Applicability of EPRI Work on Digital Common-Cause Failure (CCF) to Embedded Digital Devices (EDDs)

Ray Torok (rtorok@epri.com)

NRC Public Meeting on Safe Use of Embedded Digital Devices

October 9, 2014

Contents

- Review EPRI project on common-cause failure (CCF)
- Expected characteristics of embedded digital devices (EDDs)
- CCF contexts for EDDs
- Review important CCF concepts
- Summary and Conclusions

EPRI Project on Common-Cause Failure (CCF)
Supporting NEI effort on NEI 01-01

- Provide technical input on CCF issues
- Refocus the conversation –
  - It’s not just about diversity or 100% testability
  - It’s about protecting against plant level CCF effects
- More holistic approach
  - Assess susceptibility to digital failure and CCF from all sources
  - Credit design features that address vulnerabilities (including diversity where appropriate)
  - Apply engineering judgment to assess CCF protection
  - Use coping analysis where appropriate

Expected Characteristics of EDDs

First, what are EDDs?

- Special purpose devices with predefined functionality?
- Subcomponents that can affect the primary system function, but have no human interface?
- Subcomponents that can affect primary function, but need very limited configuration settings?
- Subcomponents that come in as part of mods, but
  - Mod team not aware of digital component
  - Not evaluated or reviewed by digital experts
  - Need for digital review not recognized

Is this what the RIS is really after?

Expected Characteristics of EDDs, cont’d

- Commercial grade
  - Not developed to nuclear safety design or QA standards
  - Large operating history
  - “Dedicated” for safety applications per NP-5652* and TR-106439
- Limited digital expertise needed to get it working?? Could imply:
  - Limited functionality and configurability
  - Default configurations/built-in algorithms
  - Limited I/O, settings/adjustments
  - Limited communication capability

***** Superseded by: *Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications - Revision 1 to EPRI NP-5652 and TR-102260*, 3002002982, September 2014

CCF Contexts – Which Apply to EDDs?

- Redundant divisions of identical equipment/software
- Combining functions in a single controller
- Combining controls for multiple systems on a single platform
- Multiple systems with identical platforms or software elements
- Non-safety systems with internal redundancy that share resources (e.g., power supplies, timing signals, etc.)
- Multiple plant systems or controllers that share resources (e.g., data networks, workstations, sensors, etc.)

Note: EDDs could be in ESF breakers, motor control centers, diesel controllers, sequencers, time-delay relays, etc.

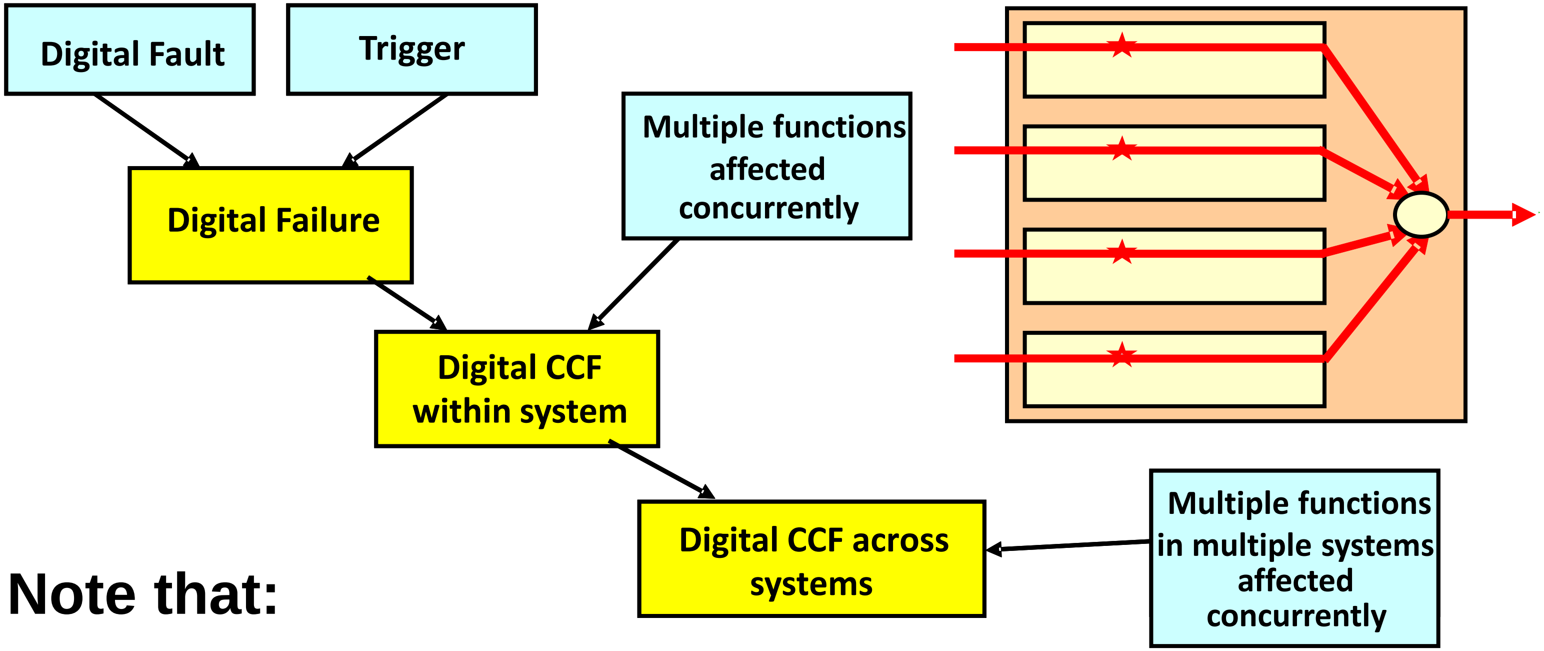
EPRI CCF Project Approach

Draw From and Expand Existing Guidance on CCF

- Consider all contributors to protection against CCF effects – both failure prevention and mitigation, including:
  - Traditional hardware practices - quality assurance, qualification testing, etc.
  - Software development practices – e.g., standards, coding practices
  - Defensive design measures in software, hardware, architecture, procedures, operation, etc.
  - Failure/hazard analysis
  - Test coverage
  - Performance records
  - Risk and fault tree analysis (FTA) insights
  - Backup systems
  - Coping and safety analysis insights, including “bounding” analysis

Which apply to EDDs?

CCF Concepts – Ingredients for Software CCF: Faults and Triggers



Digital Fault

Trigger

Digital Failure

Multiple functions affected concurrently

Digital CCF within system

Digital CCF across systems

Multiple functions in multiple systems affected concurrently

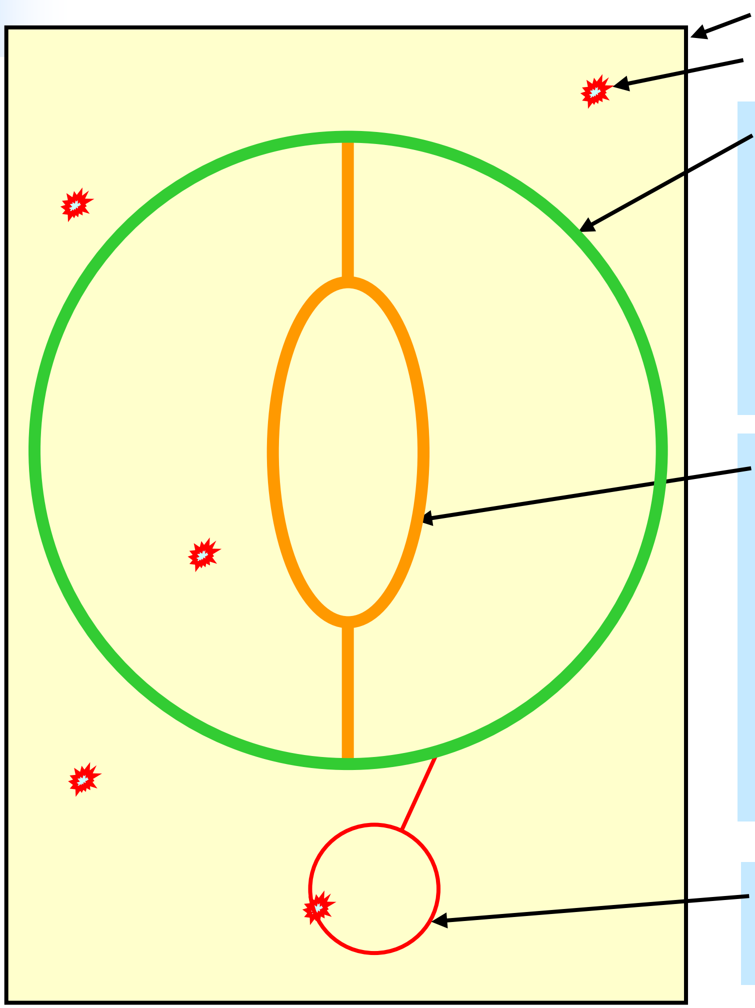
Note that:

- Not all digital faults/failures become CCFs
- Not all digital failures and CCFs are safety-significant
- Defect-free software is neither expected nor needed
- Eliminating faults and triggers reduces likelihood of failure / CCF

CCF susceptibility evaluation assesses devices for design measures and practices that reduce the likelihood of faults and triggers

CCF Concepts - Example of Trigger Avoidance

System Constrained to Well Understood and Tested Trajectories



Complete domain of behavior

May contain residual digital faults

Path exercised continuously in normal situations

Influence factors during continuous operation:

- normal process inputs (validated before use)
- short-term memory (as little as possible)
- clock interrupts (thorough verification)
- (process-related interrupts: none)
- (resource management: static)

Path exercised in occasional but tested situations

Influence factors that could disrupt cyclic behavior:

- initialization (only once)
- operator requests (single channel)
- hardware failures (single channel)
- exceptions (very simple)
- codified dates & times (e.g., Y2K)
- plant transients: affect all channels

Path exercised in unanticipated or untested trajectories

A robust system avoids unanticipated and untested trajectories

ELECTRIC POWER RESEARCH INSTITUTE

CCF Protection

Important Considerations

- CCFs can start with single random hardware failures, defects in software or hardware, or environmental disturbances
- If a defensive design measure that avoids a particular type of failure has been demonstrated, then that failure is unlikely
- Ensure credited defensive measures are maintained – a historical challenge for non-safety
- Evaluation credits protective (preventive and mitigative) measures both inside and outside the digital system
- Risk-benefit of additional protection (“reasonably practicable”)
- *Adequate* CCF protection tailored based on risk significance and complexity

CCF Protection –

Important Considerations, cont'd

- Tools that reduce likelihood of software defects, e.g., static analyzers, automated design tools
- Safety vs. non-safety – dependence on process vs. design
- Coping/bounding analysis assumptions – best estimate?
- Failure analysis techniques (e.g., FMEA, systems theoretic process analysis (STPA), and fault tree analysis) to:
  - identify potential vulnerabilities
  - identify combinations of spurious actions of multiple components
- Processed-based development standards

Summary and Conclusions
EPRI Digital CCF Guidance Will Apply to EDDs

- Most of the same CCF contexts are possible
- Same evaluation considerations apply:
  - Look at both prevention and mitigation
  - Look at both process and product
  - Tailor based on safety significance and complexity
  - Credit operating experience
  - Test coverage
  - Failure/hazard analysis insights
- Commercial grade dedication evaluations will be important
- CCF evaluation approach is consistent with CGD guidance – assess all evidence and apply engineering judgment

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Together…Shaping the Future of Electricity