NEI Comments on Draft NUREG/CR
"Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems"

General Comments

The industry and NEI are highly appreciative of the opportunity to provide comments on the draft NUREG/CR-XXXX, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems." We understand there is still a significant gap between the NRC and industry perceptions on what is required for PRA modeling of digital systems. Given this difference in perception, the current approach of performing benchmarking using traditional methods and more advanced method can provide insights into the capabilities of each.[1]

The industry is concerned about some of the conclusions made in this NUREG/CR, as the process or foundation used to make some of these conclusions appears somewhat flawed. The process used in Chapter 2 to compare previous analyses of digital systems was a specific area of concern. The use of older evaluations, not intended to meet this criterion, called into question the meaning of the results. This may have precluded methodologies from this study that held some promise in evaluating digital systems. Nonetheless, a solid basis for continuing the traditional methods side of the benchmarking is provided in the draft NUREG/CR.

It is understood that there were practical reasons that the NSR system (digital feedwater) was modeled prior to the safety related (SR) system (RPS). However, the industry would like to emphasize the problems seen in an NSR *Control* System are obviously much different from those seen in a SR *Actuation* System. As the benchmarking research continues, the results must consider the different needs for modeling these types of systems

Overall, the approach to the comparison of the reliability assessment methods has some merit, as does the goal of assessing whether new methods provide an advantage over existing methods. Some insights can be gained from the comparison performed in this report. However, specific conclusions are difficult to draw since there are only a small number of studies or applications to review and these studies will have varying goals and objective that will shape the application of the methods. The absence of discussion regarding research and development that makes the case that traditionally digital systems do not significantly contribute to the risk profile exacerbates this problem, as this renders the study even less complete.

[1] The industry TWG continues to maintain that the need for advanced methods has not been shown in a detailed evaluation. The NRC has continued to maintain that advanced methods may be needed to evaluate digital systems. This NUREG/CR and previous related NUREG/CRs have not addressed existing research and published papers that show that digital systems do not significantly impact the risk profile. The impact on advanced reactors is unclear at this time, but care must be taken when drawing conclusions based on the preliminary PRAs as the details on the ability to recover from digital CCFs are not available. In either case it appears that this professional difference of opinion continues, and that this research will move us forward into determining what methods will be acceptable.

Specific Comments

Goals of the NUREG/CR

1. The goals and objectives of the report are not well stated. Rather, a problem statement followed by a list of candidate tasks is presented. The title of the report suggests a goal or objective, but this is not directly or clearly stated. Without a clear goal or objective, one can only surmise the rationale for the content or infer a goal.

2. Having tried to infer the goals and objectives of the report from the content, the purpose of the report remains unclear. The following questions present themselves:
    a. Is the purpose of the report to develop the criteria that can be used to characterize the ability of a given method to model digital systems for applications?
    b. Why do we need to assess the capability of methods to model digital systems? Do we expect many risk informed submittals concerning digital systems? Have the concerns that are known concerning the current contributions of digital systems to the risk profile been addressed (i.e., digital systems are not likely to contribute significantly to the risk profile and therefore do not require detailed modeling)?

Chapter 2

1. The examples presented were developed for specific purposes. These digital system examples have specific goals and objectives that most likely affected their application of modeling technology. The examples are also relatively dated, as are the technology of the digital systems and the technology used to model those systems. Further, the examples that are provided cannot be used to assess the capability of the modeling methods employed as these examples were not prepared for demonstration of the modeling technology. This is not to say that some lessons cannot be learned from the examples. However, broad assertions concerning the modeling techniques may not be appropriate.

2. The contents of the report are generally not well supported by the examples or analyses performed. This is not to say that the characteristics proposed for the evaluation of the capabilities of various methods in modeling digital systems are inappropriate.

3. A significant challenge associated with this research is modeling software reliability. Advancing the state-of-the-art for predicting software failure probability is a difficult task that has seen many unsuccessful past attempts. Therefore, it may be prudent to acknowledge that a precise method for quantifying the failure probability of software may not be possible, and to focus instead on how to deal with the issue subjectively. The PRA and research communities can move forward by developing bases for subjective probability estimates and corresponding uncertainty analyses, which acknowledge the characteristics of a well-designed defense. The NRC should not delay the use of risk insights, including the insight that digital I&C represents a potential improvement in risk, in order to wait for advancement in quantitative software reliability methodology that may not be possible.

4. The criteria for software common cause failures (CCFs) are unrealistic. The criteria require the assumption of complete dependence for application software if it is "similar," and for different systems that use the same operating system. The NUREG contradicts its own repeated statements that correctly characterize software failure as requiring both a latent defect and a trigger in the input data trajectory, as the criteria of complete dependence recognize only the contribution of the software defect and not that of the data trajectory.

5. The draft NUREG makes an excellent point regarding the bounding of the level of detail used in any method of evaluation used. Specifically, it is noted that the appropriate level of component modeling varies depending upon the data that are available.

6. As this NUREG is supposed to concentrate on PRA methods, it is important that the focus be maintained and that any standards referenced are relevant to the development of PRAs. Therefore, the reference to IEEE 7-4.3.2-2003 should be removed, as I&C standards are not guidance for performing PRAs.

7. The discussion concerning experience and design features associated with shared networks are applicable to NSR control systems. Safety-related I&C designs must meet the applicable design criteria for independence and separation. Therefore, care should be taken before generalizing insights gained from non-safety-related designs to all digital I&C.

8. In the interest of removing this muddling between SR and NSR I&C systems, and consistent with defense-in-depth, it is recommended that these two applications be clearly separated, both in the research and in the NUREG reports that are produced from it. NSR control systems used for normal plant operations and SR protection systems are different problems. The design criteria are different, the effects of failure are different, and the issues and problems associated with PRA modeling are different. The NSR control systems are relatively complex compared to the protection systems, tend to be more integrated, and have less redundancy and diversity than is possible in a protection system.

Chapter 3

Although it would seem that the relevant focus for the digital feedwater analysis would have been the dynamic function after a reactor trip, the NUREG/CR concentrates on initiating event impacts. However, given the scope of this assessment and the advanced methods NUREG/CR, the results should be compared to the actual frequencies of digital failures which lead to transients at the actual site. It is anticipated that this type of evaluation will tend to overstate the actual frequency.

Chapter 6

1. It is unclear to the industry how this process will be practically implemented without extensive review of hundreds or maybe thousands of combinations. The follow up NUREG/CR which actually quantifies via this method will need to show the actual process used here.

2. The NUREG/CR notes that dependencies would typically be accounted for via common cause modeling. It notes that as more failures are required it is obvious that failure probabilities of these "cutsets" decrease significantly. In the case where an initiating event frequency is being modeled, this is generally true. If the power dependencies are lost, then in many cases, the supports to the NSR digital feedwater would be lost and the digital control would be irrelevant. However, for most SR mitigating systems, the dependencies are far more relevant. The post trip sequence can often lead to losses of dependencies and reduce the number of failures required to fail a system. For SR systems, part of this Markov evaluation must include combinations with various dependencies failed. Many mitigating systems have extremely low failure probabilities with all supports, but there failures become more relevant when power dependencies are lost.

Chapter 9

As noted in the draft NUREG/CR, it is difficult to find pertinent data for digital hardware and software. Many of the vendors have information on specific systems, but even this data becomes obsolete relatively rapidly. Additionally, the University of California-Berkeley has been doing extensive work on computer reliability. This research may uncover relevant information the industry and the NRC could use.