U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

NRC Perspectives on Control of Access:
Secure Development and Operational Environment (SDOE) & Cyber Security

Tim Mossman, NRO Sr. Electronics Engineer
Eric Lee, NSIR Sr. Security Specialist (Cyber)

Prepared for
DSRS I&C Workshop
November 2013

NRC Regulatory Framework

- Licensing reviews against the requirements of 10 CFR Part 50 specifically address safety
  - Staff will evaluate digital safety systems for a Secure Development and Operational Environment
- 10 CFR Part 73 covers security and protection from malicious activity, including cyber security
  - Staff will evaluate licensees' cyber programs and protection of Critical Digital Assets (CDAs)
  - CDAs include systems associated with safety, important-to-safety, security and emergency preparedness functions, as well as digital support systems for any of the above

Part 50 SDOE

- Regulation
  - 10 CFR 50.55a(h), IEEE Std. 603-1991
    - Clauses 5.6.3 (Independence) and 5.9 (Access Control)
  - 10 CFR Part 50, Appendix A, GDC 21, “Protection System Reliability and Testability”
  - 10 CFR Part 50, Appendix B, Criterion III, “Design Control”
- Guidance
  - Regulatory Guide 1.152, Rev. 3 (2011)
  - IEEE Std. 7-4.3.2-2003

Regulatory Guide 1.152 Rev. 3

- Secure Development Environment
  - Develop safety systems in a secure environment (e.g. verification and validation of system requirements, design, coding phases; configuration management)
- Secure Operational Environment
  - Establish an operational environment to ensure reliable system operation

Secure Operational Environment

- If the application conforms to NRC guidance and satisfies all requirements, the staff will be able to conclude that a Secure Operational Environment will be established for the digital safety system such that measures provide reasonable assurance to prevent inadvertent unauthorized access to the system and to prevent any undesirable behavior from of connected systems from affecting its operation.

Inadvertent Access?

- As previously stated, intentional, malicious activity is addressed under 10 CFR 73.54 programs
- Inadvertent access is postulated to be an event involving plant personnel (or an on-site contractor) with no nefarious motive
  - Physical points of access include open communication ports on the system that someone from the licensee's workforce may mistakenly attempt to connect into
  - Logical points of access include any points of human interface on systems connected to the same network on which the digital safety system resides

Cyber Controls for SOE?

- Licensees can credit controls in their approved cyber security plans (submitted per 10 CFR 73.54) as part of their secure operational environment story
  - However, Staff will only make findings in regard to Part 50 requirements
  - Suitability and effectiveness of controls for cyber purposes are evaluated by periodic inspection

Inadvertent access protections?

- Staff has reviewed and allowed credit for:
  - Physical barriers, administrative controls, and alarms protecting physical access to digital safety systems
  - Logical access controls on any equipment designed to interface with the digital safety system
    - Area of synergy with cyber security controls

Undesirable Behavior Protections?

- Staff has reviewed and allowed credit for :
  - Isolation of the digital safety system (!)
  - Hardware-based (*and software-based**) devices that enforce one-way communication
  - ISG#04 communication controls
  - CRC checks on software code
  - CRC checks on messages
  - Out-of-range checks on data
  - “White lists” of acceptable messages

** May not be appropriate for cyber security program based on RG 5.71*

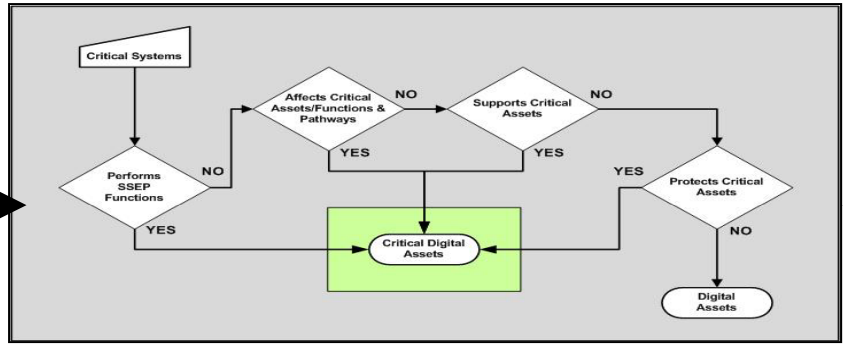
10 CFR 73.54: Protection of digital computer and communication systems and networks

- Performance-Based, Programmatic (< 2 pages)
  - Provide high assurance against cyber attack
  - Integrated with Physical Security Program (10 CFR 73.55)
- Main emphasis of regulations / guidance
  - Critical digital assets must be protected
    - Safety, important-to-safety, security, and emergency preparedness <u>functions</u> and support systems that can impact those functions
  - Defense-in-depth protective strategy
  - Records maintained until the license is terminated

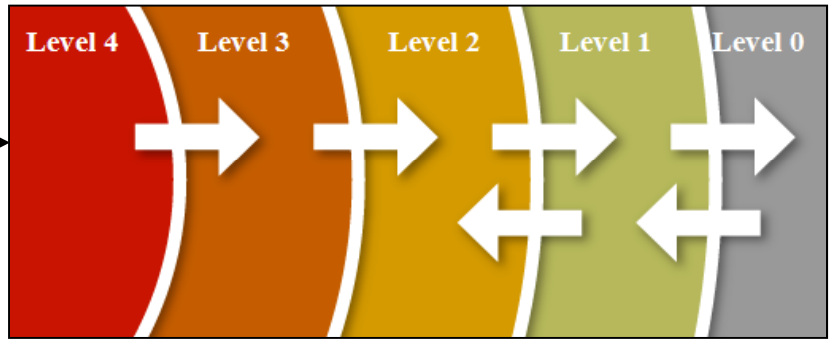
Regulatory Guide 5.71

Form Cyber Security Team

Identify Critical Digital Assets



Apply Defensive Architecture



Address Security Controls

1. Address each control for each CDA, or
2. Apply alternative measures, or
3. Explain why a control is N/A

Regulatory Guide 5.71

- Security Controls
  - Appendix A (generic Cyber Security Plan template)
  - Appendix B (technical security controls)
  - Appendix C (operational/management security controls)
- Address Security Controls
  - Apply security control to CDA
  - If security control can not be implemented then use alternative controls or countermeasures with same degree of protection
  - If the security issue does not exist, then the security control is not applicable

Cyber Security Plans (CSP)

- Licensing document / required by regulation and incorporated into licensing basis (10 CFR 73.55)
- Describes how cyber security program is established and maintained
- Essential elements – Plan must:
  - describe roles and responsibilities of a multi-disciplinary Cyber Security Team
  - describe the process for identifying Critical Digital Assets
  - <u>describe the defensive model (protective strategy)</u>
  - reference comprehensive security controls
  - describe the process for addressing controls
  - address document control and maintenance

Questions

Acronyms

- CDA – Critical Digital Asset
- CFR – Code of Federal Regulations
- CRC – Cyclic Redundancy Check
- CSP – Cyber Security Plan
- DSRS – Design Specific Review Standard
- GDC – General Design Criterion
- HA - Hazard Analysis
- IEEE – Institute of Electrical and Electronics Engineers
- ISG – Interim Staff Guidance
- I&C - Instrumentation and Controls
- RG – Regulatory Guide
- SDE – Secure Development Environment
- SDOE – Secure Development and Operational Environment
- SOE – Secure Operational Environment