Comments from Ken Scarola, Nuclear Automation Engineering, LLC Presented to NRC 2022-10-20

These are the comments I offered during the meeting on SECY-22-0076.

1. I agree with the Staff that operators must always have the ability to manually initiate control of critical safety functions, unless those critical safety functions are passively controlled. I agree with NEI in that Point 4 should not always be required unconditionally.

   There is wisdom in IEEE 603 and 279. IEEE-603 Section 6.2 and IEEE 279 Section 4.17 require that operators have the ability to manually initiate the same protective actions as automatically initiated by the Safety Systems. Therefore, compliant primary Safety Systems give the operators the ability to manually control critical safety functions. This capability has been required (1) to give operators the capability to take pre-emptive actions and (2) to give operators the capability to mitigate the event that we engineers didn't think of [We used to refer to this as the N+1 event.]. But if those manual capabilities are adequate based on the defense-in-depth and diversity assessment of Points 1-3, then there is no need for unconditional backup manual capability as currently written in Point 4.

   Therefore, I recommend:

   - The last phrase in the first sentence of Point 1 "…vulnerabilities to digital CCFs have been adequately identified and addressed" be clarified to add "… including both automatic and manual control of critical safety functions."
   - Point 4 be clarified with a preface that says "If Points 1-3 demonstrate inadequate manual or passive control of critical safety functions …" then continue as written. Also in Point 4, change "actuation" to "initiation", because the intent is to give operators the same IEEE 603/279 capability that they had in the primary Safety Systems.

2. My second comment is the most important. Industry and NRC need to recognize that the cost of nuclear power is our enemy. If nuclear power is going to remain viable there is a need for significant operating staff reduction. To achieve this, non-safety and safety systems must be more automated and have significantly improved human system operator interfaces; unfortunately, both lead to more digital complexity, and increased digital complexity leads to a higher likelihood of a design defect, which can lead to a CCF. This need for increased complexity will outpace our ability to prevent design defects or manage them through risk informed methods. Therefore, diversity may be our only viable solution. So, Staff and industry should focus also on achieving cost effective diversity. For example, Diverse Actuation Systems can be extremely simple, non-safety and cost effective, they are not the enemy; they facilitate more complex primary systems that are necessary to achieve cost effective nuclear power.

There wasn't enough time during the meeting to offer the following comment, but it's equally important:

> This comment pertains to the general basis of this SECY. I understand the intent to give licensees the option of a risk informed approach. That's fine. But a risk informed path is highly subjective with commensurate licensing risk and potential for delay. The Staff should be giving equal emphasis to clarifying Point 1 of the SECY. The industry needs to know what is acceptable to the Staff to demonstrate "that vulnerabilities to digital CCF have been adequately identified and addressed." What I'm saying is that the industry needs guidance on defensive measures, other than diversity, that are acceptable to the Staff. Some licensees don't like prescriptive guidance; I maintain (after too many years in this industry) that when the regulatory guidance is clear, reaching the goal line is always much easier. Licensees can always use alternate methods than those described in the guidance, with recognition that the Staff's review is very likely to be more onerous. My point is that adequate defensive measures to prevent a CCF due to a digital design defect are achievable, just like defensive measures to prevent a CCF due to a seismic event, EMI, electrical fault or security threats have been achievable. None of the defensive measures

defined in regulatory guidance for these CCF threats provide 100% assurance, but they are adequate. Focusing on Point 1 would be much more helpful to industry than risk informing this process.

Ken Scarola

Nuclear Automation Engineering, LLC

KenScarola@NuclearAutomation.com

412-612-1192