As of: 3/30/18 6:16 AM
Received: March 29, 2018
Status: Pending_Post
Tracking No. 1k2-92af-n4zn
Comments Due: March 29, 2018
Submission Type: Web

PUBLIC SUBMISSION

Docket: NRC-2018-0044
Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems

Comment On: NRC-2018-0044-0001
Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems

Document: NRC-2018-0044-DRAFT-0007
Comment on FR Doc # 2018-04958

Submitter Information

Name: Ken Scarola
Address:
3672 PINE TREE LN
MURRYSVILLE, 15668
Email: KenScarola@NuclearAutomation.com

General Comment

This is an additional comment that supplements my comments previously submitted.

Attachments

(7)

2018-03-29 NAE Additional Comment on Draft RIS provided for Public Comment

83 FR 11154
3/14/2018

SUNSI Review Complete
Template = ADM – 013
E-RIDS= ADM-03
Add= Tekia Govan (TXG1)

Additional Comment on DRAFT NRC REGULATORY ISSUE SUMMARY 2002-22, SUPPLEMENT 1 ML18051A084, Docket ID NRC-2018-0044 – Ken Scarola, Nuclear Automation Engineering

Comments 1 through 24 were provided in file "2018-03-28 NAE Comments on Draft RIS provided for Public Comment".

25. Table 1 – The following design attributes are defined in this table for consideration in the Qualitative Assessment to reach a "sufficiently low" conclusion:

    - Watchdog timers
    - Segmentation
    - Self-testing and self-diagnostics
    - Fail-safe or known to be the same

    These attributes are limiting measures that may contribute to a conclusion that there is not a malfunction with a different result (50.59 Question vi). They are not preventive measures; therefore, they are completely unrelated and have no effect (positive or negative) on malfunction likelihood (i.e., they have no effect on meeting the "sufficiently low" threshold). For example, a fail-safe design that is more likely to reach that failure state than its analog predecessor yields an unfavorable answer to 50.59 Question ii.

    The RIS should be very clear that "sufficiently low" cannot be reached without deterministic design attributes that address the potential for a CCF from every shared resource, including controllers, digital communications, digital HSI and shared digital designs. Here are some examples of preventive measures for various shared resources:

    1. Shared controller – Two controllers running in parallel whose control outputs are continuously compared, such that output state changes are blocked unless the output states from both controllers agree. This prevents a CCF of all functions controlled by that controller, due to a random hardware failure.
    2. Shared digital data communication network – Communication processors that are separate from function processors. This prevents a CCF of all functions controlled by each controller due to a data storm.
    3. Shared HSI – Two separate operator actions, with two separate communication messages for all control commands. This prevents a CCF of multiple control functions due to single failure or single design defect that could otherwise generate multiple erroneous commands.
    4. Shared digital design – Diversity and configuration at the application level to ensure triggered defects are (1) non-concurrent (among multiple devices) and (2) self-announcing in any device where the defect is triggered. This ensures a design defect can be corrected before it is triggered in multiple devices to become a CCF. At this time, this preventive measure is only applicable to non-safety digital upgrades, because until BTP 7-19 is revised only simplicity and diversity can be credited to prevent a CCF due to a design defect.