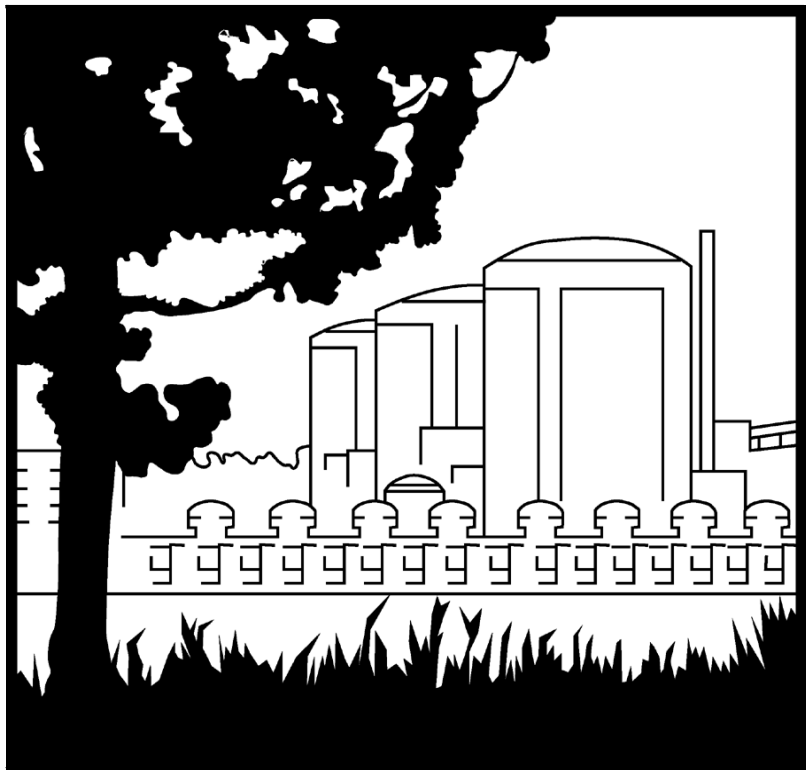
Duke Energy



Cyber Security Aspects of the Oconee Digital RPS/ES

March 9, 2010

Agenda

- Purpose
- Cyber Security Regulatory Guidance
- Digital RPS/ES Security Features
- Question and Answers

Purpose

- Provide an overview of the Cyber Security Aspects of the Oconee Digital RPS/ES Upgrade Project
- Presentation detail is limited due to the security sensitive nature of the information
- Information in Duke's License Amendment Request was labeled sensitive information per 10 CFR 2.390
- The NRC redacted the sensitive information from the SER

Cyber Security Regulatory Guidance

- NEI 04-04 – Cyber Security Program for Power Reactors
  - Issued November 2005
  - Approved by NRC letter dated December 23, 2005
- 10 CFR 73.54 – Digital computer and communication networks
  - Rulemaking completed late in the Oconee RPS/ES review process
- Regulatory Guide 5.71 recently approved with guidance for Cyber Security Plan
- NEI 08-09 – Cyber Security Plan Template is still under review by the NRC

Cyber Security Regulatory Guidance

- EPRI TR-102348, Revision 1 Report
  - Security of digital systems to control access and prevent unauthorized changes (Section 5.3.4.5)
  - Endorsed by RIS 2002-22
- Regulatory Guide 1.152, Revision 2
  - The development process should address potential security vulnerabilities in each phase of software lifecycle.
  - The lifecycle phase-specific security requirements should be commensurate with the risk and magnitude of the harm resulting from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the digital safety system.
  - NRC Task Working Group (TWG #1) addressing cyber security aspects
  - Primary source of guidance for certification of the Oconee Digital RPS/ES upgrade

Digital RPS/ES Security Features

- Review and summarize RPS/ES design features that provide layers of cyber security defense for the system relative to the following areas:
  - Corporate Program
  - System Physical Features
  - System and Support Equipment Software Aspects
  - Licensee O&M Aspects and Features

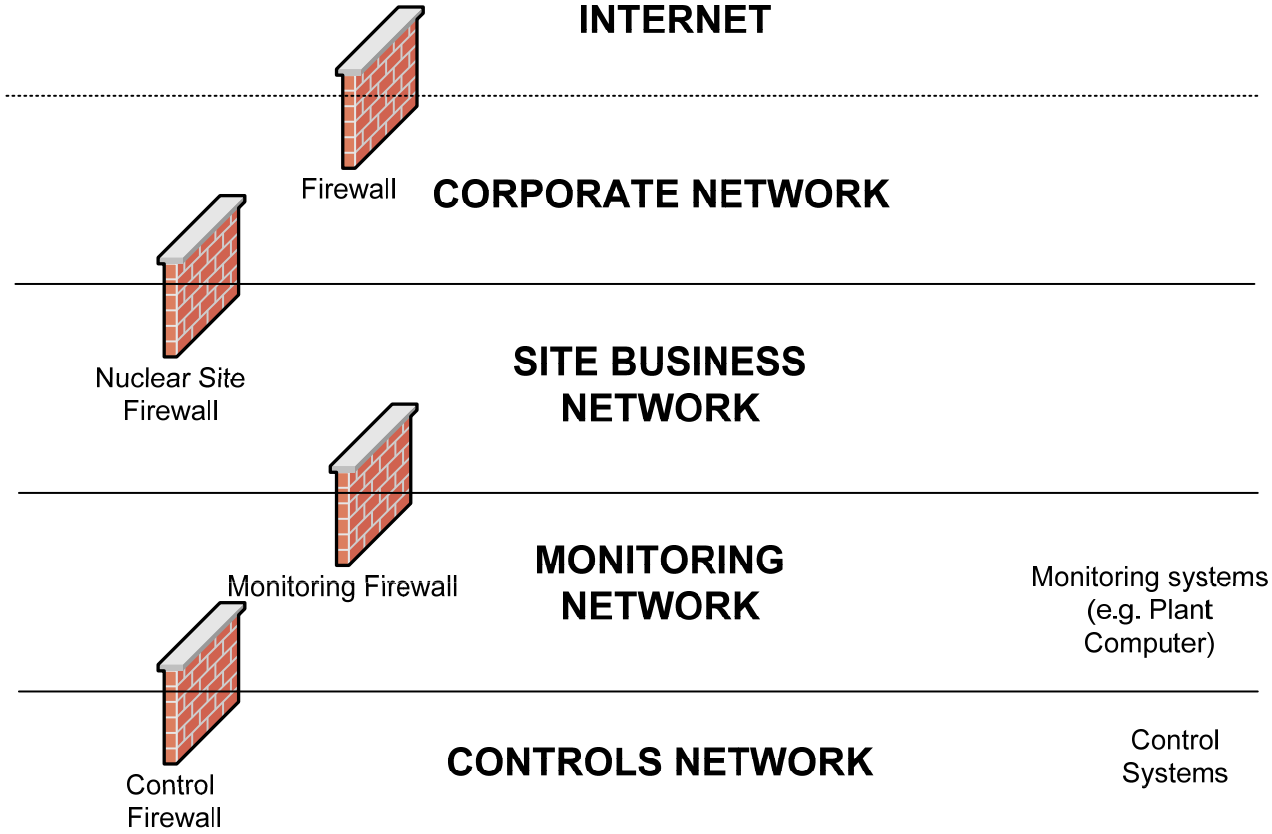
Corporate Program

- Nuclear System Directives (NSDs) developed and revised to address cyber security
  - NSD 804, Cyber Security for Digital Process Systems
  - NSD 807, Cyber Security Incident Response
- Corporate IT Standards Referenced
  - IT6000 Series, SCADA Cyber Security Policy & Standards
- Engineering Directives
  - EDM 801, Cyber Security Risk Evaluation

System Physical Features

- Multiple corporate and site network defensive features
- Numerous firewalls between Oconee networks and outside world
  - Modification to install data diode between Oconee controls network and outside world is in progress
- External connections from system are only to the Service Unit and plant computer. Connection to plant computer is via hardware based “Check-Valve”
- Plant computer connection is via single purpose dedicated gateway computer(s) which provides additional layer of defense

Isolation of Digital Systems from Network



RPS/ES Located Here

System and Support Equipment Software Aspects

- Software protections have been designed into the Digital RPS/ES
  - Service Unit
  - Gateway
  - Application Specific Interface Software
- Software features utilized in the design of system provide multiple layers of detection and defense.

Licensee O&M Aspects and Features

- Service Unit and RPS/ES system processors located in plant and access is limited to permitted personnel only.
- RPS/ES cabinets located behind control area adjacent to normal operations pathways with doors locked. Access to cabinets by Work Control and Operations authorization. Cabinet keys required for access.
- Cabinet doors alarm in the Control Room.
- Service Unit in plant computer area. Access to area limited and doors are locked.
- Keyswitch position change required for system change and is alarmed in the Control Room. Keys controlled by Operations.
- Vital access requirements, work authorization process, cabinet door alarms, and key switch position alarms provide additional layers of detection and defense.

Questions and Answers

???