



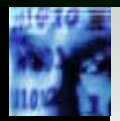

Cyber Security of Industrial Control Systems and Potential Impacts on Nuclear Power Plants

IEEE NPEC

April 18, 2006

Joe Weiss, PE, CISM
KEMA, Inc.

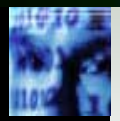
Joe.weiss@kema.com
(408) 253-7934






Why are we here?

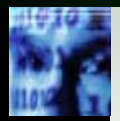
- Ostensibly:
  - Nuclear plant systems are isolated from other systems
  - Nuclear plant networks are isolated from other networks
  - Nuclear plant BOP systems are unique to nuclear plants
  - Nuclear plants have adequate cyber security
- WRONG!!!!!






My Background - Nuclear

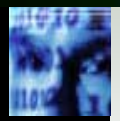
- GE
  - Development and in-plant testing of Gamma Tip
  - Analysis and assessment of in-core vibration issue
  - EQ
  - Licensing - ATWS
- Consulting
  - EQ – final NRC audit for LaSalle
- EPRI
  - Participant in INPO MART visit to Browns Ferry
  - Established Main Coolant Pump Vibration Program
  - Managed Program to Justify Elimination of Response Time Testing Requirements for Pressure Sensors






My Background- Cyber

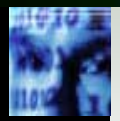
- EPRI
  - Founded and technical lead for EPRI EIS program
  - Identified vulnerabilities of control systems and differences from IT
- KEMA
  - Performed vulnerability and risk assessments of Control Centers (SCADA), power plants, and substations
  - Involved in multiple international standards organizations including ISA, IEEE, IEC, and NERC
  - Contractor to DHS, DOE, NIST, and INL
  - Testified to Congressional Subcommittees
  - Developed and lead annual KEMA Control System Cyber Security Workshop
  - Developed International Standards Coordination Meeting on Control System Cyber Security






Do Something NOW!!!!

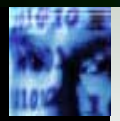
- Awareness and training
  - It's real- do something
- Vulnerability/risk assessments by knowledgeable experts
  - What are the actual issues/concerns
- Development of control system-specific cyber security policies
  - How can you minimize/mitigate concerns
- Share information with vetted (non-nuclear) groups
  - What can I learn from others






What are Industrial Control Systems

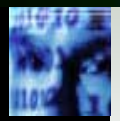
- Digital systems designed to provide real time control and/or monitoring of processes
  - eg, Turbine controls, digital feedwater controls, transformer tap changer controls
- Control systems generally consist of 2 parts
  - Operator interface – Windows, UNIX, LINUX
    - This is what most people think about
    - This is where Denial of Service occurs
  - Field controller – Proprietary Real Time Operating System
    - This part generally has been ignored
    - This is where real damage can be done






Industrial Control Systems

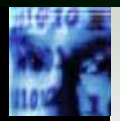
- SCADA – Supervisory Control and Data Acquisition
- DCS – Distributed Control System
- PLC – Programmable Logic Controller
- RTU – Remote Terminal Unit
- IED – Intelligent Electronic Device
- Field devices – Sensors, drives, etc
- HMI – Human Machine Interface






Generations of Control Systems

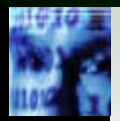
- Generations are generally 15-25 years
  - Nuclear may be longer
- Legacy (next 3-5 years)
  - No security, cyber vulnerabilities because of backfits
- Next generation (next 15-25 years)
  - Some security, cyber vulnerabilities designed in
- Following generation (20-25 years from now)
  - Security and functionality designed in






Control Systems Trends

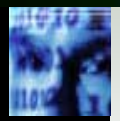
- Decentralizing monitoring and control
- Moving control down to the field devices
- Incorporating new technologies
  - Wireless
  - Neural nets, genetic algorithms, data mining
  - Optical and other advanced sensing
  - Networking technologies
- Replacing cyber “dumb” equipment with cyber “alive” equipment






Common Vulnerabilities

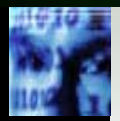
- Inadequate policies and procedures
- Ports and services open to outside
- Operating systems not “patched” with current releases
- Dial-up modems
- Improperly configured equipment (firewall does not guarantee protection)
- Improperly installed/configured software (e.g., default passwords)
- Inadequate physical protection
- Vulnerabilities related to “systems of systems” (component integration)






Culture

- The line between IT and Operations is blurring
- Operations and IT don't like or understand each other
- Engineers "like toys"
  - Including very vulnerable ones
- Engineering doesn't view security as a procurement criteria
- Operations views O&M as their driver; security is an impediment

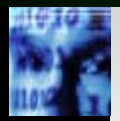





Specific Nuclear Plant Issues

- Many nuclear plant data networks are NOT isolated
  - All domestic nuclear corporate data networks have already been compromised by “white hat” hacker
  - Many nuclear plants connecting plant networks with corporate networks and other external networks
  - Modems and NIC cards found in nuclear facilities
- Vendors still building vulnerable nuclear plant I&C systems
  - Next generation may be more vulnerable
- Lack of information sharing and expertise from outside nuclear

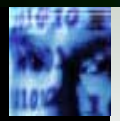
12






Nuclear Regulatory Issues

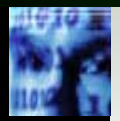
- Cyber is a new type of threat
  - Cyber affects may not have been adequately analyzed or assessed
  - Plant design bases did not consider cyber scenarios
  - Redundancy and diversity did not consider cyber
  - Nuclear plants can be affected by events outside the plant
- Digital Upgrade Methodologies
  - May not adequately address cyber
- Generic Letter 2006-02
  - Does not address cyber
  - Nuclear plant switchyards vulnerable to cyber initiated LOOP






What are the Business Reasons

- Cyber events can cause component or plant unavailability
- Nuclear plant outages can affect grid stability and vice versa
- Appropriate considerations and training to respond to cyber related events can provide additional investment protection






The Threat is Real

- More than 70 known cases (intentional and unintentional)
- All industries
  - Electric (T&D, fossil, hydro, AND nuclear)
    - 4 nuclear facility cyber incidents
  - Oil/gas
  - Water
  - Chemicals
  - Manufacturing
  - Railroads
- Damage ranging from trivial to equipment damage and death

Targeted SCADA Attack

- **Event**: Insecure GIS mapping system with no firewall led to targeted attack resulting in loss of SCADA
- **Information Source**: SCADA Engineer's presentation at 4th KEMA Cyber Security Workshop – August 2004
- **Impact**:
- SCADA servers and mapping system lost for two weeks

Installation of firewalls, proxy servers, IDS and LAN monitors

Neighboring utility networks went from trusted to untrusted

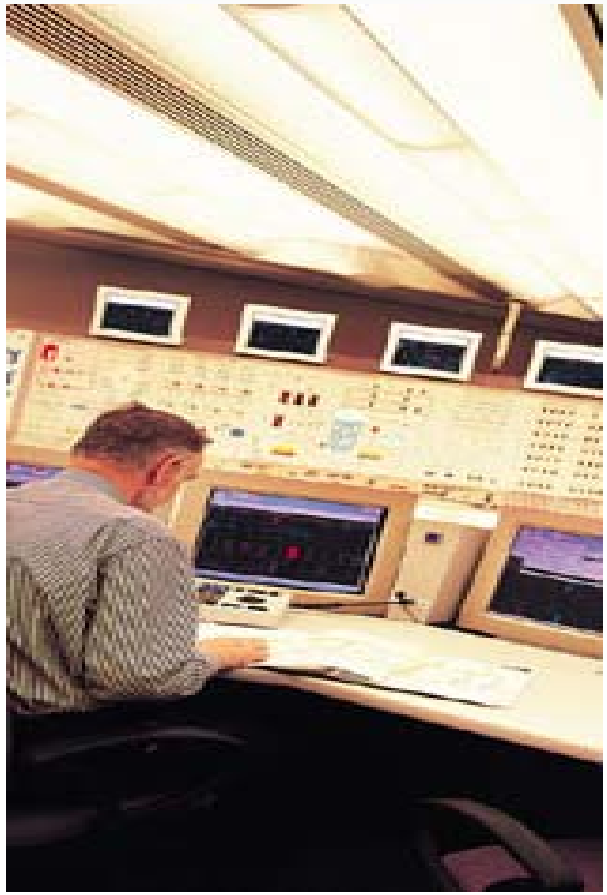
4 Man-months to recover

- **Lessons learned**:

Isolate SCADA system from corporate LAN

Install firewall between the DSL router and the corporate LAN

Install group of firewalls between the frame relay and neighbors to isolate all ports that are not business-related



16

Viruses/Worms

- **Event**: Unintentional effects from virus attack caused substation communication failures. Failures due to virus traffic jamming frame relays.
- **Information Source**: SCADA List server report followed up with telecom confirmation
- **Impact**: SCADA failed resulting in loss of control of switchyards
- **Lessons learned:** Assess and assure Telco (e.g., frame relays) has no Internet connections and they are appropriately secure

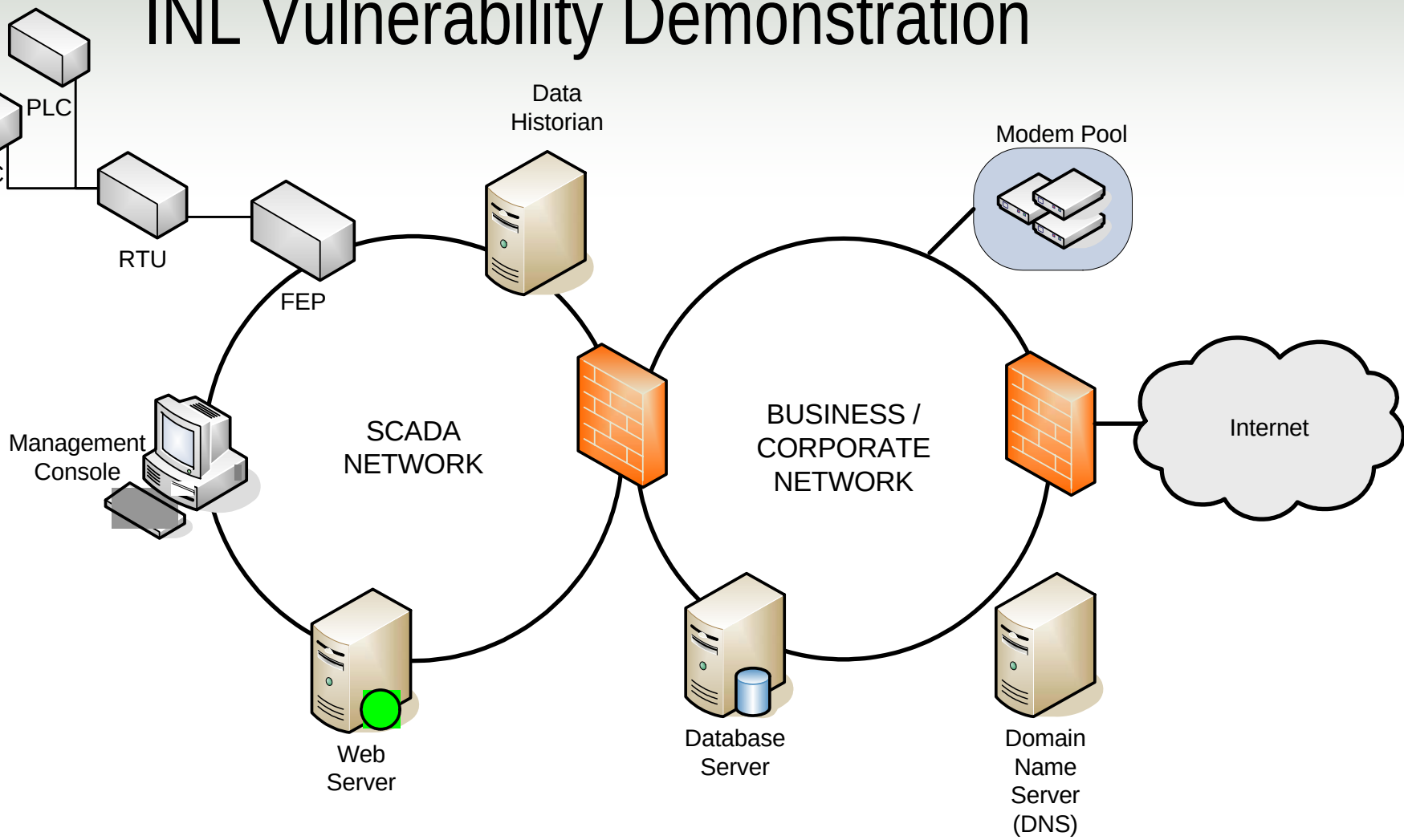
Effective cyber security protection is required

Instrumentation Failure

- **Event**: Remotely controlled Pumped Storage Dam Failure due to instrument failure
- **Information Source**: Utility & FERC
- **Impact**:
  Loss of >450 MW hydro station
  Environmental and economic loss still being evaluated
- **Lessons learned (preliminary)**:
  Hardwired safety systems could prevent catastrophic events
  Secure/Insure instrumentation

18

INL Vulnerability Demonstration



19

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.

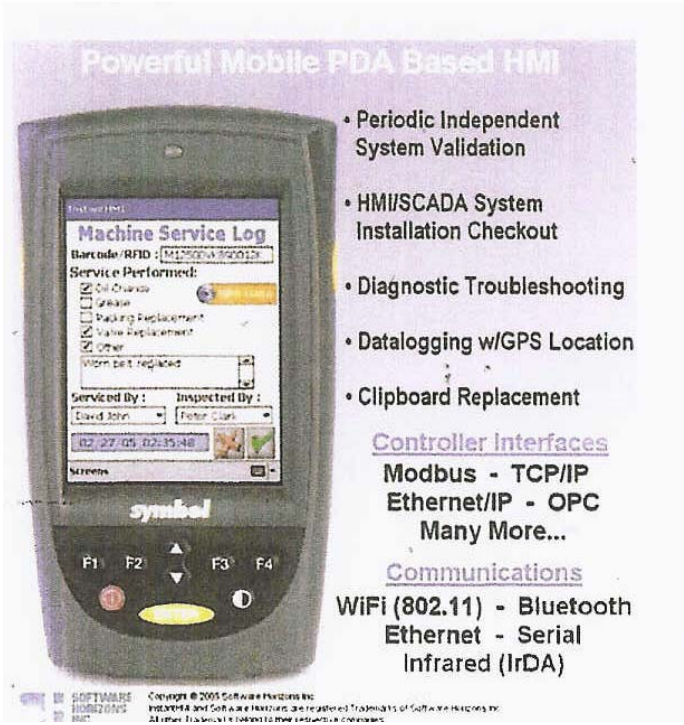
Unit substations include a Temperature Controller, which provides remote access to transformer data, in addition to its primary role in controlling cooling fans. With a simple click of a mouse, it is easy to monitor transformer coil temperatures per phase, and verify cooling fan status at a glance. Among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

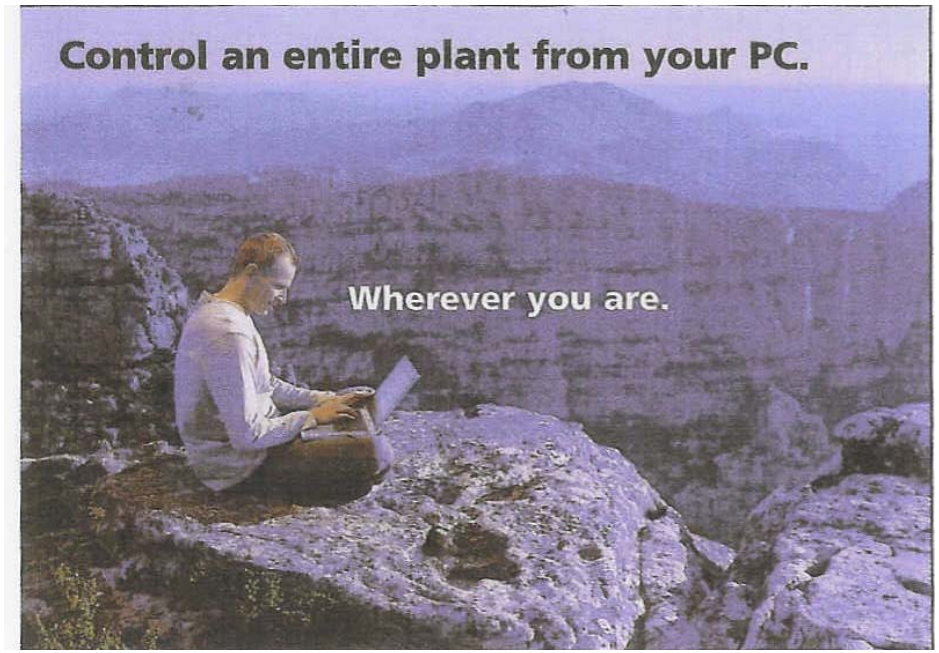
The typical unit substation incorporates Medium Voltage Metal-Enclosed Switchgear on the primary side and Low Voltage Switchgear or Low Voltage Switchboard on the secondary.

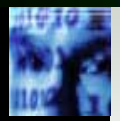
Vendor A was the first manufacturer in the world to embed an Ethernet interface and Web server into its power distribution equipment, allowing customers easier access to power system information. The family of power distribution equipment includes medium and low voltage switchgear, unit substations,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

20

Other New Technologies





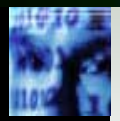





What Should Be Done - Now

- Control system cyber security awareness and training for engineering, plant staff, and senior management
- Vulnerability/risk assessments by knowledgeable experts
  - Includes the plant and switchyard
- Development of control system-specific cyber security policies and procedures
  - Review existing policies for consistency
- Revise procurement specifications to address cyber considerations
- Share information with vetted (non-nuclear) groups

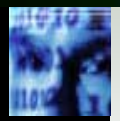
22






What Still Needs to be Done

- Assess equipment capability in controlled setting Implement “CERT for Control Systems”
- Develop secure control system specifications
- Establish baseline for best practices
- Develop secure, efficient control systems (long-term goal)






Summary

- Many nuclear plants are vulnerable to cyber
- Productivity needs and replacing obsolete technologies are making control and monitoring systems vulnerable
- Appropriate policies, procedures, and architectures can make nuclear plants more secure and more reliable
- Attention should be paid to potential cyber impacts on licensing issues