Gallagher, Carol

From: Larry Grime <lg@acroservices.com>
Sent: Friday, August 18, 2017 1:05 PM
To: Gallagher, Carol
Subject: [External_Sender] Larry Grime Comments onDraft RIS Published with NRC-2017-0154
Attachments: RIS2017-XX_Comments20170818.docx

Carol,

As we discussed my late comments are attached for the subject draft RIS.

Let's make this a great day!

Larry Grime, PE
419.654.9999

7/3/2017
82 FR 30913
13

SUNSI Review Complete
Template = ADM – 013
E-RIDS= ADM-03
Add= B. Harris (bkh4)
J. Drake (JXD24)
A. Gyran (JXG1)

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

Comments

A. Consider providing some big picture I & C digital upgrade perspective.
   1. The issues that need justification are limited to those required in the plant licensing basis. This includes the written requirements in the UFSAR, technical specification, operating license and similar documents, and this includes implied assumptions particularly as related to the reliability of UFSAR-credited components and that added equipment does not adversely affect the plant licensing basis. E.g., When replacing a non-safety-related analog indicator with a digital indicator the only issue may be the potential emi risk from the new instrument. The 10 CFR 50.59 screening and evaluation, if needed, should only discuss software and other hardware issues if they are needed to support the plant licensing basis. It would be helpful if the guidance document make this extremely clear.
   2. Justify software at three levels:
      - Operating system software: This needs to be addressed when it is a new revision or a new system. It is often not practical to get information since the operating system software author is rarely the vendor supplying equipment to the licensee and typically has no obligation to reveal qualification details. Operating experience for non-safety software and commercially dedicated components may be the most reliable justification that the operating system software is acceptable.
      - Application and custom level software: This includes commercially available software applications and custom software written by or for the licensee. For commercial applications the preference is that the software meet standards that are adequate for the application; however, for some applications the vendor will not provide the information. Operating experience may be the most reliable justification that the software is acceptable. It may be necessary to delay implementing major application software use and software revisions until the software version has sufficient operating history. Custom software using code will typically require extensive evaluation.
      - Software configuration: Application level software is typically configured. This can vary from setting a single setpoint to complex control configurations. Application configurations that include logic or similar software features should be evaluated as software changes, otherwise software do not require consideration as a software change. Note that the operating system and application level software may need consideration even if the configuration did not. In some cases it may be necessary to address vendor software that creates the configuration files as well as the configuration file itself.

B. The statement on page seven that there must be an I & C malfunction to have an operational occurrence should be revised. I know of a digital I & C system that changed the status of an output relay in response to an I & C technician's radio that was too close to the equipment. The I & C system did not malfunction but if it had happened with a different system an AOO could have been initiated.

C. In the discussion accompanying the I & C malfunction statement and in other locations, the discussion frequently uses the term 'malfunction frequency.' NEI 96-07 very consciously focused the use of frequency on accident frequencies; frequency was not used to respond to question 2. As stated in the NEI 96-07 quote 'likelihood' is used to describe malfunctions. This document should be revised to be consistent with the use of these terms in NEI 96-07. Rather than focus just on malfunction frequency as the response to questions 1 and 2. I suggest malfunctions be considered in three groupings:

- Discuss malfunctions that initiate accidents with question 1
- Discuss malfunctions that impact accident mitigation with question 2
- Discuss malfunctions that initiate accidents and impact accident mitigation with both questions. When answering question 2 it may be appropriate to discuss the equipment relevance to question 2 and then reference the increased frequency discussion in question 1.

D. The possible malfunctions listed on page 4 of 17 should be clarified.

Non-digital equipment that cause a loss of the ability to perform the design function also should be considered a 'possible' malfunction.

Original components could have different failure modes following a change; consider changing this to read 'failure modes different than the UFSAR assumed failure modes.'

Consider deleting the '...could fail in ways other...' Isn't this just another way to say different failure mode?

E. The last paragraph on page 7 of 17 implies digital designs must avoid creating a failure mode that results in the initiation of a design basis anticipated operational occurrence (AOO) or postulated accident (PA). Failure modes should be evaluated for potential increased AOO or PA frequency increases, failure mode or malfunction likelihood increases, and failures with a different result. I could interpret this statement to require a license amendment to add a digital instrument whose failure could initiate the turbine trip AOO. If so interpreted, this statement is inconsistent with the NRC endorsed criteria for 10 CFR 50.59 evaluations. Consider changing 'demonstrates how the proposed design avoids creating' to 'justify designs that create.'