NRR-DMPSPEm Resource

From: Ken Scarola <KenScarola@NuclearAutomation.com>
Sent: Tuesday, January 30, 2018 1:13 PM
To: Rahn, David
Subject: [External_Sender] My Recommendation for the RIS
Attachments: Recommendations for NRC RIS 2002-22, SUPPLEMENT 1.docx

Dave,
Attached is my recommendation for what is needed in the RIS; we don't need anything more than this. My recommendation is **two pages**! I'm trying to avoid a long RIS that will just scare licensees away. I'd appreciate your comments.

I want to send this to whomever is in charge of the RIS now. Can you send me his name and email address. 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: 178

Mail Envelope Properties (007501d399f5$ff29e7d0$fd7db770$)

Subject: [External_Sender] My Recommendation for the RIS
Sent Date: 1/30/2018 1:13:13 PM
Received Date: 1/30/2018 1:13:44 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	521	1/30/2018 1:13:44 PM	
Recommendations for NRC RIS 2002-22, SUPPLEMENT 1.docx			18345

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

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, or 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. 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.

c. 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 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 can be documented (e.g., non-concurrent triggers).
    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.b, above.