

NRC DISCUSSION ON COMMON CAUSE FAILURE

December 1, 2016



Agenda

- Action items from previous meetings
- Update to Modernization Plan #1
- Scope of CCF consideration
- Bounding & Coping Analyses



Action Items



Action items

Public meetings held on:

- March 21, 2016
- June 7, 2016
- July 11, 2016
- August 22, 2016
- September 14, 2016



Update to Modernization Plan #1



MP #1

- The part of the Integrated Action Plan that describes activities related to CCF.
- Revision to this plan was in response to industry's request for guidance for addressing the potential for CCF in digital modifications or upgrades to auxiliary and support systems.



Current Activities

- Develop guidance to address identified issues in BTP 7-19 for the evaluation of the D3 analyses to address CCF vulnerabilities for auxiliary and support systems
- Support and be compatible with proposed guidance for 50.59 licensing process, to the extent practical, and consistent with current NRC policy on CCF.
- Consider NEI 16-XX (if available) for applicability to the guidance being developed.
- Identify and document potential gaps within current policy, regulations, and guidance and make appropriate recommendations.



Additional Activities

- Complete evaluation of existing position and regulations related to CCF.
- Consider the technical basis proposed by industry for the use of defensive measures, including P measures, to address CCF
- Summarize evaluation in a NRC technical basis document.
- Using the technical basis document, prepare SECY paper with staff's recommendation.



Scope of CCF consideration



Background

- NRC position on addressing CCF is described in SRM-SECY-93-087.
- Directions were implemented in BTP 7-19
- Applies to "the proposed I&C system."
- NRC Policy is to assume software design errors are credible and therefore needs to be identified and addressed.
- BTP 7-19 refers to NUREG/CR-6303 for guidance on how to perform a D3 analysis.



Scope of CCF Considerations

- Categorize Systems, Devices, and Software (SDS) on the basis of potential impact on safety.
- "Lower impact" could imply "easier to license."
- BUT: 10CFR50.59 applies equally to ALL systems, so graduating is not a panacea.



Scope of CCF Considerations

- SDS that are required to be safety-grade and perform safety functions.
- SDS that are needed to support the operation of safety-grade SDS (i.e., enable safety systems perform safety functions/actions specifically covered in design basis accident analysis).
- SDS that have the potential to place the plant in an unanalyzed condition as a result of CCF.



Scope of CCF Considerations

- For RTS/ESFAS the guidance in BTP 7-19 applies.
- For other SDS, it is not clear as to whether all the acceptance criteria in BTP 7-19 apply.
- The objectives are to:
 - clarify to what extent the guidance in BTP 7-19 applies.
 - address the technical aspects to inform 50.59 licensing decisions.



Bounding & Coping Analyses



Bounding Analysis – Feedwater

POSTULATED TOTAL FEEDWATER SYSTEM FAILURE DUE TO CCF of BOTH FEEDWATER TRAINS BOUNDING ANALYSIS COPING ANALYSIS **REGION A REGION B REGION C REGION D NORMAL OPERATION** ABNORMAL **CHAPTER 15 DESIGN CONSEQUENCES OF OPERATIONAL BASIS ACCIDENTS THAT** THE DBA IN THAT THE OCCURRENCE **DO NOT EXCEED THE RESULT OF THE RESULTS OF THE INITIATING EVENT CHAPTER 15 ANALYSIS ALONG WITH THE CCF** SES **EXCEEDS THE** OTHER EXAMPLE SYSTEM "A" PLANTWIDE **CHAPTER 15** PLANT-WIDE **ANALYS AND EVENT ANALYSES** SYSTEM-WIDE IMPACT IMPACT IMPACT for **ANALYSIS** for SYSTEM FAILURE SYSTEM FAILURE ANALYZED **BEST-ESTIMATE** FEEDWATER SYSTEM LOSS OF FEEDWATER EVENT **EVEN WITH THE** POSSIBILITY OF A SYSTEM-WIDE **PLANT-WIDE** CCF OF THE PRIOR ASSESSMENT REVEALS THAT IMPACT for IMPACT for **FEEDWATER FEEDWATER** FEEDWATER IN THE EVENT OF A CCF OF THE SYSTEM THE SYSTEM FAILURE SYSTEM FAILURE FEEDWATER SYSTEM, THE PLANT AND **IMPACT HAS BEEN** WILL STILL RESPOND AS DESIGNED, ANALYZED AND IS **BOUNDED (AS THE** PER THE GIVEN ANALYSIS* IN CHAPTER 15 2 **FEEDWATER OVERALL IMPACT** MAX THAT RELATES TO A LOSS OF FEEDWATER TO THE PLANT WILL CHAPTER **FLOW** EVENT. NOT PLACE IT IN AN THUS, EVEN IN THE EVENT OF A UNANALYZED PREVIOUSLY ANALYZED CONDITION CCF. THE EVENT IS BOUNDED. **RELATED TO** CHAPTER 15 OR A BEST-ESTIMATE ANALYSIS) **PLANTWIDE** OTHER EXAMPLE SYSTEM "B" PLANT-WIDE SYSTEM-WIDE IMPACT **IMPACT** IMPACT for AND EVENT ANALYSES for SYSTEM FAILURE SYSTEM FAILURE ANALYZED?

+



Bounding Analysis

An assessment that shows that the result of a postulated CCF, coincident with any design basis accident, falls within a design basis accident analysis.

– If the CCF results in a need for a new accident analysis, a successful bounding analysis would show that the results of that new accident do not exceed the results of any design basis accident analysis.

(This is a conceptual description, not a definition)



Bounding Analysis – EPRI

- Bounding analysis is not defined
- Included in the description for coping analysis in Section 3.4.
 - "...comparison of the postulated event to a similar or bounding event for which the consequences have already been analyzed and are well understood."



Coping Analysis – Feedwater

POSTULATED TOTAL FEEDWATER SYSTEM FAILURE DUE TO CCF of BOTH FEEDWATER TRAINS WITH AFW SYSTEM ON THE SAME PLATFORI BOUNDING ANALYSIS COPING ANALYSIS **REGION A REGION B REGION D REGION C** NORMAL OPERATION ABNORMAL **CHAPTER 15 DESIGN CONSEQUENCES OF THE OPERATIONAL BASIS ACCIDENTS THAT DBA IN THAT THE** OCCURRENCE DO NOT EXCEED THE **RESULT OF THE RESULTS OF THE** INITIATING EVENT **CHAPTER 15 ANALYSIS** ALONG WITH THE CCF ANALYSES **EXCEEDS THE CHAPTER PLANTWIDE** OTHER EXAMPLE SYSTEM "A" **15 ANALYSIS** PLANT-WIDE SYSTEM-WIDE IMPACT IMPACT IMPACT for AND EVENT ANALYSES for SYSTEM FAILURE SYSTEM FAILURE ANALYZED **BEST-ESTIMATE** FEEDWATER SYSTEM LOSS OF FEEDWATER EVENT PRIOR ANALYSIS REVEALS THAT **NOW WITH THE** IN THE EVENT OF A CCF OF THE AN ANALYSIS MUST POSSIBILITY OF A BE CONDUCTED TO SYSTEM-WIDE PLANT-WIDE FEEDWATER SYSTEM, THE PLANT CCF OF THE IMPACT for IMPACT for DETERMINE WILL STILL RESPOND AS DESIGNED. **FEEDWATER FEEDWATER FEEDWATER** DIVERSE SYSTEM THE PER THE GIVEN ANALYSIS* IN CHAPTER 15 SYSTEM FAILURE SYSTEM FAILURE **COMPENSATORY** AND **IMPACT HAS BEEN** THAT RELATES TO A LOSS OF FEEDWATER MEASURES (e.g. ALTERED IN THAT A (OR OVER-FEED) EVENT. THUS, EVEN IN THE ALTER THE DESIGN, FAILURE OF THE 2 **FEEDWATER ADDITIONAL** EVENT OF A CCF, THE EVENT WAS BOUNDED. MAX **COMMON DIGITAL DIVERSITY) COULD** HOWEVER, WITH THE SYSTEMS' PLATFORM FOR CHAPTER **FLOW BE TAKEN TO BOTH NORMAL** INTER-RELATIONSHIP CHANGING, AN MITIGATE/ MIN **FEED AND AFW** UPDATED ASSESSMENT SHOULD REVEAL **ELIMINATE THE** HAS NOT BEEN **EFFECTS OF A CCF** THAT THE SYSTEMS MAY FAIL AT THE SAME ANALYZED FOR THE **IN BEST-ESTIMATE** TIME, PER THE CCF POLICY WHICH PLACES THE **POSSIBILITY OF A SPACE** DIFFERENT RESULT PLANT IN AN UNANALYZED CONDITION. OTHER EXAMPLE SYSTEM "B" **PLANTWIDE** PLANT-WIDE SYSTEM-WIDE IMPACT **AND EVENT ANALYSES** IMPACT IMPACT for for SYSTEM FAILURE SYSTEM FAILURE ANALYZED?

SEVERITY OF THE IMPACT TO PLANT

+



Coping Analysis – EDG Relays

BOUNDING ANALYSIS						COPING ANALYSIS
REGION A NORMAL OPERATION		REGION B ABNORMAL OPERATIONAL OCCURRENCE		REGION C CHAPTER 15 DESIGN BASIS ACCIDENTS THAT DO NOT EXCEED THE RESULTS OF THE CHAPTER 15 ANALYSIS		REGION D CONSEQUENCES OF THE DBA IN THAT TH RESULT OF THE INITIATING EVENT ALONG WITH THE CC EXCEEDS THE CHAPTER 15 ANALYSIS
OTHER EXAMPLE SYSTEM "A" AND EVENT ANALYSES SYSTEM-WIDE IMPACT for SYSTEM FAILURE		PLANT-WIDE IMPACT for SYSTEM FAILURE		IMPACT ANALYZED?		
EMERGENCY DIESEL GENERATOR SYSTEM LOSS OF EDG FUNCTION						
I'HE EDG(S), THEREFORE A COPING ANALYSIS STAF	T D	PLANT-WIDE IMPACT for EDG SYSTEM FAILURE LS TO UE TO AY CCF		THE PLANT WILL COPE WITH THE EVENT RELATED TO CHAPTER 15 OR A		IN ADDITION TO INITIATING EVENT, EDG FAILS TO START DUE TO O/P RELAY CCF PREVIOUSLY ANALYZED AS SBO COPING ANALYSIS
OTHER EXAMPLE SYSTEM "B" AND EVENT ANALYSES SYSTEM-WIDE IMPACT for SYSTEM FAILURE		PLANT-WIDE IMPACT for SYSTEM FAILURE		IMPACT ANALYZED?		



Coping Analysis

- An assessment that shows that the result of a postulated CCF, coincident with any design basis accident, falls outside of the design basis accident analysis.
- However the results may still be acceptable
 - The assessment would identify means (including operator actions) that would ensure safety despite the presence of the postulated CCF.

(This is a conceptual description, not a definition)



Coping Analysis – EPRI

Defined in Section 2.1.

Described in Section 3.4 of the EPRI guide as:

 An analysis performed to determine if the consequences of I&C failures identified in the susceptibility analyses of Section 3.3 are acceptable at the plant or system level.



Questions?



Acronyms

- BTP Branch Technical Position within the Standard Review Plan NUREG-0800
- CCF Common Cause Failure
- D3 Defense-in-Depth and Diversity
- MP Modernization Plan
- NEI Nuclear Energy Institute
- NRC Nuclear Regulatory Commission
- P Preventive measure
- SDS Systems, Devices, & Software