EPRI | ELECTRIC POWER RESEARCH INSTITUTE

EPRI CCF Guide Technical Approach

Ray Torok
EPRI

NEI / NRC "Tabletop" Meeting on CCF
11 July 2016

CCF Guide Approach - Key Concepts

I&C Failures and SSC Malfunctions

- I&C *failures* can cause controlled components or plant systems (SSCs) to *malfunction*
- SSC malfunctions can affect plant safety

I&C Failure Source Categories
1. Random hardware failures
2. Environmental disturbances
3. Design defects
4. Operations and maintenance errors

Common Cause Failure (CCF)

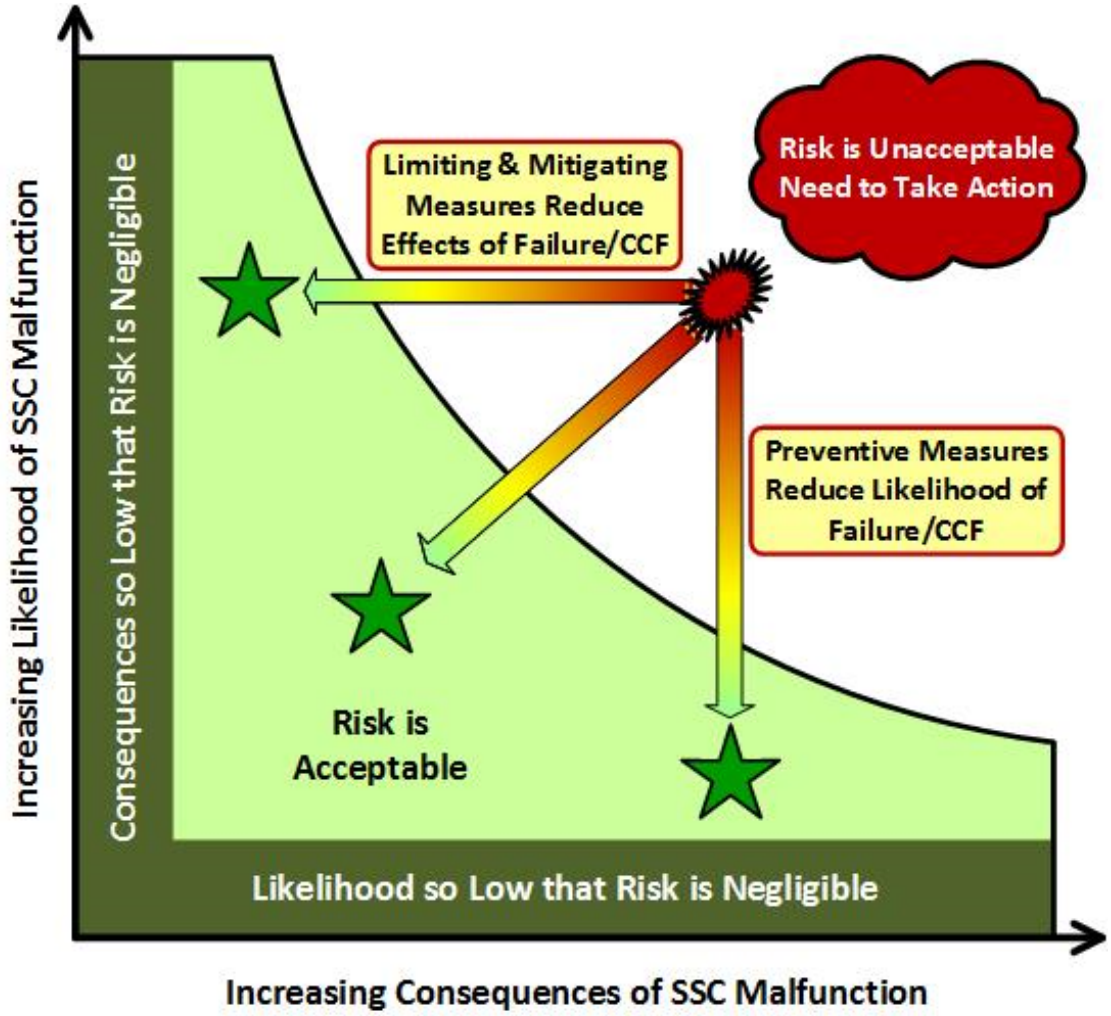
Concurrent failures (that is, multiple failures which occur over a time interval during which it is not plausible that the failures would be corrected) of systems, structures or components (SSC) that occur as a consequence of a single source (event or cause)

CCF Contexts

- Redundant divisions / systems with identical equipment/software
- Multiple functions in a single controller
- Shared resources, e.g., power supply, communications network

Focus is Managing Risk (not licensing)

- Manage risk with preventive, limiting and mitigating measures (***Defensive Measures***)
- Coping analysis shows failure effects
- Want assurance of sufficient protection against CCF effects

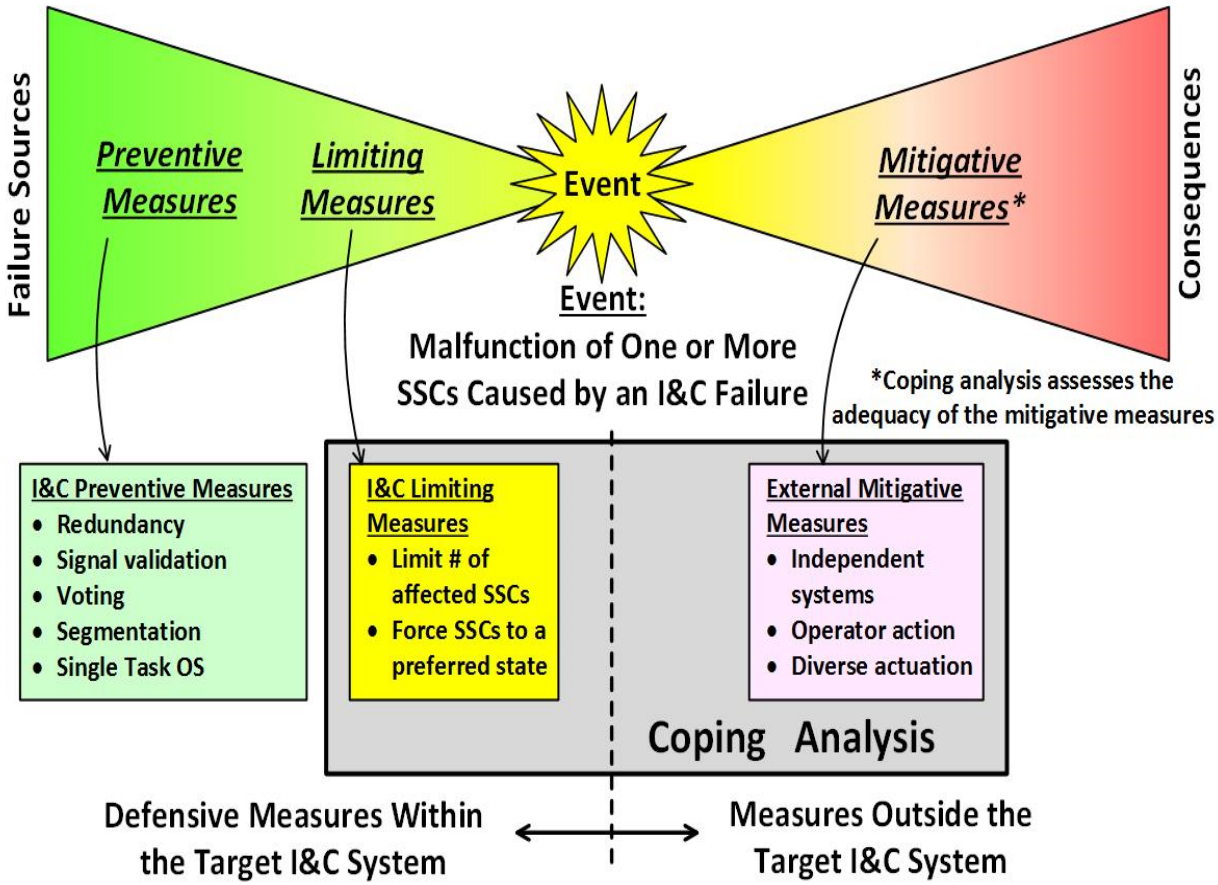


Preventive, Limiting and Mitigative Measures all Add Protection

Basic approach to establish assurance of sufficient protection:

- Credit recommended P and L measures in susceptibility analysis
- Augment as appropriate with bounding/coping analysis, crediting M measures

Note that P, L and M measures are deterministic



Bounding/Coping Analysis

Bounding/coping analysis determines if the consequences of I&C failures are acceptable at the plant or system level

Various forms possible:

- Detailed transient thermal-hydraulic (T-H) analysis
- Preexisting design, safety or risk analysis (including T-H analysis for PRA)
- Simple comparison of the postulated event to a similar or bounding event for which the consequences have already been analyzed and are well understood

Different purposes possible:

- Confirm design meets requirements (analysis treats system as it was designed to behave)
- Assess plant response under beyond design basis assumptions (“what-if” analysis)

Likelihood of CCF

CCF likelihood ranges – Qualitative assessment based on implemented preventive and limiting measures – Used to determine recommended bounding/coping analysis methods

Level 0 – Baseline – minimal documented defensive measures

- CCF likelihood considered comparable to that of failures in conservative safety analysis
- Assurance of sufficient protection based primarily on conservative coping analysis

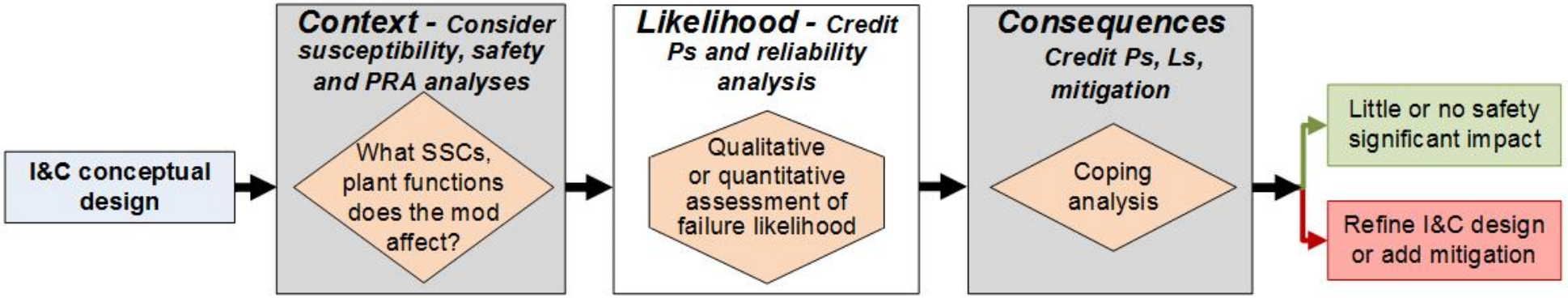
Level 1 – Estimated CCF likelihood significantly less than Level 0 due to some defensive measures

- Recognizes that an I&C system can be better than Level 0, even if it falls short of Level 2
- Assurance of sufficient protection based on a combination of a limited set of preventive measures and best-estimate (or conservative) coping analysis

Level 2 – CCF likelihood considered less than Level 1 due to extensive defensive measures

- Expected CCF likelihood ≤ that of failures considered too unlikely for plant safety analysis report (e.g., multiple random hardware failures)
- Assurance of sufficient protection based primarily on crediting preventive measures, supported as appropriate by some form of best-estimate coping analysis

Safety-Significance Based Graded Approach - Overview



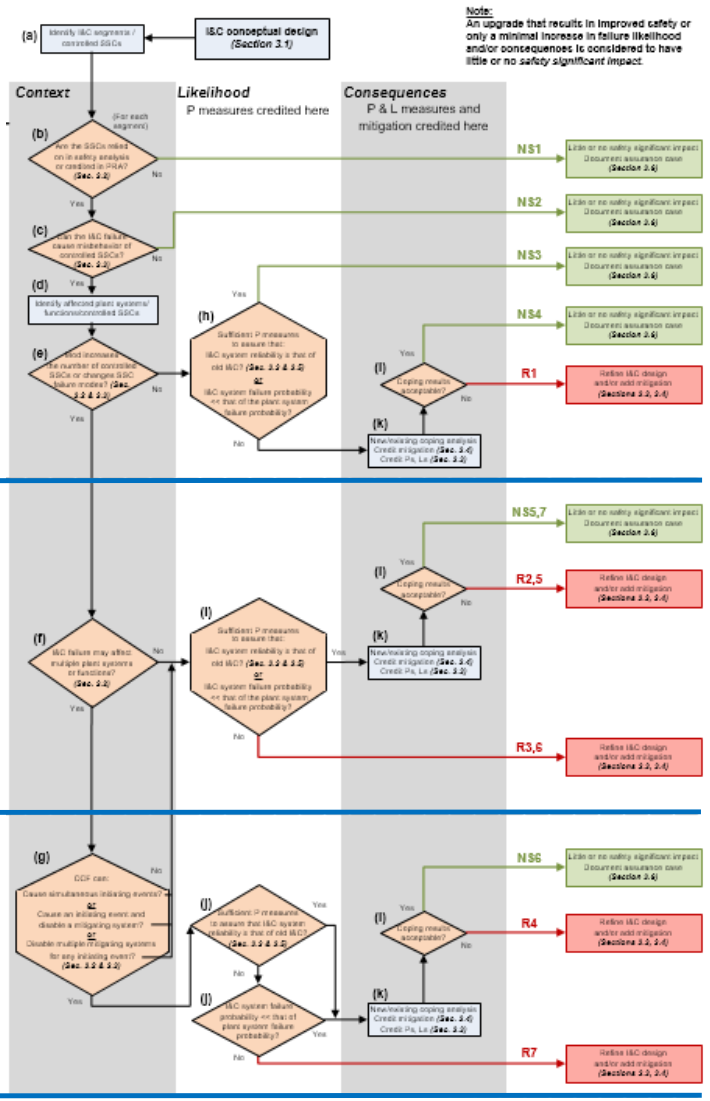
- Focuses effort on the impact the digital upgrade has on safety
- Enables user to tailor the rigor of the preventive, limiting and mitigative measures commensurate with impact of the plant mod on safety
- All paths end at:
  - *Little or no safety significant impact* or…
  - *Refine the design*
- ***Little or no safety significant impact*** means either safety is improved by the I&C mod, or any increases in likelihood or consequences of failures are minimal
- May affect:
  - Level of protection needed from P and L measures
  - Level of protection needed from mitigation
  - Overall protection acceptance criteria

Safety-Significance / Graded Approach
Consider Safety Analysis and the PRA

- **Top row**
  - Limited effects on controlled SSCs/malfunctions
  - Ps & Ls may have limited effect on safety
  - Coping analysis review recommended if significant increase in likelihood of failure

- **Middle row**
  - Change in controlled SSCs and/or malfunctions limited to a single plant system
  - Full complement of Ps & Ls may not be needed
  - Consequences changed, so coping analysis may be in order

- **Bottom row**
  - Change in controlled SSCs and/or malfunctions extents across multiple redundant plant systems
  - Potential CCF consequences may increase significantly
  - Robust set of Ps, Ls, and coping analysis recommended



EPRI ELECTRIC POWER RESEARCH INSTITUTE

Together…Shaping the Future of Electricity