EPRI | ELECTRIC POWER RESEARCH INSTITUTE

I&C Common Cause Failure EPRI Perspective

US NRC Public Meeting on Software Common Cause Failure

March 21, 2016

Robert E. Austin, III, PE, PMP, CISSP

Senior Program Manager

Overview

- Common cause failure
  - EPRI guide on digital failure susceptibility & protection (aka CCF guide)
  - Operating experience
- Have we asked the right question?
  - What are other issues?
  - A technical framework for digital I&C?

Methods for Assuring Safety & Dependability When Applying Digital I&C Systems
Purpose & Technical Approach

- Technical guidance to help utility engineers, equipment suppliers and system integrators:
  - determine whether there is sufficient (from engineering perspective) protection against potential digital I&C vulnerabilities
  - address a full range of potential failure and common-cause failure (CCF) contexts for both safety and non-safety

- Toolbox of recommended engineering practices
  - Not prescriptive, not a standard
  - Does not presuppose conclusions
  - User applies the guidance and draws conclusions

- Independent of regulatory framework

Key Concepts

I&C Failures and Misbehaviors

Can cause controlled components to *malfunction*

- "Classical" failure – component or system unable to perform to design specifications, or…
- Component or system exhibits undesired behavior, including spurious state changes and oscillations

I&C Failure Source Categories
1. Random hardware failures
2. Environmental disturbances
3. Design defects (includes software)
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

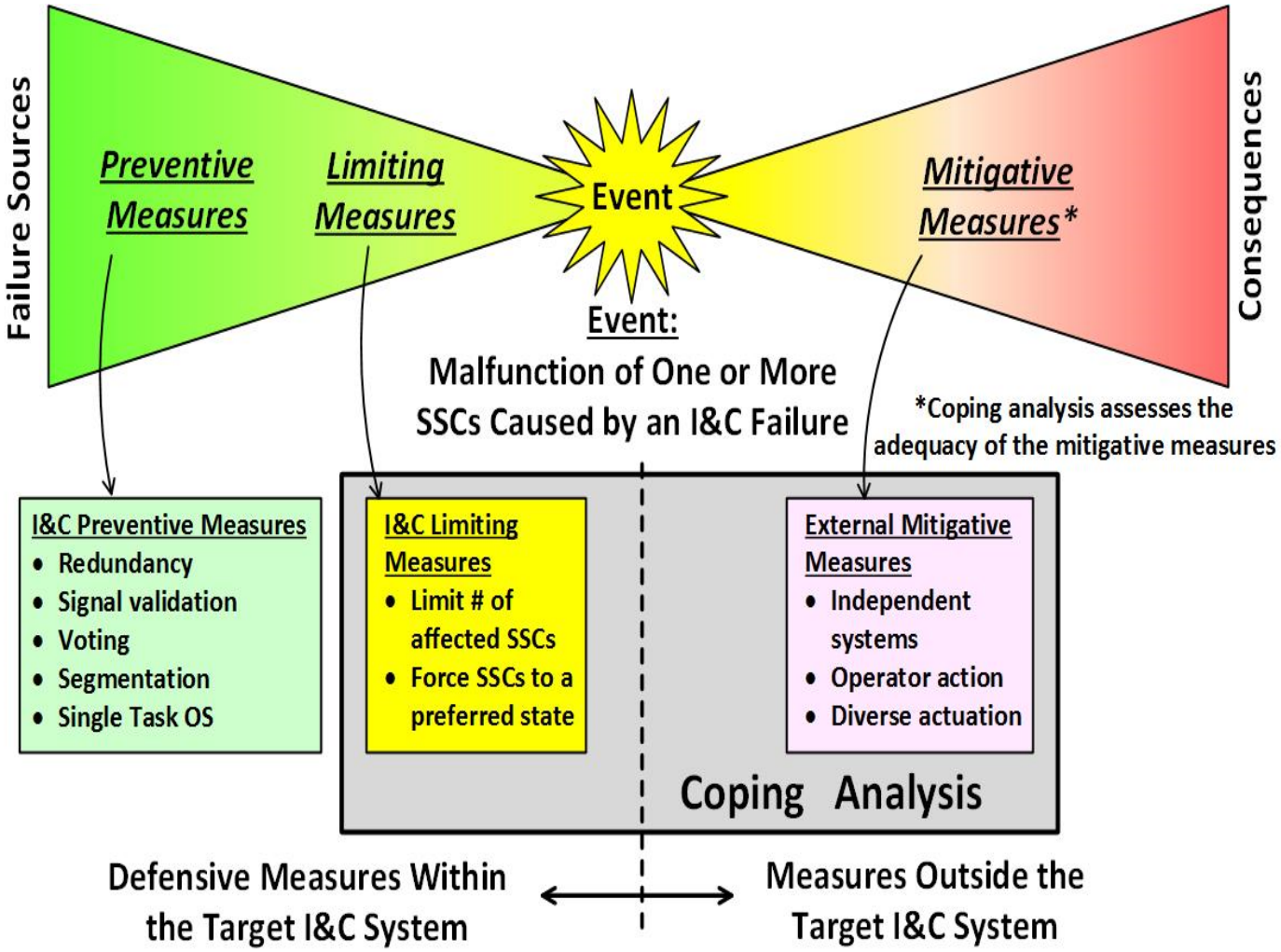
Multiple functions in a single controller

Shared resources

Not just software

Key Concepts, cont'd

Protection = Combination of: Preventive, Limiting and Mitigative Measures



Key Concepts, cont'd

Defensive Measures

Preventive Measures applied ***within the I&C system*** to reduce the likelihood of malfunctions of controlled SSCs (CCF) caused by an I&C failure

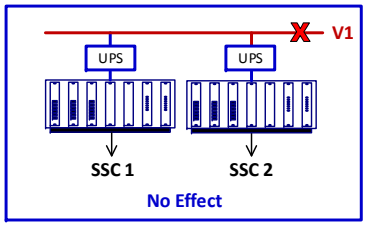
Limiting Measures applied ***within the I&C system*** to limit the effects of malfunctions of controlled SSCs (CCF) caused by an I&C failure

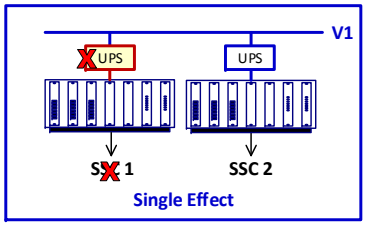
Mitigating Measures additional measures applied ***outside the I&C system*** to ensure safety given the occurrence of an I&C failure

Coping Analysis demonstrate the acceptability of the I&C failure effects given existing defensive and mitigating measures; ***may credit a previous analysis***, or a new analysis

Preventive Measures (aka "P's")

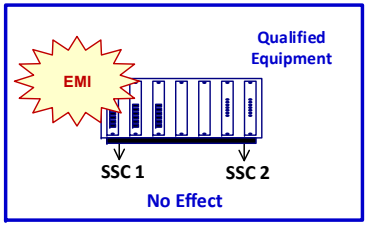
A design feature of an I&C system, or process used in developing an I&C system, that **prevents** a potential source of failure within the I&C system to reduce the likelihood of a malfunction of controlled SSCs caused by that potential I&C failure source.

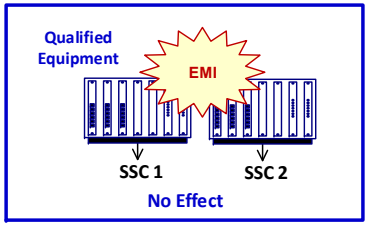




Random Power Failure

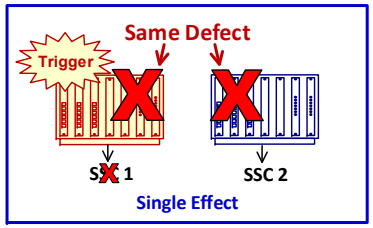
P1: Provide a dedicated, regulated UPS for each controller

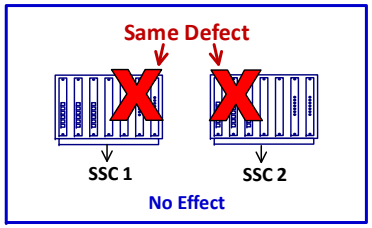




EMI Disturbance

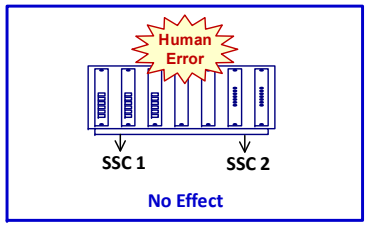
P1: Demonstrate controller can operate without failure during design basis EMI disturbance

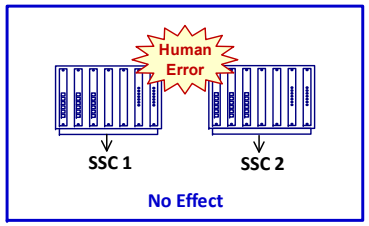




Design Defect

P1: Minimize potential for concurrent triggers, triggered defect self-announcing, minimize defect potential



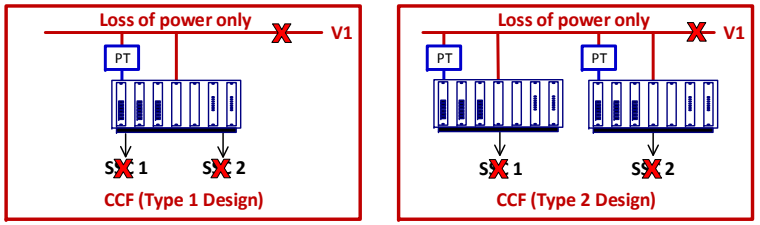


Human Error

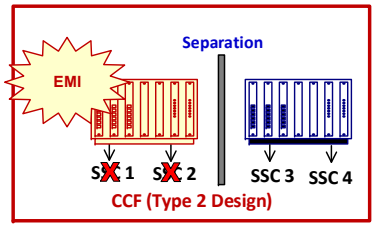
P1: Provide HFE and human performance programs

Limiting Measures (aka “L’s)

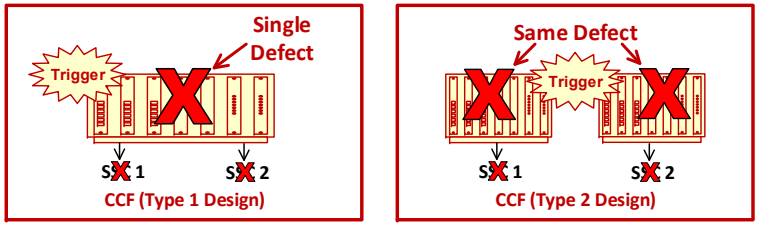
A design feature of an I&C system or component that ***restricts or limits*** the effects of an I&C failure on one or more SSCs; ideally limits to a known condition that has previously been analyzed and shown to be tolerable, so can ensure an acceptable coping analysis result.



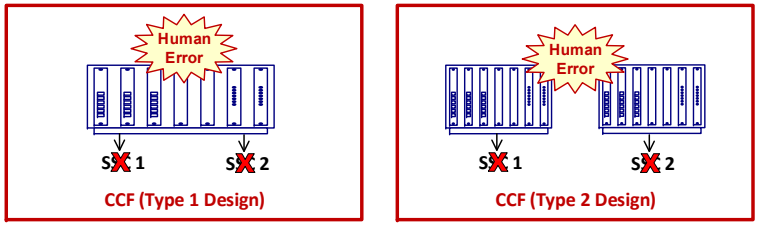
Random Power Failure
L3: Monitor power source for intolerable conditions and force a predictable loss of voltage condition



EMI Disturbance
L1: Demonstrate controller can operate without failure during normal EMI, and separate controllers from design basis EMI conditions



Design Defect
L1: Ensure low likelihood of defect via quality and simple OS, and activated defect forces controller to a predictable shutdown state



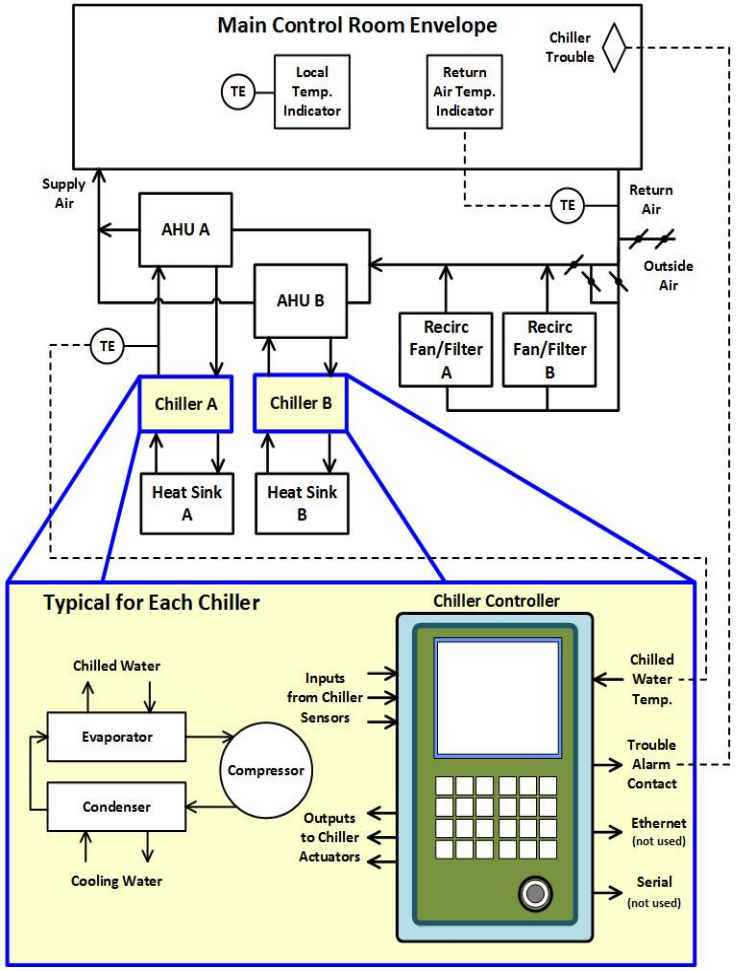
Human Error
No limiting measures identified

Coping Analysis & Mitigating Measures for Design Defects

Assess effectiveness of mitigating measures

May be a pre-existing safety analysis or T-H analysis performed for the PRA

- Are the failure effects acceptable?
- Are they bounded by another event?
- If not, may need redesign or manual or automatic backup



- Coping analysis helpful when desired P/L measures are insufficient or cannot be credited
- Part of assurance case for sufficent protection against failure/CCF

Activities for Assessing and Managing Digital Failure Susceptibilities

… it is not a linear process

Activity	Description/Purpose	Report Section
Develop/Refine Conceptual Design	Establish baseline for other analyses, iterate as needed to address issues that arise.	3.1
Review Existing Analyses	Gain insight regarding which controlled components and transients/accidents might be affected.	3.2
Perform Susceptibility Analysis	Identify potential I&C failure sources and measures in place to reduce the likelihood of resulting SSC malfunctions or limit the effects of SSC malfunctions. Qualitative estimate of failure likelihood.	3.3
Perform Coping Analysis	Assess adequacy of mitigation, should a postulated I&C failure and related SSC malfunction occur. Uses realistic or conservative assumptions.	3.4
Perform Reliability Assessment	Look at the expected reliability of the new I&C from a plant operation/availability perspective.	3.5
Overall Protection Assessment	Look at all contributors to protection (prevention and mitigation) against failure effects to assess adequacy	3.6

Operating Experience

- EPRI research to look for software common cause failures – US and South Korea
- There were no actual CCF events that disabled a safety function
- **Actual and potential CCF events were dominated by non-software issues**, e.g.,
  - Lifecycle management and human performance errors (e.g., incorrect setpoints)
  - Hardware failures (non-safety)
- Suggests that current methods are effective in keeping software a minor contributor to CCF
  - Use of software codes and standards
  - Design and process characteristics that preclude or limit CCFs ("defensive measures")

Categories	U.S. 1987 – 2007 (EPRI 1016731)	KHNP 1984 – 2010 (EPRI 1022986)
Safety-related digital events	**49**	**19**
Single failures	38 (78%)	19 (100%)
Non-software common cause failures	10 (20%)	0 (0%)
Software common cause failures	1 (2%)	0 (0%)
Non-safety related digital events	**273**	**78**
Single failures	217 (79%)	61 (78%)
Non-software common cause failures	42 (19%)	14 (18%)
Software common cause failures	14 (2%)	3 (4%)

Operating Experience & Technical Basis

- Unknown specifics of the process and design measures of the digital systems in the OE events
- Many lessons learned about good process and design measures
- EPRI formulated preventive and limiting (P and L) measures from “first principles” to assure a low likelihood of CCF
  - No direct link between data and specific P and L measures
  - Room for engineering judgment and application-specific P and L measures to provide sufficient protection

The Goal - Managing Risk

Risk = Likelihood x Consequences

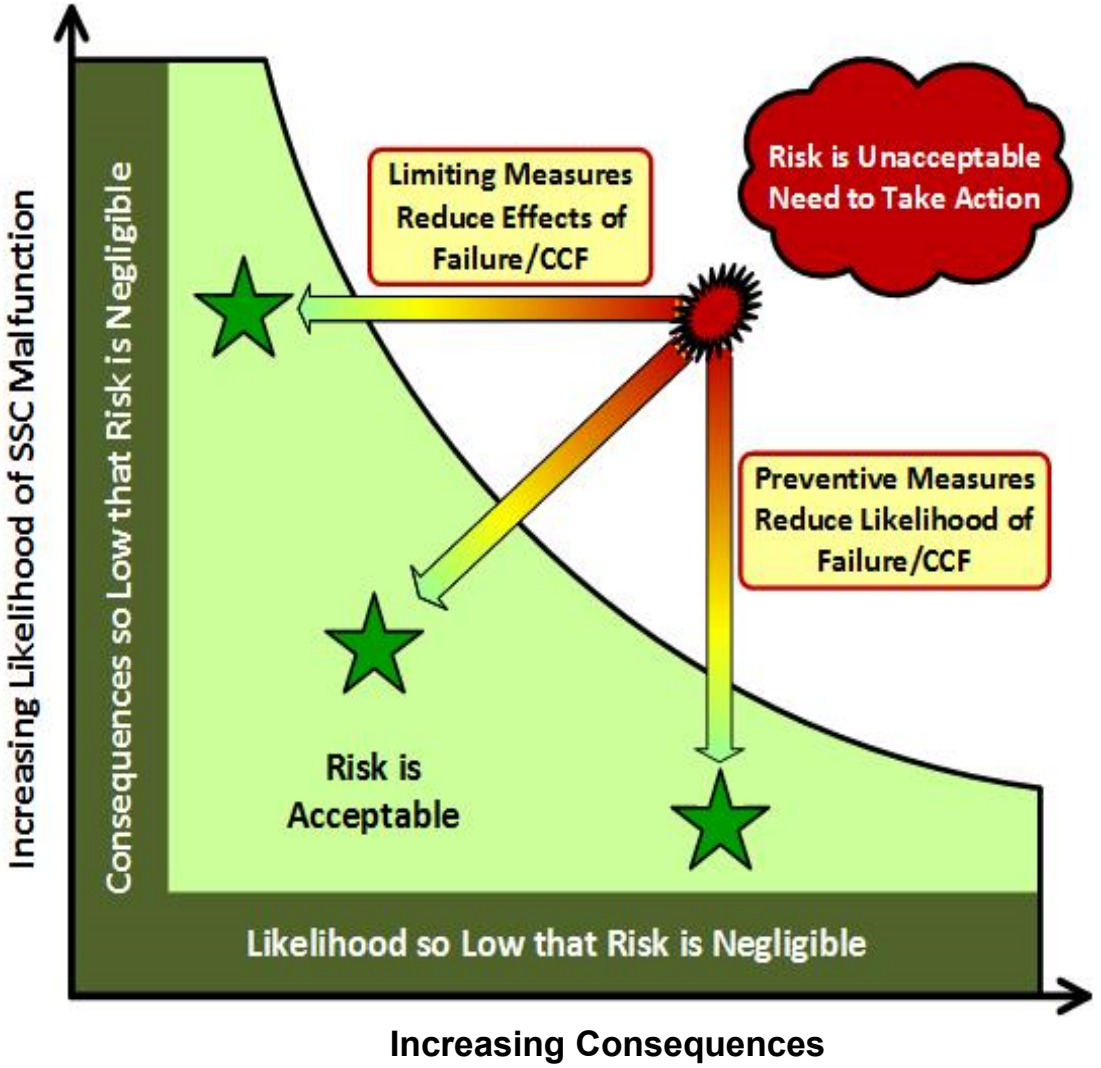
A focus on just likelihood (prevention) or consequences (mitigation) may not be effective in managing safety.

Each situation is unique, and prescriptive solutions can be mis-applied

There is no “magic formula”

Safety significance of I&C should be considered in context of the plant

- Identify important and unimportant failures
- Focus resources to maximize safety
- Guide iterations of susceptibility assessment and coping analysis



Project Status…

- Document drafted, examples being finalized & coordinated with examples in draft NEI-96-07 Appendix D
- EPRI Document No. 3002005326
- Major near-final draft out for comment to stakeholders March 3, 2016
- Final report anticipated May 2016
- Workshops and pilots to follow

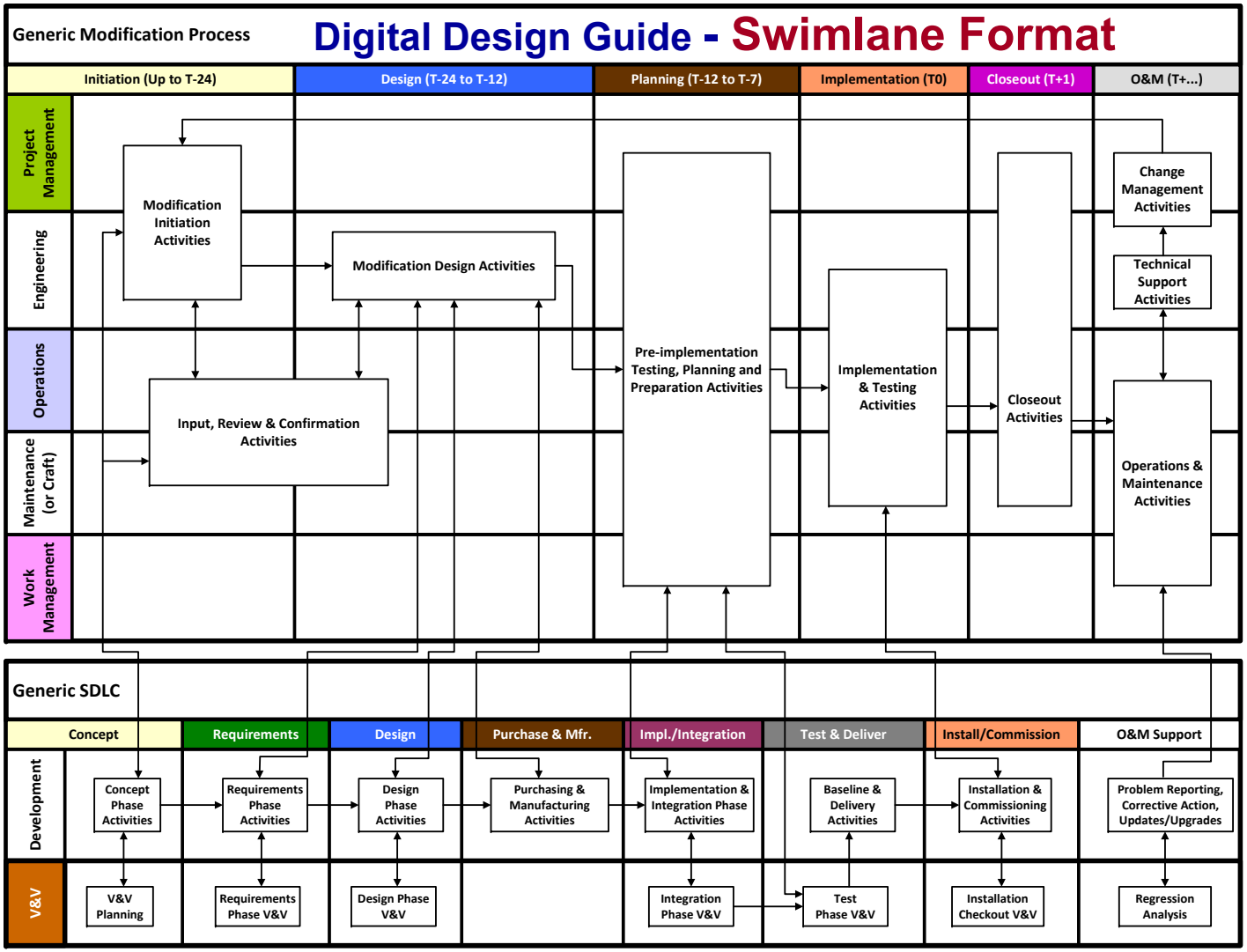
Are we asking the right question?

Categories	U.S. 1987 – 2007 (EPRI 1016731)	KHNP 1984 – 2010 (EPRI 1022986)
Safety-related digital events	**49**	**19**
Single failures	38 (78%)	19 (100%)
Non-software common cause failures	10 (20%)	0 (0%)
Software common cause failures	1 (2%)	0 (0%)
Non-safety related digital events	**273**	**78**
Single failures	217 (79%)	61 (78%)
Non-software common cause failures	42 (19%)	14 (18%)
Software common cause failures	14 (2%)	3 (4%)

- No one wants single failures, or any failures, with a new system
  - Typically do not buy things to break…
- Even without CCF issues, digital projects are difficult (reference INPO 10-02)
- But digital projects beneficial (once installed) and needed due to obsolescence
- How can effectiveness & efficiency of digital projects be improved without adversely affecting safety?

Framework for Addressing Digital Issues: *Digital Instrumentation and Control Design Guide*

- Guideline for digital design control in the plant engineering change/modification processes
  - How to integrate the unique aspects of digital design within a typical plant engineering change/modification process
  - Can be used in conjunction with existing change procedures or guide the development of procedures that can be integrated into the owner/operator's change process
  - Updates planned as technology and issues evolve
- Intended audience
  - Owner/operator design engineers and project managers involved in digital I&C modification activities
  - Architect-engineer service providers



- **Each topic is addressed in a dedicated section of the *Digital Design Guide*, with it's own swimlane**
- **Guidance is provided for each activity on the swimlane**

Digital Design Guide: Example

Guidance for each specific activity prompts the user to consider typical issues and topics

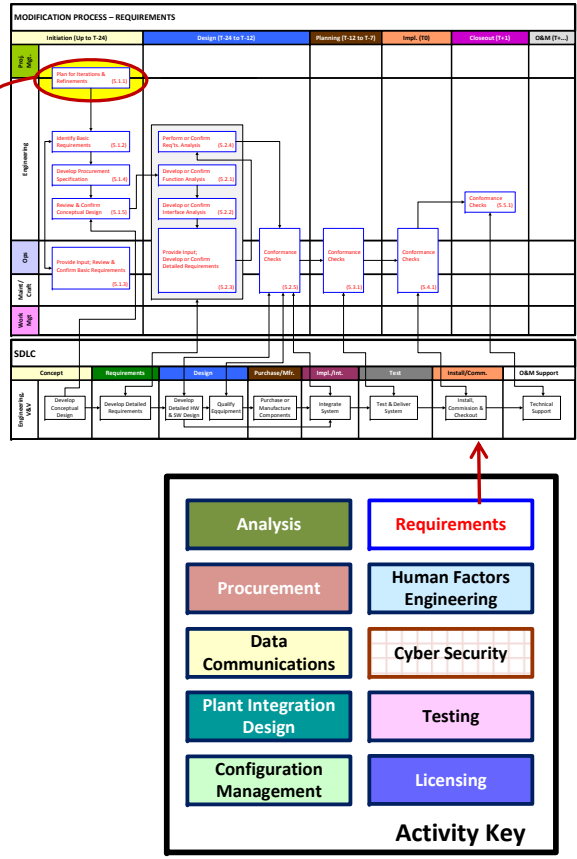
References point to detailed guidance (by section number)

5.1.1 Plan for Iterations & Refinements

Examine the system development lifecycle model being proposed or used by the system integrator, and identify the specific steps that are used for developing, refining and allocating requirements. Plan on participating in those requirements engineering activities, considering the following issues or topics:

- Iteration and refinements in requirements due to:
  - High level goals and requirements decomposed to more specific requirements
  - Identification of previously unrecognized design constraints
  - Identification and resolution of previously unrecognized hazards
- The system integrator's need for plant-specific knowledge, and the methods used for eliciting and capturing that knowledge in the form of more specific and resolved requirements
- Allocation of requirements to systems, subsystems or components
- The system integrators development lifecycle models and methods, such as:
  - Waterfall model
  - Spiral model
  - V-Model
  - Agile model
  - Digital upgrade lifecycle model (per EPRI 1002833)
  - Verification and validation plans, activities, methods and tools

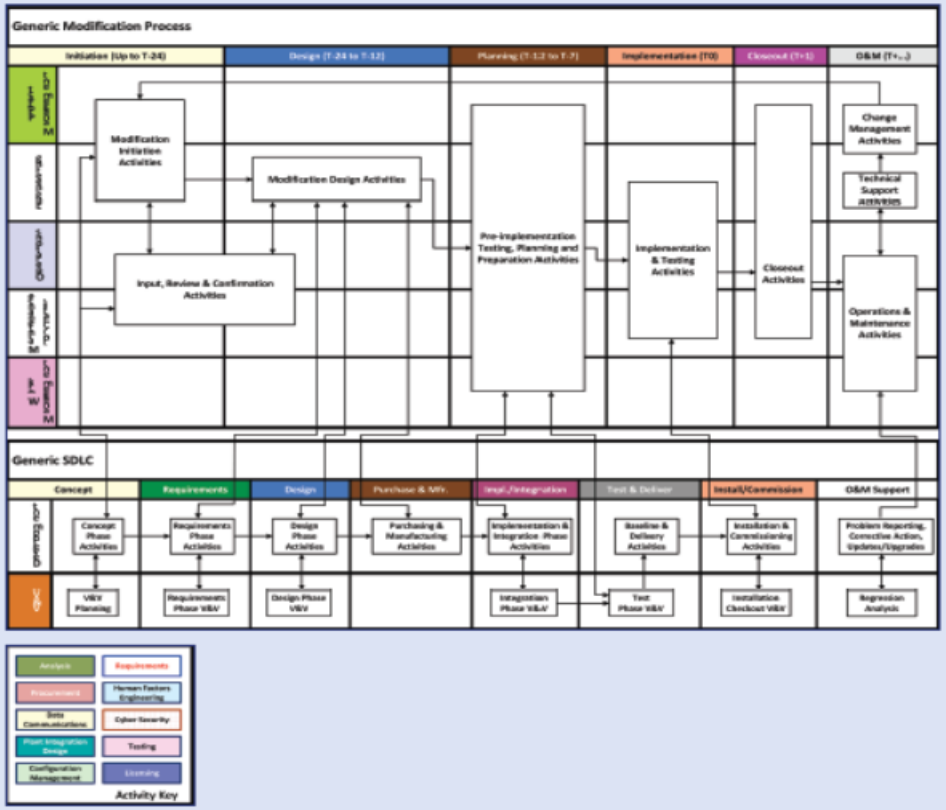
Task/Deliverable	For Detailed Guidance	Section
Plan for Requirements Iteration & Refinement	EPRI 3002002843	2.1.6 (Lifecycle Models)
		2.1.7 (Feedback & Iteration)
	IAEA-TECDOC-1066 (1999)	5.1 (Project Requirements)
	IEC Std. 61513, 2nd Edition	5.2 (Requirements)
	ISO/IEC Std. 29148 1st Ed.	5.3.2 (Iteration & Recursion in Req'ts. Engineering)
	IEEE Std. 1220-2005	6.1 (Requirements Analysis)
	IEEE Std. 1233-1998	7 (SysRS Development)

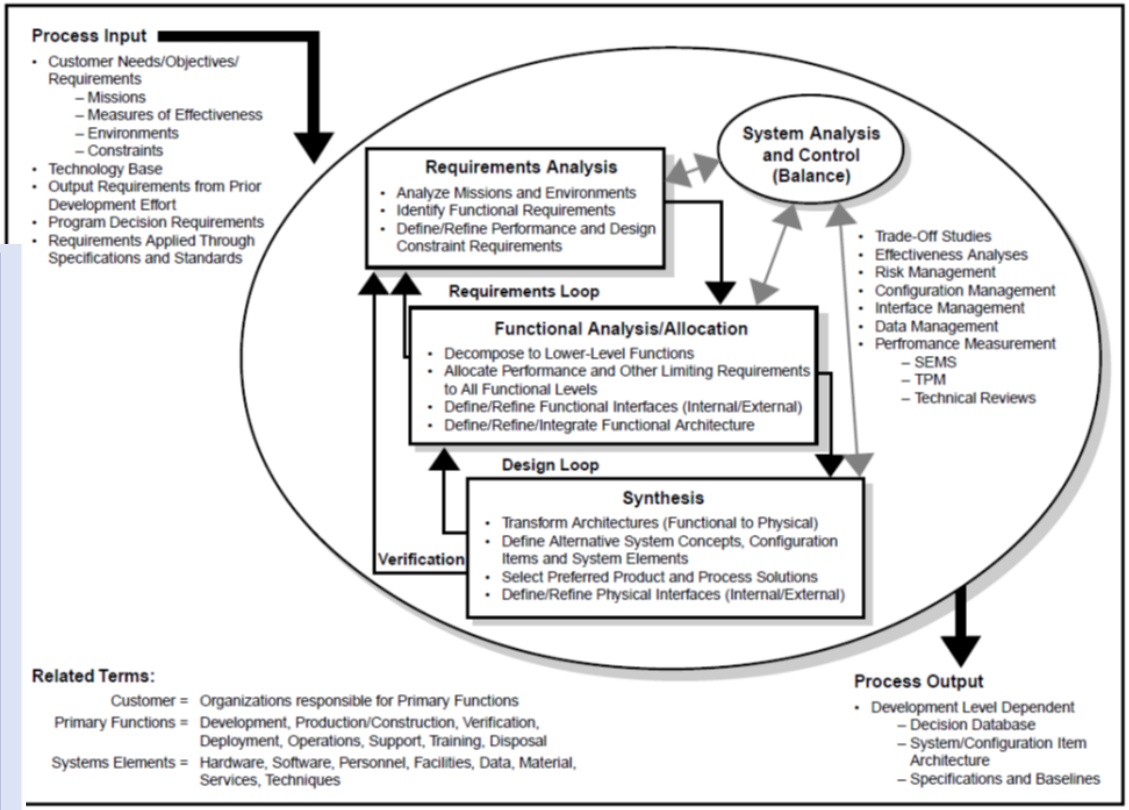


Guidance is not US-centric

Excerpt from Section 5 – "Requirements"

From the Digital Design Guide To Systems Engineering…





Together…Shaping the Future of Electricity