Nuclear Sector Mitigation Experience

An Aurora Experience

Background

Background 1996 – 2000

- **Nuclear sector organized to develop a consistent Y200K effort.**

Nuclear Sector Cyber Security Program 1999- 2003ish

- **With Nuclear Energy Institute's (NEI) facilitation developed a program for Cyber Security**
- **Submitted this program to the Nuclear Regulatory Commission (NRC) for endorsement**
- **Received NRC endorsement**
- **Completed two extensive sets of assessments.**
  - First - Nuclear Significant systems
    - those deemed most essential to plant operations, were completed by May 1st, 2007.
  - Second – Continuity of Power (Some would say NERC systems)
    - Those that could impact continuity of power and was completed this past May 1st, 2008.
- **Program is vulnerability Agnostic**

Aurora – one of many

- **June 0f 2007 the industry was made aware of a control system vulnerability**
  - Asked to implement a series of mitigation steps.
  - Weekly status meetings
  - One hundred percent of the nuclear power assets in the US completed mitigation within 60 days following the notifications.
- **Mitigation**
  - How the vulnerability was presented to the sector, some of the mitigation work performed and some of the issues of vulnerability mitigation in general.

The Program

- Roles and Responsibilities
- Policies and Procedures
- Training and Awareness
- Cyber Security Defensive Strategy
- Configuration Management
- Risk Mitigation
- Incident Response and Recovery
- Audits and Assessments

Continuing Program

- Self Assessments
- Evaluations to Support New or Modified Digital Assets
- Audits
- Contingency/disaster recovery plans
- Periodic Threat Review

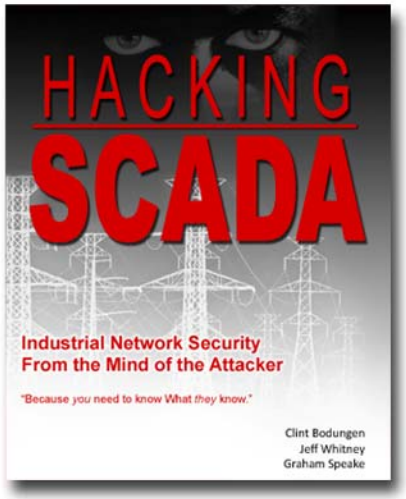
Vulnerability Agnosticism - Program and Process

- **What does it look like**
  - It's an all hazard kind of mentality
  - Forces establishment of rigor
    - Strong desire for "Process" and "Program"
    - Avoids the "winging it approach"
- **The Established Program and Process allows:**
  - Maintaining Cyber Security awareness of issues
  - Maintain well trained staff
  - Knowledge of "What is Critical"
- ***Ability to "Parse" new vulnerabilities and threats quickly***

Power systems being Hacked

- **What we *do* know**
  - Public Disclosure - Cyber attacks against Power system controls outside the US
    - Resulted in multi-city outage
    - Extortion is a motivation – Yep
  - US CERT discloses Control System Vulnerabilities

- **What we *do not* know**
  - Actual extent of hacking successes
  - Consequences of these hacks
- **What we surmise**
  - More Frequent than reported
  - More Significant consequences than claimed
  - Websites devoted to hacking our systems
  - SCADA is now on the RADAR!

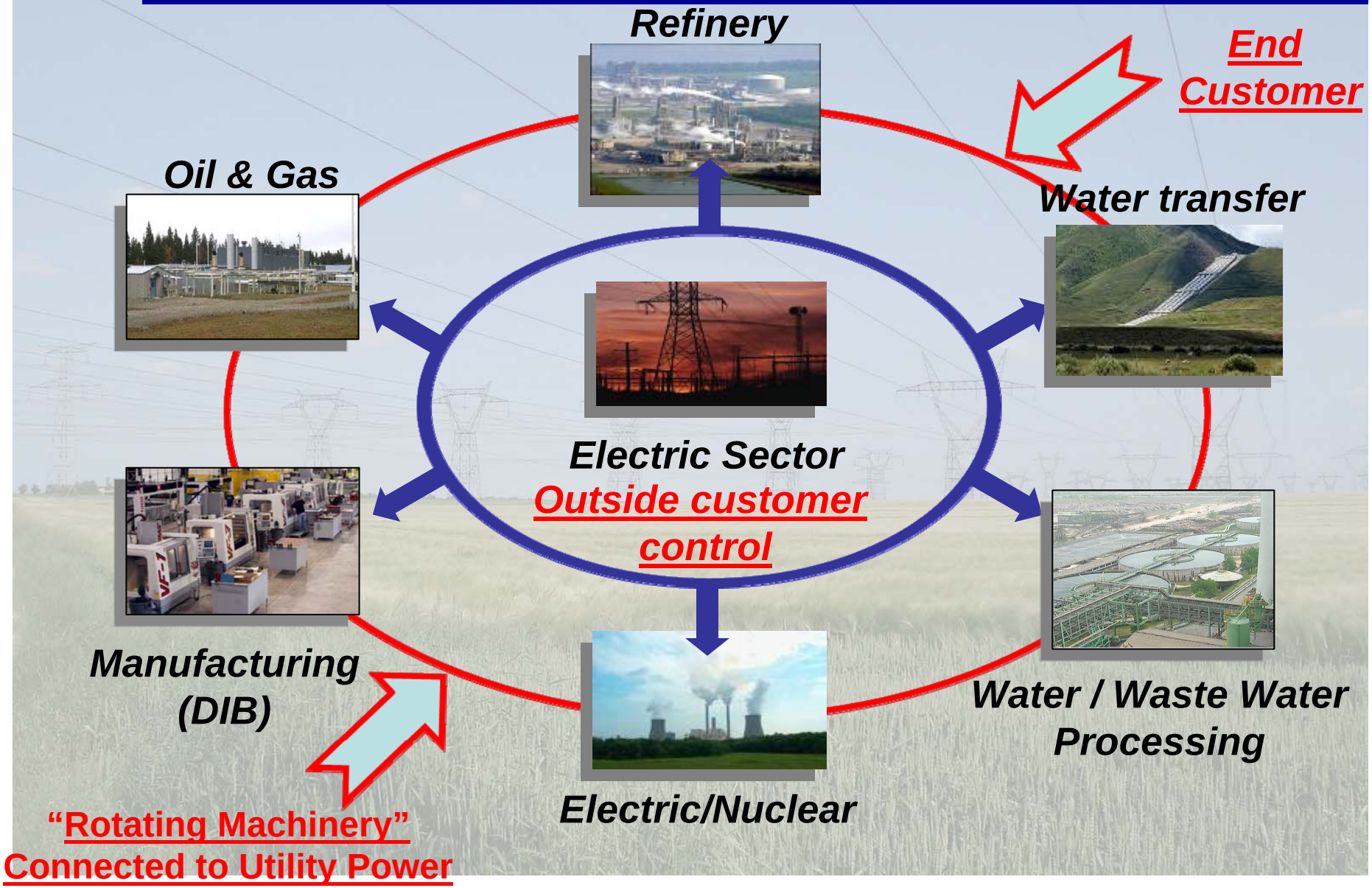


Protection Engineers
Meet Aurora

Aurora Vulnerability – The next new thing

- Vulnerability involves opening and closing breakers quickly
- A digital device that provides breaker control can be found in about 80% of major U.S. substations
- Substation digital devices may be susceptible to cyber attack and compromise by various means of access, both remote and/or physical
- Successful exploitation of the Aurora vulnerability can result in physical damage to rotating equipment connected to the power grid
- Both synchronous generators and motors that drive other devices such as water pumps and gas and oil pumps may be susceptible to the Aurora vulnerability
- Damage to large rotating equipment with long fabrication or procurement lead times is of particular concern; not simply short term power disruption (outage 2 yrs +)
- Modeling predictions have been supported with small and large-scale physical testing
- This attack is not attributable, vendor agnostic, and uses standard logic commands
- Event is too fast to detect with current protections.
- Very difficult to protect against with current measures

Vulnerability and Consequences



AURORA Requirements

- Equipment Necessary for an Attack
  - **Device able to open/close breakers**
  - **High-Speed Breakers**
  - **Laptop/Desktop Computer (or manual control switch)**
- Access required
  - **Physically through the front panel**
  - **Remotely through modem, Internet, wireless, or SCADA**
- Knowledge Necessary to launch an attack:
  - **Power Engineering (attack planning and device setting skills)**
  - **Hacking Skills (exploit the process control device and conduct the attack)**
    - **Manuals, training, and default passwords on the Internet**
- Time Required to Execute the Attack (after gaining access):
  - **Less than one minute**
  - **Logic bombs – time activated autonomously**

AURORA Test Subject

- **Test subject: Commercial diesel generator, rated at 3.8 MVA, and operated at 2.1 MW for test at Idaho National Labs**
- **All protection in place**
- **Supplying power into the 13.8 kV distribution system**

- 3,500 Hours of operation
  - **Connected to the local grid**
  - **Housed in shelter**
  - **Out of service < 2 months**
- Replaced by gas turbine (cost)
- Full machine protection in place
- Can power a 600 bed hospital
- Small-to-medium machine*

* **Small scale test also successful against a 15 hp induction motor**

Aurora Test: Participating Industry Experts

" The Aurora project did demonstrate that the ability to exploit the capability of modern protective equipment and cause them to serve as a destructive weapon"

"I feel that the same results could be achieved by any competent power system protection engineer if provided access and the desire to do so."

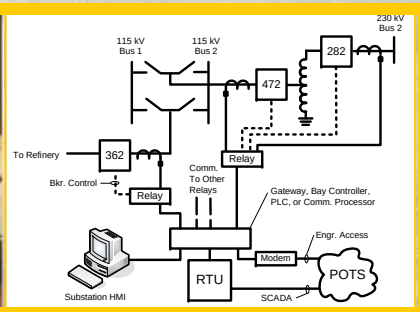
Tim Ernst, Utility power system engineer with 25+ years in the industry

"These types of results could be expected if similar operations occurred against a utility or industrial plant. "

Ed Terlau, Utility power system engineer with 35+ years in the industry

"With this demonstration... it is clearly time we address the security and integrity of substation devices and protection equipment "

Charles Mozina, Utility power system & generator expert



Mitigation Planning - DHS

- **The Electric and Nuclear sectors are considered the highest priority for mitigation implementation**
- **Technical team for the Nuclear and Electric Sector wrote a Mitigation Plan with multi-tiered approach allowing for immediate (zero-day), near, medium, and long term solutions**
- **Interagency team is reaching out to appropriate protective relay vendors to vet the Mitigation Plan and solicit additional ideas to enhance security, such as improved access control and modification of functionality**
- **Mitigation Plan Coordination:**
  - Electric, Nuclear, Water/ Waste Water, ONG Facilities, ONG Pipelines, Chemical, and Dams

Nuclear Sector Mitigation Status

What the nuclear sector did & why

Aurora Quick-Look Checklist

1. Does the facility contain rotating AC electrical equipment identified as a critical asset?

2. Is this critical rotating electrical equipment connected to commercial power at any time?

3. Are there any digital protection and control devices (DPCD) installed in the facility or commercial power system that operate circuit breakers between the rotating electrical equipment and the commercial power generators?

4. Is the electrical network, including the commercial power system, strong enough to allow damaging currents under any credible conditions?

Note: Typical DPCD and associated protective schemes are not designed to take a protective action based on events of the speed or type of the Aurora event.

DOCTOR FUN

1 Oct 2002

Copyright © 2002 David Farley, d-farley@ibiblio.org
http://ibiblio.org/Dave/drfun.html

This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

The daydreams of cat herders

Hurdles in the Process

- **Anecdotes about issues encountered**
- **How were they overcome**
- **Other Stuff**

Integrated Policy to Regional Coordinated Response

National Cross-Sector Level

Partnership for Critical Infrastructure Security

- Integrated Security Policy
- Cross-Sector
- Public-Private Partnership

Integrated Security Policy

Sector Level

18 Sector Councils

Nuclear Sector Coordinating Council

Sector-Specific Security Policies

Local/Facility Level

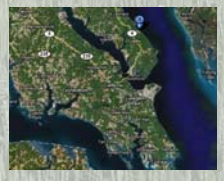
Constellation Energy

Calvert Cliffs Nuclear Power Plant

Energy - Cove Pt. LNG

Transportation - Gov. Thomas Johnson Bridge

Integrated Security Coordination



DISCUSSION