



Digital I&C Technical Issues

NRC Public Meeting with EPRI

August 5, 2009

Rob Austin, Ray Torok
EPRI

Bruce Geddes
Southern Engineering Services

N. Thuy
EDF R&D

Dave Blanchard
Applied Reliability Engineering

EPRI Purpose for Today's Meeting

- Clarify past NRC comments on EPRI research:
 - Operating experience (OE)
 - CCF applicability
 - Diverse actuation system (DAS) and risk insights
- Have further dialog with the staff to identify gaps and / or issues with our research
 - NRC (& ACRS comments) can help guide future EPRI research, will allow EPRI to make recommendation to industry on use of research
 - EPRI is very interested in NRC staff's (and ACRS') technical comments on our research, and requests an open, honest technical interchange with NRC personnel

Purpose of EPRI Research on Digital I&C Issues

- Provide the technical bases and guidance to help utilities:
 - Manage I&C obsolescence
 - Implement advanced I&C and information technologies in nuclear plants
 - Enable plants to use digital technology capabilities to:
 - Maintain safe operation
 - Enhance reliability
 - Reduce operating costs
 - Address regulatory issues regarding digital systems

Discussion Topics

EPRI technical reports related to digital I&C

- Historical overview of:
 - Subject matter
 - Upcoming ACRS presentation
 - Differences between ‘white papers’ and final reports
- Technical concerns on selected topics/reports
 - **Operating experience (OE)**
Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems (EPRI 1016731, Dec 2008)
 - **Common-cause failure (CCF) applicability**
Common-Cause Failure Applicability (white paper prepared for NEI Digital I&C and Human Factors Working Group, Feb 2008)
 - **Diverse actuation system (DAS)**
Benefits and Risks Associated with Expanding Automated Diverse Actuation System Functions (EPRI 1016721, Dec 2008)

First Topic - Operating Experience (OE) Review

Historical Perspective

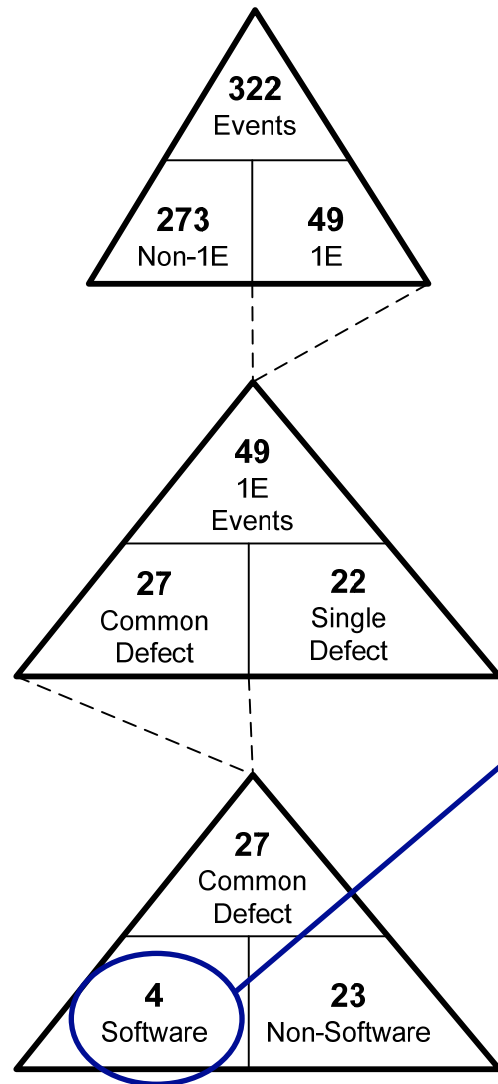
- White paper version transmitted to NRC through NEI in March 2008, presented to ACRS in March/April 2008
 - 322 safety and non-safety events in U.S. plants over 20 years
 - Look for actual and potential common-cause failures (CCF)
 - Capture insights on effective corrective actions, defensive measures
- NRC comments on white paper received November 2008
 - (Too late for response prior to publication)
- Final EPRI report (1016731) published December 2008
 - Provided to NRC in January 2009
 - **White paper methodologies and conclusions unchanged**
 - Expanded discussion of methods and observations
 - Appendix with brief descriptions of all 322 events
 - Detailed peer review by EPRI, NEI Working Group and various technical experts

Operating Experience Review

Overview of ACRS Presentation

- Review key terms used in evaluation, e.g., defect, common defect, event, potential CCF,
- Review breakdown of 1E and non-1E common defect events to find actual and potential CCFs
- Expanded discussion of failure mechanisms, modes and effects in response to ACRS questions
- Review comparison of 1E to non-1E vulnerability to CCF
- Review insights, inferences, conclusions, recommendations

Failure Mechanisms, Modes and Effects in 1E Software Events



Event	Failure Mechanism	Failure Mode ⁽¹⁾	Failure Effect	System Level Impact
1	Specification Error	Incorrect Substitute Value for Failed Sensor (Task Incorrect Response)	CPC ⁽²⁾ Channel May Not Trip When Required	No CCF
10	Design Error	Incorrect Logic While in Self-Test Mode (Task Incorrect Response)	Sequencer Blocks Safety Injection ~ 15% of Time	Potential CCF
13	Missing Requirement (Omission)	No Watchdog Timer (HW) & "WRITE" Operation (SW) (Task No Response)	RMS ⁽³⁾ Processor Lockup During Power Transient	No CCF
221	Design Error	Counter Not Initialized at the Right Time (Task Incorrect Response)	Momentary Step Change in RMS Output Signal	Spurious Actuation

1. As described in ACRS Letter dated 4/29/08
2. CPC = Core Protection Calculator
3. RMS = Radiation Monitoring System

Key Insights / Conclusions / Recommendations From the OE Report

- **Software has been no more problematic than other CCF contributors**
- **Majority of software-related common-defect events could have occurred in hardware-based systems**
- **Need to capture and promote process and design characteristics (defensive measures) that have been effective in protecting against all CCFs (both hardware and software)**

Next Topic: Digital Failure Mechanisms / Modes / Effects

Historical Perspective

- CCF Applicability white paper version transmitted to NRC through NEI in March 2008
 - Discussion of protection against digital CCF, with emphasis on design and process attributes (defensive measures) in concert with diversity
- ***“Digital I&C may introduce new failure modes that are not well understood.”*** – Letter, Chairman ACRS to Chairman U.S. Nuclear Regulatory Commission, April 29, 2008
- NRC comments on white paper received November 2008
 - Additional discussion under EPRI/NRC MOU
- **Final report on this not yet published**
 - NRC and peer review comments will be addressed as appropriate

Digital Failure Mechanisms / Modes / Effects

Overview of ACRS Presentation

“Failure mechanisms produce failure modes which, in turn, have certain effects on system operation.” - NUREG 0492 (Fault Tree Handbook)

Mechanisms, modes and effects for digital systems

- Digital system FMEAs performed today
- Realistic digital system behaviors
- Context of nuclear plant safety system
- Implications for PRA

Digital Failure Mechanisms / Modes / Effects

1E Systems – Designed for High Reliability

Failure ~~Modes~~/Mechanisms* Realistic 1E System Behaviors

1. Task Crash

2. Task Hang

3. Task Late Response

4. Task Early Response

5. Task Incorrect Response

6. Task No Response

7. Processor Crash

Defensive measure - Any software or processor problem that prevents an output from being issued within a given time frame will cause the hardware watchdog to raise a trip/alarm signal

8. Corrupted Input

9. Corrupted Output

10. Out-of-Sequence Data

* From ACRS letter to Chairman of NRC Commissioners, 4/29/08

Digital Failure Mechanisms / Modes / Effects

CCF Implications

- Failure mechanisms may be prevented or mitigated by defensive measures and/or diversity
- Diversity may be appropriate, but....
 - Not the only solution, may not be the preferred solution
 - Necessarily adds complexity, but not necessarily safety
 - May be more appropriate between different lines of defense than within a single line of defense
- Match solution to context
 - Integrate diversity, defensive measures and OE insights for CCF protection (prevention as well as mitigation)
 - OE shows importance of defensive measures
 - OE shows benefits of some types of diversity, e.g., functional and signal diversity

Digital Failure Mechanisms / Modes / Effects

PRA Implications

- Only failure modes (not mechanisms) need be represented explicitly in PRA, on an application-specific basis, with:
 - Probabilities of failure modes on demand
 - Frequencies of failure modes in continuous conditions (e.g., spurious actuation and mission time failures, if applicable)
 - Understanding of dominant failure mechanisms may be helpful in estimating failure probabilities and beta factors
- Design measures may prevent or mitigate particular failure mechanisms
 - Good design rules for digital safety systems have been honed and tried and tested over more than three decades
- Some design measures may be effective against a wide range of failure mechanisms
 - Example: Watchdog in earlier slide

Failure Mechanisms, Modes and Effects

Conclusions and Recommendations

Conclusions

- Failure **modes** of digital protection systems are well understood
 - System-level behaviors
 - Essentially same as for analog systems
 - Digital system CCF accounted for in D3 coping analysis
 - CCF effects are modeled in PRA for existing plants
 - Extensive FMEAs are being performed by equipment suppliers and licensees
- Failure mechanism evaluation useful to improve the design through incorporation of defenses against problematic failure mechanisms

Recommendation

- EPRI and NRC coordinate efforts to develop guidance on protecting against CCF, including complementary use of diversity and defensive measures

Next Topic - Diverse Actuation System (DAS)

Historical Perspective

- White paper version transmitted to NRC through NEI in May 2008
 - Risk-informed look at potential benefits and risks associated with automated DAS per ISG-2 (September 2007 version)
- NRC comments on white paper received November 2008
 - (Too late for response prior to publication)
- Final EPRI report (1016721) published December 2008
 - **White paper methodologies and conclusions unchanged**
 - Restructured to improve readability
 - Details moved to appendices, especially sensitivity studies
 - Verbal comments from TWG meetings addressed
 - Additional sensitivity study
 - Relative benefits of prevention versus mitigation (suggested by NRC staff)

Diverse Actuation System (DAS)

Overview of ACRS Presentation

Example of development of risk insights for digital systems using existing PRA methods

- Analysis approach using automated DAS example
 - Deterministic evaluations to identify sequences that might need automated DAS
 - Probabilistic results to assess potential risks/benefits
 - Estimating digital failure probabilities, beta factors
 - Modeling of failure modes and effects
- Summarize key insights and conclusions
- Sensitivity studies and effects on conclusions
- Use of risk insights to improve automated DAS design
- Potential impact of revised 30 minute criterion

Deterministic Insights from Risk Analysis – Magnitude of Potential Automated DAS Benefits

Benefit relatively small - effective defense-in-depth and diversity provided by existing plant features:

- **Prevention** strategy for LOCA and SLB – provided by reactor coolant pressure boundary:
 - Designed in accordance with piping and pressure vessel codes
 - Periodic inspection per Section XI and pressure vessel codes
 - Monitored during operation (Tech Spec leakage detection activities)
- **Mitigation** of LOCA and SLB – provided by highly reliable ESFAS:
 - Design to consensus standards, redundant, independent trains, etc.
 - Rigorous verification and validation
 - Design features that limit potential for I&C failures and CCF
- **Independence** - Initiating events (LOCA and SLB) and mitigating systems (ESFAS) share no common elements
 - LOCA with loss of ESFAS would require independent failures

Example Application of PRA to Digital I&C Issues (Automated DAS)

Conclusions

- Possible to generate risk insights using existing PRA techniques
 - Address limitations of deterministic approach
 - Identify potentially negative effects.
 - Demonstrate insensitivity to wide variations in assumptions on failure modes and probabilities
- **Automated DAS for low frequency events has little or no benefit**
 - Conclusion is insensitive to digital protection system reliability
- **Beneficial features for CCF include diverse ATWS mitigation, use of piping and pressure vessel codes, ISI/IST, diverse leak detection, etc.**

Recommendation

- ACRS consider results of this research and encourage Staff and industry use of current PRA methods to address digital I&C issues:
 - Licensing actions, e.g., automated DAS for low frequency events
 - NRC research plan

Next Steps on EPRI Digital I&C Activities

- Document existing PRA scoping and sensitivity studies
- Publish guidance on protecting against CCF
- Develop guideline on estimating digital system reliability based on design and process attributes
- Develop guideline for failure analysis of digital systems
- Continue support of NEI Working Group
- Continue activities under MOU between EPRI and NRC Research on digital I&C issues, e.g.,
 - Operating experience
 - Risk methods
 - Adequate diversity and defensive measures for CCF protection
 - Human factors



Together...Shaping the Future of Electricity