NUCLEAR ENERGY INSTITUTE

11/14/08
73FR67555

Victoria Anderson
PROJECT MANAGER
RISK ASSESSMENT
NUCLEAR GENERATION DIVISION

December 29, 2008 (2)

Chief, Rulemaking, Directives and Editing Branch
Division of Administrative Services
Office of Administration
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Industry Comments on Draft NUREG/CR-XXXX, "Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods"

Project Number: 689

As part of the industry's efforts to collaborate with the NRC staff in assessing the state of the art of modeling digital instrumentation and control systems in PRA, NEI offers the enclosed comments regarding draft NUREG/CR-XXXX, "Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods." The draft NUREG provides an informative body of work for digital control system reliability studies; however, the conclusions should be applied cautiously, as they may not necessarily apply to digital systems that do not perform control functions, such as protection systems. The enclosure offers detailed comments regarding the draft NUREG.

If you have any questions, please contact me.

Sincerely,

Victoria Anderson

Victoria Anderson

Enclosure

c: Mr. Alan Kuritzky, U.S. Nuclear Regulatory Commission
NRC Document Control Desk

E-RFDS = ADM-03
Add =

SUNSI Review Complete

1776 I Street, NW | Suite 400 | Washington, DC | 20006-3708 | P: 202.739.8101 | F: 202.533.0173 | vka@nei.org | www.nei.org

Template = ADM-013

A. Kuritzky (ASK1)

Detailed Industry Comments on Draft NUREG/CR-XXXX, "Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods"

Overview

The draft NUREG provides an interesting and informative body of work for digital control system reliability studies. However, the conclusions should not necessarily be generalized to all digital systems; specifically, they may not be applicable to digital systems that do not perform control functions, such as protection systems. Compared to control systems, protection systems have more independence between redundant channels, are less integrated in their functionality, and involve less feedback from the process system. There is no evidence that the conclusions of this study are generically applicable to safety-related protection systems, which are the digital systems of most interest to PRA studies. Therefore, the introduction and conclusion sections of this NUREG should acknowledge that the control systems and protection systems are different problems, and that the conclusions from one do not necessarily apply to the other.

Because of the complexities associated with modeling control systems, most PRA analysts have used operating experience rather than detailed models. The level of detail in this study may be of interest for a stand-alone control system reliability study; however, for control systems included in a PRA, this level of detail is not necessary. Control systems included in PRAs are generally of interest because their failure may represent a challenge to safety systems. Since the non-safety-related control systems are generally separate from the safety-related protection systems that mitigate the control system failure, it is difficult to justify a level of detail in the control system model beyond what is needed to estimate initiating event frequency. This is reinforced by the authors' conclusion that the quantitative analysis results obtained in the study are consistent with the plant's operating experience.

Objectives and scope of the analysis

The draft NUREG states that the top event of interest is loss of automatic control of the feedwater control system given that the plant is at full power operation for one year. However, the document does not make clear what need is being addressed in focusing on the modeling of balance of plant control systems. Unless one is performing a generation risk assessment, it is not necessary to model balance of plant control systems in PRA, whether analog or digital. The emphasis on upgrading current plants to digital systems and on the licensing of new plants in the digital I&C area is on mitigating systems, such as RPS and ESFAS. Feedwater control systems are not risk significant systems in PWRs; in fact, some PWRs model the entire feedwater system as a super component. Feedwater control systems are potentially risk significant in BWRs, but only as a mitigating system, in which case they are generally manually operated in accordance with EOPs.

For a PRA model, the focus of a protection system analysis is different from a control system. For protection systems, the focus is on whether the redundant channels are independent, as opposed to dynamic effects, which may be important for control systems. For example, on page 11-2 the draft NUREG states that, "There are unique features in a digital design, such as communication and synchronization, whose failure modes and effects are not well understood and may introduce dependencies between redundant equipment." This remark is unlikely to be accurate for protection systems, where independence between redundant channels is required by regulation, and where certain beneficial design features, such as asynchronous operation, that ensure this independence.

Modeling approach

The report indicates that the Markov modeling is used only for quantification purposes and not to identify system failure paths. In this regard, the analysis appears to be risk-based. Additionally, the report appears to use success criteria that are not realistic for a nuclear power plant PRA, as the feedwater system is assumed to fail if manually controlled and no repair is permitted following failure of a component that does not disable the system.

Data

The draft NUREG states that the digital feedwater control system is installed at very few plants, and that system-specific data is therefore scarce. This conclusion contradicts commonly accepted PRA practice of aggregation of data across multiple plant and vendor designs with varying configurations in producing generic data associated with initiating events. The report also makes a statement regarding why digital systems differ from their analog counterparts and cannot be quantified with methods similar to the manner in which initiating event frequencies are currently developed in PRA, and that the data used in this analysis cannot be used in support of decision making. The report should discuss how different data might affect each conclusion of the study.

The report's treatment of common cause failure appears to contradict the concept that software is deterministic and that "the same input yields the same output," as the draft NUREG assigns common cause failures a generic 0.05 beta factor based on the ALWR Utility Requirements Document. The draft NUREG needs a more detailed discussion regarding what fraction of this beta factor is software related and what fraction is hardware related, and also needs a more detailed discussion regarding how software common cause failure was treated in the analysis in general.

Failure modes

The draft NUREG implies that the failure modes of some components could not be precisely determined and were thus assumed to be undetectable. It is not clear how the impact of these components were modeled if the effects of the failure modes were not known. The draft NUREG further expresses concern regarding the completeness of the set of failure modes assumed; however, it is not clear why the failure modes of the

mechanical and electrical equipment controlled by the digital system could not be used to bound the effects of the digital system failure modes.

Quantification

The analysis in the draft NUREG estimates the loss of feedwater frequency to be 0.08/yr. This is on the same order of generic loss of feedwater frequency for nuclear power plants due to all causes given in NUREG/CR-6928. A review of NERC-GADS for this period suggests that between 10% and 15% of all loss of feedwater events in the domestic nuclear industry were instrumentation and control (I&C) related (cause codes 3370, 3408 & 3414). During the period in question, a significant number of digital feedwater upgrades were performed or were already implemented. Even assuming that no digital feedwater control systems existed for this period, the implication of the results of the Markov analysis is that a relatively significant increase in loss of feedwater transients can be expected after upgrading to digital controls. The draft NUREG further provides a comparison of the operating experience at the plant from which the digital feedwater system information was obtained. The failure modes described in the discussion are stated to be not digital-system related, or are result of component failures not included in the model. The report could be appreciably enhanced by a discussion on the dominant contributors to the 0.08/yr digital feedwater system initiating event frequency, as the results of the analysis as described do not appear to be consistent with either generic operating experience or the plant specific experience with the system.

Finally, a fault tree cut set quantification is performed and the numerical results compared to the Markov analysis. It is stated that the quantification of the fault tree was performed by assuming the mission time associated with the model. This is not an accepted approach to generating the results of a fault tree model for the purpose of developing an initiating event frequency. The fault tree analysis should either be deleted from the report or corrected based on accepted approaches such as those described in the following references related to generation of initiating event frequencies:

- ASME, "Risk-Based Methods for Equipment Life Management: An Application Handbook," CRTD Vol. 41, ASME International, 2003.
- EPRI, "Reliability Assessment of the Coronado Generating Station," Report 1007442, March 2003.
- EPRI, "Trip Monitor Customization and Implementation Guideline," Report 1009112, January 2004.
- EPRI, "Introduction to Simplified Generation Risk Assessment Modeling," Report 1007386, February 2004.
- EPRI, "Generation Risk Assessment Plant Implementation Guide," Report 1008121, December 2004.
- EPRI, "Generation Risk Assessment (GRA) at Cooper Nuclear Station," Report 1011924, December 2005.

Conclusion

It would be informative to balance and contrast this study with a similar analysis for a protection system. In the meantime, stronger statements should be made in the introduction and conclusion sections of this draft NUREG to caution that control systems and protection systems represent unique problems, and that the conclusions from one do not necessarily apply to the other to avoid promoting the misconception that the problems encountered with the control system study prevent the modeling of digital I&C systems in PRAs.