From: Ken Scarola <KenScarola@NuclearAutomation.com>
Sent: Tuesday, February 20, 2018 8:17 PM
To: Rahn, David
Subject: [External_Sender] 2018-02-21 Meeting on RIS 2002-22 Supplement 1
Attachments: Points to be Addressed in RIS 2002-22, SUPPLEMENT 1.docx

Dave,
I sent my comments (attached) to Neil Archambo. I've gotten no feedback. If you've gotten NEI's comments, please send me a copy; I'd like to see what he did with my comments. Also, please send any prepared material that the staff is planning to present. Thank you.

Ken

____

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

From: Ken Scarola [mailto:KenScarola@NuclearAutomation.com]
Sent: Wednesday, February 14, 2018 9:39 PM
To: 'Archambo, Neil G'
Subject: Comments on Draft RIS

Neil,
David Rahn tells me that you are compiling a list of input from industry stakeholders which you will send to the NRC this week, and then present on behalf of industry at the upcoming meeting February 21. Attached are the key points that I believe need to be clearly addressed in this RIS. I will be happy to send you my position on each of these points; but for me it is more important that the points be clearly addressed to end the industry confusion and uncertainty regarding 50.59 evaluations for digital upgrades, than it is to adopt my positions on these points.

Please let me know if you have any questions. Thank you.

Ken

____

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

Hearing Identifier: NRR_DMPS
Email Number: 176

Mail Envelope Properties (003601d3aab1$aa2a0450$fe7e0cf0$)

Subject: [External_Sender] 2018-02-21 Meeting on RIS 2002-22 Supplement 1
Sent Date: 2/20/2018 8:16:54 PM
Received Date: 2/20/2018 8:17:56 PM
From: Ken Scarola

Created By: KenScarola@NuclearAutomation.com

Recipients:
"Rahn, David" <David.Rahn@nrc.gov>
Tracking Status: None

Post Office: NuclearAutomation.com

Files	**Size**	**Date & Time**
MESSAGE	1401	2/20/2018 8:17:56 PM
Points to be Addressed in RIS 2002-22, SUPPLEMENT 1.docx	18755	

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

Recommendations for Points to be Clearly Addressed in NRC DRAFT REGULATORY ISSUE SUMMARY 2017-XX SUPPLEMENT TO RIS 2002-22 Ken Scarola, Nuclear Automation Engineering

Formatted: Top: 0.7", Bottom: 0.7"

1. Failure/malfunction means fail-deenergized, fail as-is, and performing the design function incorrectly, such as spurious actuation or erroneous control.
2. A new malfunction can be caused by (1) failure of a hardware resource shared by two or more design functions or SSCs (e.g., controller, power supply, measurement channel, communication interface), or (2) a defect in a common digital design shared by two or more design functions or SSCs.
3. 10 CFR 50.59(c)(2)(i) and (ii) – These questions can be answered based on a qualitative assessment that compares the likelihood of a malfunction in the digital upgrade to the likelihood of a malfunction in the analog 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) – These questions can be answered based on a deterministic or qualitative assessment. The assessment method considers the following key points:
    a. This is an assessment of the end-result caused by the potential digital malfunction. End-result refers to ….
    b. This assessment determines if the end-result is bounded by previous analysis (i.e., insignificantly different than previous analysis). An end-result is considered bounded, if ...
    c. A malfunction in a safety or non-safety event initiator (e.g., pressure control, rod 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.
    d. A malfunction due to the failure of a shared hardware resource is analyzed at the plant level as a design basis event, using conservative deterministic analysis methods. Clarify:
        i. Assumptions regarding initial plant state and equipment performance
        ii. What equipment can be credited for event mitigation
        iii. What manual actions can be credited
        iv. What previously analyzed events can be used to determine if the event is bounded
    e. 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.
        ii. For other safety or non-safety functions that are less important to plant safety than RT and ESF functions, other preventive measures can be credited (e.g., non-concurrent triggers) to reach a conclusion that a malfunction due to a design defect requires no further consideration.
        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. For example, this conclusion would 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.
        iv. 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. For example, a significantly less likely conclusion would 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. Clarify:
            a. Assumptions regarding plant state and equipment performance
            b. What equipment can be credited for event mitigation
            c. What manual actions can be credited
            d. What previously analyzed events can be used to determine if the event is bounded
            e. For a mitigator malfunction, LOOP is an AOO, but LOOP does not require consideration concurrent with other AOO/PAs.