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

RIC 2010
Application of Regulatory Guide 1.152 for Review of Safety Systems

Tim Mossman
NRC / NRR / DE / EICB
March 9, 2010

History

- Security of digital safety systems has always been a concern of industry and the NRC
  - 10CFR50.55a(h) / IEEE-603-1991 is focused on ensuring safety system reliability, and contains clauses that speak to safety system security
  - Post 9/11, focus on security – including cyber security – increased considerably
- IEEE 7-4.3.2-2003 did not address security directly
  - 9 Regulatory Positions on security added to RG 1.152 (Rev 2)
- Task Working Group 1 developed Interim Staff Guidance 1 to provide further guidance to the staff and industry on how RG 1.152 can be used to address cyber security in licensing reviews
- 10 CFR 73.54 / Regulatory Guide 5.71 issued specifically to address cyber security

Safety / Security Interface

- Part 50 licensing reviews' security evaluation will focus on reliable operation of the digital safety system
- Security Aspects of NRC Safety Reviews
  - Security – as part of safety reviews – refers to protective actions taken against a predictable set of non-malicious acts that could challenge the integrity, reliability, or functionality of a digital safety system
  - Security features specifically designed for cyber security (i.e., to combat *malicious threats*) may be submitted with a LAR, topical report, design certification or COL
    - Part 50 review will, however, strictly focus on the impact those cyber security features have on safety system integrity, reliability and functionality

Non-Malicious Events

- Examples of non-malicious events
  - Hatch, Unit 2 - March 2008 event
    - Inadvertent (i.e., *non-malicious*) access by plant personnel to a digital system via a two-way LAN connection caused the system to behave unexpectedly
  - Browns Ferry, Unit 3 – August 2006 event
    - Failure of a system on a shared integrated computer system network caused unexpected behavior of unrelated, but connected, digital systems

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

RG 1.152, Revision 3

- Revision 3 – currently out for review – is a near-term, limited revision
- With the issuance of 10 CFR 73.54 and RG 5.71, RG 1.152 is being revised to:
  - Eliminate reference to cyber-security
  - Eliminate direction to evaluate systems against intentional malicious actions or attacks
- RG 1.152 is clarifying its focus on:
  - Controls to prevent inadvertent access to systems
  - Protection against undesirable behavior of connected systems
  - Protection of the development environment from inclusion of undocumented and unwanted code

RG 1.152 (Rev 3) should be available for public comment as Draft Guide 1249.

Key RG 1.152 Clarifications

- Regulatory Position 2.1 (Concepts phase): A security vulnerability assessment of the system life-cycle is essential for review of the digital safety system
  - Design: Vulnerabilities that may permit unintended access (IEEE 603, Clause 5.9) or may permit connected systems to interfere with system reliability (IEEE 603, Clause 5.6.3) should provide basis for inclusion of security design features
  - Development: Vulnerabilities to system development which could lead to inclusion of undocumented code will provide a roadmap to identify protective actions taken to prevent system tampering
    - The assessment should address both application software, as well as any platform software

Key RG 1.152 Clarifications

- Regulatory Positions 2.2 (Requirements) and 2.3 (Design): Security design features should be part of the system requirements and design process, and the overall process should be protected against inclusion of unwanted code
  - Design: Security design features should be included in the digital safety system requirements and design documents and handled in a manner consistent with safety system development
  - Development: Overall system requirements and design descriptions are protected against inclusion of undocumented and unwanted requirements and design features

Key RG 1.152 Clarifications

- Regulatory Position 2.4 (Implementation): Translation of security feature design into the developed product, while protecting against the inclusion of unwanted code
  - Design: As-implemented security design features should reflect their respective design documentation
  - Development: Implementation phase – from first generation of code to installation of code on hardware – is conducted in a manner to prevent the inclusion of undocumented and unwanted code

Key RG 1.152 Clarifications

- Regulatory Position 2.5 (Test): Addresses conduct of security feature tests and the protection of the system test environment
  - Design: Implemented security design features should be tested in a manner commensurate with other digital safety system requirements
  - Development: Test environment and test products (i.e., *data / documentation*) are protected from inadvertent manipulation

Key RG 1.152 Clarifications

- Regulatory Position 2.6 (Site Installation), 2.7 (Operations), 2.8 (Maintenance) and 2.9 (Retirement)
  - These Regulatory Positions are being removed from RG 1.152
  - The staff has determined that licensing reviews for digital safety systems under Part 50 are complete once the factory acceptance testing is concluded

Future RG 1.152 Activities

- Additional guidance development
  - Application of RG 1.152, Rev 2 has generated lessons learned that will be further clarified and incorporated in the guidance to improve licensee submittals and facilitate consistency of staff reviews
- IEEE 7-4.3.2 – 20XX
  - NRC Staff has been working with the IEEE 7-4.3.2 working group to incorporate RG 1.152 Regulatory Positions into the standard
  - Once the next revision of IEEE 7-4.3.2 is approved, it will be evaluated for endorsement and RG 1.152 will be updated, as applicable

Back-up Slides

- Back-up Slides

Regulations

- 10 CFR 50.55a (h)
  - 10 CFR 50.55a (h) approved IEEE 603-1991 for incorporation for the design of protection and safety systems
  - Secure software is an essential part of IEEE-603 to ensure safe and reliable software
- GDC 21
  - Criterion for protection system reliability and testability
  - Ensure secure software through all phases of design, development, implementation, and testing phases regardless of the source of vulnerability or threat
- GDC 22
  - Criteria for protection system independence
- 10 CFR 50, Appendix B
  - Provides quality assurance criteria

IEEE 603-1991 Language

IEEE-603-1991:

- Clause 5.6.3 (5.6 Independence) Between Safety Systems and Other Systems. The safety system design shall be such that credible failures in and consequential actions by other system, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.
  - Clause 4.8 Design basis shall document conditions having the potential for functional degradation and for which provisions shall be incorporated to retain the capability for performing the safety functions (e.g., operator error, failure in nonsafety-realted systems)
  - Clause 5.6.3.1(1) Interconnected Equipment Classification. Equipment used for safety and non-safety . . . Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.
  - Clause 5.6.3.1(2) Interconnected Equipment Isolation. No credible failure on the non-safety side of an isolation device . . . A failure in the isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.
- Clause 5.9 Control of Access. The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

Acronyms Used

- TWG – Task Working Group
- ISG – Interim Staff Guidance
- COL – Combined Operating License
- LAR – License Amendment Request