



UNITED STATES
NUCLEAR REGULATORY COMMISSION
Nuclear Safety Research Review Committee
Washington, D.C. 20555

January 28, 1993

Dr. David L. Morrison
Chairman, NSRRC
The MITRE Corporation
7525 Colshire Drive M/S W766
McLean, VA 22102

Subject: NSRRC Subcommittee on Advanced Instrumentation and Controls
and Human Factors Meeting of December 9, 1992

Dear Dr. Morrison:

The Nuclear Safety Research Review Committee (NSRRC) Subcommittee on Advanced Instrumentation and Controls and Human Factors met with NRC staff members on December 9, 1992, in Rockville, MD to review the RES program in those areas of research. This meeting was a follow-on to the discussions of the full NSRRC on these subjects on April 29, 1992, the conclusions of which were reported to you in my letter of November 16, 1992. The meeting was intended as a broad review of the programs and not to reach specific conclusions on individual programs. This is a summary report of that meeting.

The Subcommittee's report was discussed by the full Committee at its meeting on January 15, 1993. This letter reflects the result of that committee discussion, in which the Subcommittee report was accepted by the Committee with some modifications.

The application of advanced computer controlled, digital software dependent instrumentation and control to modifications of the control systems of the present generations of reactors and to the design of the next generation of Advanced Light Water Reactors (ALWR's) is very likely to be the single most significant technological advance over presently operating plants. On the one hand, modern electronics provide the opportunity, if properly engineered, to significantly improve the interface relationships between the plant operators and the reactor plant, and improve reliability, testability, maintainability and calibration, and thus total safety of reactor systems. On the other hand, the technology is relatively unproven in reactor applications and if not applied properly would introduce new problems which would result in net reductions rather than improvements to the overall safety of reactor plant operations.

The new technologies involved in advanced I&C are double edged swords: if used skillfully, they can provide many new benefits in safety and in other areas; if used clumsily, they can create new types of problems, such as operational complexities under unusual conditions or configurations. The challenge for the NRC is to develop mechanisms that are sensitive to discriminate whether this double edge sword is wielded clumsily or skillfully. In order to know when new technological possibilities have been used skillfully, we need to learn more about how

January 28, 1993

to value simplicity over complexity, how to verify that design objectives are being met, and to validate software performance to assure that no new modes of operation are being introduced.

The NSRRC has counseled on several previous occasions that the Commission's research activities (RES) should recognize the necessity to view this area as requiring a systems approach which integrates the human perspective (operator and designer) with that of the instrumentation and control hardware and software. An important potential for improvements in integration appears to be offered by advanced I&C systems.

RES has responded by taking steps in organizing and consolidating its program management. However, based on our review we believe there is much more to be done in establishing an overarching commitment to system integration between the reactor plant and its operators via I&C systems. Indeed, it appears to us that the NRC does not presently possess in-house capability to address adequately complex issues introduced by modern I&C technology.

Based on our discussions with your staff on December 9, we offer the following suggestions to develop the basis for a strategic vision for this area of research to strengthen the integration between humans and machines:

- 1) There should be a clearly stated management commitment to the subject of human factors throughout the NRC to further assure safety of reactor design and operations. The complex nature of the subject should be well understood by all levels of management starting with the Commission, and working downward through the Offices, Divisions, and Branches having responsibility for the development of guidance and standards and for the review and regulation of advanced I&C systems.

In the past, the history of the subject has appeared to be a "chopped sine wave." A reasonable effort is started, but terminated or significantly reduced before useful results are obtained.

- 2) An agency-wide strategic vision of the concept of integration of the human, hardware, and software aspects of reactor control and operations must be developed and clearly articulated. Such a strategic vision is an essential first step if the NSRRC's recommendation in its November 1992 report is to be achieved, i.e., "criteria to define what is meant by improved safety need to be established prior to undertaking major expenditures or function allocation research." The management process must proceed from a shared vision, to the establishment of requirements, to the setting of criteria. Research programs can then be defined, and performance expectations can be set for individual research projects.
- 3) As stated in my letter of November 16, "The NRC needs to identify those issues that are important to safety and to develop criteria which, if met, will assure that NRC safety concerns are satisfied."

January 28, 1993

A principal justification from the NRC's or industry's point of view for advanced I&C systems is improvement in safety. However, as stated above, if not properly understood and applied, advanced I&C systems have a potential to exacerbate rather than cure the disease. We propose, therefore, that RES develop a statement of criteria by which I&C systems will be judged specifically as to the benefit to overall plant safety. Such criteria, properly understood, would then serve to guide the several research efforts toward a more focused and integrated approach.

- 4) There is a great deal of information and experience in the area of advanced I&C outside the nuclear industry in the U.S. and outside the U.S. Canada, France, Germany, and Japan in particular are well ahead of the U.S. in developing an experience base. Within the U.S., the military, aviation, and other activities are well ahead of the nuclear industry in studying and applying modern I&C technology. There is also information being developed in Russia on error proneness in digital as compared with analog systems.

It seems obvious, therefore, that there should be a vigorous, focused effort in RES to obtain, assimilate and apply the large amount of experience and information available from these other sources. Certainly some of that is being done, but not enough. We propose that specific directed management steps be taken to strengthen these activities.

In that regard, members of RES staff, however limited in available effort, should accept as a personal responsibility the objective of becoming technically knowledgeable and expert in the several subspecialties of advanced I&C, rather than relying mainly on presumed laboratory or contractor capabilities.

- 5) There are within the U.S. institutions which have established reputations as centers of knowledge and competence in the field of advanced I&C. These include Carnegie-Mellon University and the Crew System Ergonomics Information Analysis Center (CSERIAC) at Wright-Patterson Air Force Base. The RES activities could benefit from closer working relationships with such centers--not necessarily by contract, but by visits, personal contacts, organized workshops, participation in expert reviews and the like. We note that three members of the ACRS have proposed recently a special workshop on this general subject to be organized and conducted by the National Academies.
- 6) Consideration should be given to additional steps to strengthen the RES organization with the objective of furthering integration of human factors with machine considerations, such as providing additional personnel with recognized capabilities in both I&C and human factors fields.

During the discussions on December 9, the subcommittee was told that there were certain RES products of special early interest to NRR, e.g., Reg. Guide for Class 1E Digital Computer Systems, and a basis for establishing criteria for regulatory positions on software. These did not

January 28, 1993

appear to be receiving priority attention for completion. In other cases, reports have been completed and sent to RES but have not been edited and issued.

If the advanced I&C program is to provide timely input to the certification process greater management attention to program planning, execution and completion seems needed.

A formal prioritization, with schedule dates and progressing actions to meet them, would improve productivity of contractors and RES staff, and lead to a more timely availability of research results to those who must make informed regulatory judgments.

In conclusion, we would like to offer several pertinent observations which may be helpful to you and your managers in carrying out your responsibilities in development of regulatory information in advanced I&C.

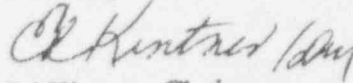
- 1) Software systems are unusual in their having certain characteristics of humans, i.e., error proneness. Like humans they very likely can not be made error free by V&V processes, but errors can be reduced to acceptable levels by sound engineering and the goal of error free operation should not be relaxed.
- 2) Digital systems offer immense processing capabilities. It is important, therefore, in applying them to nuclear operations to limit them to those which are needed for safe, reliable plant operations, and not confuse the operator with capabilities not useful in carrying out his necessary functions but are provided by the designer simply because they are available as a luxury.
- 3) There is a corollary conclusion. Experience and insight suggest that simplification of the operational functions could provide great benefits to safety in nuclear plant control rooms. There is little hard data to support that conclusion. A research of literature and plant or simulator experience which shows the relationships between operational simplicity and safety would be extremely valuable. In a sense, this is the heart of human factors I&C-reactor plant integration problem.
- 4) A clear programmatic distinction should be made between the issues encountered in the form-fit-function conversion of analog to digital systems in present plants and those encountered with advanced digital systems for future plants. While there are common issues facing the operators and the developers, the information base leading to their understanding can be significantly different.

Dr. David L. Morrison
Page 5

January 28, 1993

We appreciate the efforts of the RES staff in preparing for and conducting the presentations to the Subcommittee on December 9 and are prepared to discuss this report further with you if you so desire.

Sincerely,

A handwritten signature in dark ink, appearing to read "Ed Kintner", with a stylized flourish at the end.

Ed Kintner, Chairman
Subcommittee on Advanced Instrumentation
and Controls and Human Factors

DLM/sjc