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

Key Regulatory Concepts to be Evaluated

March 21, 2016

Steven Arndt
Division of Engineering
Office of Nuclear Reactor Regulation

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

Presentation Outline

- Current Challenges
- Key Technical and Regulatory Concepts
  - Changes in Standards and Regulation and the Effect on Evolving Technology
  - Technical Areas to be Reviewed
  - Assumptions in SECY-93-087 and BTP 7-19 to consider
  - Regulatory Issues

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

Re-Evaluate the NRC Position on CCF

- Current position includes software, firmware or programmable logic commonly used in digital systems (including EDDs)
- Significant lack of understanding by industry of need for evaluation and acceptance criteria
- Significant concern by industry associated with current position

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

Re-Evaluate the NRC Position on CCF

- Detail review of current methods, data and regulatory experience (nuclear and non-nuclear, US and international) of CCF
- Re-evaluate assumptions in SECY-93-087 and BTP 7-19 to consider impact of evolution in technology
- Evaluate options for updating NRC policy in light of any significant technology evolution
- Preparation of a technical basis paper and a SECY paper to gain alignment on direction

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

Changes in Standards and Regulation

- How has the changes to industry standards and regulatory guidance changed digital systems both safety and non-safety?
- Since the NRC position was established
  - SRP Chapter 7, 1997 has published including BTP-7-14
  - IEEE 7-4.3.2, IEEE 1012, and many other key standards have been published
  - Associated regulatory guidance
  - Guidance on new technology such as FPGA's has been published

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

Technical Concerns and Evolving Technology

- Technical Concerns
  - Ability to develop fault free digital systems
  - Ability to fully analysis digital systems
  - Ability to fully test digital systems
- Technical Progress
  - More complete design and quality standards
  - Better analysis methods
  - Better testing methods
  - More formal development and analysis methods

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

Potential Areas for Review

- Need to use deterministic analysis
- Scope of systems that need to consider CCF
- Definition of software and software failure in the context of the current NRC position
- Definitions of 100% test and internal diversity
- Concept of echelons-of-defense
- Inclusion of explicit position on hazards analysis
- Crediting manual operator actions
- Risk informing/Use of a graded approach

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

Re-Evaluate the NRC Position

- **Deterministic Analysis / Assumption of Failure**
  - **The technical concern was, that vendors can not product fault free (from design error) digital systems**
  - **We can not analysis new digital systems to the same level as earlier analog system**
- **Issue to be evaluated: Has this changed?**

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

Re-Evaluate the NRC Position

- Scope of systems that need to consider CCF
  - The current position is focused only on software or logic errors
  - This was driven by the concern about unknowns associated with software faults
- Issue to be evaluated: Should we only be focusing on software design errors or should we be look at broader digital failures?

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

Re-Evaluate the NRC Position

- **Scope of systems that need to consider CCF**
  - **Current position requires analyze for each event that is evaluated in the accident analysis**
  - **Current position call for analysis of any device that can disable a safety function**
- **Issue to be evaluated: Is this the appropriate scope? Should some systems or events be evaluated in a graded manner?**

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

Re-Evaluate the NRC Position

- **Design Attributes to Eliminate Consideration**
  - **There are two attributes that are sufficient to eliminate consideration of CCF, internal diversity and demonstrated simplicity**
  - **The concept of sufficient simplify as demonstrated by 100% testability has been a challenge to communicate and review**
- **Issue to be evaluated: Are there other attributes that can be demonstrative to be sufficient to eliminate consideration?**

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

Re-Evaluate the NRC Position

- Risk informing/Use of a graded approach
  - Current position is a consequence-based approach for addressing CCFs that does not relate to safety significance or plant risk
  - Formal risk analysis of digital systems is still very uncertain and may not capture all the hazards
- Issue to be evaluated: Can we develop a graded approach? Does it need to be based on risk or could we use a different metric?

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

Re-Evaluate the NRC Position

- **SECY with Recommendations**
  - **Key recommendation on technical issues**
  - **Should current position remain as a Commission direction on GDCs or become a rule?**
  - **How best to develop new rule or policy and regulatory guidance**
- **Issue to be evaluated: Effectiveness and timing**

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

Questions/Discussion