RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SPO1-T11

Converging IT and OT for Secure, Reliable, Resilient Industrial Networks

Jeff Lund

Senior Director, Product Line Management
Belden

David Meltzer

Chief Research Officer,
Tripwire

#RSAC

Industrial Control Systems

tripwire

BELDEN
SENDING ALL THE RIGHT SIGNALS®

Industrial Internet of Things

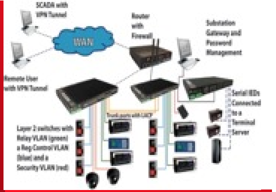
Transportation

❖ Positive Train Control & Safety

Discrete

❖ Industry 4.0 / Smart Factory

Energy

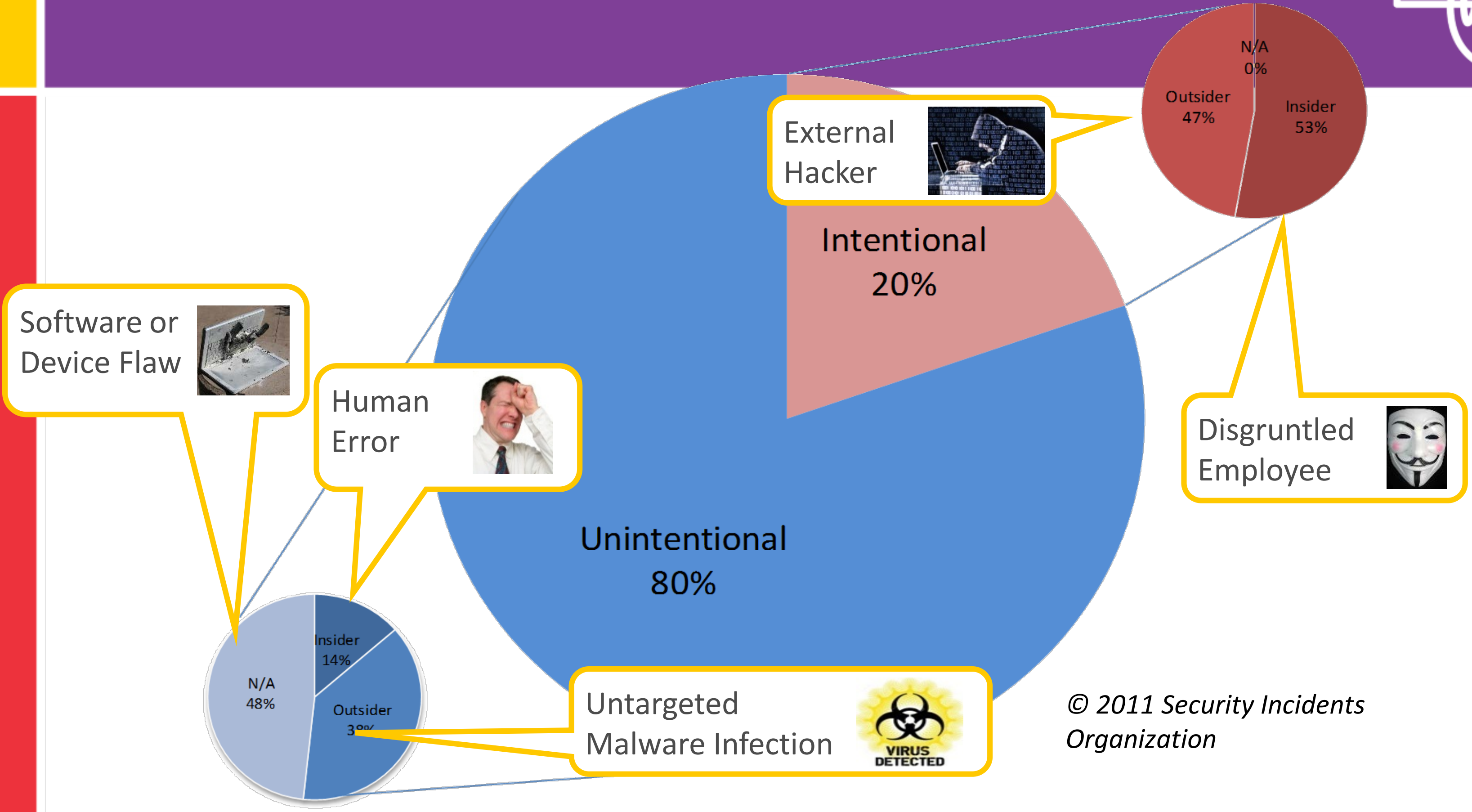

SCADA with VPN Tunnel
WAN
Router with Firewall
Substation Gateway and Password Management
Remote User with VPN Tunnel
Serial IEDs Connected to a Terminal Server
Trunk ports with LACP
Layer 2 switches with Relay VLAN (green) a Reg Control VLAN (blue) and a Security VLAN (red)

❖ Smart Grid / Energy Management

Process

❖ Remote Management & Optimization

SAFETY
FIRST
SAFETY GLASSES
REQUIRED IN
THIS AREA



External Hacker

Disgruntled Employee

Software or Device Flaw

Human Error

Untargeted Malware Infection

© 2011 Security Incidents Organization

Industrial Security Incidents Are Real

ICS security advisories **800**

245 Reported ICS security incidents in last year

Most common attack vector used in ICS breaches **Unable to Determine**

55% % of ICS attacks involving APTs

Source: ICS-CERT

Polish Trains

Event: A Polish teenager modifies a TV remote and hacks Lodz Tram system

Impact: 12 people injured, 4 derailments

Specifics: The 14-year-old modified a TV remote control so that it could be used to change track points. Local police said the youngster trespassed in tram depots to gather information needed to build the device. The teenager told police that he modified track setting for a prank.

Telegraph.co.uk

The boy, described as a 'genius' and some of the equipment he used

Lessons learned:

- Do not rely on protocol obscurity for security
- Apply appropriate access controls to all field devices

Source: DHS

Maroochy Waste Water

Lessons learned:

- Suspend all access after terminations
- Investigate anomalous system behavior
- Secure radio and wireless transmissions

Event: More than 750,000 gallons of untreated sewage intentionally released into parks, rivers, and hotel grounds

Impact: Loss of marine life, public health jeopardized, $200,000 in cleanup and monitoring costs

Specifics: SCADA system had 300 nodes (142 pumping stations) governing sewage and drinking water

- Used OPC ActiveX controls, DNP3, and ModBus protocols
- Used packet radio communications to RTUs
- Used commercially available radios and stolen SCADA software to make laptop appear as a pumping station
- Caused as many as 46 different incidents over a 3-month period (Feb 9 to April 23)

Source: DHS

Browns Ferry Power Plant

Event: Two circulation pumps at Unit 3 of the nuclear power plant failed

Impact: The unit had to be shut down manually

Specifics: The failure of the pumps was traced to excessive traffic on the control system network, possibly caused by the failure of another control system device

Recovery time:

- *SPDS – 4hours 50 minutes*
- *PPC – 6 hours 9 minutes*

Lessons learned:

- Provide adequate network segmentation
- Place controls on multiple segments to limit congestion and cascading effects
- Provide active network monitoring tools

Source: DHS

Ukraine Power Outage

Event: Power went out for 80,000 customers in Ukraine (Dec 23, 2015)

Impact: 7 substations had to be manually restarted

Specifics: Email spear-phishing introduced “BlackEnergy” malware into computer networks. This likely enabled remote access that took down the substations Phone systems were attacked, preventing customers from reporting outages. A component of the malware wiped computers, covering the perpetrators’ tracks.

Recovery time:

- *6 hours*

Lessons learned:

- Employees need ongoing training e.g., spear-phishing
- Implement good network design and segmentation
- Incorporate active network monitoring tools

Source: DHS

tripwire

BELDEN
SENDING ALL THE RIGHT SIGNALS®

Now Let’s Talk About Solutions…

Actually, What Are NOT Solutions….

Telling Control Engineers they:

- Just don’t “get” security
- Are decades behind IT when it comes to security
- Need IT security to fix their networks to make them secure

CIA-S Model

I.T. Security

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

I.C.S. Security

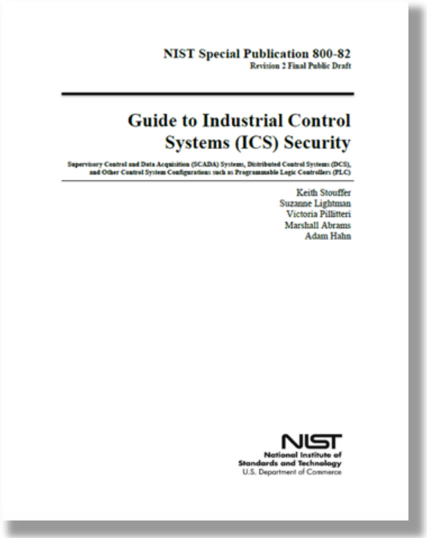
+ Safety

AVAILABILITY

INTEGRITY

CONFIDENTIALITY

Standards and Best Practices



NIST Special Publication 800-82
Revision 2 Final Public Draft

Guide to Industrial Control Systems (ICS) Security

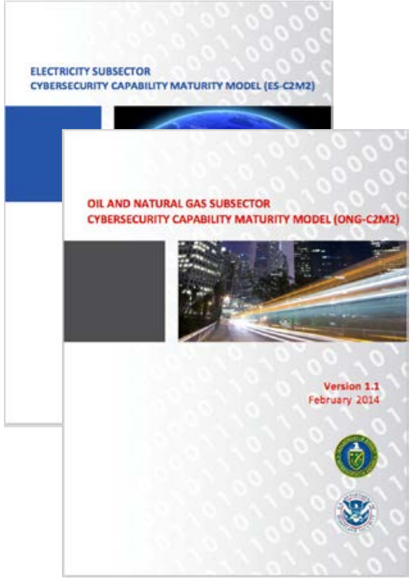
Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Suzanne Lightman
Victoria Pillitteri
Marshall Abrams
Adam Hahn

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

ISA

IEC



ELECTRICITY SUBSECTOR
CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

OIL AND NATURAL GAS SUBSECTOR
CYBERSECURITY CAPABILITY MATURITY MODEL (ONG-C2M2)

Version 1.1
February 2014

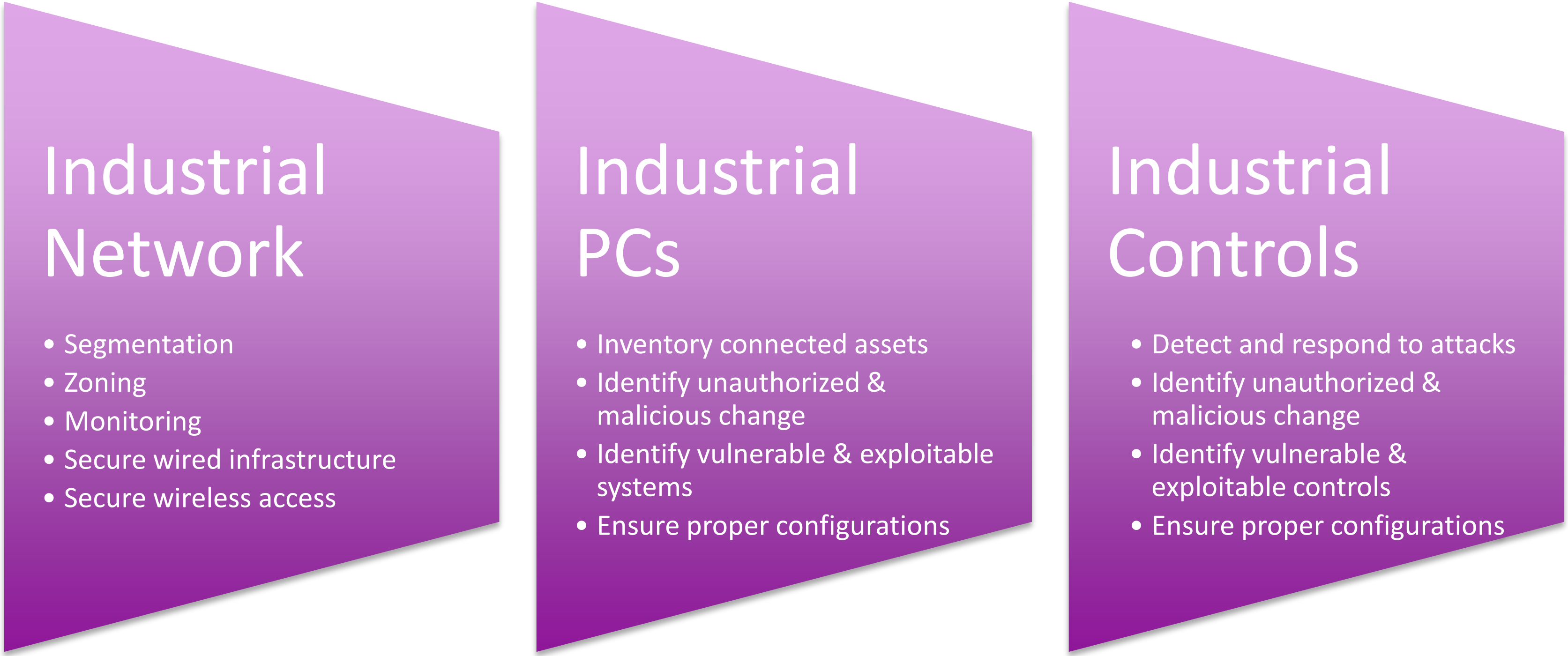
industrial internet
CONSORTIUM

Security

1-2-3 Approach to Industrial Cybersecurity

1. Secure the Industrial Network
2. Secure the Industrial Computers
3. Secure the Industrial Controls

Industrial CyberSecurity 1-2-3 Approach



Industrial Network

- Segmentation
- Zoning
- Monitoring
- Secure wired infrastructure
- Secure wireless access

Industrial PCs

- Inventory connected assets
- Identify unauthorized & malicious change
- Identify vulnerable & exploitable systems
- Ensure proper configurations

Industrial Controls

- Detect and respond to attacks
- Identify unauthorized & malicious change
- Identify vulnerable & exploitable controls
- Ensure proper configurations

Real World Example: The Problem

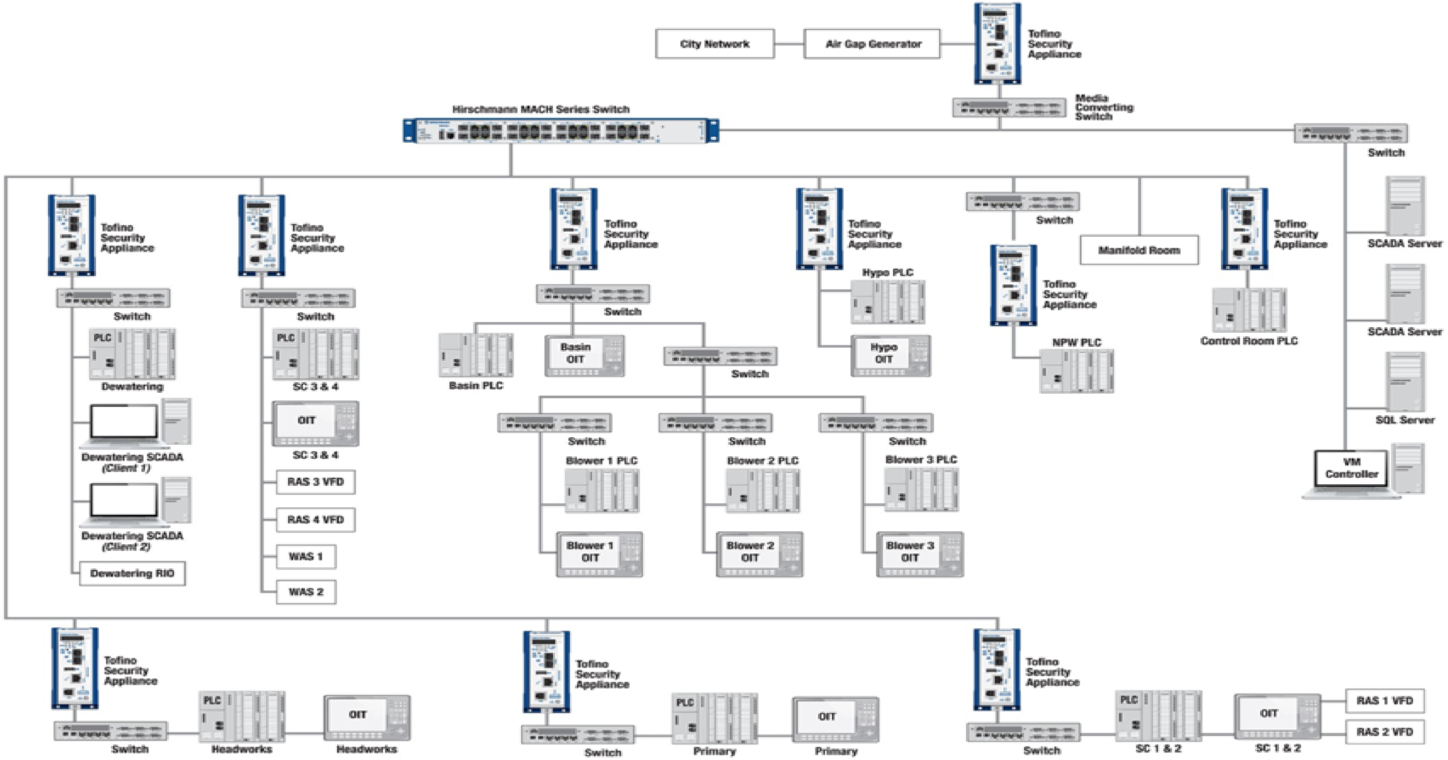
- Regional wastewater treatment plant
  - Mid-sized city in the Eastern U.S.
  - 24 buildings / 500 pieces of equipment
  - 15 treatment processes
  - 13 million gallons of wastewater daily
  - Runs 24 hours a day every day

- Little protection or separation of the SCADA network from the city's IT network
  - Even the city's high school students could gain access if they tried

The Requirements

- Protect critical plant infrastructure from malware, traffic storms, error and attacks
- Without giving up the ability to share data interdepartmentally or remote support and maintenance capability
- While increasing system reliability by following ISA/IEC 62443 cybersecurity standards
  - Partition into zones; secure through conduits
  - Security embedded throughout the system, not just as the perimeter

The Solution: Final Application



Building Resiliency: Industrial Control Systems

Assessing and monitoring control systems with purpose-built, non-invasive technology

- Connect to Industrial Automation Asset Management Products
- Gather inventory of configuration – including PLC, firmware, programs
- Identify out-of-date firmware and associated vulnerabilities
-

Keys to Successful IT / OT Convergence

Next week:

- Commit to Improving your ICS security skills
  - Take a course, read a book, get a PLC training kit

Over the next three months:

- Build relationships with OT staff (coffee and lunches)

Within six months:

- Drive or support efforts to create a collaborative environment and metrics that emphasize teamwork www.tripwire.com

www.belden.com