November 17, 2009

Dr. Mario V. Bonaca, Chairman
Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: DRAFT DIGITAL SYSTEM RESEARCH PLAN FOR FY 2010–FY 2014

Dear Dr. Bonaca:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am responding to your October 2, 2009, letter to Chairman Gregory B. Jaczko. Your letter summarized the views of the Advisory Committee on Reactor Safeguards (ACRS) on the Draft Digital System Research Plan for Fiscal Years (FY) 2010–2014. The NRC staff and I agree with the comments in your letter and will take them into consideration as the plan is refined and implemented. Specific comments on selected research projects are discussed below.

ACRS Comments on Communications Among Plantwide Systems

1. The development of a generic model that would still allow for evaluations as required by General Design Criterion (GDC) 24 will be a challenge. GDC 24 deals with the separation of protection and control systems and is cited in the technical basis sections of this project. The term "generic" implies a relatively high level of abstraction in the model of the plantwide digital network with a relatively low level of detail. It is unclear what insights could be gained from such a representation. Demonstration that GDC 24 is met will require a more detailed approach.

2. To ensure that the staff can adequately evaluate licensee design approaches, it would be very useful if the deliverables of this project included (1) the identification of data screening and evaluation algorithms that are the most robust at detecting corrupt and invalid data such that they are not injected into the program loop and (2) the identification of acceptable error detection/correction methods that meet ISG-4 guidance that would "always reconstruct the original message exactly or . . . designate the message as unrecoverable."

Staff Response. The NRC staff will revise the term "generic model" with the term "high-level architectural framework" (HLAF). The purpose of the HLAF is to establish a standard framework for the representation of digital systems used in a nuclear power plant and of the interaction of those systems with the associated business enterprise. One major item of

concern is the potential influence of business systems and other outside entities on plant safety and control systems. The HLAF itself is not intended to represent systems at a level of detail that could ensure thorough review in consideration of GDC 24 or Interim Staff Guidance (ISG) 4. The HLAF is intended to show typical systems and the needed data pathways to support review of the detailed architecture of proposed systems. One goal is to establish a consistent taxonomy so that disparate system architectures can be discussed and compared in terms of essential capabilities and protections.

It should be noted that although ISG 4 does indicate that communication into a safety division from outside can be accomplished in an acceptable manner, it places severe restrictions on the nature of that communication. In particular, it specifically disallows any type of communication that might alter the operation of the safety system during normal operation. The interdivisional communication process described in ISG 4 is physically incapable of transmitting commands or instructions that could alter the operation of the safety processor. ISG 4 also restricts incoming communications on the basis of the intent of the communication: it indicates that safety systems should perform only safety functions and, therefore, should have no need or use for incoming communications that do not directly support those functions. For example, although sensor comparison for the purpose of data validation is an important function, it is not directly related to the operation of a safety system. Consequently, ISG 4 indicates that it should be accomplished outside the safety system. Alteration of the safety processor program loop is to be possible only by means of the engineering console, and restrictions exist on the connection of that console during normal operation.

Identification of suitable communication protocols, data screening techniques, and algorithms for error detection and correction would be helpful but would be outside the envisioned original scope of the HLAF. These should be considered for inclusion as a future effort.

The staff considers this project to be limited in scope but recognizes that it could be repeatedly expanded as benefits to the review process are derived. The staff recognizes that the increased level of integration and communication among proposed digital instrumentation and control systems poses new review challenges and that future evolution of this project could provide the necessary technical basis to better address those challenges.

ACRS comment on Safety Assessment of Tool Automated Processes

It is not clear from the description of this project whether the experience of other industries, including aviation and telecommunications, will be reviewed. These industries have developed standards that address automated tools. These standards should be evaluated to help develop regulatory guidance for the use of such tools.

Staff Response. The NRC staff will evaluate the standards and experience of other industries addressing automated tools. The staff will clarify the description of this project and will include examples of relevant standards.

ACRS Comment on Development of Benchmark and Reliability Data

The stated purpose of this project is to provide a process for evaluation and validation of digital systems using a fault injection process to estimate digital system reliability. We agree that the fault injection method may contribute to our confidence that the system is of high quality by providing evidence of fault detection and recovery capabilities. However, we doubt that this project could lead to meaningful reliability estimates. The project's benefits need to be characterized properly inasmuch as the results will be neither "benchmark" nor "reliability" data.

Staff Response. The NRC staff agrees with the ACRS comment. The staff will de-emphasize the development of benchmark and reliability data estimates from this project. The staff will revise the various project descriptions and deliverables to better reflect the project benefits and to avoid reliability estimates. For example, the title will be revised from "Development of Benchmark and Reliability Data" to "Fault Injection Methodologies," and the deliverables will be revised to delete the second deliverable and to revise the first one to read: "A NUREG that describes the method for performing fault-injection of digital safety systems."

ACRS Comment on Analytical Assessment of Digital Instrumentation and Controls (DI&C) Systems and Digital System Probabilistic Risk Assessment (PRA)

We continue to believe that an integrated approach is essential to both the analytical assessment of DI&C systems and digital system PRA.

Staff Response. The NRC staff agrees with the ACRS comment and is taking the necessary steps to integrate all work and associated staff in the area of risk assessment of DI&C systems. Also, the staff recognizes that strong interrelationships exist between the Analytical Assessment of DI&C Systems and digital system PRA projects, and it intends to coordinate and integrate these approaches as work progresses.

Previous NRC research projects identified a set of desirable characteristics for reliability models of digital systems and applied various probabilistic reliability modeling methods to an example digital system. This research also demonstrated that limitations in current reliability modeling methods (e.g., for modeling software failures), as well as the weakness of publicly available digital component failure data, preclude the use of such models, at present, to support regulatory decision-making. The staff is currently performing research in the area of software failure quantification. Once sufficient progress is made in this area, the staff will return to the issue of integrating the modeling of digital system hardware and software.

The NRC staff and I appreciate the comments provided by ACRS. We look forward to continuing to work with the Committee on the various research projects as work progresses.

Sincerely,

/RA Bruce Mallett for/

R. W. Borchardt
Executive Director
for Operations

cc: Chairman Jaczko
Commissioner Klein
Commissioner Svinicki
SECY

The NRC staff and I appreciate the comments provided by ACRS. We look forward to continuing to work with the Committee on the various research projects as work progresses.

Sincerely,

/RA Bruce Mallett for/

R. W. Borchardt
Executive Director
for Operations

cc: Chairman Jaczko
Commissioner Klein
Commissioner Svinicki
SECY

DISTRIBUTION: G20090570/LTR-09-0489/EDATS: SECY-2009-0447

DE r/f	B. Mallett, DEDR	M. Johnson, NRO
ACRS File	D. Ash, DEDCM	M. Weber, NMSS
RidsResPmdaMail	N. Mamish, NMSS	R. Zimmerman, NSIR
R. Borchardt, EDO	S. Burns, OGC	A. Frazier, EDO
M. Virgilio, DEDMRT	E. Leeds, NRR	D. Rahn, NMSS
N. Hilton, OE	J. Adams, EDO	V. Ordaz, AO

ADAMS Accession No.: ML092960673

OFFICE	RES/DE	RES/DE/DICB	TECH EDITOR	D: RES/DE
NAME	D. Santos	R. Sydnor	J. Zabel (via email)	M. Case
DATE	10/26/09	10/26/09	10/20/09	10/26/09
OFFICE	RES/DRA	D: RES	EDO	
NAME	C. Lui	B. Sheron	R. Borchardt (B. Mallet for)	
DATE	10/27/09	11/02/09	11/17/09	

OFFICIAL RECORD COPY