NRC NEWS

U.S. NUCLEAR REGULATORY COMMISSION

Office of Public Affairs Telephone: 301/415-8200

Washington, D.C. 20555-0001 E-mail: opa@nrc.gov

Web Site: http://www.nrc.gov

No. S-06-031

"Achieving Improved Nuclear Plant Safety Through Digital Technologies - The Regulator's Perspective"

Prepared Remarks
by Commissioner Peter B. Lyons

at the

Nuclear Plant Instrumentation and Controls and Human-Machine Interface Technology Embedded Topical Meeting

2006 American Nuclear Society Winter Meeting
Albuquerque, New Mexico

November 13, 2006

Introduction

Good morning. I want to thank the American Nuclear Society for inviting me to speak at this topical meeting, and also to thank my fellow panelists for their participation and the contribution of their perspectives today. I must note, as always, that I am speaking today as only one Commissioner.

As I've visited many nuclear plants in the U.S., I've been struck by the predominance of generally very old analog instrumentation. The age of these analog instruments and their increasing obsolescence over many years has clearly motivated industry's interest in using more modern digital replacements.

During my time as an NRC Commissioner, I have also had the opportunity to begin - and I really mean begin - learning about the potential safety benefits and the unique challenges associated with the application of digital technologies to nuclear power plant instrument and control (I&C) systems and the improvements that these technologies make possible for control room designs and operator interface. I've visited several facilities that incorporate such applications, from the plants at Palo Verde, San Onofre, and Waterford that use relatively simple core protection calculators designed in the 1970s, to the Advanced BWR Kashiwazaki Kariwa Units 6 and 7 in Japan using fully computerized control rooms. I've also seen the advanced control room digital retrofit at Oskarshamn Unit 1 in Sweden, the computerized control room of the Civeaux N4 reactor in France with its impressive human-machine interface (HMI), and the fully modern digital systems of the research

reactors at the OPAL facility in Australia and at Tsinghua University in China. I visited the Halden facility in Norway and came away very impressed with the research into digital systems and HMI being conducted there. I am also extremely impressed with the digital I&C systems of the newest reactors in the U.S. naval nuclear propulsion program, a program renowned for its rigorous standards and impeccable safety record. Finally, I'm certainly aware of other operating commercial power reactors around the world using digital safety systems with advanced control room designs and I hope to be able to visit some of these in the future.

The Opportunity for Improved Safety

The Commission itself is engaged in ensuring that we enable the benefits of this technology through the evaluation of its safety for nuclear plant applications. The most recent such engagement, one that many of you may have observed, was the Commission meeting on digital I&C last week via our webcast. Webcasting is a tool that has greatly enhanced public accessibility to our regulatory process, obviously achieved through the wonders of digital technology. But I know I'm "preaching to the choir" in touting such benefits to this audience.

As a technical person I'm drawn to the potential benefits of digital technology, but as a regulator I'm sobered by the challenge of the many failure modes that must be addressed for its intended safety-related uses. Nevertheless, as an optimist with a technical background, I believe it is possible through a systematic and thorough treatment, both by industry and the NRC, to enable the safe and beneficial use of this technology in nuclear power plants.

So the key message in my remarks today is that I believe digital I&C and safety systems offer the potential for improved HMI and safety performance provided that the failure and security vulnerabilities are thoroughly identified, understood, and mitigated. As a regulator, the potential for enhanced safety motivates our ongoing efforts to refine the regulatory requirements that enable such enhancements. As this country experienced a hiatus of new nuclear plant construction, we watched as highly integrated computerized control rooms were put into operation in international nuclear power plants. As we now prepare for potential new plant construction, I believe we must leverage this international experience to efficiently gain the safety benefits we seek.

NRC International and Research Activities

As an important step in this direction, the international Organisation for Economic Co-operation and Development (OECD), through its Nuclear Energy Agency (or NEA) recently became the Secretariat for an initiative, originated by former NRC Chairman Nils Diaz, to standardize worldwide nuclear power plant designs, regulatory reviews, and quality assurance standards to improve efficiency and promote safety and security. Known as the Multi-National Design Evaluation Program (or MDEP), the NRC recently joined nine other countries in launching this initiative, having already started a first stage effort to collaborate with the Finnish and French regulators on their reviews of the AREVA EPR design. As part of this first stage effort, the NRC is actively engaged in discussions with the Finnish regulator on their reviews of the digital I&C system for the Olkiluoto Unit 3 currently under construction. Although the MDEP participants include only regulators, interactions with industry are planned as an important aspect of this project.

In addition, the NRC continues to support the digital I&C and HMI research that I have already mentioned is being done at the OECD Halden Reactor Project. This work is aimed at addressing challenges that include the impact of rapidly changing technology, increasing complexity, new failure modes, system and human reliability metrics, new concepts of operation, and the need for updating acceptance criteria and review procedures. Halden is helping to provide us with a growing technical basis for more realistic safety decisions related to the software and hardware of digital systems, as well as the humans that operate and maintain them. This work includes developing surveillance and monitoring techniques based on advanced decision algorithms, particularly in the areas of on-line monitoring and diagnostics.

Also, I'm very pleased that Halden is working with the OECD's NEA to develop a new database, named Computer Systems Important to Safety, or COMPSIS, to collect digital system failure information to support improved operation and regulation of digital systems. The NRC encourages this effort and expects that it will improve our understanding of digital system failure modes and frequencies based on a worldwide data gathering effort. Halden also cosponsored a workshop in May with the NEA's Working Group on Human and Organizational Factors on "Future Control Station Designs and Human Performance Issues in Nuclear Power Plants," which will help focus human factors work at Halden and elsewhere.

Our international work is part of an NRC Digital System Research Plan that aims to address many related technical regulatory needs. This publically available Plan organizes our digital system safety research into categories of: system characteristics, software quality assurance, risk assessment, cyber-security, emerging new technologies, and advanced reactor I&C and control room designs. In its recent periodic review of the NRC safety research program, the Advisory Committee on Reactor Safeguards (ACRS) gave this Plan good marks. I was also pleased that they recommended further enhancements involving exploring the acceptability of international standards for meeting regulatory requirements as an element of an MDEP.

The NRC's research in this area has also sought to take advantage of the application of digital technology to safety-critical systems in industries beyond nuclear power. Specifically, we have been seeking insights from industries such as aerospace (including the International Space Station), medical devices, military, and foreign accreditation agencies such as TÜV in Germany. In seeking to utilize these insights, we are careful to ensure we fully understand the differences in their safety functions and the degree to which they are relied upon to control the hazards.

Cyber-Security Issues

Cyber-security is another major consideration for digital systems. Through my own work at our national labs, I am very familiar with the need to provide for cyber-security as part of any digital system. For example, the digital systems that provide highly useful plant parameter and status information to the NRC Incident Response Center and other authorized recipients during exercises and real events, like the soon to be upgraded Emergency Response Data System (ERDS), must be designed to absolutely ensure they do not provide any possible mechanism for an outsider to gain access or interfere with internal plant systems. In addition, viruses, trojan horses, and other malware remain a concern for any software-based system, and software used in safety or security applications must be protected through multiple strategies including effective configuration and access controls. The NRC is actively engaged in these issues, having revised regulatory guidance in 2005, reviewed industry

cyber-security program guidelines, and proposed new cyber-security requirements to 10CFR73.55. Through these efforts I believe NRC will be prepared to meet the evolving challenge of cyber-security.

Near-Term Retrofitting and Licensing Challenges

Moving now to the immediate needs and applications, I believe that continued and expanded NRC-industry dialog is imperative to maintain the focus of both NRC and industry efforts on the most important challenges for the retrofitting of existing plants and in potential licensing of new plants. Specific examples of the types of digital I&C system regulatory issues that must be addressed are:

- What is acceptable independence for inter-channel communication, for one-way and two-way communication, and between safety and non-safety channels?
- What are acceptable diversity and defense-in-depth?
- What is acceptable digital system reliability, and can it be estimated with any confidence?
- Will advances in digital technology create new failure modes that affect the reliability and maintainability of safety systems?
- How do we reasonably ensure that emergency preparedness, security, and safety of nuclear power plants are protected from cyber-threats?

For new plant designs, overall safety in a plant's design must be considered at every step, from initial concepts through high-level design certification to the final engineering design details, giving special consideration to the role and failure modes of the digital components. The first design certifications under 10 CFR Part 52, the ABWR, CE System 80+, and the AP600 and AP 1000 all required intensive industry/NRC dialog on the high-level architecture of the I&C systems and control room designs. However, much of the details within this high-level architecture remained purposefully undefined and open to new technological advances. The current design certification, in progress for the ESBWR, and for those that follow will all require this same dialog. As we delve further into actual design details, the level and extent of this dialog will need to expand.

For both retrofit and new licensing, the NRC is working to clarify digital-based safety system regulatory standards and acceptance criteria in updates to regulatory guides and the Standard Review Plan. At its most fundamental level, this dialog must lead to regulatory requirements that address:

- The taxonomy of possible digital system failure modes,
- How each failure mode can be mitigated, and
- For a specific plant design, how overall plant safety will be maintained in the event of a digital system failure.

I personally will continue to value the advice of our Advisory Committee on Reactor Safeguards, which should stay very active in these matters.

A significant challenge moving forward into the future will be to keep regulatory guidance current with the pace of digital technology progress. Rulemaking cannot always keep pace - so we need to rely on guidance documents that can. I see no other answer than for the staff, nuclear research community, and the nuclear industry to maintain a joint and active engagement with the larger multi-industry technical community for this rapidly evolving technology.

Advanced Control Room Designs

Until now I've primarily discussed issues associated with digital system safety. But today, building on a wealth of experience from other industries as well as the nuclear power industry, human operators and their information gathering and cognitive processes are being considered to a greater extent than ever before in the design of NPP information displays and controls, aided by ongoing and extensive research. Once again, and in no way to minimize other research work, the example with which I am most familiar is the work at Halden.

Halden experiments include those related to human error, human performance, teamwork and the effects of computer-driven interfaces on human performance. We in the U.S. don't have a reconfigurable simulator for research use, so access to Halden's facilities is invaluable. The Halden simulator can be driven by either a PWR or BWR model, and offers a prototype reconfigurable advanced control room with an integrated surveillance and control system, data collection facilities, and capabilities in virtual and augmented environments. This is a unique resource operated by a staff of knowledgeable and dedicated I&C and Human Performance researchers.

We have used the results of Halden human factors research as an input to our technical bases for regulatory guidance in areas such as alarm systems, control room design, display navigation, and development of human performance measures. The results have also been used as part of the basis for our Standard Review Plan. These guidance documents are for use in reviewing changes to control stations at current reactors, for licensing reviews of new reactors, for license amendment requests, and for plant inspections.

Halden researchers are also investigating the effects of context, task complexity factors, sustained workload and work practices in computer-based control rooms and team cooperation in new operational settings. Future plans include investigating human system interfaces that

- deliver relevant data and information in comprehensible and understandable formats,
- present the data and information in a manner that does not cause cognitive overload or confusion, and
- will be useful for developing guidance for new advanced control rooms.

In addition, the Halden research in virtual environments is an application of exciting new technologies to support human-factors-design input into control room configurations, into radiation (and possibly fire) visualization methods, and into virtual reality-based team training.

Human Resources and Technical Expertise

One of my continuing areas of concern since becoming a Commissioner has been the overall need for the NRC and industry as a whole to attract new people to reemerging work in nuclear power in order to build and maintain the necessary pool of talent to successfully accomplish growth without compromising the safety performance of existing plants. One of the most significant of these challenges is that we are competing for digital system technical expertise with many other industries in a very competitive job market. At the NRC, I believe the solution will be a balance of attracting and building in-house expertise combined with close links to the expertise at our national laboratories and with programs and facilities that are part of the larger technical infrastructure and communities-of-practice for digital systems across all the industries that use these systems for safety or critical functions. By maintaining our connection with this larger infrastructure and utilizing organizations with broad expertise among many industries, we would expect to efficiently be able to take advantage of the most applicable and relevant national and global work being done on safety-critical digital systems.

Another perspective on this same point is that the move toward state-of-the-art I&C systems and HMI in our power reactors and away from antiquated and obsolete technology will certainly enhance the interest and recruitment of the next generation of students to the nuclear industry. But unfortunately, as I visit research reactors throughout the U.S., I am struck by our national failure to upgrade the instrumentation and controls at our research reactor facilities to state-of-the-art capabilities and the negative impact this must have on our ability to attract new students.

A final perspective on this topic is the need for NRC to stay current in training its own staff on digital system technology and regulatory requirements. We use self-study courses in programmable controllers and early next year will launch a new course for our inspectors and other staff on the fundamentals of digital system design, licensing, and operations as used in the nuclear power industry.

Closing

In closing, I will reemphasize my key point: Digital I&C and safety systems offer the potential for improved HMI and safety performance provided that the failure vulnerabilities are thoroughly identified, understood, and mitigated. Achieving this potential will require industry, the research community, and the NRC to work through new and complex technical issues systematically and thoroughly, with the constant mutual goal of justifying the adequacy of overall plant safety. Further, to accomplish this efficiently, we must all seek to fully leverage the experience of others in the international community who have moved ahead in applying digital systems to nuclear power plants.

Lastly, based on my personal experiences, I have long been concerned that we temper our enthusiasm in creating complex computer models with the recognition that our models must be verified against experimental data wherever possible and practicable. We must then always remember the level of validation when judging the extent to which such models can be relied upon for decisions. An extension of this concern is that, although we have an ever-expanding set of new tools to create digital I&C systems that function in more and more complex ways, like the ‘brain and nervous system’ of a nuclear plant, I also believe that we must constantly remind ourselves that increasing complexity will exponentially increase the cost of demonstrating and maintaining safety and also the difficulty in detecting and correcting problems.

I am encouraged by the ongoing dialogue between NRC staff and the industry to tackle topics such as inter-channel communication, improving the methods to achieve defense-in-depth and diversity where necessary, cyber-security, and advanced control room design. As we continue this dialogue and move forward, I think it is useful to remind ourselves that the greatest difficulties reside in the multitude of details that must be considered. Therefore success will require a constant discipline to master the complexity to ensure it serves only the cause of safety.

I believe a brief quote ascribed to G.F. McCormick says this best, taken from Dr. Nancy Leveson's book, Safeware - System Safety and Computers, A Guide to Preventing Accidents and Losses Caused by Technology:

> *Software temptations are virtually irresistible. The apparent ease of creating arbitrary behavior makes us arrogant. We become sorcerer's apprentices, foolishly believing that we can control any amount of complexity. Our systems will dance for us in ever more complicated ways. We don't know when to stop. . . . We would be better off if we learned how and when to say no.*

As I noted earlier, I'm an optimist with respect to my confidence that this industry, the research community, and the NRC together will systematically and thoroughly address the safety aspects of applying digital systems to nuclear power plants. This embedded topical meeting is an excellent forum for the necessary information exchanges in support of focused and constructive dialog. I very much look forward to meeting the challenges ahead.

Thank you.

###