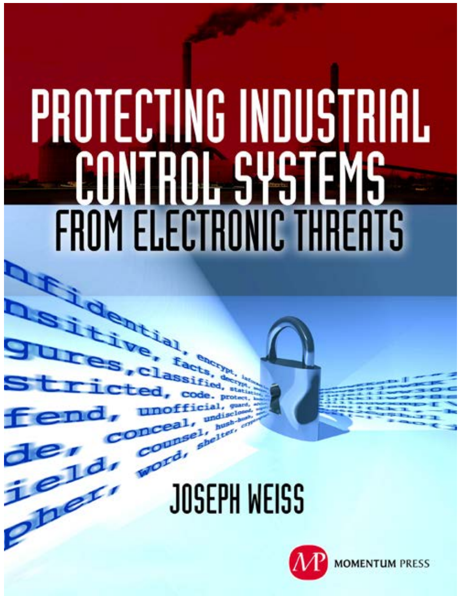
# ICS Cyber Security-The Impact on National Security


PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ELECTRONIC THREATS
JOSEPH WEISS
MOMENTUM PRESS

Prepared for

AFRI Cyber Security Conference

October 10, 2012

Joe Weiss

PE, CISM, CRISC, ISA Fellow

(408) 253-7934

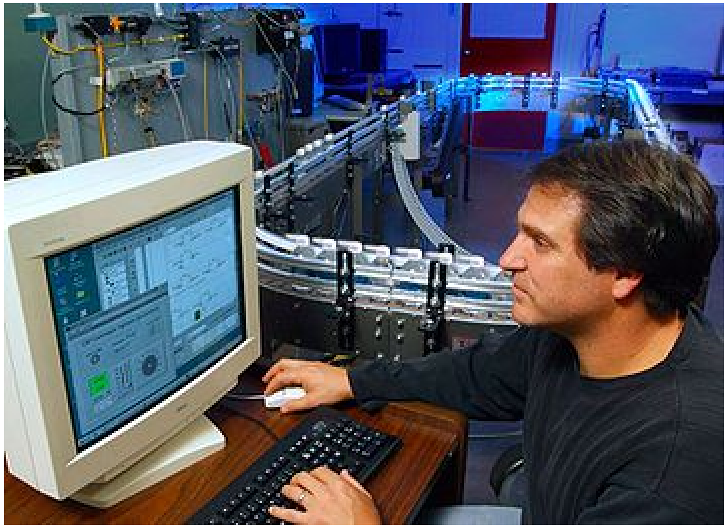
joe.weiss@realtimeacs.com

# What are Industrial Control Systems (ICSs)

- Industrial control systems (ICSs) operate power, water, chemicals, pipelines, military systems, medical systems, etc

- ICSs include SCADA/EMS, DCS, PLCs, RTUs, IEDs, smart sensors and drives, emissions controls, equipment diagnostics, AMI (Smart Grid), programmable thermostats, building controls,…

- Focus is reliability and safety

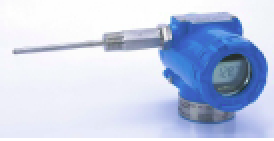


# How can ICS Cyber Security Affect National Security?

- ICSs are used throughout the critical infrastructure and DOD
- We are absolutely dependent on them working PROPERLY
- When they don’t, physical processes can fail and people can die
- ICSs are not cyber secure and are now becoming a target

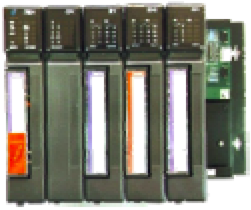
# Control Systems Basics

Sensors

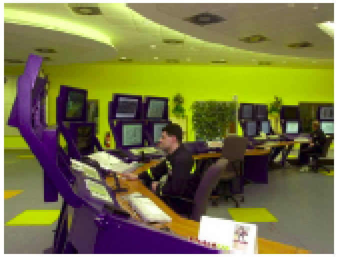


Motor Controls

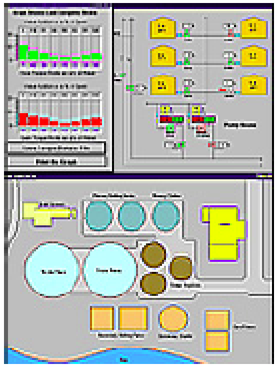
Control Valves

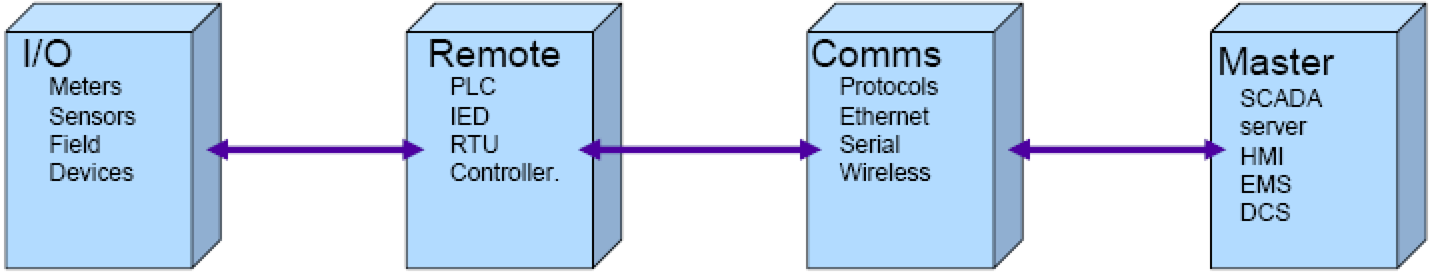


Programmable Logic Controllers (PLC)



Human Machine Interfaces (HMI) and Operator Displays





I/O
Meters
Sensors
Field
Devices

Remote
PLC
IED
RTU
Controller.

Comms
Protocols
Ethernet
Serial
Wireless

Master
SCADA
server
HMI
EMS
DCS

Field Devices

Control Center

Slide courtesy of Anixter © Proprietary 04-2009

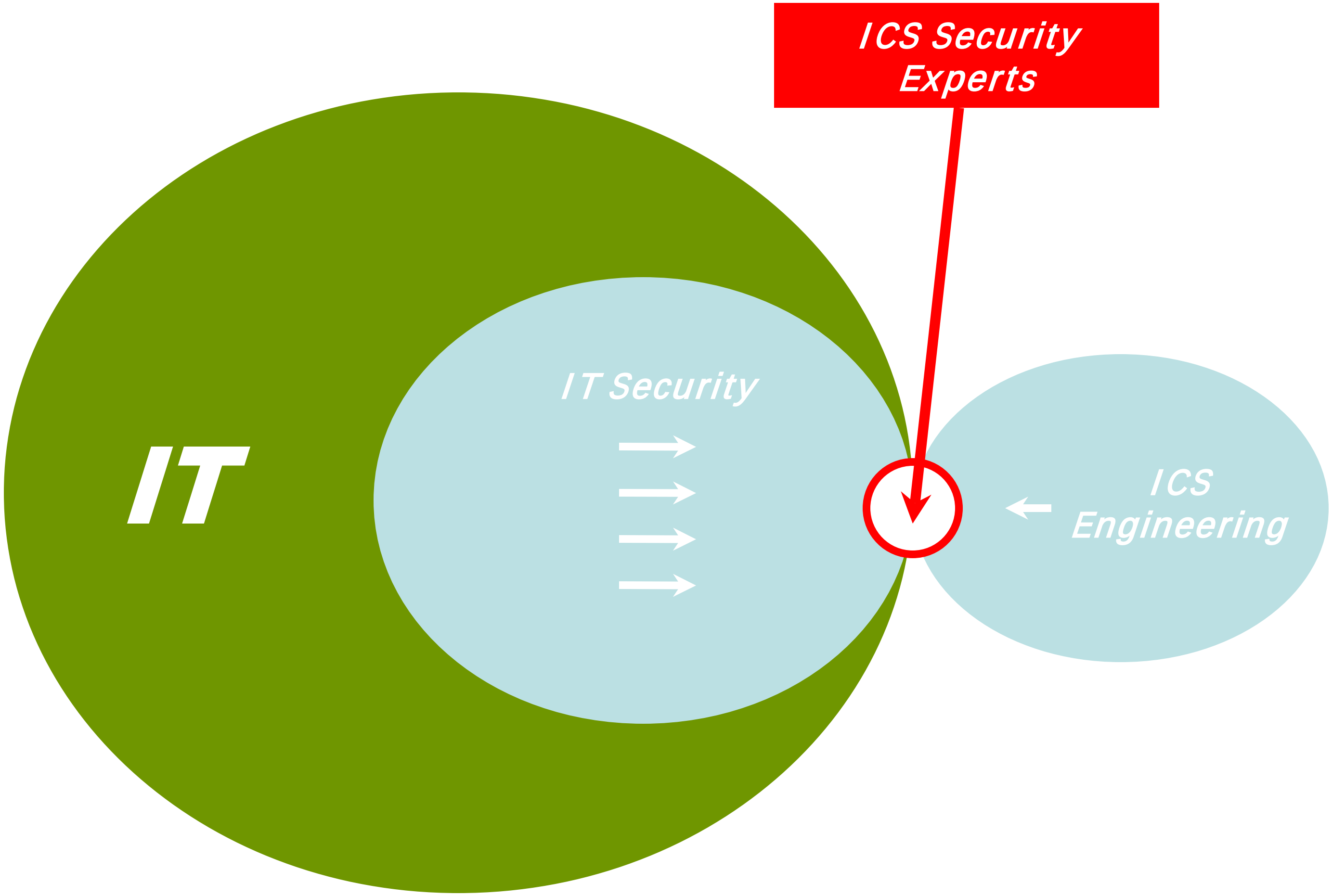
# ICSs are not Mainstream Information Systems

- The Internet and Microsoft are not necessarily the biggest ICS cyber threats
- External malicious threats are not necessarily the biggest concerns
- Firewalls and VPNs may not be adequate
- IDS will probably not identify ICS attacks
- Field devices have been hacked
- Default passwords and backdoors are not uncommon
- Many ICSs have hardware configurations that are cyber vulnerable and cannot be patched or fixed
- Patching is difficult and can have unintended consequences
- Cyber forensics and logging may not exist

# Selected Differences Between IT and ICS

| Attribute | IT | ICS |
|---|---|---|
| Confidentiality (Privacy) | High | Low |
| Message Integrity | Low-Medium | Very High |
| Availability | Medium | Very High |
| Authentication | Medium-High | High |
| Lifetime | 3-5 years | 10-25 years |
| Cyber Logging and Forensics | Available | SEIM only at the IP layer |
| Operating Systems | COTS (Windows, Linux,…) | COTS at HMI, RTOS at field devices |
| Patching | Standard and expeditious | Non-standard and potentially long time |

# ICS Security Expertise Lacking



# Where is ICS Technology Going

- More intelligence
  - Intelligence moving closer to the process
- More interoperability
  - With ICS and IT
- More networking
  - Inside and outside the plant
- More two-way communication for on-line interactions
  - Affecting control and safety

Cyber!

# What Has Changed About ICS Cyber Vulnerability

- Designed for performance and safety
  - Security not a consideration and actually in conflict
  - Originally designed to be isolated
  - Now have remote access for maintenance and vendor support
  - Long life and very reliable
- ICSs generally weren’t hackers targets until post-Stuxnet
  - Now being targeted and many vulnerability disclosures
  - Remote access now an issue
- Sophisticated attackers know what industries and systems are critical

# ICS Cyber Attack Concerns

- Minimal ICS cyber forensics and logging
- ICSs are not robust against cyber
- Don’t know what an ICS cyber attack looks like
  - No training
- Don’t know what is currently in the wild that can affect ICS
- Older attacks can affect ICS and safety systems
  - Doesn’t need to be “zero-day”
- “Knee-jerk” reactions can affect cyber
  - Response to San Bruno
- IT and ICS defenders don’t work well together

# What has Happened Recently

- Brazilian control system network infections
- Russian Sayano–Shushenskaya Dam failure
- ExxonMobil Yellowstone River gasoline pipeline break
- China bullet train crash
- BART computer failure
- San Bruno
- Illinois water SCADA hack?
- South Houston water SCADA hack
- ICS metasploits now available
- Polish train crash
- Digital camera shuts down nuclear plant
- International power plant with loss of all control logic
- Iranian paper on Stuxnet
- Telvent notice
- Class 1 Trauma system compromise
- Mining truck vulnerabilities
- …

# PLC Issues

- Many legacy controllers with hardcoded default passwords
  - Cannot be changed
- Lack of detection of rogue software in controller
- Lack of security with older protocols and serial communications
  - 14 lines of code can take control
- Metasploit code available for many PLCs
- Many cyber vulnerable PCS cannot be “patched” and will not be replaced

# Stuxnet

- International problem – with potential “blowback”
- Root kit – affects ALL Siemens PCS7 controllers
- Hardcoded default passwords – publicly available
- Many parts of Stuxnet reusable for other vendors and applications
- Iranian Stuxnet paper and CV
- Lack of detection of rogue software in controller
- ICS-CERT response not adequate
- Recent NERC Cyber Attack Task Force did not address Stuxnet
- NERC CIPs do not address Stuxnet- effectively exclude it
- NRC Reg Guide 5-71 doesn’t address Stuxnet

# Aurora

- Gap in protection of electric grid- requires hardware fix
  - Currently, industry not employing hardware fix
  - Persistent physical vulnerability – not APT
- Affects all AC rotating equipment, not just generators
  - Not just North American problem
- All substations can be vectors in
  - Not just electric – Mass transit, large industrials, etc
- Affects predictive maintenance programs
  - Cannot be seen in unmanned facilities
  - Will be felt in manned facilities but no training to identify event as Aurora

# Why DOD cares about Aurora

- Damage very critical DOD assets
- Damage defense critical infrastructures
  - Aircraft assembly lines, etc
- Affect long term ability to provide power to bases

# Turbine overstress due to systems incompatibility

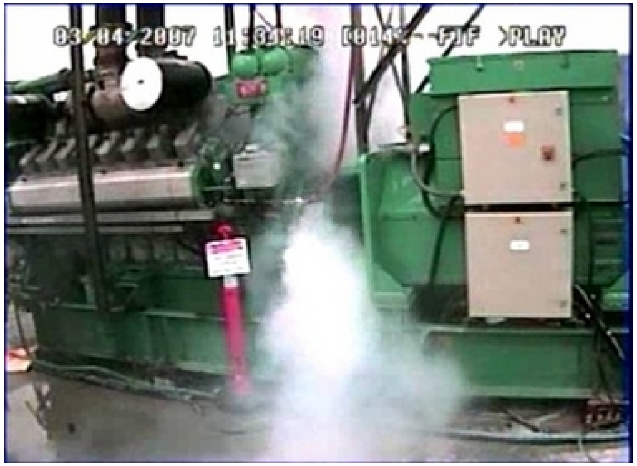
# Pipeline Ruptures

June 1999 Bellingham, WA

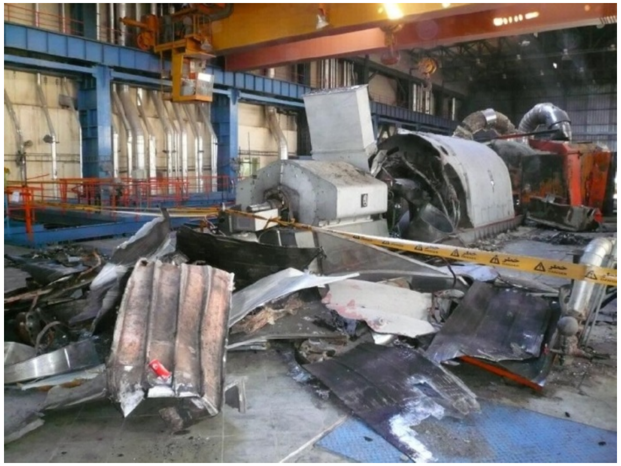
September 2010 San Bruno, CA

# Possible Aurora Attack

Aurora Demonstration - INL



Iranshahr Power Plant - Iran



Common thread- Coupling failures

# What Needs to be Done

- Appropriate regulation
- ICS, IT Security, and Forensics working together
- Improved security of legacy ICSs
- New ICSs with security as part of the initial design
- Resilience and recovery
- ICS cyber security training
- Appropriate information sharing

# Conclusions

- ICSs are a “legitimate” target
- Can not fully secure ICSs
  - Worry about intentional and unintentional
  - Lack of forensics complicates root cause analysis
  - Need to be able to recover
- Need appropriate knowledge, coordination, and legislation

# ICS Cyber-Security Conference 2012

October 22-25, 2012
Norfolk, Virginia

In cooperation with the
Virginia Modeling, Analysis and
Simulation Center (VMASC)

Pas attendees and sponsors

## Why attend the conference?

Learn details of the most recent control system cyber-incidents, from people on the front-lines,

Exchange best practices with peers and control system users from various industries,

Become part of the solution by analyzing root-causes and working with vendors to resolve them,

Expand your network of industrial control system users and solution providers.

## A unique and much-needed event

The conference is focused on the specific cyber-security challenges of **industrial control systems**.

In recent years, hopes of achieving security through obscurity and isolation were dashed by the increased connection of control systems to the internet and contagion from outside elements such as USB thumb-drives.

Control systems differ from IT systems in key aspects – communication protocols & OS, memory & processing capacity, accessibility, lifespan…– as well as in their purpose and priorities – physical world interaction, availability above all else, etc.

Despite those differences, cyber-security discussions lump ICSs into Enterprise and Cloud IT and as a result, ill-fitting security processes and products leave large parts of these particular, complex and impactful systems exposed.

The conference pursues three objectives:

- **To inform**, through the sharing of cyber-vulnerability accounts, in the trusted setting of the conference.
- **To explain**, by analyzing adverse events on ICSs and understanding the interaction of their components
- **To improve** the status quo, by allowing users to be informed and discuss their needs with vendors of control systems and of security solutions in a constructive environment.

More information and registration at

www.ICScybersecurityconference.com

Applied Control Solutions Proprietary Information