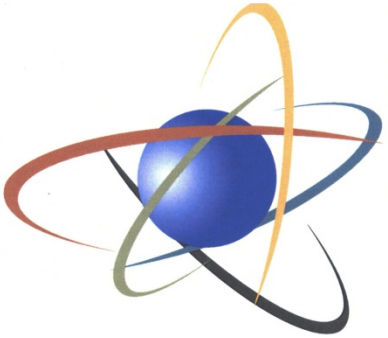

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Cyber Security in Design SECY

Scenarios of Cyber Design Controls Licensing Reviews

Deanna Zhang

08/18/2015

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

ACRONYMS

- CDA: critical digital asset
- DC: design certification
- FOR: fiber optic receiver
- FOT: fiber optic transmitter
- ITAAC: inspection, test, analyses, and acceptance criteria
- LAR: license amendment request
- NRC: Nuclear Regulatory Commission
- RG: regulatory guide

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

Introduction

- **The NRC is in the process of drafting a SECY to request Commission direction on evaluating cyber security-related design features**
  - No expansion to the scope of cyber security requirements beyond the requirements currently stated in 10 CFR 73.54
  - Two options modify the licensing process to enable the review of cyber security design information during I&C licensing activities

- **During the last public meeting, industry representatives requested for the NRC to provide scenarios to demonstrate what a cyber security design review could look like**

Scenario #1
Relevant Sections of RG 5.71

- **Scenario #1: Review of one-way boundary device between level 4 and level 3 and between level 3 and lower levels**
  - RG 5.71 Section B.1.4
    - enforcing and documenting assigned authorizations for controlling the flow of information, in near-real time, within CDAs and between interconnected systems in accordance with the established defensive strategy
    - implementing and documenting information flow control enforcement using protected processing level (e.g., domain type-enforcement) as a basis for flow control decisions
    - implementing near-real time capabilities to detect, deter, prevent, and respond to illegal or unauthorized information flows
    - **implementing one-way data flows using hardware mechanisms**
    - implementing dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations

Scenario #1
DC Applicant Actions

- **Scenario #1: Review of one-way boundary device between level 4 and level 3 and between level 3 and lower levels**
  - Design Certification Applicant submittal information:

    Applicant provides design descriptions of a device that physically enforces one-way communication between level 4 and level 3 and between level 3 and lower levels as part of the design certification application

    - Device uses optical isolation that only has a FOT on the higher security level and a FOR on the lower security level
    - Communication is one way from the FOT on the higher security level to the FOR on the lower security level

Scenario #1
Licensee Actions

- **Scenario #1: Review of one-way boundary device between level 4 and level 3 and between level 3 and lower levels**
  - Licensee submittal information: A licensee who is modifying an existing safety or important to safety system and is required to submit a LAR based on the 10 CFR 50.59 evaluation.
    - If the LAR changes the existing communication between (1) level 4 and level 3 and (2) between level 3 and any of the other layers, as part of the LAR, the licensee submits design descriptions of a device that physically enforces one-way communication
    - Device uses optical isolation that only has a FOT on the higher security level and a fiber optic receiver FOR on the lower security level
    - Communication is one way from the FOT on the higher security level to the FOR on the lower security level

Scenario #1
NRC Licensing Reviews

- **Scenario #1: Review of one-way boundary device between level 4 and level 3 and between level 3 and lower levels**
  - NRC license review:
    - Reviews the design description to determine whether the boundary device is one way and reviews the diagrams and schematics to verify the FOR and FOT locations
    - For DC applications, an ITAAC will be used to verify the as-built system employs this design and the as-built boundary device meets the design commitments
    - For LAR submittals, the staff will audit the development process for this device and may witness the FAT on this device as well as review the FAT results during the audit.

Scenario #1
NRC Inspections

- **Scenario #1: Inspection of one-way boundary device between level 4 and level 3 and between level 3 and lower levels**
  - NRC inspection:
    - Conduct an inspection to ensure that the device is properly installed and that documentation exists that identifies the boundary device as a CDA
      - This CDA will be controlled under the plant's cyber security program
    - No need to reconfirm that the device performs its intended function during the inspection

Scenario #2
Relevant Sections of RG 5.71

- **Scenario #2: Review of means used to protect time-stamps utilized in layer of 4 of the cyber security defensive architecture**
  - RG 5.71 Section B.2.8:
    - **CDAs use a time source protected at an equal or greater level than the CDAs** or an internal system clocks to generate time stamps for audit records, and licensees/applicants synchronizes the time on all CDAs
    - **Synchronizes the time of all CDAs from a dedicated source protected at an equal or greater level than the CDA existing on the security network**, attached directly to the CDA or via SNTP and a trusted key management process

Scenario #2
Applicant Actions

- **Scenario #2: Review of means used to protect time-stamps utilized in layer of 4 of the cyber security defensive architecture**
  - DC Applicant submittal information:

    A design certification applicant provides information regarding how timestamps are generated for important data from both safety systems and important-to-safety systems
    - Acquires timestamp from a protected source (unprotected sources such as GPS signals are not used)
    - Security features to protect the source of the time stamp signal
  - Licensee submittal information:

    A licensee who is modifying an existing safety or important to safety system and is required to submit an LAR based on the 10 CFR 50.59 evaluation
    - If timestamping required for system modified, acquires timestamp from a protected source
    - Security features to protect the source of the time stamp signal

Scenario #2
NRC Licensing Reviews

- **Scenario #2: Review of means used to protect time-stamps utilized in layer of 4 of the cyber security defensive architecture**
  - NRC license review:
    - Reviews the design description to determine whether the security features that protect the time stamp is acceptable and that the time stamp source is securable
    - For DC applications, an ITAAC will be used to verify the timestamp source for the as-built system and the security features for the timestamp source meet the design requirements
    - For LAR submittals, the staff may perform audits regarding how the timestamp source is generated and security features for the timestamp source and review the FAT results during the audit

Scenario #2
NRC Inspections

- **Scenario #2: Review of means used to protect time-stamps utilized in layer of 4 of the cyber security defensive architecture**
  - NRC inspection:
    - Conduct a cyber security program inspection to ensure that the security features for protecting the timestamp as described in the design certification application and LAR are properly installed and that documentation exists that identifies these features
    - Verify that the time stamp source is protected in the same cyber security defensive architecture as the systems that will be receiving this time stamp

Scenario #3

Relevant Sections of RG 5.71

- **Scenario #3: Review of test plans on verifying that safety and important to safety systems are free from known, testable vulnerabilities and malicious code**
- **RG 5.71 Section C.12.5**
  - Documents and requires that system developers and integrators of acquired CDAs create, implement, and document a security test and evaluation plan **to ensure that the acquired products meet all specified security requirements (1) that the products are free from known, testable vulnerabilities and malicious code by identifying and eliminating these following vulnerabilities** and other vulnerabilities that may change with new technology

Scenario #3
DC Applicant Actions

- **Scenario #3: Review of test plans on verifying that safety and important to safety systems are free from known, testable vulnerabilities and malicious code**
- **<u>DC Applicant submittal information</u>: Submittal of a test plan that documents how known, testable vulnerabilities and malicious code will be identified in the system**
  - Develop plan in coordination with the vendor, and includes descriptions of plans for conducting tests and analysis of system (e.g. static code analysis, black box and white box testing)
  - Document plans for controlling any identified testable vulnerabilities and malicious code
  - Provide ITAAC to verify that the implementation of this test plan and confirm the test outputs meets the specified requirements

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

Scenario #3
Licensee Actions

- **Scenario #3: Review of test plans on verifying that safety and important to safety systems are free from known, testable vulnerabilities and malicious code**
- **<u>Licensee submittal information</u>: A licensee who is modifying an existing safety or important to safety system and is required to submit an LAR based on the 10 CFR 50.59 evaluation. If the LAR makes changes to software or if new software is added then licensee:**
  - Submits a test plan that documents how known, testable vulnerabilities and malicious code will be identified in the system
  - Describe plans for identifying know, testable vulnerabilities and malicious code
  - Document plans for controlling any identified testable vulnerabilities and malicious code
  - Submits of summary of test results

Scenario #3
NRC Licensing Review

- **Scenario #3: Review of test plans and results on verifying that safety and important to safety systems are free from known, testable vulnerabilities and malicious code**
- **<u>NRC license review</u>:**
  - The staff reviews the test plan to determine whether the test activities are sufficient to identify testable vulnerabilities and malicious code
  - For DC applications, the staff will also review the ITAAC to determine if the design commitments and the acceptance criteria are sufficient to verify that the implementation of the test plan and the verification of the test results
  - For LARs, the staff will review the summary of the test results and may conduct an audit to witness the FAT

Scenario #3
NRC Inspection

- **Scenario #3: Review of test plans on verifying that safety and important to safety systems are free from known, testable vulnerabilities and malicious code**
- **<u>NRC inspection</u>:**
  - For DC applicants, during ITAAC closure conduct an inspection to ensure that the test plan was adequately implemented and any identified vulnerabilities and malicious code are adequately controlled
    - Inspect any documentation supporting this verification
  - For the cyber security program inspection, NRC will inspect the documentation provided as supplemented by the staff's previous review, audits, and inspection results

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

Summary

- **Proposed SECY paper seeks commission direction on evaluating cyber security-related design features**
- **No expansion the scope of cyber security requirements beyond the requirements currently stated in 10 CFR 73.54**
- **For DC applicants, provide added assurance that certified designs can be secured upon implementation**
- **NRC licensing review of cyber security design controls can be used to support subsequent cyber security program inspections thereby reducing information that need to be reviewed during inspections**