U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Cyber Security System Development ISG

September 2, 2009

Background

- Digital I&C safety systems should be designed with high functional reliability to preclude cyber attacks or preserve the safety functions during a cyber attack.
- RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” Rev. 2, Regulatory Positions 2.1-2.9, provides cyber security criteria as a part of the system development lifecycle to secure the development process in order to ensure that the system software does not contain malicious code.
- Recent reviews of digital upgrades at existing plants, design certification and combined operating license applications of new plants have shown that the guidance of RG 1.152 needs to be clarified to provide regulatory consistency.
- A proposed new ISG cyber security system design and development is currently being developed to augment and clarify the criteria of Regulatory Positions 2.1-2.9 of RG 1.152 Rev. 2 based on lessons learned from recent regulatory reviews related of digital safety systems

Scope

- This proposed new ISG will provide guidance on secure code development to ensure that the safety system software does not contain malicious code.
  - Security controls implemented in the development environment.
  - Treatment of pre-developed and/or COTS software
  - Tests and validation needed to demonstrate that the system does not contain hidden or malicious code (e.g. logic bombs).
- The ISG may also provide optional guidance on secure system design to ensure that the software is free from known vulnerabilities.
  - Draft RG 5.71 requires documentation to demonstrate that the sufficient security testing and security controls are addressed in the development of critical systems.
  - The optional guidance within this ISG would provide guidance on how to address security testing and development controls.

Roles and Responsibilities

System vs. Programmatic Security Review

- The I&C system design licensing reviews for the security controls listed in Appendix B and Appendix C of RG 5.71 would be restricted to the review of any feature included in the safety system design, intended to address these security controls.
  - These security features would be part of the overall system requirements, and thus would be designed and developed in accordance with the software development process stipulated in SRP BTP 7-14.
  - The SER would only confirm that these security controls have followed the software development process, and that they do not adversely impact safety functions. The SER would not evaluate these security features' ability to perform cyber security protective measures.

- The I&C system design licensing review will also ensure that the software code development environment is secure and that sufficient testing has been completed to ensure that the software does not contain malicious code. The portion of the cyber security programmatic review that addresses these safety systems can be based on the SER for the given I&C system.

Summary

- A new proposed cyber security system development ISG is currently being developed to provide guidance on secure code development.
- The proposed ISG may address some of the secure system design criteria described in draft RG 5.71.
- Elements of the system security design and development review for a given system may support the cyber security programmatic review performed by NSIR.