Cyber Security for Nuclear Power Plants

Matthew Bowman
Director of Operations, ATC Nuclear
IEEE NPEC Meeting
July 2012
ATC Nuclear

- ATC-N serves the commercial nuclear utilities in the US and many foreign markets.

- ATC-N uniquely integrates three business areas to serve our nuclear customers:
  1. Commercial Grade Dedication (CGD) and Seismic/Envir. Qualification
  2. Obsolete or Hard-to-Find component Sourcing
  3. E&O inventory cost recovery and management
Overview

- The Cyber Threat: Fact or Fiction?
- Regulatory Background
- Program Implementation for Utilities
- Supply Chain Implications for Vendors
Fact or Fiction?

❖ A topic of much debate over the years

❖ “Is the threat of cyber war grossly exaggerated?”

❖ The cyber threat makes for great TV…
  ▪ 24
  ▪ Mission Impossible
  ▪ WarGames
Reality Check

- Cases of malicious cyber-activity
  - Stuxnet Virus
    - A directed weapon
    - Designed to take control of certain PLCs controlling certain centrifuges
  - Flame Virus
    - Stuxnet follow-up?
  - RSA Security Codes Stolen
    - Google reports state sponsored attacks on Gmail
- All signs point to a new theater for conflict
Recent Statistics

- ICS-Cyber Emergency Response Team Report on Critical Infrastructure
  - 2009: 9 Incidents
  - 2011: 198 Incidents

![Pie chart showing the distribution of incidents across various sectors.](chart.png)
High Tech, High Risk

- Internet Facing Systems...are they worth it?
  - High Vulnerability
  - SHODAN and Penetration Testing

- Hacker toolboxes are readily available

- Implications of SCADA Systems and Digital Upgrades

- The risk must be managed...
February 2002: NRC Order EA-02-026
  - “Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants”
  - Direction to address certain cyber vulnerabilities following 9/11

April 2003: NRC Order EA-03-086
  - “Design Basis Threat for Radiological Sabotage”
  - Provided further definition for the DBT regarding cyber attack

October 2004: NUREG/CR-6847
  - “Cyber Security Self-Assessment Method for US Nuclear Power Plants”
  - Issued to address the growing use of digital equipment, however, not completely sufficient
Regulatory Timeline, cont.

- **December 2005:** NRC endorses NEI 04-04, Rev. 1
  - “Cyber Security Program for Power Reactors”
  - Contained an acceptable approach to developing a CS program in the absence of further guidance from the NRC

- **January 2006:** NRC RG 1.152, Rev. 2
  - “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”
  - Intended to fill in the gaps of IEEE 7-4.3.2-2003 related to code development

- **March 2007:** NRC BTP 7-14, Rev. 5
  - “Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems”
  - Provided guidelines for software lifecycle management
Regulatory Timeline, Cont.

- March 2009: 10 CFR 73.54 Issued
  - “Protection of Digital Computer and Communication Systems and Networks”

- September 2009: NEI 08-09, Rev. 3 Issued
  - Was accepted as adequate by the NRC for compliance with 10 CFR 73.54
A Roadmap for Compliance

- NRC Regulatory Guide 5.71
  - “Cyber Security Programs for Nuclear Facilities,” issued January 2010

- Provides an approach that the NRC deems acceptable for complying with the regulations (10 CFR 73.1) regarding protection of digital systems from a cyber attack

- Based on:
  - NIST SP 800-53 and 800-82: “Guide to Industrial Control Systems Sec.”
  - Findings of bodies such as ISA, IEEE, and DHS

- NEI 10-09
Utility Perspective:
Steps to Program Establishment

- Establish a Team of Experts
- Survey the Landscape – Detailed System Analysis
- Determine what are Critical Digital Assets
- Deploy a Defensive Architecture
- Address Potential Vulnerabilities using Security Controls
- Implement Security Program Lifecycle Management Activities
Identification of Critical Systems

- Conduct a Wide Assessment of Systems
  - Which systems perform Safety, Security, and Emergency Preparedness (SSEP) Functions?
  - Which systems provide support functions for SSEP related systems?
  - Information in the SAR
Critical Digital Asset Determination

Diagram:

1. Critical Systems
   - Performs SSEP Functions
     - YES
     - NO
   - Affects Critical Assets/Functions & Pathways
     - NO
     - YES
2. Supports Critical Assets
   - NO
   - YES
3. Protects Critical Assets
   - YES
   - NO

Result:
- Critical Digital Assets
Is It Critical?

- If the Digital Asset:
  - Performs SSEP Functions
  - Could adversely affect SSEP Functions directly or indirectly
  - Provides a pathway to a CS or CDA
  - Protects CSs, CDAs, or pathways from a cyber attack

- Then it is a **Critical** Digital Asset, and subject to the Cyber Security Regulation

- Note that there is no exemption for “autonomous” systems
Know the Enemy

- Threat Vectors
  - Direct Network Connectivity
  - Wireless Access Capacity
  - Portable Media and Equipment
  - Supply Chain
  - Direct Physical Access

- Defense in Depth starts here
Are the systems connected in any way?

- **Direct Connections**
  - Can be wired or wireless

- **Indirect Connections**
  - Air gap systems
  - “Sneaker Net” – manual carrying of data
  - Electro magnetic fields
How to Protect?

- All Guidance Points to Defense in Depth System Architecture

- A Layered System

- All CDAs directly relevant to Safety and Security are placed in Level 4

- Data only flows from one level to other levels through a device or devices that enforce security policy between each level
One way communications (Data-Diode or an Air Gap) are required between Level 4 and 3, and between Level 3 and 2.

Initiation of communications can only come from a higher level.

Digital isolation recommended by NRC, but not required.
Security Controls

- Fall into Three Categories
  - Technical Controls
    - Executed through non-human mechanisms
  - Operational Controls
    - Executed through human mechanisms
    - Guarding against the insider threat
  - Management Controls
    - Risk management and general policy
    - Includes procurement controls

- Should not be implemented if the control adversely impacts SSEP functions
Technical Controls

- The use of hardware, firmware, operating systems, or application software to perform protective measures

- Provide electronic enforcement of policies such as:
  - Access control: Who can do what…
  - One way communication
  - Reporting of Cyber Attacks

- The Data Diode
  - Provides a means to comply, but still obtain valuable system data
Vendor Perspective: Supply Chain Implications

- Procurement Engineering Guidance
  - EPRI Cyber Security Procurement Project
  - Purchase Order clauses related to Cyber Security

- Rigor in Development and Dedication of Digital Systems
  - IEEE 7-4.3.2 2010
    - Subclause 5.9: Emphasis on Developer/Utility Partnership
  - EPRI TR-106439

- More scrutiny is coming
Vendor Actions

- Get ahead of the game
  - Develop documentation that addresses CS
  - Be prepared to commit the resources needed to do the job right.
  - Make sure that people with the required expertise are applied to the job.
  - Ensure your organization is aware of the new issues related to the “Digital Delta”
In Conclusion

- The threat is real
- Licensees are on the clock
- Suppliers of digital equipment and software must be considering cyber security implications
- Defense in Depth Strategy
  - You are part of the team
  - How we interact with our computer systems is a large part of CS
Questions?
For Further Reference

- NRC Reg Guide 5.71
- IEEE 7-4.3.2, 2003 and 2010 editions
- “Cybersecurity: Authoritative Reports and Resources,” Congressional Research Service
- NY Times articles on Stuxnet and Flame