CCF Criteria Summary

CCF Source	Single Malfunction[1]		Digital Design Defect[2]	
	Failure to Actuate[3]	Spurious Operation[4]	Failure to Actuate[3]	Spurious Operation[4]
Design basis	Within		Beyond	
Analysis method	Conservative		Best Estimate	
Concurrent event considered in analysis	Each AOO or PA in accident analysis; loss of offsite power also considered concurrent with other AOO/PAs	None	Each AOO or PA in accident analysis; loss of offsite power is considered alone (i.e., not concurrent with other AOO/PAs)	None
Analysis acceptance criteria	As defined for AOOs and PAs in accident analysis.	As defined for AOOs in accident analysis.	As defined for PAs in accident analysis, or do not exceed: • RCS integrity limit • Containment integrity limit • 100% of 10CFR100 offsite dose limit	
Methods to preclude further consideration of failure source	None		A1 systems - Diversity for all common aspects of the digital design, or testability that encompasses all external and internal states.	A1, A2, B1[5] systems - Qualitative assessment considering design process, operating experience and defensive measures.
Method to limit effect of failure source	For safety systems, inherently limited to a single division by compliance to single failure criterion For all systems, segmentation limits effect to a smaller number of functions/components within a division.	For all systems, segmentation limits effect to a smaller number of functions/components. However, analysis must consider propagation of spurious signals between segments.	None because failure is not self-announcing; therefore, defect can be triggered in multiple segments over time, even if segments have some diversity.	For all systems, segmentation along with sufficient diversity among segments to achieve non-concurrent triggers, limits effect to a smaller number of functions/components.
Equipment that can be credited for mitigating a plant event resulting from failure	Redundant safety equipment only, because this is an AOO; must also demonstrate that same malfunction cannot adversely affect equipment credited for mitigation (i.e., functional independence). The operability of credited equipment must be controlled (e.g., technical specification, maintenance rule).		Any equipment in continuous operation or demonstrated to be highly reliable (e.g., equipment with augmented quality); must also demonstrate that same digital design defect cannot adversely affect equipment credited for mitigation (i.e., functional independence). The operability of credited equipment must be controlled (e.g., technical specification, maintenance rule). Redundant equipment is not required.	

CCF Source	Single Malfunction[1]	Digital Design Defect[2]	
Credit for mitigating manual actions	Yes, if there is sufficient margin between time available to take the action (as determined by thermal hydraulic analysis) and time required to take the action (as determined by human factors analysis); margin less than 30 minutes requires more detailed justification.		
Backup indications and manual controls to maintain critical safety functions.	Not required	Required[6]; must also demonstrate that same defect cannot adversely affect this equipment (i.e., functional independence).	Not required

(1) Single malfunctions are limited to single failure of active components; failure of wires and terminations, electrical faults, fire and flood are excluded. This column also applies to a design defect in a system not developed with a robust design process.

(2) This column applies only to systems with a robust design process. It is noted that this only applies to design defects; implementation and fabrication defects require no further consideration because they are precluded through quality assurance programs.

(3) Failure-to-actuate applies only to safety systems. For safety systems, single malfunctions are encompassed by compliance to the single failure criterion RG 1.53.

(4) Spurious operation includes erroneous operations for control functions

(5) CCF does not require any analysis in B2 systems, because spurious operations from these systems cannot challenge critical safety functions and these systems are not credited for AOO or PA mitigation.

(6) These indications and manual controls are required for compliance to Position 4 of the SRM to SECY 93-087. The effectiveness of these does not require demonstration for any specific event.