July 8, 2008

Dr. William J. Shack, Chairman
Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

SUBJECT: DRAFT NUREG/CR-6962, "APPROACHES FOR USING TRADITIONAL PROBABILISTIC RISK ASSESSMENT METHODS FOR DIGITAL SYSTEMS," AND RELATED MATTERS

Dear Dr. Shack:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am responding to your letter to Chairman Dale E. Klein, dated May 19, 2008, which summarized the views of the Advisory Committee on Reactor Safeguards (ACRS) regarding draft NUREG/CR-6962, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems," and related matters. We appreciate the recommendations provided in your letter, and they will be reflected in the final version of NUREG/CR-6962 and in the staff's updated digital instrumentation and control (DI&C) research plan. Please see below the staff response to the individual ACRS recommendations, as well as some further clarification of the staff's research in this area.

ACRS Recommendation 1. Draft NUREG/CR-6962 provides convincing evidence that "traditional" probabilistic risk assessment (PRA) methods are not sufficient to adequately identify failure modes of DI&C systems.

Staff Response. Draft NUREG/CR-6962 defines traditional PRA methods as those that are well established but that do not explicitly attempt to model the following: (1) the interactions between a plant system and the plant's physical processes (i.e., the values of process variables), or (2) the exact timing of these interactions. Nontraditional (dynamic) PRA methods explicitly model the interactions between the plant system and the plant physical processes, as well as the timing of these interactions. Draft NUREG/CR-6962 identifies several current limitations in the state-of-the-art for using traditional PRA methods to develop and quantify reliability models of DI&C systems. Draft NUREG/CR-6962 also provides a preliminary list of areas that need additional research and development. Most of the limitations that draft NUREG/CR-6962 identifies are associated with analyses that support application of the traditional PRA methods (not limitations of the methods themselves). Examples of these limitations include the need for a more structured process for DI&C component-level failure mode identification and better databases for hardware failures of DI&C components.

However, draft NUREG/CR-6962 also states that in order to capture all of the DI&C system design features that could affect system reliability, the level of detail of the benchmark study reliability models will be extended down to the DI&C component level. A principal insight from the work-to-date on the first benchmark study of a digital feedwater control system (DFWCS) is that given the complexity of the system, at the DI&C component level, it is often difficult to determine how specific component-level failure modes affect the system. Moreover, it is nearly impossible to determine how combinations of multiple component failure modes affect the

system. Therefore, as part of the first benchmark study, Brookhaven National Laboratory developed a simulation tool to determine the combinations of component-level failure modes that lead to DFWCS failure.

The use of the simulation tool postdates the work covered by draft NUREG/CR-6962. Nonetheless, the final version of NUREG/CR-6962 will state that a failure modes and effects analysis (FMEA) alone is not sufficient for determining how specific component-level failure modes affect systems as complex as DI&C systems; analysts should use more sophisticated tools, such as simulation tools, to study the interactions between the components of a DI&C system and the effects of one or more failures. The subsequent report documenting the results of the first benchmark study will highlight the need for a simulation tool to support development of the DFWCS reliability models.

ACRS Recommendation 2. Before publication of NUREG/CR-6962, it should be revised to state clearly that its methods do not address software failures and that it employs simulation in addition to traditional PRA methods. The revised NUREG/CR report should focus on failure mode identification only.

Staff Response. Consistent with the ACRS recommendation, the final version of NUREG/CR-6962 will state clearly that its methods do not address estimation of risk from software faults. The staff recognizes the need to fundamentally reexamine estimation of risk from software faults. More generally, there is also a need to reexamine estimation of risk from failures from systemic causes (also known as systematic failures), including further research of best practices in industries outside of the U.S. commercial nuclear power industry. Note, however, that as stated in draft NUREG/CR-6962, the Markov and fault tree models for the first benchmark study will include the normal behavior of the application software and placeholders for relatively high level software failures (i.e., software halts and software generates incorrect output). These failures will not be quantified. Contingent upon results of the research mentioned above, future extensions of the modeling framework may include a more refined treatment of failures attributable to software and other systematic failures.

As stated previously, the final version of NUREG/CR-6962 will state that an FMEA by itself is not a sufficient tool to determine how specific component-level failure modes affect DI&C systems and that more sophisticated tools, such as simulation tools, be used to analyze the interactions between the components of a DI&C system and the effects of one or more failures.

Consistent with the ACRS recommendation, the final version of NUREG/CR-6962 will focus on failure mode identification. Failure mode identification implies identification, but not quantification, of system failure paths (as opposed to the component-level failure mode identification that would occur as part of an FMEA). As discussed in the staff response to ACRS Recommendation 4, any quantification performed as part of the benchmark studies will only be used to demonstrate the reliability methods and exercise the models; results of the quantification will not be published in the reports on these studies.

ACRS Recommendation 3. The distinction between traditional and non-traditional methods of modeling and analysis is artificial and should be abandoned. The staff should establish an integrated program that focuses on failure mode identification of DI&C systems and takes advantage of the insights gained from the investigations on traditional PRA methods and on advanced simulation methods.

Staff Response. As mentioned previously, for the NRC DI&C risk research program, the distinction between traditional and nontraditional (dynamic) methods is the extent that the methods model interactions between a plant system and the plant's physical processes. The purpose of this distinction and the two parallel NRC research projects is to gain insight as to whether the additional accuracy (and complexity) of dynamic modeling is necessary to obtain a reasonable estimate of the DI&C system failure probability or frequency. Issues with the DI&C system models (e.g., completeness of failure mode identification and availability of hardware failure data), are associated with supporting analyses and likely apply to all reliability modeling methods. With respect to the issue of systematic failures, including those attributable to software, as part of its routine updating of the DI&C research plan, the staff will seek knowledge and information from other safety-critical, mission-critical application domains and relevant literature. It is too early to determine how this issue may influence the choice of reliability modeling methods for DI&C systems.

Nonetheless, the staff agrees that the agency should explore an integrated program that focuses on failure mode identification for DI&C systems. In preparing its updated DI&C research plan, the staff will consider the insights gained from the investigations of both traditional PRA methods and dynamic methods, as well as the other ACRS recommendations.

ACRS Recommendation 4. The quantification of the reliability of DI&C systems should be given a low priority until a good understanding of the failure modes is developed.

Staff Response. The staff is in agreement with this recommendation. The final version of NUREG/CR-6962 will not provide the failure parameters used in the study. The final version will emphasize that due to limitations in publicly available failure parameters of DI&C components, the data developed for this study will only be used to demonstrate the reliability methods and exercise the models and are not appropriate for quantifying models used in support of decisionmaking.

We appreciate the comments and recommendations provided by the ACRS. We look forward to continuing to work with the ACRS as we move forward in this challenging area.

Sincerely,

/RA/ Martin J. Virgilio for

R. W. Borchardt
Executive Director
for Operations

cc: Chairman Klein
Commissioner Jaczko
Commissioner Lyons
Commissioner Svinicki
SECY

Staff Response. As mentioned previously, for the NRC DI&C risk research program, the distinction between traditional and nontraditional (dynamic) methods is the extent that the methods model interactions between a plant system and the plant's physical processes. The purpose of this distinction and the two parallel NRC research projects is to gain insight as to whether the additional accuracy (and complexity) of dynamic modeling is necessary to obtain a reasonable estimate of the DI&C system failure probability or frequency. Issues with the DI&C system models (e.g., completeness of failure mode identification and availability of hardware failure data), are associated with supporting analyses and likely apply to all reliability modeling methods. With respect to the issue of systematic failures, including those attributable to software, as part of its routine updating of the DI&C research plan, the staff will seek knowledge and information from other safety-critical, mission-critical application domains and relevant literature. It is too early to determine how this issue may influence the choice of reliability modeling methods for DI&C systems.

Nonetheless, the staff agrees that the agency should explore an integrated program that focuses on failure mode identification for DI&C systems. In preparing its updated DI&C research plan, the staff will consider the insights gained from the investigations of both traditional PRA methods and dynamic methods, as well as the other ACRS recommendations.

ACRS Recommendation 4. The quantification of the reliability of DI&C systems should be given a low priority until a good understanding of the failure modes is developed.

Staff Response. The staff is in agreement with this recommendation. The final version of NUREG/CR-6962 will not provide the failure parameters used in the study. The final version will emphasize that due to limitations in publicly available failure parameters of DI&C components, the data developed for this study will only be used to demonstrate the reliability methods and exercise the models and are not appropriate for quantifying models used in support of decisionmaking.

We appreciate the comments and recommendations provided by the ACRS. We look forward to continuing to work with the ACRS as we move forward in this challenging area.

Sincerely,

/RA/ Martin J. Virgilio for

R. W. Borchardt
Executive Director
for Operations

cc: Chairman Klein
Commissioner Jaczko
Commissioner Lyons
Commissioner Svinicki
SECY

DISTRIBUTION: G20080377/LTR-08-0311/EDATS: SECY-2008-0327

RBorchardt	MVirgilio	BMallet	DAsh	VOrdaz	KCyr/SBurns
ELeeds	MJohnson	JMonninger	ACRS file	BSheron	CLui
JUhle	PAppignani	RSydnor	MFranovich	SBailey	DSantos
SBirla	SArndt	DHerrmann	CDoutt	AKuritzky	DRA r/f

ADAMS Accession No.: ML081630578

OFFICE	RES/DRA/PRAB	SUNSI Review	RES/DRA/PRAB	Tech Editor	RES/DE	RES/DRA	RES	EDO
NAME	AKuritzky:dfw	AKuritzky	PAppignani	CHsu (via email)	JUhle	CLui	BSheron	RBorchardt (MVirgilio for)
DATE	06/11/2008	06/11/2008	06/12/2008	06/16/2008	06/12/2008	06/23/2008	06/27/2008	07/08/2008

OFFICIAL RECORD COPY