# Control System Cyber Security for T&D Systems

2008 IEEE T&D Conference

Joe Weiss, PE CISM
(408) 253-7934
joe.weiss@realtimeacs.com

ACS APPLIEDCONTROLSolutions

# Definition

- Cyber Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional. (FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information System*, March 2006.)
  - What is important about this definition
    - Intentional or unintentional
    - Actual or potential compromise of CIA
    - Violation or imminent threat to CIA

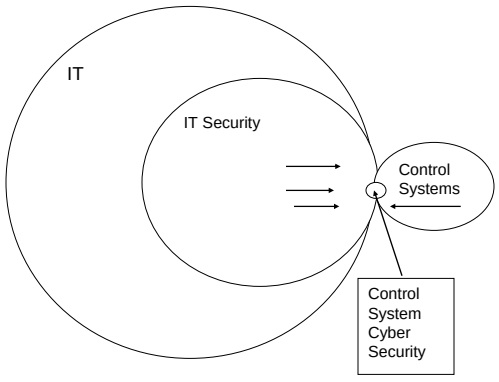
ACS APPLIEDCONTROLSolutions

# Myths

- Using Windows and TCP/IP makes it IT
- External, malicious threats are the biggest concerns
- Firewalls make you secure
- VPNs make you secure
- Encryption makes you secure
- IDSs can identify control system attacks
- Messaging can be one-way
- Field devices can't be hacked
- You are secure if hackers can't get in
- More and better widgets can solve security problems
- …

ACS APPLIEDCONTROLSolutions

# Why Are There So Few Experts




ACS APPLIEDCONTROLSolutions

## Generational Issues with Control Systems

- Legacy equipment
  - Security agnostic
  - Vulnerabilities backfit and security often turned off
  - Will be around for at least another 5 years
- New equipment
  - Vulnerabilities designed in
  - Will become pervasive in about 5 years for the next 15-20 years
- Future equipment
  - Security and performance part of initial design criteria
  - Probably about 20 years away before pervasive

ACS APPLIEDCONTROLSolutions

## Other Vulnerabilities

- Dial-ups still being used with new equipment
  - Many dial-up connections are not even owned by the end-user
  - War-dialing may not be possible if telephone line installed by vendor
- Use of wireless modems, bluetooth, web services, Telnet, SNMP, DCOM, ActiveX, and other vulnerable applications in new equipment
- Use of vulnerable versions of remote access including PCAnywhere, Hummingbird, etc
- Connections between plant and corporate networks
- Backdoors designed in (“Onstar” for control systems)

ACS APPLIEDCONTROLSolutions

# Pipeline Rupture with Fatalities

June 10, 1999 SCADA failure resulted in a pipeline rupture

- –Gasoline leaked into two creeks in the City of Bellingham, Washington and ignited
- –Fireball killed three persons, injured eight other persons
- –Caused significant property damage
- –Released approximately ¼ million gallons of gasoline causing substantial environmental damage

ACS APPLIEDCONTROLSolutions

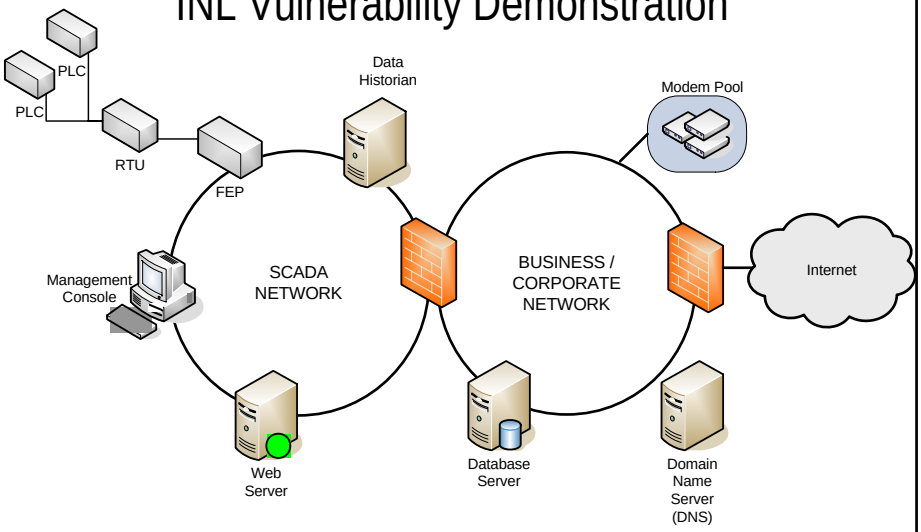
# Targeted SCADA Attack

Insecure GIS mapping system with no firewall into SCADA led to targeted attack

- No SCADA servers or mapping system for two weeks
- Neighboring utility networks went from trusted to untrusted
- 4 Man-months to recover

ACS APPLIEDCONTROLSolutions

# INL Vulnerability Demonstration



**UNIT SUBSTATIONS NOW WEB-ENABLED TO SIMPLIFY ACCESS TO POWER TRANSFORMER DATA**

**Aug. 29, 2005 –** Equipped with an Ethernet interface and Web server, Vendor A Unit Substations now provide simple, affordable access to power system information – including transformer coil temperatures – using a standard Web browser. The pre-engineered equipment ships in standard lead-times and connects to a customer's existing Ethernet Local Area Network much like adding a PC or printer.

Unit substations include a Temperature Controller, which provides remote access to transformer data, in addition to its primary role in controlling cooling fans. With a simple click of a mouse, it is easy to monitor transformer coil temperatures per phase, and verify cooling fan status at a glance. Among the many potential benefits, these new capabilities make it possible to correlate circuit loading with transformer temperatures to extend equipment life.

The typical unit substation incorporates Medium Voltage Metal-Enclosed Switchgear on the primary side and Low Voltage Switchgear or Low Voltage Switchboard on the secondary.

Vendor A was the first manufacturer in the world to embed an Ethernet interface and Web server into its power distribution equipment, allowing customers easier access to power system information. The family of power distribution equipment includes medium and low voltage switchgear, unit substations, motor control centers, switchboards and panelboards.

ACS APPLIEDCONTROLSolutions

# Disclosure Issues (Black Hat)

- Technical disclosures to "Black Hat" community (2005)
  - Step-by-step instructions on how to hack Modbus, DNP3, UCA, GOOSE

  http://toorcon.org/2005/slides/mgrimes/mgrimes-scadaexposed.pdf
- Hacker shows flaw in software that controls key infrastructure (2007)
  - "After the basics I will be getting into the finer details of the protocols as to what function code, internal indication flags does what and how that can be used to attack or take down the SCADA system. I shall as well discuss and demonstrate the current level of security implementation that these sites have."

  http://dvlabs.tippingpoint.com/appearances/
- Class on hacking PLCs at Black Hat Las Vegas (2008)

ACS APPLIEDCONTROLSolutions

# Summary

- Leaping from mid-80's to mainstream networking technologies has advantages and disadvantages
  - We need to understand them enough to make prudent decisions or we will become less secure
- We need to be able to specify security in products and employ relevant best practices
  - This requires an understanding of security and system performance

ACS APPLIEDCONTROLSolutions