Observations Regarding Non-Concurrence NCP-2014-003

SUMMARY

Non-concurrence NCP-2014-003 was submitted by five individuals in the Office of Nuclear Reactor Regulation concerning proposed criteria for data communications in new reactors as found in "Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009" (ADAMS Accession No. ML113191306). The non-concurrence claims that adoption of the proposed criteria for data communications in new reactors would make NRC staff reviews of such systems more troublesome and prolonged given the greater review uncertainty (e.g., without a review plan and associated guidance) should an applicant choose the alternative.

The non-concurrence makes the assumption that the purpose of the proposed criteria for new reactors was to simplify the regulatory decision-making process. This is not correct. Rather, the proposed criteria was developed to address safety issues that pertain to bi-directional data communications between safety and non-safety instrumentation and control (I&C) systems and between redundant safety I&C divisions. Specifically, undesired dependencies and behaviors may be created between systems that must be independent of one another when bi-directional data communications share information and signals between these systems, as evidenced by operating experience and identified during the new reactor licensing reviews. As a preferred means of addressing hazards associated with bi-directional data communications, the proposed criteria are intended to eliminate hazards that are associated with bi-directional data communications. The NRO staff believes that the proposed criteria would accomplish the expectations laid out in the Commission's policy for new reactors with respect to independence by encouraging an inherently safe, simple, and straightforward way to achieve data communication, while at the same time allowing much of the functionality that improves I&C system reliability and plant operation. As a corresponding advantage of addressing the data communication independence issue in this manner, the required design and analyses effort on the part of the applicants, and review effort by the NRC staff, is reduced, thus supporting the industry's and Commission's desire for more efficient and effective, and predictable licensing reviews of digital I&C.

The non-concurrence claims that applicants will likely seek alternatives to the proposed criteria due to pre-design systems and the level of effort to change them. In addition, it claims that NRO staff does not have the guidance to address these alternatives. Experience with licensing reviews of new reactor designs shows that applicants generally proposed or modified designs, during licensing reviews, consistent with the proposed criteria. Additionally, discussions with potential future applicants show that they are already considering designs consistent with the proposed criteria. Recent new reactor reviews have used Digital I&C Interim Staff Guidance (ISG) 04, "Highly Integrated Control Rooms – Communication," Revision 1, as guidance and would continue to do so if an alternative were proposed. NRO staff

understanding is that the same guidance would be used for digital upgrades at operating reactors if bi-directional, interdivisional data communications were proposed.

The non-concurrence states that an aim of the proposed criteria is to eliminate use of engineering judgment. Engineering judgment will be present in both applicant analyses and NRC staff reviews. However, engineering judgment should not be used as a justification to waive necessary analyses and assessments to demonstrate safety, and it should be carefully evaluated in its use. As described in this document, NRO staff often found a lack of the design information and analyses on the part of applicants to justify the safe use of bi-directional, interdivisional data communications. Without sufficient justification in the licensing basis, the staff would not be able to approve such designs.

Finally, the non-concurrence determines that the proposed criteria are not safety-focused and not performance-based. As identified earlier, the premise for the criteria is to address safety issues with data communication independence. NRO staff believes the proposed criteria are fundamentally more safety-focused as they are intended to eliminate the potential hazards of concern in design at the architectural level. In addition, the existing criteria in 10 CFR 50.55a are not performance-based, as found in other regulations, but provide limitations on how designs, analyses, tests, and inspections are performed in order to ensure safety. In comparison with the existing criteria in 10 CFR 50.55a, the proposed criteria for data communication for new reactors are consistent with those criteria.

Non-concurrence NCP-2014-003 recommends that the agency incorporate the independence criteria of IEEE Std. 603-2009 without exception. As discussed in the body of the document, we respectfully disagree. The criteria for new reactor data communications was developed to address a safety issue involving data communication independence between safety and non-safety systems and between redundant safety divisions (also referred to as interdivisional communication). The proposed criteria provides a means to address independence when using data communications while allowing for functionality that digital technology may bring to new reactors. The criteria takes the approach of eliminating the potential hazards with interconnection and bi-directional communication rather than allowing such design implementations and attempting to mitigate hazards at a detailed design level. Operating experience with digital systems thus far highlights the potential for such hazards to impact plant safety if not properly addressed. This approach ensures the safety of data communications using simple design techniques by which the analysis is readily straightforward for all stakeholders; both in the present and years to come. The simplicity and straightforwardness of the criteria support the expectations laid out in Commission's policy regarding advanced reactors.

DISCUSSION

Non-concurrence NCP-2014-003 was submitted by Royce Beacom, Richard Stattel, Steven Wyman, Clifford Doutt, and Samir Darbali in the Office of Nuclear Reactor Regulation regarding the incorporation of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-

2009 by reference into 10 CFR 50.55a(h), and it is focused on the restrictions of data communications for the digital I&C systems in new reactors. The non-concurrence identifies one regulatory process issue if the proposed criteria for new reactor data communications are adopted. Specifically, the non-concurrence states that if the criteria are adopted, "the existing burden to complete the review of plant-wide, highly complex I&C architectures would remain unresolved. In fact, the NRC staff's review could be made more troublesome and prolonged given the greater review uncertainty (e.g., without a review plan and associated guidance) should an applicant choose the alternative."

For Non-Concurrence NCP-2014-001, which was focused on the same document and the same criteria for new reactor data communications, NRO staff provided observations to that non-concurrence [1], [2]. In that non-concurrence, similar issues were raised regarding the potential for applicants to pursue alternatives and the regulatory process issues that may be created. The recommendation in Non-Concurrence NCP-2014-003 is similar to the recommendation that was provided in Non-Concurrence NCP-2014-001. Specifically, the recommendation is to incorporate the independence criteria of IEEE Std. 603-2009 without exception and to complete guidance development for Regulatory Guide 1.152. For brevity, the observations to this non-concurrence rely on the background and supporting information in our earlier memorandum regarding our observations to NCP-2014-001.

The non-concurrence makes the assumption that the criteria for new reactor data communications is intended to simplify the regulatory decision making process and remove the necessity for the staff to use their judgment when applying the guidance that is available. This is not correct. The criteria for new reactor data communications was developed to address a safety issue involving data communication independence between safety and non-safety systems and between redundant safety divisions (also referred to as interdivisional communication). As described in our observations to NCP-2014-001, and in the Statements of Consideration for the proposed rule, use of bi-directional, interdivisional data communications can create unknown and undesired dependencies between systems that must be independent because information and signals are shared between these systems. Software and hardware design features can be used to mitigate hazards when bi-directional communications are used, but such designs can be significantly complex in their interactions and size that impacts the identification and resolution of undesired dependencies and unexpected behaviors. NRO staff developed the proposed criteria for new reactor data communications to incorporate the following aspects.

1. Safety engineering principles – first attempt to eliminate hazards and then mitigate them if elimination is not possible.

2. Operating experience and new reactor licensing review experience – events at nuclear power plants point to the potential for compromising independence with bi-directional data communications and licensing of new reactors has shown that applicants do not possess sufficient design information and analysis to demonstrate independence with bi-directional data communications at the time of licensing.

3. Commission policy – the Commission's expectation is that new reactors would incorporate features to make them inherently safe as demonstrated by simple designs and straightforward engineering analysis.

The proposed data communication criteria for new reactors limits data communication between safety and non-safety related I&C systems to be one-way from the safety system to the non-safety system. The one-way communication is implemented through physical means, such as a single wire or fiber optic cable connected from the transmit port of the safety I&C system to the receive port of the non-safety system. Data communication between redundant safety divisions is limited to those necessary to complete a safety function (e.g., voting). From a safety engineering perspective, safety I&C divisions should be independent from redundant safety divisions and from non-safety systems. There should not be a need for safety I&C divisions to receive information from outside sources except as noted in the proposed criteria. As a preferred means of addressing hazards associated with data communications, the proposed criteria also eliminate hazards that are associated with bi-directional data communications since no data or handshaking signals are received by the safety I&C divisions. The NRO staff believes that the proposed criteria accomplish the objectives in the Commission's policy with respect to data communications by encouraging an inherently safe, simple, and straightforward way to achieve data communication, while at the same time allowing much of the functionality that improves I&C system reliability and plant operation.

The non-concurrence proposes that applicants are likely to pursue the alternative process since: (1) applicants would maintain the use of bi-directional data communication already in their designs, (2) an alternative would be preferable to re-design of their I&C systems that could impact some safety and non-safety features, and (3) there would be commercial impacts due to engineering efforts to meet the proposed rule. The proposition that applicants, in general, will pursue the alternative process is speculative and not supported by past experience. Experience with licensing reviews of new reactor designs shows that applicants generally proposed or modified designs, during licensing reviews, consistent with the proposed criteria. For example, the original AP1000 design certification amendment proposed one-way data communication through physical means from safety systems to non-safety systems. While the original U.S. EPR design utilized a number of bi-directional, interdivisional data communications, later modifications to the design either eliminated or converted those into one-way data communications enforced by physical means. Discussions with future applicants and digital I&C vendors show that many are taking into consideration the lessons learned from previous industry implementation experiences and new reactor licensing reviews, domestic and international, with regards to data communications and are developing their designs accordingly.

The non-concurrence claims that the NRC staff's review would be "more troublesome and prolonged given the greater review uncertainty (e.g., without a review plan and associated guidance) should an applicant choose the alternative." The alternative process is a viable means to propose a design that does not follow the mechanical and electrical codes and standards that are incorporated into 10 CFR 50.55a. This process has been used on a number of occasions where the alternative has been demonstrated to be safe, and it was not practical to

meet a requirement. If a new reactor applicant proposes an alternative that would utilize bi-directional, interdivisional data communications, the staff would use the existing guidance on the subject, which is the same guidance that would be used for operating reactors utilizing that type of data communication. Currently, that guidance is mainly found in ISG-04, which was applied to new reactor reviews. As discussed in our observations to NCP-2014-001, recent experience with licensing reviews of new reactors has demonstrated that the main issue with accepting bi-directional, interdivisional data communication was not the lack of the existing guidance, but the lack of design information and supporting analysis at the appropriate level of design where independence is claimed to have been accomplished.

The non-concurrence discusses the use of engineering judgment and how the proposed criteria for new reactors data communication would limit the use of such judgment. The non-concurrence is correct that with all safety reviews there is a level of engineering judgment that is applied. However, engineering judgment must be used with care to ensure safety margin is not significantly eroded, and it does not become a replacement for due diligence when performing engineering analyses. NUREG-1913, "Design Control: In Pursuit of Engineering Excellence," was written as a quick reference guide for inspectors, but contains principles regarding the use of engineering judgment that are applicable to licensing activities [3]. The document describes engineering judgment as the technical judgments made by knowledgeable engineers experienced in the particular subject matter. Reliance on engineering judgment is predicated on the consistent and appropriate use of engineering "rules of thumb" and reliance on well-developed, understood, and widely-accepted industry practices and standards. The appropriateness of engineering judgment should be considered in light of the following questions:

1. Does the engineering judgment rely on assumptions or data that are not relevant to this issue (i.e., reliance on past successes to justify current assumptions)?

2. Did the licensee consider other data that contradict the engineering judgment?

3. Does the engineering judgment apply to "rules of thumb" alone?

4. Does the conclusion seem reasonable?

5. Does the conclusion account for industry operating experience?

6. Is there conservatism incorporated in the engineer's conclusion?

7. Is unsupported engineering judgment being relied upon in lieu of testing to demonstrate design adequacy or system operability?

With respect to the use of bi-directional, interdivisional data communications, recent licensing reviews of new reactors revealed that over-reliance on engineering judgment in this area could be problematic. For instance, reliance on past successes in using bi-directional data communication is an issue since (1) industry operating experience also illustrates past problems

and (2) each digital I&C application (i.e., application software development) has its own unique design context, operation, interfaces, etc. that could invalidate past experience. The staff in NRO believe that the proposed criteria for new reactor data communication incorporates a conservative approach to the issue of data communication independence by eliminating potential hazards associated with communication rather than mitigation of those hazards at a detailed design level. More important, experience in licensing reviews of new reactors has shown that engineering judgment was often relied upon by applicants in lieu of design information and analysis. Specifically, applicants proposed the use of bi-directional, interdivisional data communication, but did not have the requisite design information and analyses, in the licensing basis, for the same level of the design where independence would be accomplished (e.g., hardware and software).

The non-concurrence suggests that new reactors apply the current guidance as found in ISG-04 using engineering judgment. As stated above, the guidance in ISG-04 was applied to new reactor licensing activities. Experience shows that some applicants took departures from the guidance in ISG-04 in several areas, including permanent, bi-directional data communication between non-safety engineering workstations and safety-related I&C systems and performance of non-safety functions on safety-related processors. These departures not only occurred for new reactors but on a digital upgrade for operating reactors as well. As mentioned above, the applicants did not have the requisite design information and analysis to justify the departures from guidance that they were proposing. In other situations, NRO staff applied engineering judgment and entertained alternatives as they apply to the current regulations and ISG-04. For example, in the U.S. EPR proposed digital I&C design, each division of the reactor protection system acquires a set of in-core instrument readings and shares them with the other divisions. For the departure from nucleate boiling and high linear power reactor trip functions, each division needs the instrument readings from the other divisions. Because the divisions are relying upon information outside of their divisions, the design does not comply with Clause 5.6 of IEEE Std. 603-1991, as incorporated into 10 CFR 50.55a(h)(3). To meet the independence requirement, the applicant advised that either additional reactor vessel head penetrations would be required to include four sets of independent instruments or divide the current set of instruments into four independent sets. After discussions with the applicant and NRC mechanical and reactor systems technical staff, neither approach was favorable from a safety perspective. Specifically, from a reactor coolant system integrity perspective, the first option was not favorable as it was desirable to limit the number of reactor vessel head penetrations. From a reactor core measurement perspective, the second option was not favorable as it would reduce the resolution of the reactor protection system's ability to observe real-time core performance. The applicant proposed an alternative to not meet independence in the case of the in-core instruments, but maintain single failure protection by assuming a worst-case instrument failure as a nominal condition in the safety analysis. The staff applied engineering judgment to this case, considering mechanical, nuclear, I&C, and overall plant safety objectives, and ensuring other I&C design aspects would support this approach. While the staff has not given final approval for the U.S. EPR design, the staff did not have issues with the proposed alternative in its safety evaluation report with open items.

Similarly, the NRO staff would support alternatives regarding bi-directional, interdivisional data communications if there is a clear and complete safety basis that supports such an approach.

Finally, the non-concurrence suggests that the proposed criteria for new reactor data communication would not be a safety-focused, performance-based rule. As discussed earlier, the purpose of the proposed criteria was to address the safety issue of data communication independence and ensure adequate safety when it is used. As part of the rulemaking process, the data communication criteria, along with the rest of the proposed rule, would be available for public comment and allow stakeholder input. The proposed rule seeks to incorporate IEEE Std. 603-2009 into 10 CFR 50.55a. The mechanical and electrical codes and standards incorporated by reference into 10 CFR 50.55a are not performance-based criteria. Rather, they specify limitations that would be placed on system designs, analyses, and tests based on physical properties, analysis, and experience. Performance-based rules, such as 10 CFR 50.65 and 10 CFR 73.54, are goal- and program-oriented. When compared to the other criteria in the American Society of Mechanical Engineer's Boiler Pressure Vessel Code and IEEE Std. 603, including the exceptions to these codes and standards, the NRO staff found that the proposed criteria for data communication in new reactors is consistent with those already in 10 CFR 50.55a.

CONCLUSIONS AND RECOMMENDATIONS

The recommendation in Non-Concurrence NCP-2014-003 is similar to the recommendation that was provided in Non-Concurrence NCP-2014-001. Specifically, the recommendation is to incorporate the independence criteria of IEEE Std. 603-2009 without exception and to complete guidance development for Regulatory Guide 1.152. As described in the our observations to NCP-2014-001, based on the technical and policy basis provided in the Statements of Consideration and discussed in this document, the proposed criteria for independence should go forward in the draft rule for public comment. The proposed criteria address safety issues that pertain to bi-directional data communications between safety and non-safety I&C systems and between redundant safety I&C divisions. Undesired dependencies and behaviors may be created between systems that must be independent of one another when bi-directional data communications share information and signals between these systems, as evidenced by operating experience and identified during the new reactor licensing reviews. The proposed criteria provide a means to address independence when using data communications while allowing for the functionality that digital technology may bring to new reactors. The criteria take the approach of eliminating the potential hazards with interconnection and bi-directional communication rather than allowing such design implementations and attempting to mitigate hazards at a detailed design level. Operating experience with digital systems thus far highlights the potential for such hazards to impact plant safety if not properly addressed. By taking this technical approach, the safety of data communications can be addressed using simple design techniques by which the analysis is readily straightforward for all stakeholders; both in the present and years to come. The simplicity and straightforwardness of the criteria support the Commission's policy regarding advanced reactors. The proposed criteria directly support the

agency's defense-in-depth strategy for safety and enhance the efficiency and effectiveness of licensing reviews of complex digital I&C designs. The lessons learned from the Fukushima event highlights the need to begin establishing a new norm as we learn new information and a clear and strong defense against credible hazards that could have high consequences, such as failures and faults caused by unnecessary dependencies and complexities.

REFERENCES

1. R. Stattel et al., "Non-concurrence on Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009," NCP-2014-001.

2. T. Jackson, I. Jung, and D. Zhang, "Observations on NCP-2014-001: "Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009," with Respect to Coverage of Overall System Safety for Modern Instrumentation and Control (I&C) Systems," ADAMS Accession No. ML14094A612 (OUO); ML14097A146 (Public).

3. NUREG-1913, "Design Control: In Pursuit of Engineering Excellence," U.S. Nuclear Regulatory Commission, August 2009, http://pbadupws.nrc.gov/docs/ML0926/ML092650379.pdf.