NRR-DMPSPEm Resource

From: Ken Scarola <KenScarola@NuclearAutomation.com>
Sent: Sunday, February 04, 2018 10:32 AM
To: Govan, Tekia
Cc: Rahn, David; Carte, Norbert; Chernoff, Harold
Subject: [External_Sender] Recommendations for NRC DRAFT REGULATORY ISSUE SUMMARY 2002-22, Supplement 1
Attachments: Recommendations for RIS 2002-22, SUPPLEMENT 1.docx

Tekia,
Thank you for responding.

I know that the public comment period for this RIS closed August 16, 2017. I provided many written comments prior to that date; those comments were discussed with the Staff at the 4/20/2017 and 10/25/2017 public meetings. Since those meetings, the draft RIS has changed significantly; most of the changes are unrelated to the comments provide by industry during the public comment period and at those meetings. At the 1/26/2018 meeting, several industry representatives expressed concern that the significance of these most recent NRC initiated changes warrants an additional period for public comments; I strongly agree with this consensus industry position. An additional public comment period would also be consistent with the Commissioner's direction in SRM SECY-16-0070 "In resolving these complex issues, the staff should seek frequent stakeholder interactions."

Even if the Staff does not reopen the RIS for public comments, as a minimum I would hope that the Staff would use my input (attached) to ensure the points I have identified are addressed with simplicity and clarity in the new RIS. The lack of clarity on these points is the underlying source of industry errors and inconsistencies in executing 10CFR50.59 screens and evaluations, which were identified by the Staff when this effort was started in November 2013 (see ML13298A787 Summary of Concerns with NEI 01-01). As I noted in my original email, that needed clarity can be achieved in two pages (attached); the current draft RIS of 36 pages is not necessary. Even more important is that the complexity of a 36 page RIS is likely to result in further delays in digital upgrades. Of course, I would welcome the Staff adopting my positions on these points; but that is significantly less important to me than the need for the RIS to address these points with simplicity and clarity, even if the Staff's positions on these points are different than mine.

Ken

_____
Ken Scarola
Nuclear Automation Engineering, LLC
3672 Pine Tree Ln.
Murrysville, PA 15668
412-612-1192

From: Govan, Tekia [mailto:Tekia.Govan@nrc.gov]
Sent: Friday, February 2, 2018 10:35 AM
To: 'KenScarola@NuclearAutomation.com' <KenScarola@NuclearAutomation.com>
Cc: Rahn, David <David.Rahn@nrc.gov>; Carte, Norbert <Norbert.Carte@nrc.gov>; Chernoff, Harold <Harold.Chernoff@nrc.gov>
Subject: RE: RE: Who's in Charge

Good morning Mr. Scarola:

My name is Tekia Govan and I am the project manager and point of contact for the Regulatory Issue Summary (RIS) 2002-22, Supplement 1, “Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Controls Systems.” Harold Chernoff is my Branch Chief in the ROP Support and Generic Communications Branch.

We are in receipt of your email with the attachment of suggested changes to the RIS. The NRC published a notice of opportunity for public comment on this RIS in the *Federal Register* on July 3, 2017 (82 FR 30913). The public comment period for this RIS closed on August 16, 2017. As with all public interactions related to NRC documents that have been noticed for public comment, your email and attachment will be captured in the NRC’s Agencywide Documents Access and Management System and made publically available. Should the NRC decide to open an additional comment period on the RIS, the public will be notified through the issuance of a federal register notice.

Should you have any additional questions or concerns regarding the process of this RIS, please contact me directly at 301-415-6197 or tekia.govan@nrc.gov.

Thanks
Tekia

From: Ken Scarola [mailto:KenScarola@NuclearAutomation.com]
Sent: Tuesday, January 30, 2018 4:14 PM
To: Chernoff, Harold <Harold.Chernoff@nrc.gov>
Cc: Carte, Norbert <Norbert.Carte@nrc.gov>; Rahn, David <David.Rahn@nrc.gov>
Subject: [External_Sender] RE: Who's in Charge

Dear Mr. Chernoff,
I recall hearing your name during the draft RIS meeting last Friday. I was on the phone; I had several comments.

One common industry comment that stood out for me was that the length of the draft RIS is going to scare industry away from digital upgrades. In an attempt to address that, I created the file attached. This 2 page file identifies the key points that need to be included in the RIS (1) to clarify previous industry inconsistencies when applying NEI 96-07 and NEI 01-01 (i.e., the inconsistencies that were identified in 2012, when we started this effort), and (2) to clarify the methods available to industry to reach a favorable 59.59 conclusion and thereby facilitate more digital upgrades. Anything more than these two pages is unnecessary and likely to have a detrimental effect. The Staff can certainly provide more background and explanation, but that could be through meetings, workshops and future guidance documents.

I hope you will consider my input. If you have questions, please contact me.

Ken

_____

Ken Scarola
Nuclear Automation Engineering, LLC
3672 Pine Tree Ln.
Murrysville, PA 15668
412-612-1192

From: Carte, Norbert [mailto:Norbert.Carte@nrc.gov]
Sent: Tuesday, January 30, 2018 2:52 PM
To: Ken Scarola <KenScarola@NuclearAutomation.com>
Cc: Chernoff, Harold <Harold.Chernoff@nrc.gov>
Subject: RE: Who's in Charge

See cc.

From: Ken Scarola [mailto:KenScarola@NuclearAutomation.com]
Sent: Tuesday, January 30, 2018 2:47 PM
To: Carte, Norbert <Norbert.Carte@nrc.gov>
Subject: [External_Sender] Who's in Charge

Norbert,
Can you tell me who is leading the RIS effort now and give me his contact information. I'd like to give him my recommendations for a two page RIS. I believe that's all we need and anything more will just scare licensees away.

Ken

_____

Ken Scarola
Nuclear Automation Engineering, LLC
3672 Pine Tree Ln.
Murrysville, PA 15668
412-612-1192

Hearing Identifier: NRR_DMPS
Email Number: 152

Mail Envelope Properties (002301d39dcd$5af839b0$10e8ad10$)

Subject: [External_Sender] Recommendations for NRC DRAFT REGULATORY ISSUE SUMMARY 2002-22, Supplement 1
Sent Date: 2/4/2018 10:32:19 AM
Received Date: 2/4/2018 10:32:43 AM
From: Ken Scarola

Created By: KenScarola@NuclearAutomation.com

Recipients:
"Rahn, David" <David.Rahn@nrc.gov>
Tracking Status: None
"Carte, Norbert" <Norbert.Carte@nrc.gov>
Tracking Status: None
"Chernoff, Harold" <Harold.Chernoff@nrc.gov>
Tracking Status: None
"Govan, Tekia" <Tekia.Govan@nrc.gov>
Tracking Status: None

Post Office: NuclearAutomation.com

Files	**Size**	**Date & Time**
MESSAGE	6353	2/4/2018 10:32:43 AM
Recommendations for RIS 2002-22, SUPPLEMENT 1.docx	19304	

Options
Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

Recommendations for NRC DRAFT REGULATORY ISSUE SUMMARY 2017-XX SUPPLEMENT TO RIS 2002-22

Formatted: Top: 0.7", Bottom: 0.7"

1. Failure/malfunction means not performing the design function at all, or performing the design function incorrectly such as spurious actuation or erroneous control. The potential for performing a design function incorrectly has not been adequately considered in previous screenings and evaluations.
2. Digital technology lends itself to integration that has the potential to result in multiple design function (or SSC) malfunctions, that can result in unanalyzed plant transients. This potential exists when (1) a digital upgrade shares a common hardware resources (e.g., controller, power supply, measurement channel, communication interface) among two or more design functions (or SSCs) whose failures were previously analyzed separately, or (2) when a common digital design is employed for two or more design functions (or SSCs) that remain separate with no shared resources. These potential sources of common cause failure are very important bases for screening-in a digital upgrade. These are not the only screening criteria, but these are specifically noted because digital upgrades with these attributes for potential CCF have been incorrectly screened out.
3. 10 CFR 50.59(c)(2)(i) and (ii) – To answer these questions, the evaluation documents the qualitative basis for reaching a conclusion regarding the likelihood of a malfunction in the digital upgrade compared to the likelihood of a malfunction in the predecessor. For example, a comparable qualitative likelihood conclusion can be reached for a digital upgrade that follows industry standards (safety or non-safety standards, as applicable) for high reliability and dependability, and has acceptable operating history in equivalent applications.
4. 10 CFR 50.59(c)(2)(v) and (vi) – To answer these questions, the evaluation documents the deterministic or qualitative basis (as explained below) for reaching a conclusion regarding the possibility of a malfunction that can lead to a different end-result than previously analyzed. This requires the following considerations:
   a. End-result refers to the plant level critical safety function(s) that may be threatened by the malfunction. An end-result is considered bounded by previous analysis (i.e., not different than previous analysis), if the margin to the analytical limit of the critical safety function(s) is not eroded or insignificantly eroded compared to a similar event previously analyzed. A plant level analysis is not required for a digital malfunction that does not cause a different system level result, as determined through a deterministic FMEA.
   b. A malfunction in a safety or non-safety event initiator (e.g., pressurizer pressure/level control) is evaluated with no other concurrent AOO or PA. A malfunction in a safety system credited for event mitigation, is evaluated with a concurrent AOO/PA(s) for which it is credited. For this evaluation LOOP is an AOO, but LOOP does not require consideration concurrent with other AOO/PAs; the basis for this is that a malfunction with concurrent LOOP and concurrent AOO/PA is sufficiently unlikely to require no further consideration.
   c. Hardware failures are random and expected during the life of the plant. Therefore, when the system level results are different, a malfunction due to the failure of a shared hardware resource (as described in Item 2, above) is analyzed at the plant level as a design basis event, using conservative deterministic analysis methods. These methods employ worst case assumptions regarding plant state and equipment performance, and credit for event mitigation using only

existing safety equipment. Manual actions using existing safety equipment can be credited when there is margin between the time required to take the action (as determined through an HFE analysis) and the time available to take the action (as determined through a transient analysis). To determine if the plant level end-result is bounded (or not), the end-result is compared to the end-result of corresponding previously analyzed AOOs, not PAs, because random hardware failures are expected during the life of the plant, PAs are not.

d. When the system level results are different, a malfunction due to a design defect is analyzed at the plant level as either a design basis event, a beyond design basis event, or not analyzed at all (i.e., requires no further consideration), depending on its likelihood, as follows:
   i. For RT and ESF, including both automatic and manual functions credited for accident mitigation as well as instrumentation and plant components that supports those functions, a malfunction due to a design defect requires no further consideration if (1) the design is simple, as demonstrated by testing that encompasses all internal and external state combinations (i.e., considered 100% testable) or (2) the design has internal diversity. The NRC is working with industry to expand this list of deterministic preventive measures. Until additional preventive measures are endorsed, they cannot be credited unless specifically approved by NRC through an LAR for the digital upgrade. For other safety or non-safety functions that are documented (e.g. in the PRA) to be less important to plant safety than the RPS and ESF functions described above, a basis for crediting other preventive measures (e.g., non-concurrent triggers) can be documented in the evaluation.
   ii. A malfunction due to a design defect can be analyzed as a beyond design basis event (i.e., not expected during the life of the plant), if the likelihood of the malfunction is significantly less than that of a single random hardware failure, as determined through a documented qualitative assessment. For example, a significantly less likely conclusion can be reached for a digital upgrade that follows industry standards (safety or non-safety standards, as applicable) for a high quality design process, and has acceptable operating history in equivalent applications. A beyond design basis analysis allows “best estimate” methods, which employ realistic assumptions regarding plant state and equipment performance, and credit for event mitigation using safety or non-safety plant equipment with suitable quality. Manual actions using existing safety or non-safety equipment can be credited when there is margin between the time required to take the action (as determined through an HFE analysis) and the time available to take the action (as determined through a transient analysis). To determine if the plant level end-result is bounded (or not), the end-result is compared to the end-result of corresponding previously analyzed AOOs or PAs, because a malfunction due to a design defect is not expected during the life of the plant.
   iii. A malfunction due to a design defect is analyzed as a design basis event (i.e., expected during the life of the plant), if the likelihood of the malfunction is not significantly less than that of a single random hardware failure, as determined through a documented qualitative assessment. This conclusion would typically be reached when a digital upgrade does not follow industry standards (safety or non-safety standards, as applicable) for a high quality design process, or does not have acceptable operating history in equivalent applications. The plant level analysis method and acceptance criteria are the same as described in Item 4.c, above.