

United States Nuclear Regulatory Commission
Office of Public Affairs
Washington, DC 20555
Phone 301-415-8200 Fax 301-415-2234
Internet: opa@nrc.gov

No. S-96-07

"DESIGNING FOR, AND ACHIEVING SAFETY IN, DIGITAL
INSTRUMENTATION AND CONTROLS"

BY

DR. SHIRLEY ANN JACKSON, CHAIRMAN
U.S. NUCLEAR REGULATORY COMMISSION
AT THE
AMERICAN NUCLEAR SOCIETY
TOPICAL MEETING ON NUCLEAR PLANT
INSTRUMENTATION, CONTROL AND HUMAN-MACHINE
INTERFACE TECHNOLOGIES
AT
PENNSYLVANIA STATE UNIVERSITY
MAY 8, 1996

INTRODUCTION

Good evening ladies and gentlemen. It is a pleasure to have this opportunity to address the American Nuclear Society's Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies. The nuclear power industry, along with virtually every industry requiring process control instrumentation, inevitably will move to greater use of digital technology to enhance reliability and safety, particularly as analog technology becomes increasingly obsolete. I believe that the proper use of digital technology will enhance safety in instrumentation and control systems as well as in human-machine interfaces within nuclear power plants.

Meetings of this type are important in fostering international cooperation to address common problems, share solutions, and determine future research needs on issues associated with the implementation of digital technology. The 200 technical papers presented at this meeting, with approximately half from overseas authors, demonstrate that a great deal of cooperation in this area has been achieved. Although the specific approaches to the acceptance of digital technology in nuclear power plants may differ from country to country, the overall objectives remain: ensuring that an appropriate level of safety has been designed into nuclear plants and once built, demonstrating that this level of safety has been achieved in the operating environment.

Before I describe how these objectives are being addressed by the NRC, I would like to make a quick pictorial digression. I know that a technical meeting such as this enjoys "visual displays." I also realize that you have had a long day. Therefore, I would like to share with you a few pictures from my recent trip to Japan's Kashiwazaki-Kariwa 6 (K-6) reactor, the first operational Advanced Boiling Water Reactor.

Slide #(3) Here you see an official "posed" group picture. Note how compact the control room is. Well lit, large displays. And by the way... the baggies on our feet are only for cleanliness.

(4)+(8) Note the operator's workstation and control boards. There is easy access to numerous computer screens.

(5) Here is a closeup of the center control board. The large overview display is a very effective summary of plant status. Note the diesel generator and electrical mimics on your right. Tracking right to left you see turbine controls, feed pump indications, and the containment boundary. Right above the main steam safety valves you can see the plant was at 350 Mw during my visit. Finally, on the far left - note the safety injection pumps with flow indications (all "0", obviously).

(6) To the right you have the large, easily read, alarm board. (even easier to read without that flash bulb reflection...)

(9) I was very impressed with the touch screen controls... and yes - I received permission before I actually touched anything.

(10) Note that the computer-based visual displays are very easy to read, with noticeable alarm status change of states.

(13) Finally, here is a picture of the entire control room. There was no need for a wide angle lens... everything is compact. What these pictures don't do justice to is the amount of information which can be accessed from this relatively small area - and the control and monitoring features that are available.

The K-6 plant, and its fully computer-based control room, is very impressive and is a significant accomplishment for the Japanese nuclear industry. I know that the NRC staff has been following the design and construction of K-6, since that plant represents the end result of an extensive review of its design, as part of the NRC certification of the advanced reactor designs. Almost three years have passed since the Commission approved the four point position for defense against common-mode failures in digital instrumentation and control systems. This position

ensured that designers, in relation to common-mode failures: (1) demonstrate that vulnerabilities are adequately addressed, (2) analyze each Safety Analysis Report accident analysis event, (3) establish, where necessary, a diverse means for fulfilling safety functions, and (4) provide independent displays and controls in the main control room to support the safety functions. I noted the defense-in-depth aspects of the Japanese advanced boiling water reactor design, and was shown several examples of diverse means for accomplishing the required safety functions should a common mode software failure occur. It was exciting to see the application of digital instrumentation and control systems on such a large scale in Japan.

BACKGROUND

Actual implementation of digital system modifications in operating U.S. nuclear power plants is not new - such systems have been in use since the late 1970's. Several of the later model Combustion Engineering plants were licensed with core protection calculators, comprised of a digital computer that calculates a conservative value of plant local power density and generates trip signals to prevent exceeding safety limits. Additionally, the NRC has noted since the late 1980's that obsolescence in current analog system equipment has forced an increase in the number and types of digital system upgrades proposed by licensees. Typical upgrades have been in the areas of neutron flux and radiation monitoring, feedwater and turbine control, portions of the reactor trip system, and others.

This move toward an increased use of digital technology on the part of licensees highlighted the need to update NRC review criteria - which dealt primarily with analog systems. The process of updating review criteria was not always smooth, as many of you know -- having "lived" through various reviews and policy discussions. There were many differing views on the safety of the use of digital systems. Efforts to fit digital technology into the well established regulatory requirements for analog instrumentation and control systems (e.g. redundancy, testability, and qualification) also had to be addressed. Ultimately, these efforts have led to the creation of what the NRC believes is a stable digital system licensing approach and an up-to-date set of technical review guidelines. These currently are being drawn together into a Standard Review Plan (SRP) for digital I&C upgrades, which I have asked the NRC staff to develop on an expedited basis.

DESIGN ISSUES

Digital systems offer a number of clear advantages over existing analog systems, such as resistance to drift, increased functional capability, process control flexibility, and user friendly human-

machine interface features. However, it is also clear, from interactions with digital systems experts and experience with a wide range of digital system applications, that these same advantages can lead to potentially significant problems, if the technology is not implemented properly. Key among them is the potential for loss of redundancy and corresponding safety function due to a common cause failure resulting from errors in the software. This concern obviously is not unique to the NRC and the U. S. nuclear power industry. It is an issue that comes up in virtually every interaction the NRC has had with its counterparts in other industries, and with regulatory authorities in other countries. Events involving software failures in non-nuclear industries, including telecommunications and medicine, have borne out this concern.

Events at nuclear plants also have served as reminders that even with the promise of a system that offers better reliability and accuracy, flaws in design and inadequate testing can cause troublesome system performance with the potential for adverse safety impacts. A report last year from the Massachusetts Institute of Technology's International Program on Enhanced Nuclear Power Plant Safety presented a case where a new "failsafe" digital upgrade to the annunciator system -- which assists nuclear power plant operators by providing status indication in the control room -- failed when an operator punched in a wrong command. The report identified that only the operator was disciplined, even though design and testing of the so-called "failsafe" system had been flawed. Although, a failure of this type highlights a system weakness, still, the advantages of digital technology clearly outweigh the disadvantages.

The challenge for the NRC has been to incorporate the advantages of digital systems, while maintaining the level of safety prescribed in the existing regulations and individual plant licensing bases. The experience gained from reviews of many digital system upgrades, the reviews of the advanced light water reactor designs, and interactions with experts in academia, industry and government (here and abroad) have led to the stable licensing approach discussed earlier, which we intend to be viable for future upgrades.

The licensing approach for digital systems to which I refer is similar to that used by most industry and regulatory authorities concerned with the safe application of digital technology. It consists of a two-fold demonstration-- (1) a high quality software and hardware design and development process, and (2) a level of defense-in-depth and diverse capability which recognizes that software cannot be made error-free despite a high quality design and development process. The software development process calls for effective documentation of the software lifecycle, including the requirements specification, and the verification

and validation program. The principal feature of NRC criteria for this demonstration is endorsement of industry standards on the quality of the software development process and other industry guidelines on digital system implementation. For the computer-based human-machine interfaces, the NRC staff has developed updated guidance, based on validated human factors engineering practices, such as display configuration, taken primarily from the military and aerospace industries.

CURRENT ACTIONS

Let me elaborate on something I briefly discussed earlier. In November of last year, based on briefings and concerns I had since joining the Commission, I directed the NRC staff to prepare a regulatory framework which would be applicable to the use of digital instrumentation and control in U.S. nuclear power plants.

In particular, the staff was tasked to expedite actions to ensure that safety margins are addressed, and to formally document the approach and criteria for review of digital system designs in an update to the Standard Review Plan (SRP). An initial draft should be ready for public comment by this September. The staff is also incorporating the new guidance on computer-based human-machine interface designs in the SRP update.

A primary part of this SRP update is (as mentioned earlier) the endorsement of industry standards - the very standards the nuclear power industry has used in the design of digital upgrades in the past. As with any new guidance, the NRC staff has begun a series of detailed interactions with the NRC Advisory Committee on Reactor Safeguards in order to obtain independent advice on the proposed digital system review criteria. However, because of the unique aspects of digital systems, and differing views on the means for ensuring digital system safety, the Commission determined that a further independent study of the staff's regulatory approach and guidance was appropriate. This study is being conducted by a panel of experts under the direction of the National Academy of Sciences. These experts have completed an initial review. They are now drafting recommendations which will be evaluated along with the public comments on the draft SRP update. The new Standard Review Plan guidance should be completed by the first quarter of next year.

Earlier, I mentioned NRC interactions over the years on issues of mutual interest with many different groups involved in digital technology, both within the U.S. and internationally. These exchanges have been a valuable source of information and experience upon which to draw for reviews of U.S. plant design proposals and criteria development. These interactions are continuing at many levels. Next month in Paris, senior management from the NRC Office of Nuclear Reactor Regulation will

attend the Organization for Economic Cooperation and Development/Nuclear Energy Agency (OECD/NEA) Special Issues Meeting on Licensing of Computer-Based Systems. At this meeting, regulatory authorities from many countries will discuss some of the same issues that I have mentioned in my remarks, and that you are addressing at this meeting. The timing of these various topical meetings demonstrates the continued importance being placed on digital systems safety and the attention the issues command.

During a recent trip abroad I spoke at both the Korea and Japan Atomic Industrial Forum meetings. On both occasions I underscored the similarity of the challenges that currently face the many nations with nuclear power programs. The effective display and accuracy of information available to reactor operators is one of the continuing challenges we all face. Given this, and recognizing the changing economic and regulatory environments all countries confront, it is important that we share not just technology and operating experience, but also better coordinate our combined resources to meet future challenges.

FUTURE CHALLENGES

While I have spoken of the challenge involved in the development by the NRC of a licensing approach and criteria for digital technology, I do not want to forget an additional issue for both the NRC and its licensees: the challenge to ensure that a sufficient level of knowledge exists to make informed decisions. This challenge is not new, but the ever-tightening availability of NRC resources highlights the necessity of extra caution. I believe the NRC, over the years, has made a significant effort to familiarize itself with the issues involved in the use of digital systems in nuclear power plants and has provided formal training to the reviewers to permit them to understand digital technology safety possibilities and concerns. The NRC has also benefitted greatly from DOE National Laboratories' expertise in both the reviews of digital systems designs, and in the development of review criteria.

It is equally important for licensees to recognize that their plant staffs must be familiar with the differences in operation, maintenance, information display, and modification of digital systems in order to avoid many of the problems experienced in the past.

I have spoken of the importance of the Standard Review Plan update for digital systems, and indeed it is important. However, the rapid evolution of digital technology will mean further changes in future systems. Maintaining our interactions with the nuclear power industry, through mechanisms such as this meeting,

is essential to ensuring that the NRC and its licensees are ready when future technological advances in instrumentation and control systems and the human-machine interface are proposed for implementation. If neural networks, fuzzy logic or voice-activated controls are proposed for nuclear power plants, the NRC must be able to address the regulatory challenges they present. Because the SRP is meant to be a living document, I am confident that the review criteria it contains can be further updated as needed to ensure the safety of new technology. It also is important that relevant areas of research are identified as new technology emerges, to assist in the development of any needed new review criteria.

CONCLUSION

In conclusion, I believe the NRC, in conjunction with the nuclear power industry, has accomplished much in recent years to stabilize digital systems licensing and criteria. We welcome your comments on the Standard Review Plan update when it is issued in draft form. I challenge you to continue to design for and to achieve safety in the use of digital systems technology in nuclear plants.

Thank you.