

***NEI 01-01,
Revision 1 to EPRI TR-102348,
“Guideline on Licensing
Digital Upgrades”***

October 11, 2001



Agenda

- ❖ Overview of Project Status
- ❖ Purpose of Meeting and Expected Outcome
- ❖ Schedule
- ❖ Discuss Resolution of Key NRC Comments
- ❖ Other Anticipated Changes to Licensing Guideline
- ❖ Wrap Up (Action Items, Expectations)



Project Status

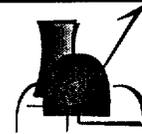


- ❖ NEI/EPRI Task Force met with NRC on April 26, 2001
- ❖ Revised Licensing Guideline (Draft E) issued in July for NRC and broad industry review
- ❖ NRC provided comments on draft E
 - ▶ Most easily incorporated into final revision
 - ▶ Discussion beneficial on some proposed resolutions

NEI

EPRI

Expected Outcome



- ❖ Reach a mutual understanding of NRC comments and proposed resolutions
- ❖ Meeting with NEI/EPRI Task Force to finalize changes
- ❖ Take away results of these meetings to produce *final* Revision 1 to be submitted for NRC endorsement

NEI

EPRI

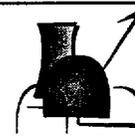
Project Schedule



- ❖ October 2000 First meeting of small working group
- ❖ December 2000 Complete approach for revised guideline
- ❖ March 2001 Full Task Force meeting
- ❖ April 2001 First meeting with NRC
- ❖ June 2001 Issue first draft for industry and NRC review
- ❖ July - Sept. 2001 Discuss draft with NRC
- ❖ Dec. 2001 Submit guideline to NRC for formal approval
- ❖ TBD NRC issue endorsement in _____(?)



Discussion of NRC Comments



- ❖ Proposed resolution of NRC comments is described in handout
 - Do not intend to discuss comments marked "resolved"
 - Revisit these at the end of the meeting, time permitting
- ❖ Save discussion of comments regarding treatment of software common mode failure in the licensing guideline for the end
 - Most "open" comments listed in the handout relate to this topic
 - Review "open" comments after discussion



Software Common Mode Failure

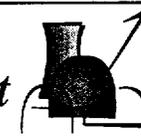


- ❖ Based on NRC and industry comments, need clarification of the Licensing Guideline approach for treatment of software common mode failure (SWCMF):
 - Put SWCMF in context
 - When is defense-in-depth and diversity evaluation per BTP-19 required?
 - Under what conditions does the potential for SWCMF cause a modification to “screen in” to 10 CFR 50.59?
 - Under what conditions is the likelihood of a SWCMF sufficient such that an LAR is required?

NEI

EPRI

Common Mode Failure in Context



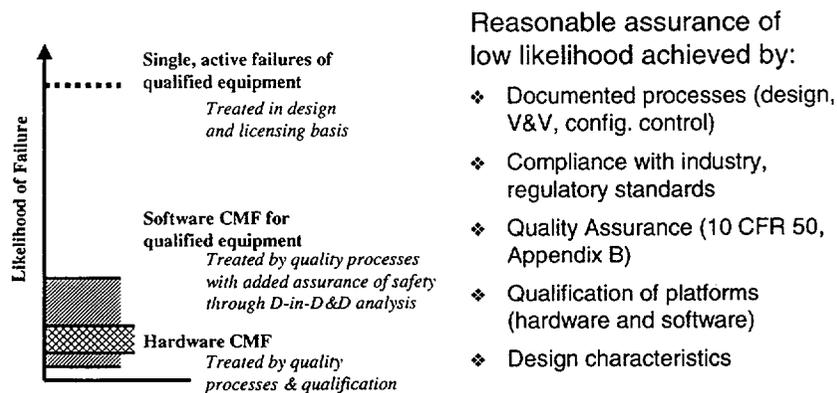
- ❖ Single, active failures considered in licensing basis
 - Single failure criterion in IEEE 603, 279, 379
- ❖ Plant is not designed to cope with common mode failures of hardware (HWCMF)
 - Hardware failures result from design/manufacturing flaws or degradation processes such as wear/corrosion
 - Likelihood of HWCMF minimized by design control, qualification, maintenance, testing
- ❖ Software failures are a result of design flaw
 - Apply similar controls to minimize likelihood

For qualified software-based systems, where is the likelihood of failure in the context of other failures?

NEI

EPRI

Software Common Mode Failure



Reasonable assurance of low likelihood achieved by:

- ❖ Documented processes (design, V&V, config. control)
- ❖ Compliance with industry, regulatory standards
- ❖ Quality Assurance (10 CFR 50, Appendix B)
- ❖ Qualification of platforms (hardware and software)
- ❖ Design characteristics

D-in-D&D (per BTP-19) compensates for uncertainty in likelihood

NEI

EPRI

Defense-in-Depth and Diversity

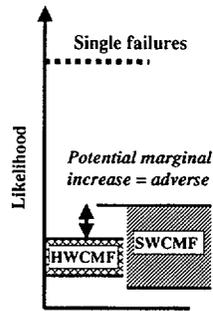


- ❖ SRM to SECY 93-087 (ALWR) addressed SWCMF:
 - Common mode failures are "beyond design basis"
 - Still warrants evaluation of Defense-in-Depth and Diversity (D³) on best-estimate basis to demonstrate vulnerabilities to CMF have been adequately addressed
 - May require diverse backups to cope (can be non-safety*)
- ❖ BTP-19 reflects understanding that software failures in qualified systems are "beyond design basis"
- ❖ D³ per BTP-19 expected as part of design for upgrades to RTS/ESFAS systems (with or without LAR)
 - Also for cumulative effect of multiple digital upgrades
 - For component upgrades D³ may be very simple
 - If likelihood is comparable to HWCMF, may not be necessary

NEI

EPRI

10 CFR 50.59 Screening

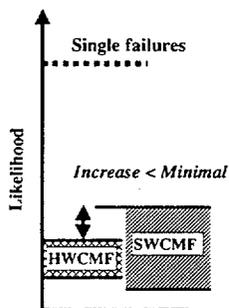
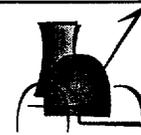


- ❖ Does the upgrade create an adverse effect?
- ❖ With high assurance that likelihood of SWCMF is comparable to HWCMF, there would be no adverse effect
 - High quality, excellent operating history screen out
 - Otherwise, identical upgrades to redundant safety system I&C channels screen in

NEI

EPRI

10 CFR 50.59 Evaluation



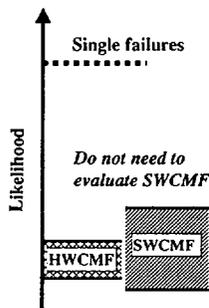
Likelihood of Malfunctions:

- ❖ Determine if reasonable assurance exists that likelihood of software failure is significantly below that of single, active failures
- ❖ Qualitative evaluation
 - Standards, regulations, processes, qualification
- ❖ If likelihood is low, then there is no more than a minimal increase
 - Otherwise, prior NRC review would be required

NEI

EPRI

10 CFR 50.59 Evaluation



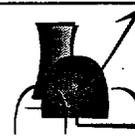
Results of Malfunctions of SSCs:

- ❖ Determine if results are different than (and not bounded by) those evaluated in UFSAR
- ❖ Consider malfunctions that are as likely as those already considered in UFSAR (NEI 96-07, Rev. 1)
- ❖ Do not need to evaluate SWCMF as a malfunction in 50.59 evaluation if likelihood is shown to be low
 - Otherwise, SWCMF would create different results, and prior NRC review would be required

NEI

EPRI

Other 50.59 Issues

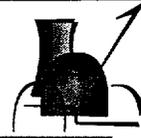


- ❖ License Amendment could be required due to:
 - Tech Spec changes
 - Combining previously separate functions (in a way that creates malfunctions with different results)
 - Reducing diversity (using one platform in multiple applications)
 - Reducing performance (response time, accuracy, etc.)
 - Introducing different failure behavior that affects design function
 - Significant HSI changes

NEI

EPRI

Wrap Up



- ❖ Additional Questions/Issues?
- ❖ Action Items
- ❖ Expectations



	A	D	E	F	G
	Name/ Organizatio n	Section of Licensing	Comment	Resolution	Status
1					
2	NRC	1.1	"Background." First paragraph, last sentence, suggest changing the concluding phrase to read, "...require special <u>prior</u> Nuclear Regulatory Commission (NRC) scrutiny <u>approval</u> ."	Incorporate change as noted.	Resolved
3	NRC	2.0	"Definitions and Terminology." Definition for "safety related" states, "see safety systems." This should be "see safety systems, structures, and components."	Incorporate change as noted.	Resolved
4	NRC	2.0	The definition of "diversity" references IEC 880 and EPRI TR-100516. The definition should also be reconciled with the definition of diversity as stated in NUREG/CR-6303, BTP-19, and with respect to the single failure criterion 10 CFR 50.55a (h) (IEEE 279, 603).	Make sure the definition is consistent with the NUREG and BTP, and add reference to these regulatory documents. (See also NRC comment on Sect. 6.3).	Resolved
5	NRC	3.1.1	"Digital Issues in the Upgrade Process." The second paragraph implies that a Defense-in-Depth and Diversity (D-in-D&D) analysis would be expected for only large scale safety system upgrades. A series of small digital retrofits performed and integrated over a period of years across systems may ultimately require a D-in-D&D analysis.	Delete "large scale" in 2nd paragraph. Discussion about the need to do defense-in-depth and diversity (D3) analysis per BTP-19 is provided in Sections 4.2.1 (brief) and 6.5 (more detail). Add words to Section 6.5.1 to clarify that the cumulative effects of modifications should be considered when determining when D3 should be performed.	Open
6	NRC	3.1.2	"Failure Analysis." In the introductory paragraph, reference to SRP Chapter 7 and particularly to BTP-14 could be added.	Further discussion with Matt Chiramal indicated that other parts of the guideline adequately refer to and provide discussion on BTP-14 and chapter 7 of the SRP. Matt agreed no action is required to address this comment.	Resolved

	A	D	E	F	G
	Name/ Organizatio n	Section of Licensing	Comment	Resolution	Status
1	NRC	3.1.2, 4th paragraph	The fourth paragraph discusses "dependability" where "reliability" may be more appropriate.	Add a definition of "dependability" (from COTS guideline based on NUREG) to section 2 definitions. We believe dependability is used appropriately in this case. Also see resolution for comment in row number 21.	Resolved
7	NRC	3.1.2, 6th paragraph	In the sixth paragraph, the last sentence should be revised, to distinguish the failure analysis in the design process with that in the 50.59 process, to read, "Here <u>in the 50.59 process</u> , it is important to maintain focus ..."	Incorporate change as noted.	Resolved
8	NRC	3.2.2	"Requirements." First paragraph, last sentence discusses the need for adequate communication between licensee and vendor. This could be elaborated to add the need to continue communication between the vendor's design team and licensee's plant systems engineers, operators, maintenance and testing staff to ensure that the system requirements have been correctly and completely included in the software and hardware requirement specifications.	Incorporate change as noted.	Resolved
9	NRC	3.2.5	"Operation, Maintenance, and Support." Last paragraph could include a reference to BTP-17.	A reference to BTP-17, "Guidance on Self-Test and Surveillance Test Provisions" will be added as noted.	Resolved
10					

	A	D	E	F	G
	Name/ Organizatio n	Section of Licensing	Comment	Resolution	Status
1	NRC	4.2.1	"Technical Evaluations." The second paragraph discusses D-in-D&D analysis for substantial upgrades to the RPS and ESFAS. Such an analysis may be necessary if upgrades are made to other safety systems that would impact RPS and ESFAS. For example, if the analog sensors and transmitters that provide separate and isolated input to RPS, PAMS, other safety systems, and control systems were changed to be digital systems by using A/D converters, then a D-in-D&D analysis would be necessary.	Further discussion with Matt Chiramal revealed that his primary concern is that the diversity and defense-in-depth for plant protection functions in the original plant design could be affected if changes are made to systems other than RPS/ESFAS (e.g., systems that provide input to RPS/ESFAS). Therefore, for any change to the plant, consideration should be given as to the effects the change may have on diversity and defense-in-depth for RPS/ESFAS functions. If the change would affect the diversity and defense-in-depth of the original plant design, then the D3 analysis should be performed.	Open
11	NRC	4.2.1, 5th paragraph	We agree with the statement in the 5th paragraph about the decrease in reliability and safety of un-needed diverse back-ups. Therefore, assure that the level of quality for back up systems are commensurate with the safety significance of their functions.	Add a statement to 5th paragraph to clarify that level of quality should be "sufficient for the system to perform the function" (use verbiage consistent with BTP-19).	Resolved
12	NRC	4.2.1, Figure 4- 3	Indicates regulatory guidance and industry standards - should include regulatory requirements. Suggest "Regulatory Requirements and Guidance." In the 5th paragraph, first sentence, add regulatory requirements to the phrase "regulatory guidance," to read "...regulatory requirements and guidance."	Incorporate change as noted.	Resolved
13					

1	A Name/ Organizatio n	D Section of Licensing	E Comment	F Resolution	G Status
14	NRC	4.2.1, Example 4 3	Should include a cautionary note that if the analog transmitter provided inputs to other systems (control, indication, alarm, etc.), then the change to smart transmitter is likely to "screen in."	Based on further discussion with Matt Chiramal, the main concern behind this comment is screening of changes that may compromise diversity (such as when the same transmitter is installed in different systems where a common mode failure may be introduced). The screening process should address whether the upgrade is applied to redundant or diverse systems. Develop another example to illustrate when a similar upgrade (possibly implemented in redundant equipment) would screen in.	Open
15	NRC	4.3.1	"Does the activity result in more than a minimal increase in the frequency of occurrence of an accident?" The last sentence of the last paragraph states that new equipment is expected to be more reliable than replaced equipment thus the change would not be more than a minimal increase in likelihood of occurrence. The sentence should be changed to include a statement that the expected reliability must be assured in some manner - e.g., refer to paragraph 5 of Section 4.3.2.	Supplement 4.3.1 with discussion such as that which appears in paragraph 5 of 4.3.2.	Resolved
16	NRC	4.3.2	"Does the activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety?" In the 6th paragraph credit is being taken for diagnostics to reduce system malfunctions. Diagnostics identify failures, but to reduce the likelihood of system malfunctions, immediate analysis for root cause and subsequent corrective actions need to be undertaken to return the equipment and system to service.	Clarify that self-diagnostics accompanied by corrective action procedures and program can improve the dependability of a train of a system, therefore the system-level design function is preserved.	Open

	A Name/ Organizatio n	D Section of Licensing	E Comment	F Resolution	G Status
17	NRC	4.3.2, Example 4 4	Not a good example - the NRC's SER for pre-qualified PLC platforms has several plant-specific open items that the licensee is required to close out, and some items that are to be submitted for NRC review.	Example will be clarified to indicate that the open items in the SER that are appropriate and applicable to the specific plant will be addressed and the 50.59 process will be followed.	Open
18	NRC	4.3.2, Example 4 5	Second sentence contains "...therefore, there is no concern with common mode failure issues." The phrase "no concern" should be replaced by something like "low likelihood of common mode failure."	The example refers to the motor driven pumps using different controls. Change the second sentence to read: "This single pump provides backup to the two motor driven Auxiliary Feedwater pumps that <u>do not</u> use different <u>digital</u> controls, and therefore there is no concern with common mode failure <u>is not an issue for this modification.</u> "	Resolved

	A Name/ Organizatio n	D Section of Licensing	E Comment	F Resolution	G Status
1	NRC	4.3.6, Paragraphs 7 and 8	<p>"Does the activity create a possibility for a malfunction of an SSC important to safety with a different result?" NEI 96-07, Rev. 1 states "A malfunction that involves an initiator or failure whose effects are not bounded by those explicitly described in the UFSAR is a malfunction with a different result." It also has "An example of a change that would create the possibility for a malfunction with a different result is a substantial modification or upgrade to control station alarms, controls, or displays that are associated with SSCs important to safety that creates a new or common cause failure that is not bounded by previous analyses or evaluations."</p> <p>The discussion in paragraphs 7 and 8 of NEI 01-01, Section 4.3.6, on credible failure analysis and D-in-D&D analysis, apparently contradicts the above statements in that changes to the facility with failure effects not explicitly described in the UFSAR, are being implemented under 50.59.</p>	<p>The key question is when does a digital upgrade to a system with redundant channels need a license amendment on the basis of software common mode failiure (SWCMF)? The draft Licensing Guideline used D-in-D&D results to answer this question, but we agree that this approach can lead to contradictory conclusions.</p> <p>We propose a revised approach which places greater emphasis on the likelihood of SWCMF. If the likelihood is very low (e.g., close to that for comon mode hardware failures due to design), then the upgrade does not "create a new or common cause failure." If the likelihood is significant (close to that for single, active failures that are evaluated in the UFSAR), then the upgrade would create a new common cause failure with different results. This approach is consistent with NEI 96-07, section 4.3.6 which states that "The possible malfunctions with a different result are limited to those that are as likely to happen as those described in the UFSAR." Add the example of "substantial upgrades to control stations..."</p>	Open
19		4.3.6, paragraphs 7&8 and Example 4 7	To comply with 50.59 criterion(c)(2)(vi), the discussion in paragraphs 7 and 8 should lead to a conclusion that the changes described require the licensee to obtain a license amendment per 50.90. This also applies to Example 4-7.	See resolution above. Revise the example to clarify how the conclusion of "no new results of a malfunction are created" is reached.	Open
20					

	A	D	E	F	G
	Name/ Organizatio n	Section of Licensing	Comment	Resolution	Status
21	NRC	6.3	"Digital System Quality." First paragraph discusses "reliability." It appears that reliability and dependability may be used interchangeably throughout the document. As an example see Section 6.6. Title uses dependability and body of document uses reliability and dependability. See also Sections 4, 5.3, and 5.4. It is not always clear what was intended.	Add a definition of "reliability" to section 2 definitions (taken from appropriate standard, e.g. IEEE 353 and/or 577). Verify that "reliability" and "dependability" have been used appropriately throughout the guideline.	Resolved
22	NRC	6.4	"Digital System Design and Performance." Most operating plants were designed to IEEE Std. 279-1971. Digital equipment designed and installed to IEEE 603 will satisfy the requirements of IEEE 279 and is the most current guidance. However, it should be noted that incorporating a digital system into a plant per the requirements of IEEE 603 may require modifications (603's scope is larger) to the plant beyond the plant's license base (IEEE 279).	Based on further discussion with Matt Chiramal, the punchline of this comment is that licensees that have been licensed to IEEE-279, do not have to meet IEEE 603 (although many vendors are now designing equipment to meet 603), but if they do meet 603, by default they will meet 279 also. Add discussion clarifying this issue to this section.	Resolved
23	NRC	6.4.5	"Security Considerations." Security has been an item of consideration for I&C systems, as reflected in IEEE Std. 279, 1971 requirements for access control. The NRC has revised its regulations and guidance to reflect the conversion to digital technology. In June 1997, the NRC issued its Standard Review Plan (SRP) Chapter 7, Revision 4, (http://www.nrc.gov/NRC/NUREGS/SR0800/CH7/homepage.htm) to address digital technology issues. See NRC comment write-up for additional discussion on the specific regulations and guidance.	Add a new section for security/access control to emphasize the importance of security considerations, with reference to the appropriate regulatory guidance in the SRP.	Resolved

	A	D	E	F	G
	Name/ Organizatio n	Section of Licensing	Comment	Resolution	Status
1					
27	NRC (J. Bongarra	3.1.2, Page 3-4	Second full paragraph, beginning with, "At the engineering design stage..." Suggest including the design of the HSI as one of the several factors that can affect the likelihood of system failure/dependability. The current text, and Figure 3-2, emphasize hardware/software influences on risk but are silent on the potential adverse effects of the HSI on risk/failure.	Incorporate change as noted.	Resolved
28	NRC (J. Bongarra	4.2.2, page 4-10	"Screening Human-System Interface Changes" - In the second paragraph that begins, "However, minor changes in the human-system hardware interface..." This sentence introduces a new term, "human-system hardware interface." Is an HSI the same as a "human-system hardware interface" or different? More importantly, I suggest striking the first two sentences of this paragraph. The quotation from NEI 96-07 Rev. 1 cited in the paragraph preceding and the examples given in the paragraph that follows stipulate those types of changes that should be screened in. Introducing the concept of "minor changes in the human-system hardware interface..." forces the user/reviewer, using subjective judgement, to distinguish between "minor changes" and those that are not minor. I think that introducing the concept of minor changes is confusing and unnecessary.	Agree that "minor changes" and "hardware interface" are not well defined. Propose to revise the second paragraph to read as follows: "It is important to note that not all changes to the human-system interface fundamentally alter the means of performing or controlling design functions. Some HSI changes that accompany digital I&C upgrades leave the method of performing the functions essentially unchanged. Technical evaluations should determine whether ..."	Resolved
29	NRC (J. Bongarra	6.4.2, page 6-9	"Human Factors" - See previous comment re: using the term "interface" to define "interface." Also suggest, in the paragraph that begins, "The principal concern related..." that "plant procedures" be substituted for "maintenance procedures" because system failure due to human error may be caused not only by maintenance procedures by plant operating procedures.	Agree that use of the word "interface" could be confusing here. Will change wording to ""The human-system interface includes all points of interaction between the digital system and plant personnel..." Also agree to substitute "maintenance procedures" with "plant procedures".	Resolved

	A	D	E	F	G
	Name/ Organizatio n	Section of Licensing	Comment	Resolution	Status
1					
30	NRC (J. Bongarra	6.6, page 6-15, 4th paragraph from bottom+D7	Suggest adding the following at the end of the last sentence, "and the effective design of associated HSIs that support operator/personnel performance." The overall risk of failure of digital upgrades is highly influenced by the adequacy of the HSI.	Incorporate change as noted.	Resolved
31					