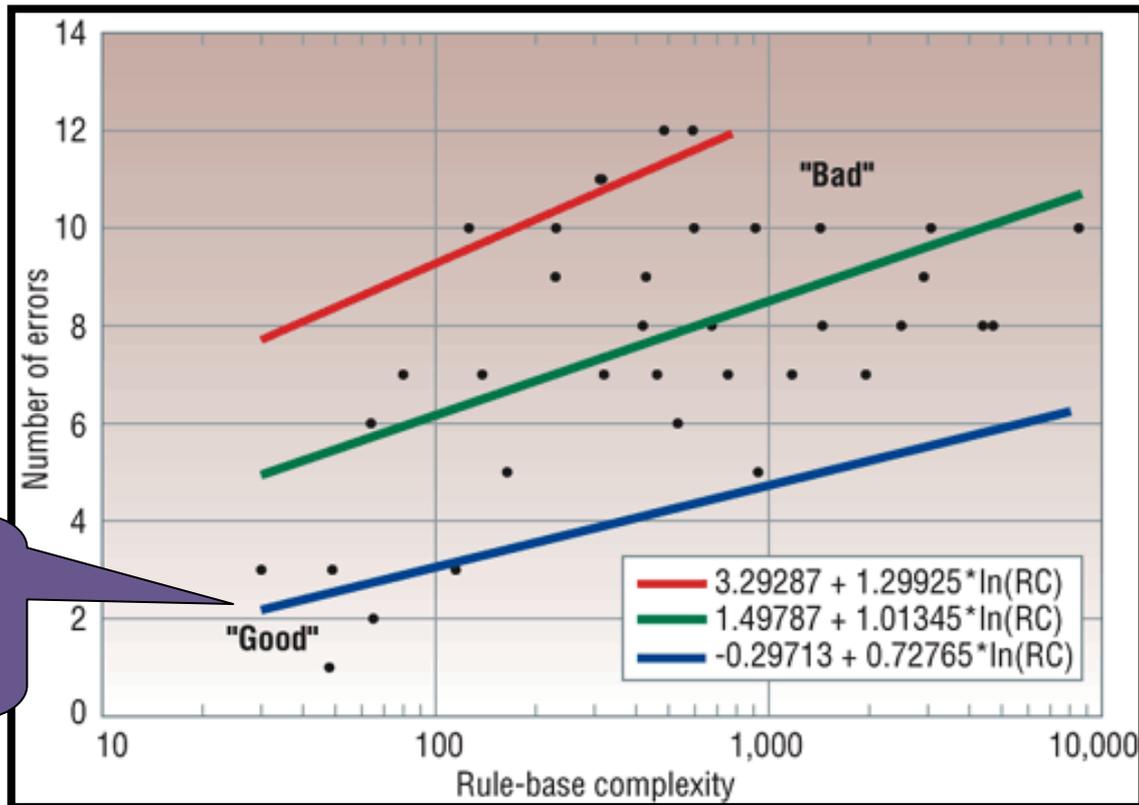
A Few Incorrectly Configured Firewalls...

- ◆ **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

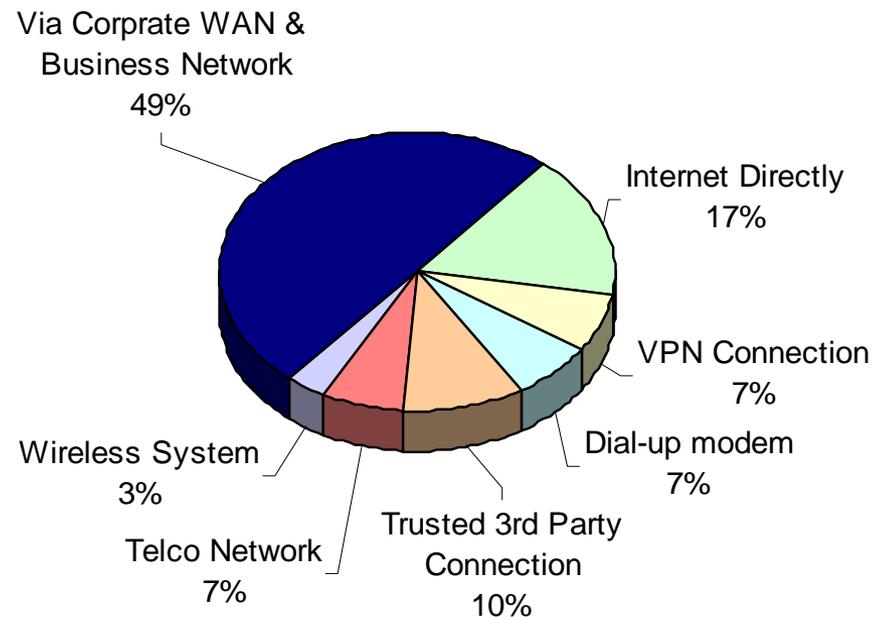
A Few Incorrectly Configured Firewalls...



Only 5 out of 37 Good Firewalls?

Sneaking Past the Firewall

- Corporate WANs & Business Networks
- The Internet directly
- Trusted third parties
- Infected laptops being connected to the PCN



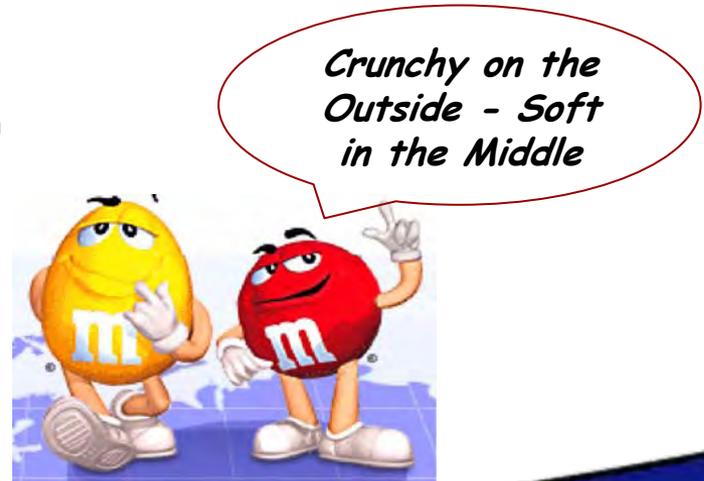
NERC Top 10 Vulnerabilities of Control Systems – 2007

#2. Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms.

- Design specifications include comprehensive security standard references providing in-depth security coverage.**
- Implement host based protection in conjunction with network based protection.**

A Perimeter Defence is Not Enough

- ◆ We can't just install a control system firewall and forget about security.
- ◆ The bad guys will eventually get in.
- ◆ So we must harden the plant floor.
- ◆ We need Defence in Depth.



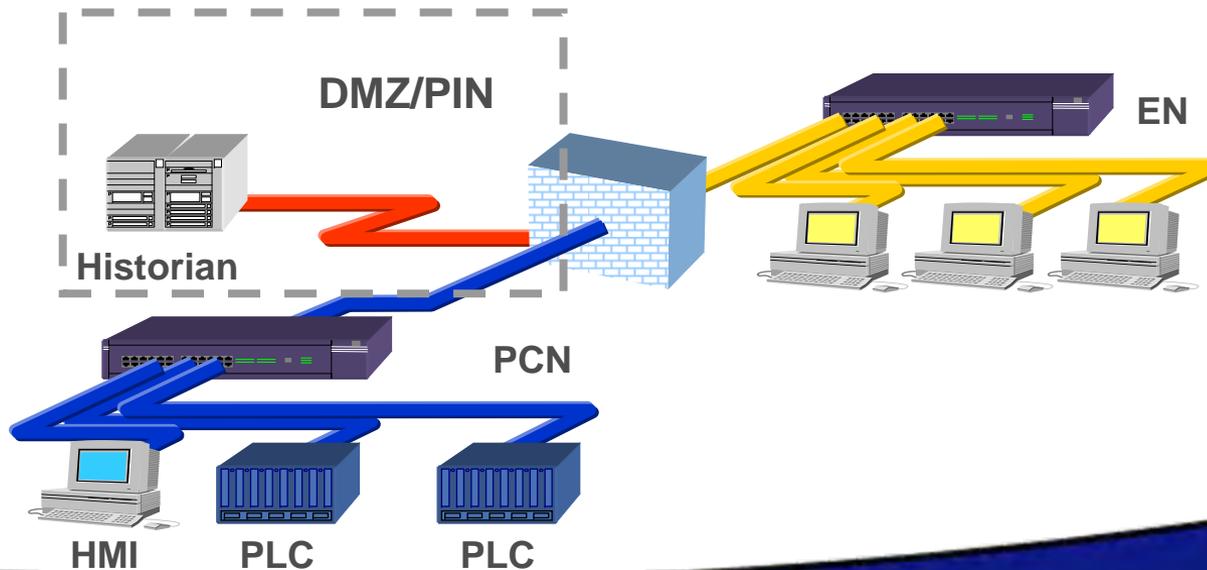
Creating Defense in Depth

Building Layers of Security

- ◆ A single firewall does help...
- ◆ But it is only a single layer of defence (like the Great Wall of China).
- ◆ Need to both defend the fort **AND** arm the troops!

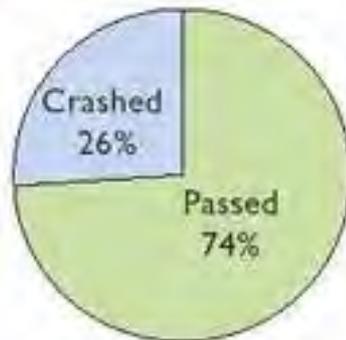
Using 3 Layer Architectures

- ◆ Three zone designs have separate DMZ for EN/PCN shared equipment (like the historian).
- ◆ All traversing traffic must terminate in DMZ.
- ◆ Use an Application Layer Firewall, not a router.



Next - Protecting the Edges

- ◆ The most important devices in a SCADA system are the edge devices like PLC, RTU, IED.
- ◆ They are very vulnerable to even simple attacks.



NETWOX



NESSUS

CERN pie charts of test results against controllers

- ◆ How do we protect them?

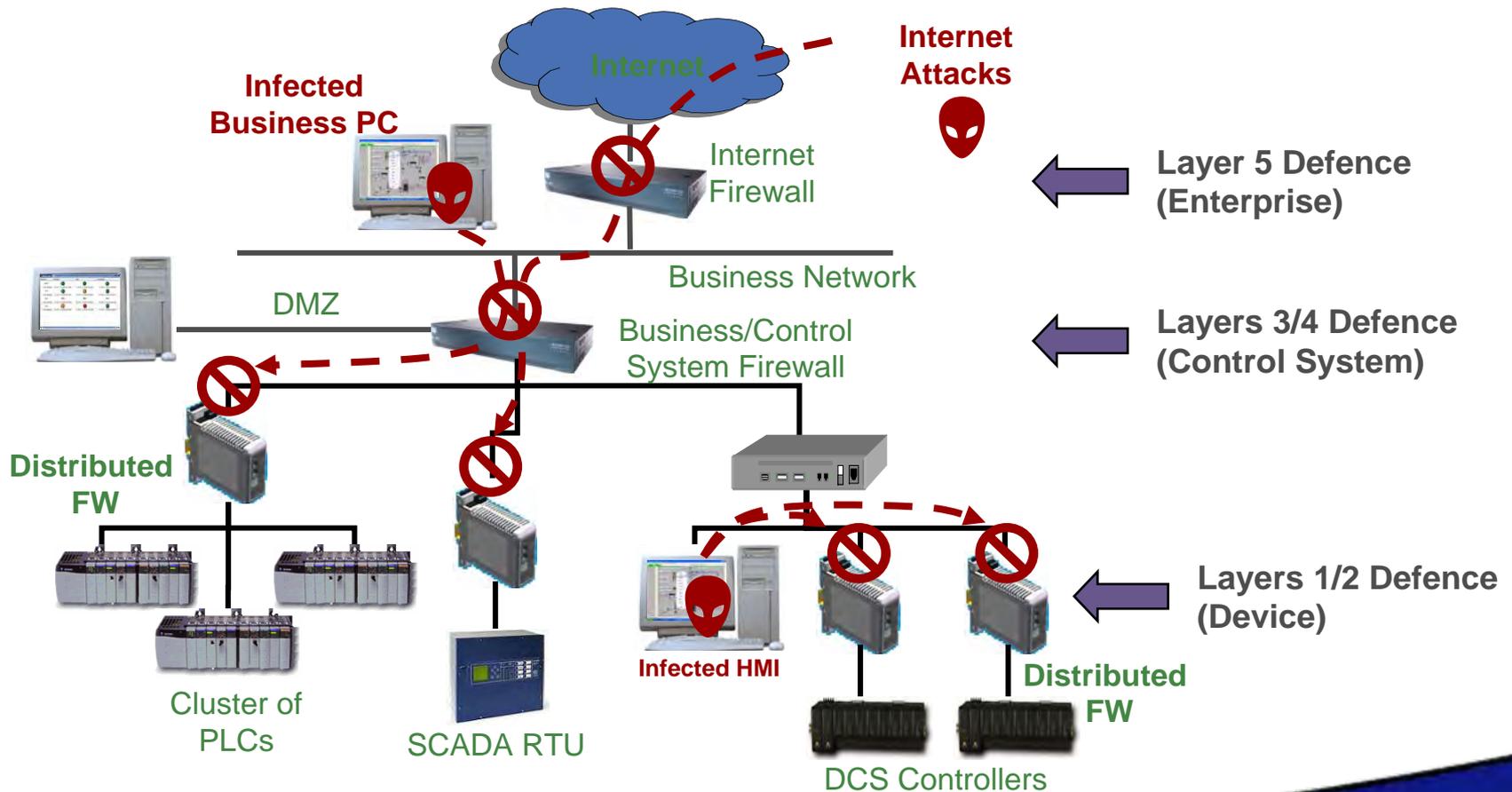
The Solution in the IT World

- ◆ **Your desktop has flaws so you add security software:**
 - Patches
 - Personal Firewalls (like ZoneAlarm)
 - Anti-Virus Software
 - Encryption (VPN Client or PGP)
- ◆ **But you can't add software to your PLC or RTU...**

Distributed Security Appliances

- ◆ **Add hardware instead - a micro-firewall designed to be placed in front of individual control devices.**
- ◆ **Protects the device from any unauthorized contact, probing, commands, etc.**

Distributed Security Appliances



Why Not Use a COTS Personal Firewall?

- ◆ **Not industrially packaged or hardened.**
- ◆ **Doesn't understand controls protocols so it can't selectively filter commands.**
- ◆ **Not extensible to control requirements.**
- ◆ **Not easy for maintenance staff to configure.**
- ◆ **Difficult to manage hundreds of personal firewalls from a central administration point.**

What is Required in a Industrial Security Appliance?

- ◆ **Industrial form factor and robustness**
- ◆ **Electrician-friendly deployment**
- ◆ **Control tech-friendly remote configuration and monitoring**
- ◆ **Control system functionality**
- ◆ **Extensible**

The Tofino Industrial Security Solution

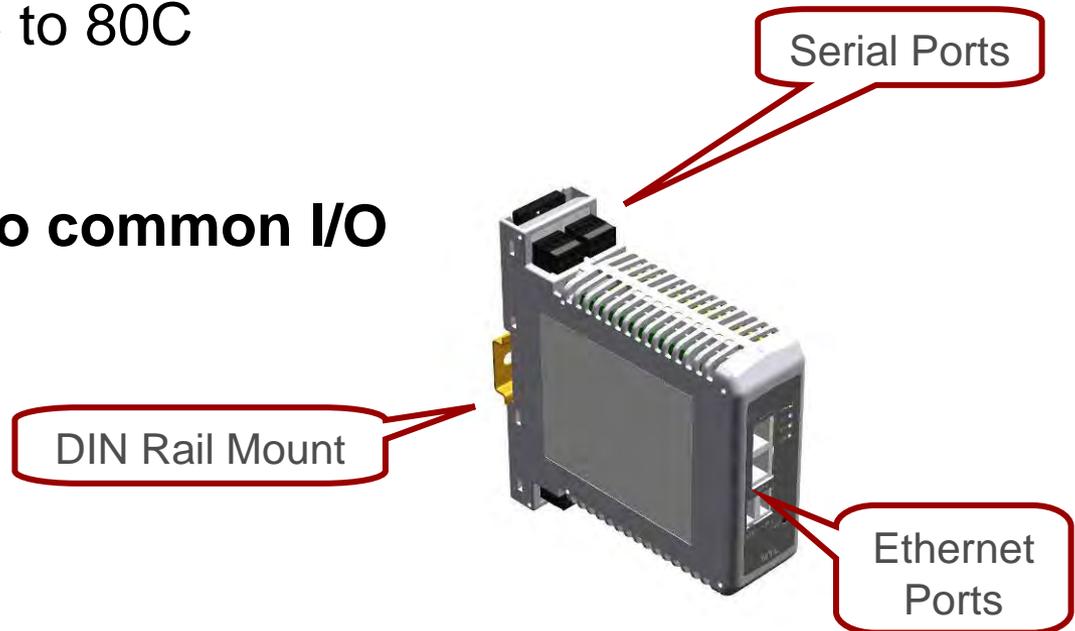
**Intrinsically Secure
Designed for Industry**

Form Factor and Robustness

- ◆ **Hardware specifications:**

- G3 Corrosion
- Temperature -40C to 80C
- Zone 2 (Future)

- ◆ **Form factor similar to common I/O or barriers**

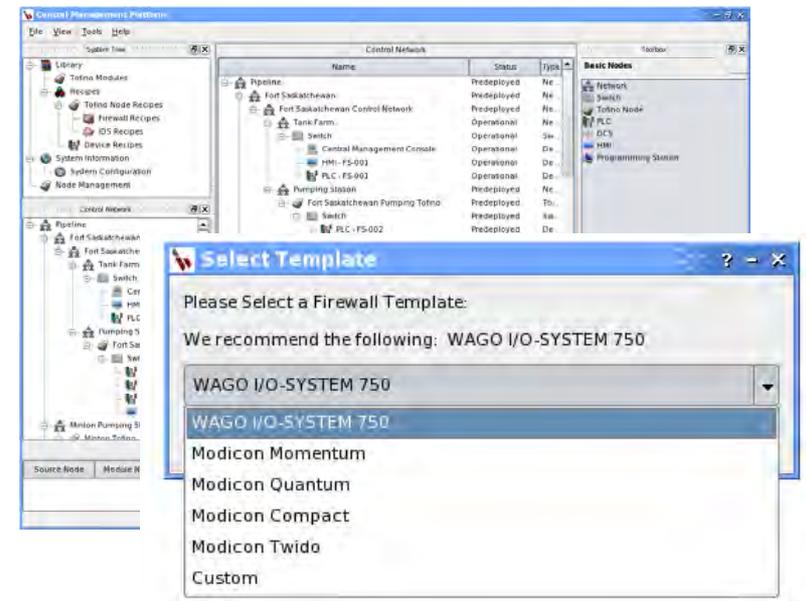


Zero Configuration Deployment Model

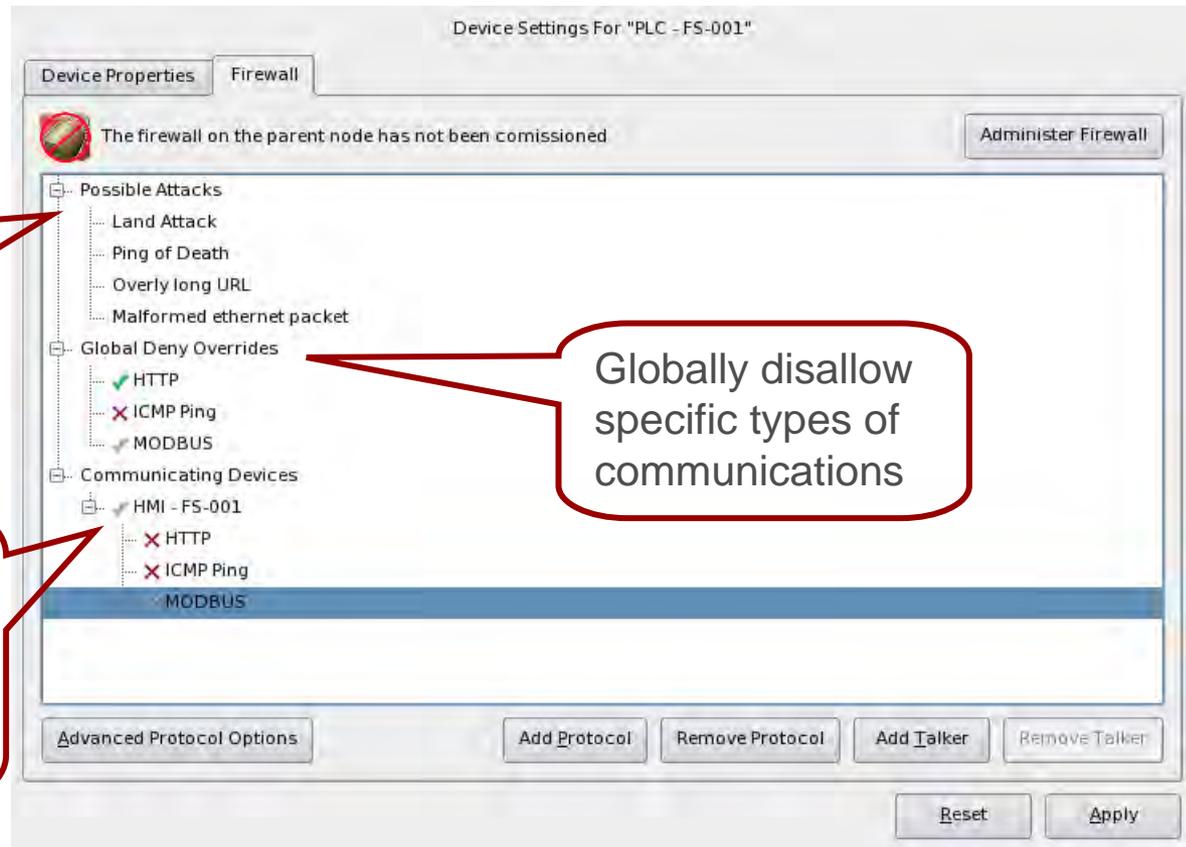
- ◆ **Field technician need do no more than:**
 - Attack the firewall to the DIN Rail
 - Attach instrument power
 - Plug in network cables
 - Walk away...

Simple to Operate

- ◆ **Plug security appliance onto the control network in front of a PLC, DCS or HMI station:**
 - Learns what type of device it needs to protect,
 - Looks up the device's vulnerabilities in a central database
 - Tunes itself to protect that specific device.



No Complex Rules to Create



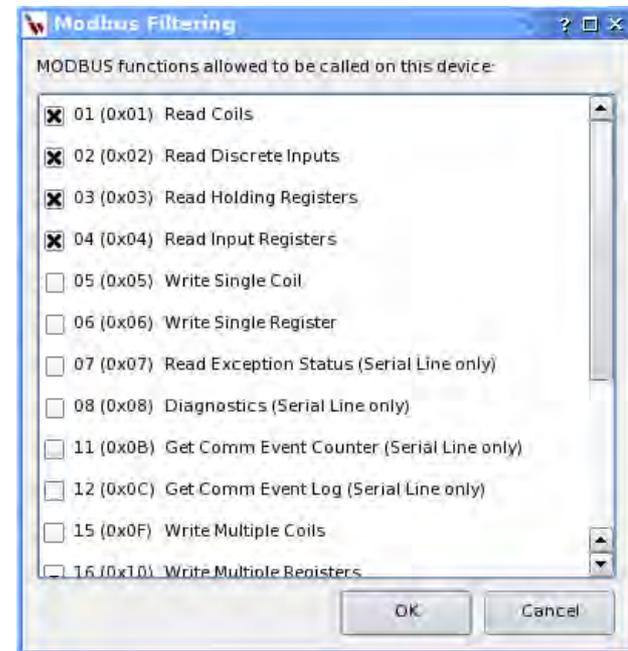
Preconfigured to block known device flaws

Globally disallow specific types of communications

Select from list what devices on network can "talk" to a device and how.

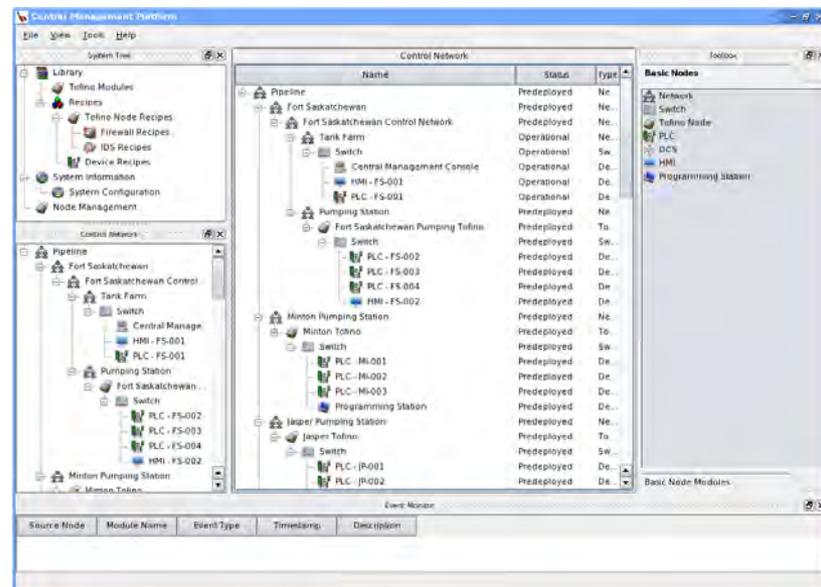
Functionality for Control Protocols

- ◆ Able to filter control protocols intelligently
- ◆ Allows user to specify what MODBUS functions are allowable.
- ◆ Example:
 - Allow Register Reads from data historian
 - Drop all Write Registers



Administration and Global Management

- ◆ One management station can monitor and manage thousands of firewalls, deployed in remote locations.
- ◆ Reports with encrypted heartbeat (like a fieldbus) to report status and events.

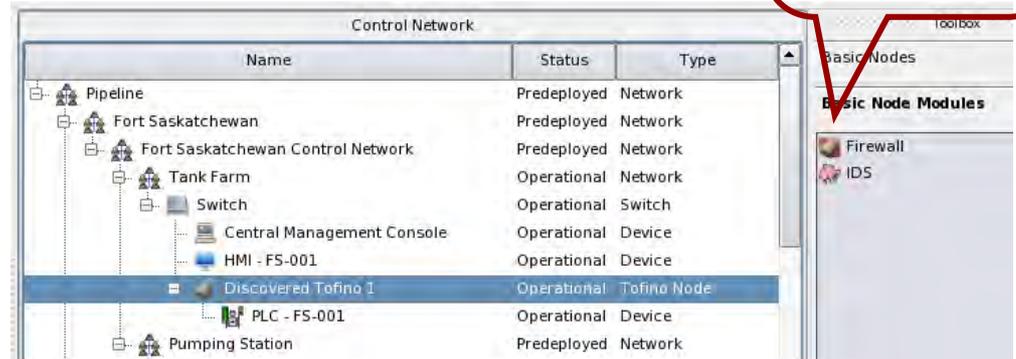


More Than Just a Firewall

- ◆ **Loadable Security Modules (LSM) allow multiple security functions to be deployed in one appliance:**

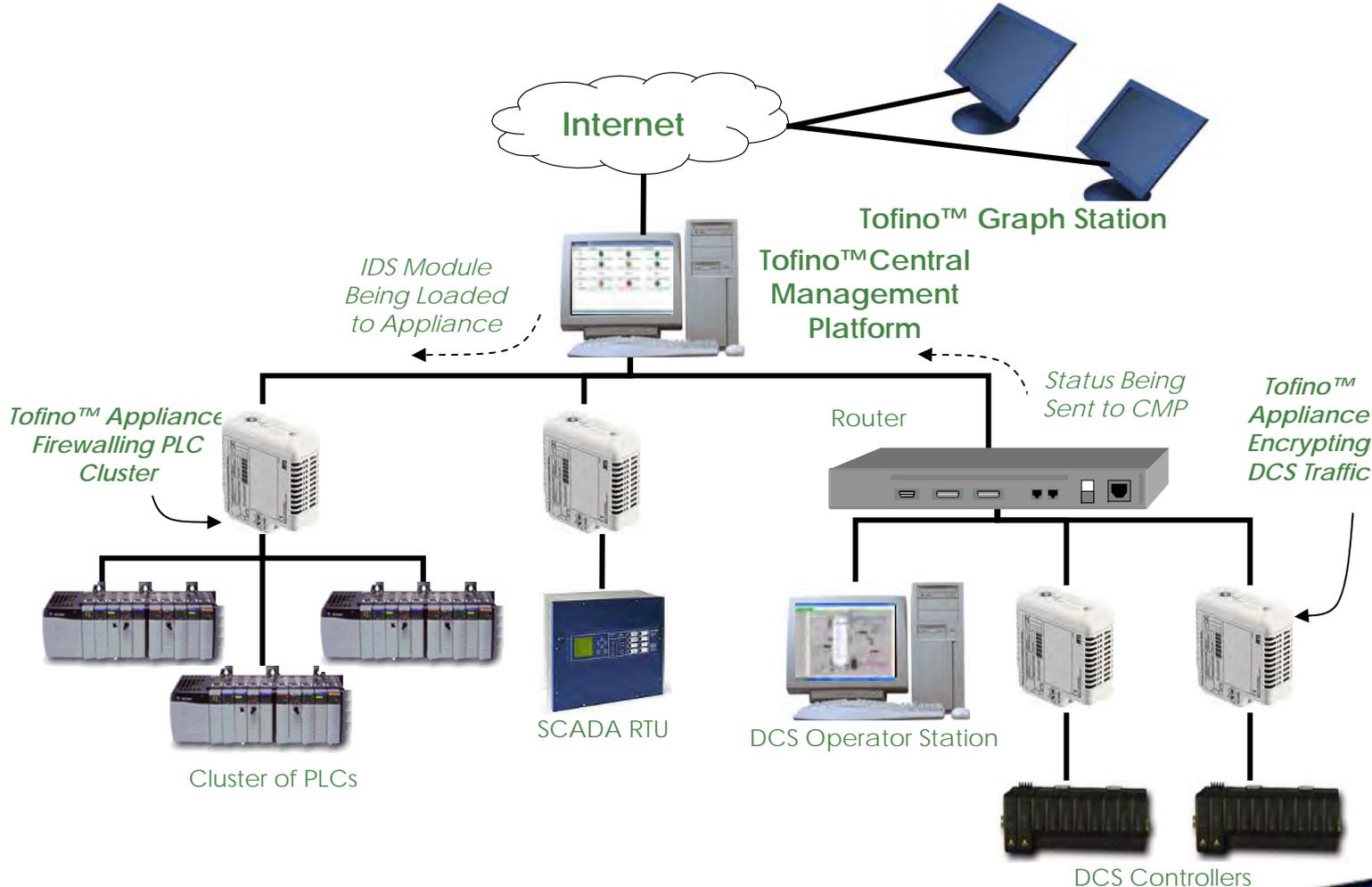
- Firewall IDS VPN/Encryption
- Anti-virus Asset Discovery
- Traffic Monitoring

- ◆ **New modules can be deployed at any time.**



Tofino Demo

The Tofino™ Architecture



Key Tofino™ Components

- ◆ **Tofino™ Security Appliance**
- ◆ **Tofino™ Loadable Security Modules (LSM)**
- ◆ **Tofino™ Central Management Platform (CMP)**
- ◆ **Tofino™ CMP Graphics Station**

Tofino™ Security Appliance

- ◆ Industrially hardened hardware appliances.
- ◆ Installed in front of individual and/or clusters of HMI, DCS, PLC or RTU control devices that require protection.



Tofino™

Loadable Security Modules (LSM)

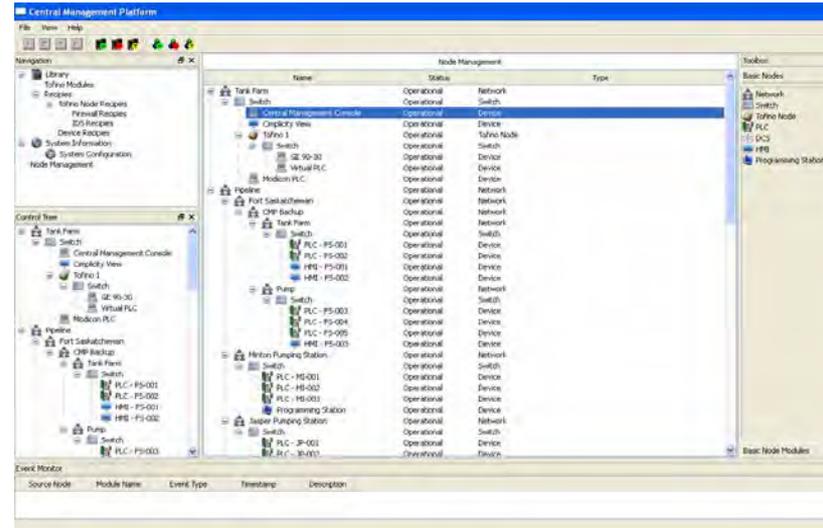
- ◆ **Software plug-ins providing security services such as:**
 - Firewall,
 - Intrusion detection system (IDS),
 - VPN encryption.
- ◆ **Each LSM is downloaded into the security appliance to allow it to offer customizable security functions, depending on the requirements of the control system.**

Tofino™ Central Management Platform (CMP)

- ◆ A heavily hardened Linux-based centralized management server for data and configuration storage.
- ◆ Provides database for monitoring, supervision and configuration of each security appliance.

Tofino™ CMP Graphics Station

- ◆ Windows Station for remote access to the CMP by controls and security specialists.



Industry Feedback and Q/A

Industry Feedback

- ◆ **Would you use a product like this?**
- ◆ **If yes, how would you deploy it?**
- ◆ **What type of devices would you want to protect with this system?**
- ◆ **Most important loadable security modules?**
- ◆ **Important protocols for advanced firewalls?**
- ◆ **Would you want to use this system on Non-Ethernet networks?**

Into The Future

- ◆ **Industry can't hide behind a big firewall.**
- ◆ **Defense in depth is critical.**
- ◆ **Best practices and solutions are now available.**
- ◆ **We need to start to use them...**

Thank You!