Three Threads of Security at Nuclear Power Plants

Key Concept: Understanding and evaluating three distinct threads of cybersecurity is crucial for nuclear facility safety and security

Tim Roxey

Overview of the Three Domains

1. Systems, Structures, and Components (SSC) view of risk
    1. Focus on critical physical systems that maintain nuclear safety
2. Computer Application view of risk
    1. Focus on software and digital systems that support critical functions
3. Target Set view of risk
    1. Focus on physical security and command & control system

Each of these three domains has an impact on the facility design basis.

Why This Matters

- Each assessment area evaluates specific types of risk
- A complete cyber assessment requires all three perspectives
- All domains ultimately relate to the facility's Safety Analysis Report (SAR)
- Proper assessment ensures comprehensive protection of nuclear facilities

Domain 1: Systems, Structures, and Components (SSCs)

What Are Critical Systems?

- Nuclear Safety Systems: Prevent/mitigate design basis accidents
- Continuity of Power Systems: Ensure operational control

Key Characteristics:

- Directly contribute to core damage frequency (CDF)
- Functions documented in the Updated Final Safety Analysis Report (UFSAR)
- Subject to Maintenance Rule (MR) documentation
- Evaluated in Probabilistic Risk Assessment (PRA)

Domain 1: SSC Risk Assessment

Focus Areas:

- SSCs with the highest contribution to Core Damage Frequency
- Systems that prevent or mitigate design-based accidents (DBAs)
- Components with cyber elements that could affect safety functions

Risk Perspective:

- Cyber compromise could deny the availability of critical safety functions
- Protecting cyber components ensures SSC reliability and availability
- Direct implications for regulatory compliance and nuclear safety

Domain 2: Application View of Risk

Critical Applications Include:

- Engineering codes that support critical systems analysis
- Programs that evaluate nuclear core parameters
- Applications calculating risk probabilities
- Structural analysis software
- NRC Emergency Response Data System (ERDS) elements
- Security codes and systems

Domain 2: Application Assessment Approach

Assessment Methodology:

- Based on an inventory of "safety-related" software
- Managed through the facility's Software Quality Assurance (SQA) program
- Includes systems that may not be classically "safety-related" but support security and regulatory functions
- Focus on maintaining the integrity of critical calculations and analyses

Domain 3: Target Set View of Risk

Understanding Target Sets:

- Related to the physical security of critical SSCs
- Ensures the continued functioning of physical systems
- Focuses on defense capabilities against physical threats

The C4 Model:

- Command
- Control
- Communications
- Computers

Sometimes C4I, when Intelligence is included

Domain 3: Target Set Assessment

Assessment Approach:

- Review target sets for cyber dependencies
- Evaluate the impact of cyber compromises on defense capabilities
- Identify communication vulnerabilities
- Ensure redundancy in command and control systems
- Maintain the defense force's ability to protect critical assets

Key Terminology

- Design-basis accident (DBA):
  - Postulated event used to establish performance requirements
- Critical digital asset (CDA):
  - Digital device affecting critical system function
- Critical system (CS):
  - Systems categorized as nuclear-significant or continuity of power
- Nuclear Significant:
  - Systems required for public health and safety protection
- Operational Control Systems:
  - I&C systems for normal operations, not relied on for safety functions

Contact Information

Tim Roxey Email: Tim.roxey@gmail.com