



UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, D.C. 20555-0001

ACRSR-1888

PDR

April 18, 2000

Dr. Williams D. Travers
Executive Director for Operations
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555-0001

Dear Dr. Travers:

SUBJECT: PROPOSED NRC RESEARCH PLAN FOR DIGITAL INSTRUMENTATION AND CONTROL

During the 471st meeting of the Advisory Committee on Reactor Safeguards, April 5-7, 2000, we met with representatives of the NRC staff to discuss the Proposed NRC Research Plan for Digital Instrumentation and Control (I&C). We also had the benefit of the referenced documents.

This Proposed Research Plan for Digital I&C is the first formal response of the NRC to the 1997 National Research Council study entitled, "Digital Instrumentation and Control Systems in Nuclear Power Plants (Safety and Reliability Issues)." This Research Plan is essential for a definitive road map for research in the digital I&C area that is critically important to the Agency.

BACKGROUND

Digital I&C has been widely used in many high-technology fields, including some safety-critical fields, such as nuclear weapons safety and global aircraft navigation and control, for more than three decades. However, they have only been introduced into safety-related systems of nuclear power plants in the United States in the last decade. Although digital technology has the capability of improving performance and safety, it generally may introduce complexity and new failure modes that have resulted in NRC review being difficult and time consuming. The methodology and procedures prescribed in Chapter 7, "Instrumentation and Control Systems" of the Standard Review Plan (NUREG-0800) are process oriented. A year to review a topical report on a digital I&C system is not uncommon. Unfortunately, the NRC staff does not have tools and procedures to expedite the review process while providing the needed assurance of safety.

In its 1997 study, the National Research Council recommended, among other things, that NRC develop a research and development plan that would balance short-term needs and long-term anticipatory research needs. In NUREG-1635, Vol. 1, "Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program," the ACRS cautioned that "Vulnerabilities of digital systems are different than those of analog systems. Failure probabilities and the failure

Handwritten signature/initials

characteristics of these systems are also different. Appropriate methods to include digital and software systems in PRAs do not exist." These concerns were also expressed in NUREG-1635, Vol. 2 and Vol. 3. The proposed I&C Research Plan is in response to the issues raised in our reports and those identified by the National Research Council study.

Digital I&C systems are advancing in capability and complexity at a rapid rate. Increased use of automation for traditional tasks such as calibration, surveillance, and fault diagnostics are beginning to appear in nonsafety systems, and NRC must ensure that there are no inappropriate interactions with safety systems. Furthermore, the introduction of "smart systems" with additional complex features, such as self-adaptive compensation and non-mechanistic modeling capabilities provided by neural networks and fuzzy logic appears on the horizon.

CONCLUSIONS AND RECOMMENDATIONS

1. Specific anticipated output or product for each research task should be identified and the way in which this output or product meets the Agency needs should be clearly established. It is not sufficient to indicate that the task output is a report or a computer software code.
2. The approach to be taken or tools to be developed to reduce review time or to increase the assurance of the safety of digital systems being reviewed (e.g., how the proposed task accomplishes the specified goal or research result) should be stated and justified.
3. Quantitative estimates of the anticipated benefits should be given where possible.
4. The software systems program being conducted at the University of Virginia is currently the "magnum opus" of the Office of Nuclear Regulatory Research (RES) Digital I&C research effort. Showing how this program is meeting the research needs of NRC (or progressing toward this goal) could illustrate how activities proposed in this Research Plan could meet their specific objectives.
5. Each proposed task should be analyzed to determine the best approach to accomplish its goal. In some cases, buying commercial software, obtaining technology from other Government Agencies or industries, or adopting industrial standards rather than research may be adequate.
6. The priorities for the various tasks should be explicitly stated in the Proposed Research Plan.

DISCUSSION

The four research areas addressed in the Proposed Research Plan are discussed below:

1. Systems Aspects of Digital Technology

The Plan addresses the systems aspects of digital technology, including diagnostic and fault tolerance, the computer operating systems, and systems requirements

specifications. These items are related to component and system design, and research in these areas logically is the domain of the I&C vendors. The principal issue for NRC is how to ensure that Commercial Off-The-Shelf software can safely and reliably handle safety-critical functions. The Plan needs better focus on this principal issue.

The proposed investigation of environmental stressors on digital I&C components is a continuation of an ongoing RES program involving the influence of smoke, fire, temperature, humidity, and lightning. Unless there are new unforeseen aspects of these stressors, this program should be concluded expeditiously.

2. Software Quality Assurance

Gaining a better understanding of software faults and how to identify them is very important for the NRC. Although the NRC has guidance for software quality assurance, it does not specify the amount of testing required because there currently is no scientific basis for such a requirement. Establishing objective criteria for the adequacy of software quality assurance based on sound principles is an important task.

Current procedures for reviewing software are resource intensive for the staff. The staff urgently needs tools to expedite its review of software systems as documented in the Office of Nuclear Reactor Regulation (NRR) user need memorandum of March 17, 2000. We support elements of the Proposed Research Plan that are directed toward meeting NRR needs.

3. Risk Assessment of Digital I&C Systems

NRC has immediate needs for databases on failure rates of systems containing digital electronic components and the failure modes of digital components and software. These databases are needed to aid the staff reviews of digital I&C systems now being proposed by licensees. Work to develop these databases deserves priority support.

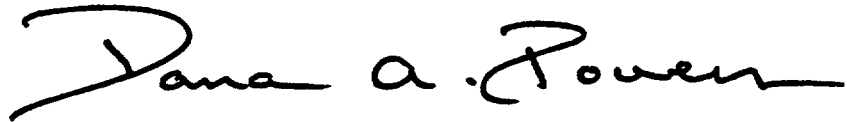
On a longer time scale, the NRC will need probabilistic methods to analyze the performance of systems with digital elements. Development of such probabilistic tools for use by the NRC line organizations should be supported.

4. Emerging I&C Technologies and Applications

The inclusion of emerging I&C technologies as anticipatory research was recommended by the National Research Council's study. It is particularly important that NRC understand the uses and limitations of these emerging technologies as well as the safety implications of such systems. In the long run, automated operation of nuclear power plants with advanced features, such as automatic replacement of signals from faulty sensors, self-adaption to changing conditions, and the use of non-mechanistic (data based) models, seems inevitable. NRC must be prepared to address such issues when these new systems are brought in for review. Automation, or perhaps intelligent systems that back up the operators (operator assistants), is likely to be introduced into

current generation plants to reduce operational errors within the next decade. Preparing for such predictable developments is a desirable element of anticipatory research.

Sincerely,

A handwritten signature in black ink, reading "Dana A. Powers". The signature is fluid and cursive, with the first name "Dana" being the most prominent.

Dana A. Powers
Chairman

References:

1. Memorandum dated March 17, 2000, from Sher Bahadur, Office of Nuclear Regulatory Research, to John T. Larkins, ACRS, transmitting Draft NRC Research Plan Digital Instrumentation and Control (Predecisional).
2. National Research Council, "Digital Instrumentation and Control Systems in Nuclear Power Plants (Safety and Reliability Issues)," 1997.
3. U. S. Nuclear Regulatory Commission, NUREG-1635, "Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program, Volumes 1 and 2 (Volume 3 is in Print), 1988, 1999, and 2000, respectively.
4. Memorandum dated March 17, 2000, from Samuel J. Collins, Office of Nuclear Reactor Regulation, to Ashok C. Thadani, Office of Nuclear Regulatory Research, Subject: User Need for Digital Instrumentation and Controls Research.