U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Security by Design – Physical and Cyber Security Design Considerations

Pete Lee and Kim Lawson-Jenkins

Office of Nuclear Security and Incident Response

April 25, 2017

Regulatory Requirements for Nuclear Power Reactors

10 CFR Part 73

- When adequately met and implemented, these requirements provide protection of nuclear power reactors against acts of radiological sabotage, prevent the theft or diversion of special nuclear material, and protect safeguards information against unauthorized release
- Establishes various requirements for design of engineered physical security systems for power reactors
- Contains performance and prescriptive regulatory requirements

Commission Policy Statement
Advanced Reactors

The design of advanced reactors should

> "include considerations for safety and security requirements together in the design process such that security issues (e.g., newly identified threats of terrorist attacks) can be effectively resolved through facility design and engineered security features, and formulation of mitigation measures, with reduced reliance on human actions."

73 FR 60612; October 14, 2008

Physical Security Design Considerations

- Security design considerations are not requirements
- Identify considerations in design of physical security systems to achieve its intended functions
- Provide guidance to non-LWR applicants
- Security design considerations issued for public comment (FRN 2017-04873; March 13, 2017)

Security Design Considerations for Non-Light Water Reactors

Intrusion Detection Systems

- Design of engineered SSC relied on for detection (interior and exterior) should
  - Provide assurance of detecting unauthorized access into vital and protected areas
  - Apply the principle of diversity necessary for reliability and availability of SSC to achieve intended detection functions
- The initiation of plant security response begins and is based on this critical function

Security Design Considerations for Non-Light Water Reactors

Intrusion Assessment Systems

- Design of security SSC relied on for assessment (interior and exterior) should
  - Provide assurance of rapid remote assessment to determine cause and initiate security response
  - Apply the principle of diversity
- Reliability and availability of SSC to achieve intended detection functions
- Implementation of security response relies on information provided by these systems for protecting the nuclear power plant

Security Design Considerations for Non-Light Water Reactors

Security Communication Systems

- Design of security SSC relied on for security communications should
  - Provide assurance of continuity and integrity of communications
  - Account for design basis threats that can interrupt or interfere with continuity or integrity
  - Apply the principles of redundancy and diversity
- Engineered systems for communications (dedicated or plant systems) are relied on for security response to the DBT onsite and for offsite assistance

Security Design Considerations for Non-Light Water Reactors

Security Delay Systems

- Design of security SSC relied on for delay functions should
  - Provide assurance for security response
  - Provide appropriate layering for defense-in-depth
- Sufficient delay times achieved by design of delay barrier systems and plant configurations enable security responses to interrupt adversaries from completing tasks

Security Design Considerations for Non-Light Water Reactors

Security Response

- Design of engineered SSC performing neutralization functions and engineered fighting positions relied on to protect security responders performing neutralization functions should
  - Provide assurance of overlapping field of fire
  - Provide opportunities for security response, with each layer assuring that a single failure does not result in the loss of capability to neutralize DBT adversary

Security Design Considerations for Non-Light Water Reactors

Control Measures Protecting Against Vehicle Bombs

- Design of security SSC relied on to protect against vehicle bomb assaults should
  - Protect reactor building and structures containing critical safety and security SSC or functions from the explosive effects of the maximum DBT quantity
  - Provide bounding minimum safe stand-off distance

Security Design Considerations for Non-Light Water Reactors

Access Control Portals

- Design of access control portals should
  - Provide assurance of detecting and denying unauthorized access to persons and pass-through of contraband material
  - Apply the principles of redundancy and diversity to achieve intended control functions
- Engineered SSC detect and deny unauthorized persons and material into the protected area

Some Design Approaches

Plant Layout – layered security boundaries

- Owner controlled Area (OCA)
  - enclosed by fence (signage, lighting, etc.)
- Security controlled area (SCA)
  - inside OCA
  - vehicle and personnel barrier systems
  - alarms/assessment, standoff from PA

Some Design Approaches

- Protected Area (PA) - inside SCA
  - Multiple delay barriers, perimeter intrusion detection and assessment system, isolation zones, engagement space – interdict/neutralize
  - PA enclose the nuclear reactor building
  - Arrange PA, nuclear reactor building, and physical barriers to efficiently achieve security functions
- Vital Area (VA) - Inside PA
  - Limit access to VA to only those needed

Some Design Approaches

Building Configuration

- Enhance line of sight – eliminate blind spots
- Harden access – walls, doors, windows, openings
- Limit number of entry and exit access
- Harden entry and exit points
- Separate vital equipment
- Compartment building areas
- Limit access pathways between areas

Some Design Approaches

Physical security systems

- Active delay barriers
- Automated access authorization verification
- Remotely control physical access
- Remotely operated weapon systems
- Deployable interdiction or neutralization systems

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Security By Design – Cybersecurity Considerations

Kim Lawson-Jenkins
Cyber Security Specialist

Introduction

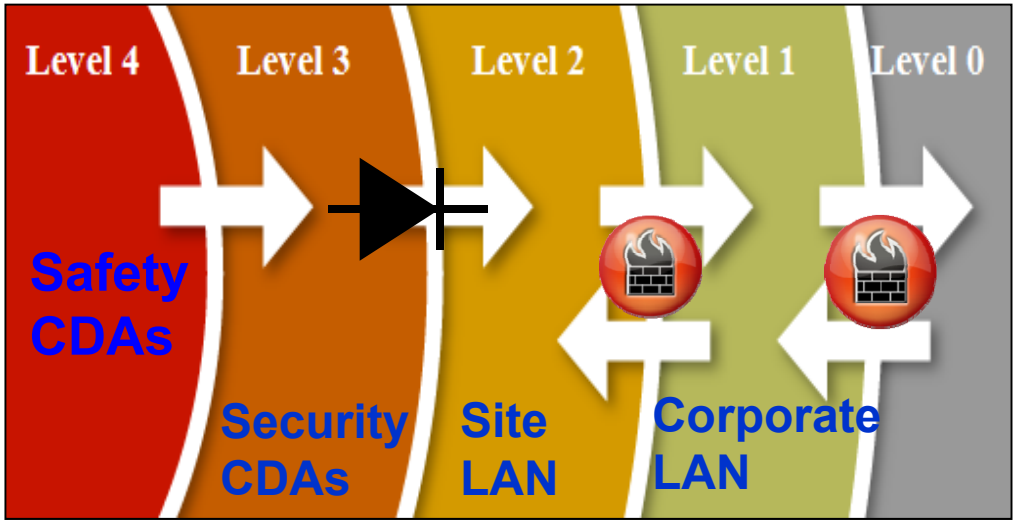
- 10 CFR 73.54
- Regulatory Guide 5.71
  - Defensive Model Architecture
  - Defense in Depth
  - Least Functionality

Defense Model Architecture

- The design of the defensive architecture for digital systems and networks to protect against a cyber attack should establish the logical and physical boundaries between digital assets with similar risks and digital assets with lower security risks.

Defense Model Architecture

- Digital assets associated with safety, important to safety, and security functions should be located at the highest security level and protected from all lower levels.



Cyber Security Defense-in-Depth

- A defense-in-depth protective strategy consisting of complementary and redundant cyber security controls should be employed to establish layers of protections to safeguard critical digital assets, critical systems, or both.

Cyber Security Defense-in-Depth

An Example -

- A CDA in a vital area of the plant is effectively protected from malware.
  - Host intrusion detection system
  - Flaw remediation
  - Malicious code protection
  - Security functionality verification
  - Security alerts and advisories
  - Software and information integrity

Least Functionality

- The design should:
  - Eliminate unused/unnecessary functionality, protocols, ports, and services; or
  - Disable unused/unnecessary functionality, protocols, ports, and services; or
  - Provide protections to prevent the use of unused/unnecessary functionality, protocols, ports, and services when eliminating or disabling the capabilities is not practical.

Least Functionality

- Reduce attack surface and attack vectors
- Minimize data to be monitored and analyzed
- Makes it easier for the licensee to know the capabilities of their system and what is normal behavior on their system

Questions