

August 23, 2001

Ms. Lynnette Hendricks
Director, Licensing
Nuclear Energy Institute
Suite 400
1776 I Street, NW
Washington, DC 20006-3708

SUBJECT: NRC COMMENTS ON DRAFT NEI 01-01 (EPRI TR-102348-R1 DRAFT E,
JULY 2001)

Dear Ms. Hendricks:

By letter dated July 24, 2001, the Nuclear Energy Institute (NEI) submitted a draft NEI 01-01 (EPRI TR-102348-R1 Draft E, July 2001), "Guideline on Licensing Digital Upgrades," for staff review. This document and NEI's plan to update guidelines for licensing digital system upgrades were discussed during a public meeting on April 26, 2001. The staff has completed a preliminary review, and is providing the attached comments to be discussed in our meeting scheduled for September 11, 2001.

If you have any questions please contact me at 301-415-2832.

Sincerely,

/RA/Signed by P. Wen

Peter C. Wen, Project Manager
Generic Issues, Environmental, Financial
and Rulemaking Branch
Division of Regulatory Improvement Programs
Office of Nuclear Reactor Regulation

Project No. 689
Attachment: NRC Comments on Draft NEI 01-01
cc: See next page

NRC Comments on Draft NEI 01-01, "Guideline on Licensing Digital Upgrades"

General comments

The document captures most of the items of concern regarding plant changes involving digital systems. However, in certain areas, a few more examples of changes that are permissible and not permissible under 50.59 would clarify the intent of the guideline.

Specific Comments (Referencing NEI 01-01 section number)

1. Section 1.1, "Background." First paragraph, last sentence, suggest changing the concluding phrase to read, "...require ~~special~~ **prior** Nuclear Regulatory Commission (NRC) ~~scrutiny~~ **approval**."

2. Section 2.0, "Definitions and Terminology." Definition for "safety related" states, "see safety systems." This should be "see safety systems, structures, and components."

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).

3. Section 3.1.1, "Digital Issues in the Upgrade Process." The second paragraph implies that a Defense-in-Depth and Diversity (D-i-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-i-D&D analysis.

4. Section 3.1.2, "Failure Analysis." In the introductory paragraph, reference to SRP Chapter 7 and particularly to BTP-14 could be added.

The fourth paragraph discusses "dependability" where "reliability" may be more appropriate.

In the sixth paragraph, the last sentence could be revised, to distinguish the failure analysis in the design process with that in the 50.59 process, to read, "Here **in the 50.59 process**, it is important to maintain focus"

5. Section 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.

6. Section 3.2.5, "Operation, Maintenance, and Support." Last paragraph could include a reference to BTP-17.

7. Section 4.2.1, "Technical Evaluations." The second paragraph discusses D-i-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-i-D&D analysis would be necessary.

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.

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."

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."

8. Section 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.

9. Section 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 I&C system malfunctions. Diagnostics identify failures, but to reduce the likelihood of system malfunctions, immediate analysis for root cause and subsequent corrective actions need be undertaken to return the equipment and system to service.

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 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."

10. Section 4.3.6, "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."

The discussion in paragraphs 7 and 8 of NEI 01-01, Section 4.3.6, on credible failure analysis and D-i-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.

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.

11. Section 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.

12. Section 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).

13. Suggest adding Section 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.

The specific regulations and guidance are as follows:

1. Regulations - 10 CFR 50.55a (h) was revised in 1999 to refer to IEEE Std. 603-1991. This standard has in Section 5.9 requirements addressing "Control of Access" viz., "The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof."
2. In the SRP Chapter 7, Section 7.1-C, additional guidance on the IEEE Std. 603 requirement on access control is provided - "Review of digital computer-based systems should consider controls over electronic access to safety system software and data. Controls should address access via network connections, or via maintenance equipment."
3. In SRP Chapter 7, Section 7.9, Data Communication Systems (DCS), Paragraph III, Review Procedures on control of access states: "The review should confirm that the DCS does not present an electronic path by which unauthorized personnel can change plant software or display erroneous plant status information to the operators. If computers or equipment outside of the control of the plant staff may be connected to the DCS (e.g., connections to remote data displays off-site) the connections should be through gateways that prevent unauthorized transactions originating from off-site. Such

connections should be one-way communication paths as discussed in Annex G of IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations." "

4. In SRP Chapter 7, Appendix 7-A, Branch Technical Position 14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," has guidance on security issues both in the planning and implementation of the design of software and in the software that is installed in the I&C systems. Security aspects for planning is defined as "The methods used to protect the information created by or reviewed by the organization covered by the planning document from inadvertent or malicious alteration," and for software as "The ability to prevent unauthorized, undesired, and unsafe intrusions. Security is a safety concern insofar as such intrusions can affect the safety-related functions of the software."

Additional guidance on security is provided in BTP-14, Section B where planning and software review guidance are provided.

August 23, 2001

Ms. Lynnette Hendricks
Director, Licensing
Nuclear Energy Institute
Suite 400
1776 I Street, NW
Washington, DC 20006-3708

SUBJECT: NRC COMMENTS ON DRAFT NEI 01-01 (EPRI TR-102348-R1 DRAFT E,
JULY 2001)

Dear Ms. Hendricks:

By letter dated July 24, 2001, the Nuclear Energy Institute (NEI) submitted a draft NEI 01-01 (EPRI TR-102348-R1 Draft E, July 2001), "Guideline on Licensing Digital Upgrades," for staff review. This document and NEI's plan to update guidelines for licensing digital system upgrades were discussed during a public meeting on April 26, 2001. The staff has completed a preliminary review, and is providing the attached comments to be discussed in our meeting scheduled for September 11, 2001.

If you have any questions please contact me at 301-415-2832.

Sincerely,

/RA/Signed by P. Wen

Peter C. Wen, Project Manager
Generic Issues, Environmental, Financial
and Rulemaking Branch
Division of Regulatory Improvement Programs
Office of Nuclear Reactor Regulation

Project No. 689
Attachment: NRC Comments on Draft NEI 01-01
cc: See next page

Distribution:

ADAMS-PUBLIC RGEB R/F
DMatthews/FGillespie CCarpenter S West EMckenna
JStrosnider/FELtawila JCalvo EMarinos MChiramal
JBongarra CDoutt KMortensen

Accession#ML01239021 NRR-106

DOCUMENT NAME: G:\pxw\Digital I&C Comments Ltr.wpd

OFFICE	RGEB	SPSB	RGEB	EEIB
NAME	PWen	CDoutt	EMckenna	MChiramal
DATE	08/22/01	08/22/01	08/22/01	08/22/01
OFFICE	SC:EEIB	BC:EEIB	SC:RGEB	
NAME	EMarinos	JCalvo	SWest	
DATE	08/22/01	08/22/01	08/23/01	

OFFICIAL RECORD COPY

cc:

Nuclear Energy Institute

Project No. 689

Ms. Lynnette Hendricks
Director, Licensing
Nuclear Energy Institute
Suite 400
1776 I Street, NW
Washington, DC 20006-3708

Mr. Fred Madden
Project Manager
Nuclear Energy Institute
Suite 400
1776 I Street, NW
Washington, DC 20006-3708

Mr. Ray Torok
Project Manager
Electric Power Research Institute
P.O. Box 10412
Palo Alto, CA 94303-0813