PUBLIC SUBMISSION

As of: 7/24/17 11:35 AM
Received: July 17, 2017
Status: Pending_Post
Tracking No. 1k1-8xkk-lzwl
Comments Due: August 02, 2017
Submission Type: Web

Docket: NRC-2017-0154
Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems

Comment On: NRC-2017-0154-0001
Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems; Request for Comment on Draft Regulatory Issue Summary and Public Meeting

Document: NRC-2017-0154-DRAFT-0002
Comment on FR Doc # 2017-13918

Submitter Information

7/3/2017
82FR 30913
1

Name: Kenneth Scarola
Address:
3672 Pine Tree Ln
Murrysville, 15668
Email: KenScarola@NuclearAutomation.com

General Comment

Attached are my comments on the Draft RIS 2017-XX. Thank you for considering my comments.

Attachments

Comments on Draft 50.59 RIS

SUNSI Review Complete
Template = ADM – 013
E-RIDS= ADM-03
Add= B. Harris (BKH4)
J. Drake (JXD23)

Comments on "NRC DRAFT REGULATORY ISSUE SUMMARY 2017-XX SUPPLEMENT TO RIS 2002-22"

1. The RIS describes the potential for new malfunctions due to common software in redundant trains of safety systems. But it also needs to emphasize the potential for new malfunctions due to non-safety control systems with shared resources (both hardware and software). This is important, because the use of shared resources can reduce the diversity among control functions that is credited in the FSAR, thereby increasing the potential for unanalyzed transients that can be caused by these malfunctions; this potential for unanalyzed transients is overlooked too often.

   This comment is reflected in the following recommended changes:

   Page 3, paragraph 3, second sentence:

   > For digital I&C modifications, particularly those that introduce identical software into redundant trains, divisions, or channels within a system, and those that introduce new shared resources, hardware or software, among multiple non-safety control functions (e.g., controllers, communication networks or video display units), there may be a potential for an increase in the likelihood of malfunctions, including common cause failure...

   In the last phrase of the sentence above "marginal" was deleted, because no basis is provided for this "marginal increase" conclusion. A "marginal increase" conclusion should not be assumed by either the Staff or the licensee, because digital systems typically have more shared resources than their analog predecessor, and a shared hardware or software resource may result in more than a "marginal" increase in the likelihood of malfunctions, if the built-in defensive measures against those malfunctions are not adequate.

   Attachment, page 6, Item 2:

   > ... or diversity credited in the FSAR (including a reduction in diversity due to shared hardware or software resources among non-safety control functions), and ...

   Attachment, page 10, first paragraph:

   > If these individual SSCs are combined with (e.g., controlled by a common digital component), employ the same software in separate digital devices, or coupled to each other....

2. A failure likelihood assessment and a conclusion of no more than a minimal increase in failure likelihood is required for 10CFR50.59 (i) and (ii). But saying that low likelihood of failure is "the key element" to support the conclusions for (v) and (vi), is not correct. This is because for (v) and (vi) failure likelihood is irrelevant, if the accident/malfunction is previously evaluated.

   To determine if the malfunction is previously evaluated, a failure modes and effects analysis (FMEA) is required, to identify the malfunctions that result due to a single random hardware failure (i.e., any single point vulnerabilities), and the malfunctions that result due to a digital design defect. Malfunctions due to single point vulnerabilities can only be precluded through design attributes, not a likelihood assessment. Similarly, as discussed in the Attachment,

Section 3, Item 3, malfunctions due to a design defect can only be precluded through the design attributes of diversity or 100% testability. Therefore, performing a deterministic FMEA is much more important for (v) and (vi) than conducting a qualitative failure likelihood assessment. The need to perform this deterministic FMEA is greatly overshadowed by the RIS guidance to perform a qualitative likelihood assessment.

The Attachment, Section 3, Item 3, defines the scope of digital modifications for which the "qualitative assessment framework described herein may be used ... Digital I&C upgrades to facility components and systems, where a malfunction due to a design defect is precluded through simplicity (as demonstrated through 100 percent testing) or adequate internal or external diversity, or where a design defect is assumed, postulated to be triggered and demonstrated to result in no new malfunction or a malfunction that is bounded by previous FSAR analysis". As discussed above, a qualitative likelihood assessment cannot be a substitute for these deterministic design attributes or deterministic malfunction result analysis. Therefore, based on the scope of digital upgrades for which a qualitative assessment may be used, as defined in this RIS, the purpose of the likelihood assessment for 10CFR50.59 (vi) is only to determine if "best estimate" methods can be used, or "design basis" methods must be used, when demonstrating that the plant level end-result of a new malfunction is bounded by previous FSAR analysis. Based on the scope of digital upgrades for which a qualitative assessment may be used, as defined in this RIS, the likelihood assessment cannot be used to determine if an analysis of a new malfunction is necessary. That analysis is necessary for most digital upgrades; it is precluded only if there are no new malfunctions based on design attributes of diversity or 100% testability, and by an FMEA, as commented above. Therefore, the correlation of likelihood to (vi) should be clarified to only apply to the method used to analyze postulated malfunctions, not to the need to analyze those potential malfunctions.

To address the comments above, the following paragraphs should be changed as follows:

Attachment, Section 2.1, paragraph 3:

> A qualitative assessment that finds there is reasonable assurance that a digital modification will exhibit a low likelihood of failure supports the following conclusions that are necessary to a 50.59 evaluation:
> □□The activity does not result in more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the UFSAR (10 CFR 50.59(c)(2)(i)).
> □□The activity does not result in more than a minimal increase in the likelihood of occurrence of a malfunction of a structure, system, or component (SSC) important to safety previously evaluated in the UFSAR (10 CFR 50.59(c)(2)(ii)).
>
> A qualitative assessment that finds there is reasonable assurance that a digital modification will exhibit a low likelihood of failure <u>cannot</u> be used to support the following conclusion that is necessary to a 50.59 evaluation:
> □□The activity does not create a possibility for an accident of a different type than any previously evaluated in the UFSAR (10 CFR 50.59(c)(2)(v)). This is because single random hardware failures cannot be precluded through a qualitative likelihood assessment, and for the scope of systems for which the qualitative assessment framework described herein may be used (see the Attachment, Section 3, Item 3) a design defect can be precluded only through the deterministic design attributes of diversity or 100% testability, not through a qualitative likelihood assessment. Therefore,

a 10 CFR 50.59(c)(2)(v) conclusion can be reached only by determining, through an FMEA for both single random hardware failures and design defects (if not precluded through the deterministic design attributes of diversity or 100% testability), that there are no new malfunctions that can create an accident or that any resulting accident has been previously evaluated. Therefore, a qualitative assessment of failure likelihood is not pertinent to 10 CFR 50.59(c)(2)(v).

A qualitative assessment that finds there is reasonable assurance that a digital modification will exhibit a low likelihood of failure can be used to support the following conclusion that is necessary to a 50.59 evaluation:□□The activity does not create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the UFSAR (10 CFR 50.59(c)(2)(vi)). However, single random hardware failures cannot be precluded through a qualitative likelihood assessment, and for the scope of digital upgrades for which the qualitative assessment framework described herein may be used (see the Attachment, Section 3, Item 3), a design defect can be precluded only through the deterministic design attributes of diversity or 100% testability, not through a qualitative likelihood assessment. Therefore, for 10 CFR 50.59(c)(2)(vi) the likelihood assessment is used only to determine if "best estimate" methods may be used, or "design basis" methods must be used, for the analysis of any new malfunctions when demonstrating that the plant level end-result of a new malfunction is bounded by previous FSAR analysis. This 10 CFR 50.59(c)(2)(vi) conclusion can also be reached by determining through an FMEA and an assessment of deterministic design attributes of diversity or 100% testability (which preclude the need to consider a design defect) that there are no new malfunctions. However, as stated in the Attachment, Section 3, Item 3, if these deterministic design attributes of diversity or 100% testability do not exist, a design defect must be "assumed, [and] postulated to be triggered". Therefore, an analysis of the new malfunction would be required using the analysis method determined by the qualitative likelihood assessment.

Attachment, page 2, paragraph 3, last sentence:

This final determination of the likelihood of failure is the key element of the evaluation of criteria 10 CFR 50.59(c)(2)(i) and (ii), and it can be used to establish the malfunction results analysis method for (vi).

3. The RIS has an internal conflict regarding the use of a qualitative likelihood assessment or deterministic design attributes and analysis in reaching 10CFR50.59 conclusions.

   In many sections, the RIS states that a qualitative likelihood assessment can be used to conclude that there are no new malfunctions. But then the Attachment, Section 3, Item 3, limits the scope of upgrades that can employ this qualitative assessment to those where a design defect is "assumed, postulated to be triggered and demonstrated to result in no new malfunction or a malfunction that is bounded by previous FSAR analysis". Assuming a design defect exists and is triggered, precludes the need for a qualitative assessment to determine the likelihood that a design defect exists or the likelihood that a design defect is triggered.

   The Attachment, Section 3, Item 3 is consistent with current staff policy in BTP 7-19 Section 1.9 which says that further consideration of CCF can be eliminated only through "design attributes" of internal diversity or 100% testability. The other sections of this RIS that allow a qualitative likelihood assessment to reach a conclusion that "failures due to software,

including common cause failures" require no further consideration, contradicts that current Staff policy. Design attributes are deterministic features of a system for which a likelihood assessment is not pertinent. A RIS should not contradict current Staff policy.

In addition, since this RIS contradicts current staff policy, it establishes criterion for operating plants that is different than for new plants which must comply with BTP 7-19 Section 1.9. This different criterion for new and operating plants, contradicts the direction of the Commissioners in Staff Requirements Memorandum (SRM) to SECY-15-0106, which states "The same requirements should apply to operating and new reactors."

A RIS that confuses the industry, conflicts with current Staff policy and conflicts with Commissioners direction, will not help promote digital upgrades.

To address the comments above, the following paragraphs should be changed as follows:

Attachment, page 5, bullet 1:

> The qualitative assessment "determines if there is reasonable assurance that the likelihood of failure due to software is..."sufficiently low" [which] means much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other common cause failures that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors). However, for the scope of digital upgrades for which the qualitative assessment framework described herein may be used (see the Attachment, Section 3, Item 3), a design defect can be precluded only through the deterministic design attributes of diversity or 100% testability, not through a qualitative likelihood assessment. Therefore, for digital upgrades, where these deterministic design attributes do not exist, failures due to software, including common cause failures, should be considered further in the 10 CFR 50.59 evaluation. If there is reasonable assurance that the likelihood of failure due to software is significantly lower than failures currently assumed in the FSAR, then the resulting malfunctions may be analyzed using "best estimate" methods to determine if the plant level end-result is bounded by previous FSAR malfunctions (see Step 3). An upgrade with a bounded malfunction result would not require prior NRC review on the basis of software common cause failures.

Attachment, page 5, Step 3:

> Only for possible malfunctions due to a single random failure, or due to a design defect where there is not diversity or 100% testability (see Attachment, Section 3, Item 3), determine whether the malfunction has a different result. Employ "best estimate" or "design basis" analysis methods depending on the qualitative likelihood assessment in Step 2. [This section should explain the key differences between "best estimate" methods and "design basis" methods.]

> Attachment, page 6, paragraph 4, Item c:can be shown to have diversity or 100% testability, or capable of demonstration that the resulting replacement or upgrade design can tolerate the postulated triggering of a design defect.

4. Most digital upgrades will not have diversity or 100% testability. Therefore, for most digital upgrades, in accordance with the Attachment, Section 3, Item 3, a design defect must be analyzed to reach a conclusion for 10 CFR 50.59 (vi). Therefore, this RIS needs to give

additional guidance for that analysis, including (1) when 'best estimate' methods can be used, (2) what distinguishes 'best estimate' methods from 'design basis' methods, including what concurrent events must be considered and what it means to be bounded. If 'best estimate' methods are not clearly explained in this RIS, for most digital upgrades it will be too difficult to demonstrate acceptable conclusions for 10 CFR 50.59 (vi); this will not promote digital upgrades.

High level guidance for "best estimate" methods should be added to Section 2.1, bullet 4, as recommended in Comment 2, above. Detailed guidance should be added to the Attachment, Page 5, Step 3, as recommended in Comment 3, above.

5. There is an internal conflict in the RIS regarding what malfunctions need to be considered for 10 CFR 50.59 (v) and (vi).

   Several sections state the possible malfunctions to be considered "are limited to those that are as likely to happen as those described in the UFSAR". Then there are statements (sometimes in the same paragraph) that say to preclude consideration the likelihood must be "comparable to other CCF that are not considered in the UFSAR". The latter is a significantly more conservative likelihood threshold than the former. The first statement should be eliminated, because (in accordance with BTP 7-19, as discussed above) CCFs due to a design defect require consideration unless a design defect is precluded through deterministic design attributes of diversity or 100% testability, which makes the CCF likelihood "comparable to other CCFs that are not considered in the UFSAR".

   This conflict within the RIS is also evident in the definition of "sufficiently low" on page 5 paragraph 1 of the Attachment "[which] means much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other common cause failures that are not considered in the UFSAR". This definition is consistent with the statement which says to not require further consideration the malfunction likelihood must be "comparable to other CCF that are not considered in the UFSAR". But the statements that say to require further consideration the malfunction must be "as likely as the malfunctions already assumed in the UFSAR" contradict this definition of "sufficiently low".

   Several sections of the RIS imply that low likelihood CCFs do not require consideration for (v), because the only malfunctions that must be considered are those that are "as likely as the malfunctions considered in the UFSAR". But accidents evaluated in the UFSAR include LOOP, ATWS, LOAF and SBO, which are the result of low likelihood CCFs; this encompasses CCFs that may be due to a design defect. Again, this presents a conflict within the RIS, because low likelihood CCFs are considered in the UFSAR; therefore, they do need to be considered in the response to (v).

   To address the comments above, the following paragraphs should be changed as follows:

   Attachment, page 3, first paragraph:

   > Possible accidents of a different type are limited to those that are as likely to happen as those previously evaluated in the UFSAR; and, based on an FMEA of equipment that can initiate events that lead to accidents that are of different type, including postulated triggering of a design defect (See Attachment, Section 3, Item 3), the activity does not create an accident of a different type that is as likely to happen as those previously evaluated in the UFSAR.

Attachment, page 3, paragraph 4

> 10 CFR 50.59(c)(2)(vi): The activity does not create a possibility for a malfunction of an SSC important to safety with a different result because possible malfunctions with a different result exclude those that are comparable to other CCF that are not considered in the UFSAR (e.g., design flaws in analog equipment, maintenance errors, calibration errors). [Note: This likelihood threshold is not interchangeable with that for "credible"/"not credible," which has a threshold of "as likely as" (i.e., not "*much lower than*") malfunctions already assumed in the UFSAR. Due to the potential for complexity, including shared hardware and software resources, a design flaw in digital equipment is considered to have higher likelihood than a design flaw in analog equipment, unless there is diversity or 100% testability (See Attachment, Section 3, Item 3).]

Attachment, page 3, paragraph 5:

> For activities that introduce a failure mode (e.g., CCF) that does not meet the above thresholds and cannot be shown to be previously evaluated in the UFSAR, the CCF would need to become part of the design basis; a license amendment or other approved change process would be required.

Attachment, Section 2.2, paragraph 1:

> The 10 CFR 50.59 evaluation of criterion (c)(2)(vi) can be viewed as a three-step process that stems from the possible malfunctions with a different result that are more likely to happen than those that are not described in the UFSAR (e.g., design flaws in analog equipment, maintenance errors, calibration errors)."

Attachment, Section 2.2, Step 2:

> ...If there is reasonable assurance that the likelihood of potential failures is comparable to those that are not described in the UFSAR, then such failures do not merit further consideration...with a different result.) However, single random hardware failures cannot be precluded through a qualitative likelihood assessment, and for the scope of digital upgrades for which the qualitative assessment framework described herein may be used (see the Attachment, Section 3, Item 3), a design defect can be precluded only through the deterministic design attributes of diversity or 100% testability, not through a qualitative likelihood assessment. Therefore, for the scope of digital upgrades for which the qualitative assessment framework described herein may be used, for 10 CFR 50.59(c)(2)(vi) the likelihood assessment is used only to determine if "best estimate" methods may be used, or "design basis" methods must be used, for the analysis of any new malfunctions when demonstrating that the plant level end-result of a new malfunction is bounded by previous FSAR analysis.

Attachment, page 4, Step 1, bullet 8:

> "for the purpose of the 10 CFR 50.59 evaluation, "credible" malfunctions are defined as those that are more likely than the malfunctions not assumed in the UFSAR."

Attachment, page 4, Step 2, Paragraph 1:

Perform a qualitative assessment of the likelihood of occurrence of possible malfunctions identified in Step 1. The possible malfunctions with a different result are limited to those that are more likely to happen than those that are not described in the UFSAR.

6. It appears the Staff is trying to exclude RPS and ESF from the scope of digital upgrades that can employ the qualitative assessment method described in this RIS. However, on Page 5, Item b second paragraph the words "other than" mean that integration for RPS and ESF is acceptable and is therefore within the scope of systems that can employ the qualitative assessment method described in this RIS. To avoid this conflict, Item (c) should be added to this section:

   c) Do not affect reactor trip or engineered safety feature functions.

7. It should be clearly stated that an emergency load sequencer is considered part of the ESF actuation system because an emergency load sequencer can block ESF actuation. This is important to maintain plant safety, because emergency load sequencers can be very complex digital devices with many inputs, outputs and internal states. Therefore, without adequate defensive measures against a CCF, they have a likelihood of a malfunction due to a design defect that is not "much lower than the likelihood of failures that are considered in the UFSAR" and not "comparable to other common cause failures that are not considered in the UFSAR".

   To address the comment above, the following paragraph should be changed as follows:

   Page 6, paragraph 4:

   ... that are not a part of the actuation logic portion of RPS and ESF actuation systems, and not a part of the emergency load sequencer which directly affects ESF actuation, such as changes to ...

8. Figure 1 - ...Flowchart

   The Yes/No outputs of the first decision block are reversed (i.e., if a proposed change does not have the characteristics described in the attachment to this RIS, then the change cannot be implemented under 10CFR50.59).