1. Purpose/Background/Applicability/Definitions

- Definition of CCF
- Why CCFs are an important consideration to plant safety and safety analysis
- Why digital I&C presents new and different CCF challenges
- Scope/Applicability: Any digital equipment that affects components, systems, or functions described in the UFSAR, regardless of safety classification, if:
    - The component, system or function can initiate a plant transient
    - The component, system or function is credited for AOO and PA mitigation, or is credited to support and/or not complicate that mitigation
- Fundamental Questions
    - Is a CCF credible or not?
        - CCF Susceptibility Analysis – Systematically assess CCF sources and their likelihood based on available defensive measures among different failure sources in the I&C. Determines if CCF is credible or not. If the CCF is credible, its likelihood then drives the malfunction result analytical method to be used.
    - If a CCF is credible, then is it bounded or not?
    - If a CCF result is not bounded, is it still acceptable or not?
    - Methods to address these questions:
        - Conservative vs. best estimate analysis methods – Based on CCF likelihood (See below)
    - All of the above are considered in the answer to Question 6 in 50.59

2. CCF Susceptibility Analysis

- Categories of I&C Failure Sources that can Cause a CCF of Multiple Controlled SSCs (i.e., a malfunction that results from an I&C failure)
    - Single random hardware failure [e.g., power supply, sensor, controller]
    - Single environmental disturbance [e.g., heat, seismic, EMI, fire]
    - Single design defect [e.g., requirements, platform hardware/OS, application software/configuration, data comm's]
    - Single human error
- Available defensive measures are assessed for each applicable failure source within each category (assessment results may be different for each failure source)
    - **Preventive measure** – An aggregation of defensive measures that reduces the likelihood of a CCF of controlled SSCs from a specific I&C failure source to reach a not credible conclusion.
        - Not credible means no more likely than other sources of CCFs that are considered not credible in deterministic safety analyses (e.g., multiple, concurrent random failures, environmental hazards that exceed design basis envelopes, human errors).
        - This method does not guarantee 100% prevention assurance, because 100% assurance cannot be achieved, nor is it required. However, by systematically

assessing all I&C failure sources that can cause a CCF, and applying a preventive measure for each source, a CCF not credible conclusion is achievable.

- A CCF not credible conclusion then precludes the need for further analysis of the CCF malfunction result.

- **Limiting measure** – In the absence of a preventive measure (i.e., when a CCF is credible for any given failure source):
  - The designer can limit the extent of the resulting malfunction by limiting the number of controlled SSCs, force a preferred malfunction, or a combination of both.
  - A limiting measure can simplify the bounding analysis or coping analysis, but it does not preclude the need for such analysis.
- **Likelihood Reduction Measure** - In the absence of a preventive measure for a source of I&C failure, other measures may be credited to reduce the likelihood of CCF caused by the I&C failure to a level at which best-estimate analysis methods can be used. This can simplify the bounding or coping analysis, even if the CCF is not limited by a limiting measure.
- **Graded Approach -** Many defensive measures described in this methodology apply a graded approach based on safety vs. non-safety classification.

3. **<u>Analysis of CCF Malfunction Result</u>**

- ***Bounded or Not?*** – An assessment of the CCF (i.e., the malfunction of multiple controlled SSCs) to determine all of the following (in many cases, nothing more than an inspection of an existing deterministic plant safety analysis):
  - If the same type of malfunction is already included in the deterministic plant safety analysis (e.g., excess feedwater event)
  - If the margin is maintained to the critical safety limit(s) described in the deterministic safety analysis (e.g., DNBR, containment pressure, etc.)
- ***If not Bounded,*** a new analysis is needed to demonstrate plant safety.
- ***Analysis Methods and Acceptance Criteria***
  - For CCFs caused by I&C failures within the design basis – Analysis of CCF Malfunction Results uses conservative design basis analysis methods and existing AOO acceptance criteria. Mitigating systems are safety related.
  - For CCFs caused by I&C failures where likelihood reduction measures are applied. Mitigating systems can be safety or non-safety. Analysis of CCF Malfunction Results can use:
    - Methods:
      - Conservative design basis methods, <u>or</u>
      - Best estimate methods
    - Acceptance Criteria:
      - AOO <u>or</u> PA acceptance criteria, or
      - Best estimate acceptance criteria:

  - coolable core geometry
  - containment integrity
  - releases do not exceed 10CFR100 limits

- ***Coincidence of CCF and Plant Events***
  - CCF leading to malfunctions that are event initiators (e.g., malfunctions due to a control system CCF) are analyzed with no other coincident event (e.g., no other AOO or PA) and no other CCF (e.g., no unrelated CCF in a safety system)
  - CCF leading to malfunctions in event mitigators (e.g., malfunctions due to a safety system CCF) are analyzed coincident with all AOOs (note: LOOP is an AOO) and PAs, but with no additional CCF (e.g. no LOOP with coincident PA).

Defensive Measures

- Preventive Measures
- Limiting Measures
- Likelihood Reduction Measures