Integrating Cyber Security into Nuclear Power Plant Safety Systems Design

Deanna Zhang

U.S. Nuclear Regulatory Commission

Document Date: 05/21/2010

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Objectives

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

To provide methods for utilizing safety features, and implementing additional cyber security features within safety systems, to mitigate cyber security vulnerabilities without impacting safety functions.

To discuss various configuration management and access control methods that may implemented throughout system development to ensure safety system integrity.

Agenda

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

- Overview
- Safety Features That Enhance Cyber Security
- Improving Security Without Impacting Safety
- Securing the Development Environment
- Summary

Cyber Security for Nuclear Power Plants (NPPs): Overview

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

- Cyber security has become a significant component in the overall protection of nuclear I&C safety systems
  - Increased use of digital safety and control systems within NPPs
  - Increased level of connectivity between safety systems and other systems
- To mitigate new safety concerns, cyber security should be included in the overall security program
  - Cyber security features that ensure confidentiality, integrity, and availability may be integrated into system design
  - An information security program should be used to prevent malicious manipulation of the system throughout development
- Cyber security features must be implemented so that they do not adversely impact the performance and operation of safety systems

Safety Features That Enhance Cyber Security: Overview

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

- Several features already implemented in the safety system to address design basis requirements may also protect the system from potential cyber attack:
  - Features that support communications independence
  - Features that support system reliability
  - Features that support and system diversity

Safety Features That Enhance Cyber Security: Communications Independence

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

- Safety systems should be designed to prevent failures of non-safety systems from adversely impacting or degrading safety functions
  - Most safety applications do not receive any data from non-safety systems, or only allow uni-directional from safety to non-safety systems
  - In the few cases where bi-directional communication is allowed:
    - Implement error detection
    - Limit the data that is sent to pre-defined messages

Safety Features That Enhance Cyber Security: Communications Independence

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

- Features that ensure communications independence also augment cyber security measures by enforcing communications flow
  - Safety systems that communicate uni-directionally with non-safety systems utilize an isolation device as a logical barrier, to prevent unauthorized access
  - For bi-directional communication, design features ensure that any malicious data sent from non-safety systems to safety systems is detected and isolated

Safety Features That Enhance Cyber Security: System Reliability

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

- To ensure high functional reliability, safety systems should be:
  - Designed with sufficient independence and redundancy
  - Designed to fail into a safe state
  - Designed with multiple redundant divisions

Safety Features That Enhance Cyber Security: System Reliability

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

- Features that ensure system reliability can be used to prevent cyber attacks from disabling or degrading safety functions
  - Safety systems that have sufficient redundancy and independence from non-safety systems prevent a successful cyber penetration from impacting multiple redundant portions of the safety systems
  - Assurance that a safety system will fail in a safe state prevents a successful cyber penetration from defeating the safety function provided by the system
    - This assurance must be provided by physical constraints.

Safety Features That Enhance Cyber Security: System Diversity

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

- Safety systems should employ diversity in the design, as well as depth-in-depth, to prevent loss of the safety functions function
  - Prevents common-cause failures in digital safety systems from defeating safety functions
  - To meet these requirements, safety systems should:
    - Be designed with sufficient diversity or have an independent and diverse backup
    - Incorporate adequate defense-in-depth design principles to maintain the safety function

Safety Features That Enhance Cyber Security: System Diversity

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

- System diversity can be used to prevent cyber attacks from disabling or degrading safety systems
  - A diverse system that is not susceptible to cyber attack (e.g. analog system) can maintain safety function if digital safety systems are compromised
  - Defense-in-depth may also thwart or delay a cyber attack so that operators can safely shutdown the reactor before safety functions are compromised

Improving Security Without Impacting Safety: Ensuring Confidentiality

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

- Confidentiality prevents information transmitted/received by a safety system from being intercepted and used by an adversary
  - Typically ensured via cryptographic mechanisms
- Cryptographic mechanisms should be limited to communication between safety and non-safety systems
  - Alternative protective measures may be used in cases for which cryptographic methods add unreasonable overhead , which may include:
    - Physically and logically limiting access to the system
    - Actively monitoring and recording all physical and logical access
    - Ensuring the qualifications and trustworthiness of individuals who have access to the system

Improving Security Without Impacting Safety: Ensuring Integrity

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

- Integrity prevents an attacker from maliciously tampering with safety systems
  - Typically ensured by preventing unauthorized modifications/tampering of safety system software/hardware
    - A combination of access control measures should be implemented to prevent unauthorized modification of the system from direct interfaces
    - Cryptographic mechanisms may be used to protect the integrity of communication from the data link or network
    - When cryptographic measures cannot be used, consider the following options:
      - Mechanisms that prevent “man-in-the-middle” (MITM) attacks
      - Implement a network monitoring mechanism to detect MITM attacks

Improving Security Without Impacting Safety: Ensuring Availability

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

- Safety system availability may be compromised by:
  - Disrupting the operation of the safety system
  - Preventing authorized users from accessing the system
- Attacks intended to impact the availability of a safety system may be mitigated by:
  - Implementing mechanisms at the system's external interface to protect against or limit the effects of denial of service attacks
  - Configuring systems to restrict the ability of users to launch Denial of Service (DoS) attacks against other systems (especially safety systems)
  - Configuring systems and/or their corresponding networks to manage excess capacity and/or bandwidth

Securing the Development Environment: Overview

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

- High functional reliability for a safety system is achieved by having protective measures in place throughout design and development
  - Should include mechanisms for protecting critical systems from cyber intrusions, including those that may impact the integrity of system design
- The development environment is typically secured via a robust information security program
  - Used to prevent tampering or manipulation of the system while under development

Securing the Development Environment: Information Security Program

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

- **Physical security:** Prevents unauthorized physical access to system design information and development tools
- **Personnel Security:** Ensures that individuals who have unescorted access (electronic/physical) to the development facility can be trusted
- **System and Services Acquisition:** Ensures that systems/services acquired for system development have not been compromised prior to acquisition
- **System Hardening:** Ensures that all existing software development tools and networks are securely configured to protect the integrity of system design

Securing the Development Environment: Information Security Program

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

- **Configuration management:** Ensures that:
  - Modifications to development tools do not reduce existing security controls
  - Unauthorized/unintended modifications to development tools is detected
  - Unauthorized/unintended modifications to the safety system design is detected
  - All modifications to the safety system hardware and software are tracked
- **Access control:** Ensures that only authorized individuals and/or secured electronic devices can access the development tools

Summary

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

- Cyber security features may be integrated into the design of safety systems in a manner that does not adversely impact safety function
- Several current safety requirements can be leveraged for cyber security
- A robust information security program that is implemented during the development process can further mitigate cyber security concerns within the supply chain

Questions/comments?

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