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
Site: http://www.nrc.gov

No. S-08-026

Opening Remarks

by The Honorable Peter B. Lyons

Commissioner, U.S. Nuclear Regulatory Commission

at the

Digital Instrumentation and Control and Human-Machine Interface Professional Development Workshop

2008 American Nuclear Society Annual Meeting
Anaheim, California

June 8, 2008

Good morning. I want to thank Ted Quinn for inviting me to provide opening remarks at this professional development workshop on a topic I consider of vital importance both to the nuclear industry and the NRC. Although I've spoken on this topic several times now, including at the 2006 ANS meeting in Albuquerque, I am certainly not an expert. But I'd like to give you my perspective based on what I've seen in my travels and what I've heard from both the NRC staff and the industry. I must note, as always, that I am providing my personal views today as only one Commissioner.

It is clear that the age of digital technology at nuclear power plants and other nuclear facilities is upon us, and I'm extremely pleased that you are willing to give up a portion of your weekend to learn more about it. In addition to replacements of specific systems in existing plants, the new reactor designs under review at the NRC will incorporate digital I&C and safety systems in a highly integrated fashion, with the potential for improved human-machine interfaces as well as greater precision in monitoring and controlling plant functions to maintain safety.

Highly integrated digital systems have been successfully used to provide safety-critical control functions in other industries, such as commercial aviation and the NASA space shuttle, as well as the nuclear power industry in other countries. These systems have demonstrated greater

reliability over analog systems by using features such as on-line diagnostics. It is clearly time for the U.S. nuclear industry to take advantage of such gains.

But we must proceed thoughtfully and cautiously. Along with the significant potential benefits offered by digital technology, there are new (to us) and complex technical and regulatory issues. We all know the maxim that quality can't simply be verified at the end of a process. Plant designers and digital I&C system designers must join together and begin with the safety end in mind, recognizing that design features based on fundamental defense-in-depth safety principles need to be incorporated throughout the design process. If your work, now or in the future, includes involvement or management in this area, it will be up to you to ensure that the design process is implemented with a high degree of discipline.

In our reviews, the NRC will continue to be disciplined in applying the fundamental concepts of defense-in-depth. Independence and diversity are the key supporting concepts. As digital I&C system designers increase the number and types of software and hardware interconnections and resource sharing between components in pursuit of better overall system performance, the NRC must equally increase the scrutiny of how the designers have achieved the necessary independence and diversity to address common-cause and other failures.

I believe being disciplined also means that all of us, including designers, researchers, and regulators, must be systematic, methodical, and thorough in identifying and cataloguing all the ways that digital systems can fail. This means identifying, documenting, and addressing all known failure modes of software, hardware, and the interactions between the two. I have previously spoken on the need for the creation of a taxonomy or catalog of these insights. Such insights must be gathered from the designers, from our regulatory reviews, and from our operating experiences both domestically and internationally. The cataloging process must be ongoing and result in an expanding knowledge base that NRC can use to help ensure that our regulatory requirements remain comprehensive. I note that our Advisory Committee on Reactor Safeguards (or ACRS) recently gave similar advice to the Commission and staff regarding the staff's draft Interim Staff Guidance on reviewing new reactor digital I&C probabilistic risk assessments, or PRAs. Based on a literature review, the ACRS offered a sample list of application-independent classes of failure modes. Whatever such a list or catalog might turn out to look like, I believe that it can only help add discipline and structure to the regulatory and technical framework within which we must all communicate effectively to be successful.

I brought with me today copies of two recent public ACRS letters (dated April 29, 2008 and May 19, 2008) on digital I&C matters and the NRC staff's public response to one of them, to share with you. I hope it will enhance your course by contributing some of the most current regulatory dialog on these matters.

One of the ACRS letters also commented on the NRC staff's review guidelines for cybersecurity. Through my own work at our national labs, I am very familiar with the need to provide for cybersecurity as part of any digital system. All digital systems installed in a nuclear plant must be designed to prevent an outsider from defeating or challenging the safety systems in

the plant. The NRC is actively engaged in these issues, by developing regulatory guidance, having strengthened the cyber threat component of the design-basis threat, reviewing industry cybersecurity program guidelines, and proposing new cybersecurity regulations. One area of current high interest is the regulatory interface between NRC and the Federal Energy Regulatory Commission (FERC). As the NRC, FERC, and the industry work on addressing cyber threats to our electric grid and power plant critical infrastructures, we must all continue to maintain an acute awareness of how digital systems can open new vulnerabilities to malevolent intent.

In closing, I would note that as digital technology continues to evolve, it will continue to inspire great creativity and enthusiasm to innovate and take advantage of the increasing capabilities. Our world history is a continuum of tremendous positive advances made possible through new technological development. But I am also mindful of a quote I saw from someone who had a more pessimistic view of the nature of digital technology, saying*:

> *"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."*

Although I do not believe this quote accurately characterizes today's nuclear plant I&C designers, it does provide a vivid cautionary image that we should not forget as we all maintain a disciplined approach to the utilization of digital technology.

I thank you once again for your interest in learning more about this subject. I encourage you to continue actively increasing your knowledge of this technology, so that together the industry and the NRC will keep the *safe* in digital safety system designs.

Thanks for your kind attention and have a great course and a great conference.

*G. F. McCormick quoted by author Dr. Nancy Leveson in *Safeware - System Safety and Computers, A Guide to Preventing Accidents and Losses Caused by Technology*