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

NRC EFFORT TO RE-EVALUATE ITS POSITION ON COMMON CAUSE FAILURE

June 7, 2016

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

Summary of March 21 Meeting

June 7, 2016

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

Background

- SRM-SECY- 15-0106 – Develop an Integrated Strategy to Modernize the DI&C regulatory infrastructure
  - Ongoing review of the NRC policy on CCF
  - Develop a technical basis to recommend to the Commission possible changes to the current NRC policy

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

Common Cause Failure Action Plan

- Current regulatory treatment and acceptance criteria are problematic for some I&C upgrades
- Re-evaluate assumptions in SECY-93-087 to consider impact of evolution in technology
- Evaluate options for updating NRC policy in light of any significant technology evolution
- Prepare technical basis paper and SECY paper
- Maintain appropriate interfaces with industry stakeholders to consider input on this item

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

Action Plan Milestones

- Public meetings to gather insights on key technical and policy issues (March 21, June 7, TBD)
- Prepare a technical basis document (October 2016)
- Review/Comment of technical basis document (December 2016)
- Public meeting to discuss technical basis and proposed modification of the NRC regulatory position (April 2017)
- SECY paper to Commission identifying proposed actions (July 2017)
- Implement resolution identified in SECY paper (TBD)

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

3/21 Meeting Summary

- Industry and NRC agreed CCF needs to be addressed as a high priority in the short-term
- Initiated discussions on the technical basis for CCF in digital systems
- Discussed current challenges, technical concerns, regulatory concepts, and NRC position
- Industry provided its perspective on CCF developed through EPRI research
- Had a productive discussion on the NRC position on CCF and associated industry challenges

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

3/21 Meeting Summary

- Gathered information on what areas of the current NRC policy on CCF need to be updated or modified
- Areas that required clarification or have been challenging
  - Scope of systems that need to be considered in the NRC CCF policy/rule
  - Design attributes to reach a conclusion that a CCF need not be further analyzed
  - Whether and, if so, how a bounding analysis can be used to assess a CCF
  - Criteria to determine when a CCF analysis is acceptable

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

CURRENT APPROACH AND TABLE OF CONTENTS FOR THE NRC TECHNICAL BASIS DOCUMENT

June 7, 2016

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

TECHNICAL BASIS DOCUMENT

- Evaluate current NRC position on defense against CCF
- Evaluate alternatives available to adequately consider and address CCF. For example,
  - A graded approach based on safety significance, including consideration of the likelihood of CCF and a risk-informed, consequence based regulatory structure
- Evaluate state-of-the-art analysis in other application sectors, industries, and countries
- Support NRC staff's recommendation to the Commission

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

TABLE OF CONTENTS

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

TABLE OF CONTENTS

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

TABLE OF CONTENTS

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

EXAMPLES OF KEY TECHNICAL ISSUES

- Scope of system/component included within CCF position
- Design attributes and their effectiveness
- Use of bounding analysis in CCF evaluation
- Defense in Depth and Echelons of Defense in I&C systems
- Independence of SSCs
- Licensing basis of the safety systems (adequacy of the FSAR bounding analysis for NSR system changes to address common-cause failures)

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

Technical Issues Currently Being Considered

June 7, 2016

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

TECHNICAL BASIS DOCUMENT

- Evaluate current NRC position on defense against CCF
- Evaluate alternatives available to eliminate considerations of CCF. For example,
  - A graded approach based on safety significance, including consideration of the likelihood of CCF and a risk-informed, consequence based regulatory structure
- Evaluate state-of-the-art analysis in other application industries and countries
- Support NRC staff's recommendation to the Commission

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

Common Cause Failure Analysis Scope Considerations

June 7, 2016

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

SCOPE CONSIDERATIONS

- In SRM/SECY 93-087, the scope is currently software/logic only
  - Should this be expanded?
  - Are other failure modes covered by other regulations or guidance?
- Should the scope of components be based on safety significance?
- Is there a method for grading what components need to be included within the policy, and if so, should it address the type of analysis needed?
- How can risk insights or safety significance be used?

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

SCOPE CONSIDERATIONS

Possible Safety Classification Methods (Examples)

1. Maintenance Rule Considerations
2. Q-List/Appendix B Considerations
3. Safety System Considerations
4. Specific Safety Function Considerations

Possible Risk Analysis Methods

1. Level 1 PRA-based Risk Mitigation Considerations
2. Reg Guide 1.200 Considerations
3. Others Risk-Informed Methods

Crediting of High-Quality Independent Non-Safety Systems

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

SCOPE BASED ON SAFETY CLASSIFICATION METHODS

Maintenance Rule

- PROS
  - Simple to apply—easy to identify whether the equipment being replaced is covered by the Rule or not
  - New digital I&C applications are easy to classify against the definitions in 10 CFR 50.65(b)(1) or (b)(2)
- CONS
  - Categorization is broad–covers just about everything important to safety, and there may be valid reasons justifying exclusion from the CCF policy

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

SCOPE BASED ON SAFETY CLASSIFICATION METHODS

Q-List/Appendix B

- PROS
  - Simple to apply—easy to identify whether the existing equipment being replaced is already on the Q-List.
  - Narrower Scope than Maintenance Rule (10 CFR 50.65)
- CONS
  - Categorization is still broad–covers just about everything required to be qualified in some aspect, and there may be valid reasons justifying exclusion from the CCF policy

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

SCOPE BASED ON SAFETY CLASSIFICATION METHODS

Safety System Considerations (i.e., member of a safety system)

- PROS
  - Simple to apply—easy to identify whether the existing system being upgraded performs a safety function consistent with the plant licensing/design basis
  - Narrower Scope than Maintenance Rule or Q-List/App. B program. Does not include non-safety components whose failure could prevent a safety function from being achieved or which could cause a scram or actuation of a safety function
- CONS
  - Categorization is still broad—covers every component that is an element of a safety system—regardless of whether it performs a key safety function. There may also be valid reasons justifying exclusion from addressing CCF. There may be non-safety systems that are risk significant

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

SCOPE BASED ON SAFETY CLASSIFICATION METHODS

Specific Safety Function Considerations

- PROS
  - Simple to apply—easy to identify whether the existing equipment being replaced or new application performs a safety function credited in the plant licensing/design basis analyses
  - Narrower Scope than simple membership in a safety system
- CONS
  - There may be valid reasons for justifying exclusion from addressing CCF based on the function being replicated in the design by diverse means or its failure being bounded in existing analyses

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

SCOPE BASED ON RISK ANALYSIS METHODS

Level 1 PRA-based Considerations

- PROS
  - If the plant has a sufficiently-detailed model of its risk profile, risk analysis methods are valuable tools for identifying whether a safety function failure of the digital equipment has been adequately modeled, and found to be mitigated/bounded by other modeled functions
    - Screening methods can often be employed to show that the contribution of many external events to CDF and/or LERF/LRF is insignificant
  - Much narrower scope than simple identification as having a specific safety function
- CONS
  - Not all plants have risk modeling completed to the same degree—the level of detail in a plant's risk model is determined by its original intended use, the plant operating states included for evaluating risk, and risk metrics identified

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

SCOPE BASED ON RISK ANALYSIS METHODS

Regulatory Guide 1.200-based Considerations

- PROS
  - Similar to Level-1 PRA: If the plant has a sufficiently-detailed model of its risk profile, risk analysis methods are valuable tools for identifying whether a safety function failure of the digital equipment has been adequately modeled, and found to be mitigated/bounded by other modeled events
    - Evaluation of results for plant performance under existing fire, wind, flooding, and seismic event analyses may provide insights as to the consequences of a loss of function in the equipment due to CCF
  - Much narrower scope than simple identification as having a specific safety function
- CONS
  - Not all plants have risk modeling completed to the same degree—the level of detail in a plant's risk model is determined by its original intended use, the plant operating states included for evaluating risk, and risk metrics identified

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

SCOPE BASED ON RISK ANALYSIS METHODS

Other Risk-Informed Methods?

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

SCOPE INFLUENCE BASED ON CREDITING NON-SAFETY SYSTEMS

Determination of Adequate Defense-in-Depth in Licensing Decisions

Example: ATWS Capabilities—Alternate Rod Insertion (ARI) (BWRs) and AFAS & Aux Feedwater Actuation/ Turbine Trip Initiation (PWRs)

- To the degree for which reactor trip functions are duplicated in the ATWS capability, provide credit for independent and diverse detection of key adverse reactor conditions and initiation of alternative/backup sub-systems to trip reactor.

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

Possible Methods for Using Bounding Analysis in CCF Evaluations

June 7, 2016

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

NRC CURRENT POSITION

- Applicant or Licensee shall assess the defense-in-depth and diversity of the proposed I&C system to demonstrate that vulnerabilities to CCF have been adequately addressed
- In performing the assessment the applicant or licensee shall analyze each postulated CCF for each event that is evaluated in the accident analysis section of the UFSAR using best-estimate methods

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

APPROPRATE ANALYSIS

- Should the analysis be “best estimate”?
- What should be the acceptance criteria?
  - Is the acceptance criteria based on Part 100 release appropriate?
  - Are there alternatives that provide the same level of assurance with less effort?

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

APPROPRATE ANALYSIS

- Can analyses be used?
  - Existing Analysis
    - Previous design basis analysis
    - Analysis used to support PRA acceptance criteria
  - Bounding analysis
- What credit can be given for mitigating measures in the analysis?

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

APPROPRATE ANALYSIS

- Can analysis be bounding?
  - Can analysis be used to bound the effects of CCF of digital systems?
    - Can this be done at a functional failure level?
    - Do Chapter 15 analysis lend themselves to bounding the effects of digital system CCF?
  - Can current analysis be modified in such a way that a complete new analysis is not needed?
    - Digital systems can influence the characteristics of the initiators
    - Digital systems can affect the response of mitigating systems

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

APPROPRATE ANALYSIS

- What should the requirements be for an analysis to be usable?
  - How complete does the analysis need to be?
  - Do the same analysis quality requirements as Safety Analysis apply?
  - Can we/should we use the same standards that apply to PRA quality?

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

Design Attributes Sufficient to Eliminate Consideration of CCF

June 7, 2016

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

NRC CURRENT POSITION

- Design attributes are qualities that can significantly reduce the likelihood of CCF
- BTP 7-19 focuses on software CCF, therefore:
  - We only look at design attributes associated with software/logic faults
  - Accepted design attributes to eliminate consideration of CCF:
    - Simplicity - Sufficiently simple systems that can be tested to the point of demonstrating that all software errors have been removed
    - Diversity - Internal diversity that remove the potential for common cause failure

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

ACCEPTED DESIGN ATTRIBUTES

- PROS
  - Current attributes address technical concern that digital systems can not be made error free
  - Current attributes address technical concern that digital systems can not be fully analyzed and are not continuous or linear
  - Internal diversity provides a level of assurance that common cause failure will not occur
  - Simplicity provide assurance that systems is error free with respect to software/logic errors

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

ACCEPTED DESIGN ATTRIBUTES

- PROS
  - Current attributes are measureable and have been effective (Wolf Creek, Westinghouse SSPS)
  - Current attributes are technology neutral
- CONS
  - Current attributes are not fully performance-based
  - Current attributes are not risk-informed or graded
  - Current attributes do not address faults other than software

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

DESIGN ATTRIBUTES CONSIDERATIONS

Are there other design attributes that can be demonstrative to be sufficient to eliminate consideration of CCF?

- Alternative attributes are available with varying level of theoretical and practical evidence to support them

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

DESIGN ATTRIBUTES CONSIDERATIONS

- Items to consider in the evaluation of alternative design attributes:
  - What characteristics are they trying to demonstrate?
  - What failure mode are they trying to remove or mitigate?
  - Do they need to be used in conjunction with other design attribute or they can stand alone?
  - What evidence is available to support claim?

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

EXAMPLE DESIGN ATTRIBUTES

- Use of formal methods
  - It demonstrates that the software is error free
  - It primarily looks at software coding errors
  - It generally is used alone to demonstrate this attribute
  - Theoretical analysis available to support claim
- Use of communication processors (as in ISG-04)
  - It protects against common failure of network
  - It protects against data storms and similar challenges
  - Used to demonstrate communication independence but does not help with design failures
  - Design information needed that provides evidence of needed design features and there correct implementation

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

DESIGN ATTRIBUTES CONSIDERATIONS

- To be effective the properties of design attributes would need to be:
  - Predictable;
  - Consistent;
  - Unambiguous;
  - Repeatable;
  - Measureable; and
  - Technically defensible

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

DESIGN ATTRIBUTES CONSIDERATIONS

- Should the alternative design attributes be defined in policy/rule or guidance?
  - One of the concerns with the current position (in BTP 7-19) is that by setting the two current design attributes (internal diversity and simplicity) in guidance, no other method is considered acceptable
  - What would be the best way to implement this concept?