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-07-028

Keeping the "Safe" in New Digital Safety System Designs

Dr. Peter B. Lyons, Commissioner
U.S. Nuclear Regulatory Commission

Keynote Address
to the
IAEA International Conference on
Common-Cause Failures of Digital Instrumentation and Control Systems in Nuclear Power Plants

June 19, 2007

I. Introduction and Overview

I want to add my welcome to all of you in attendance at this conference and particularly to those who have traveled far. I am extremely pleased that you have made the effort to be here. I truly hope that you find this conference and its information exchanges beneficial in helping us all to better achieve nuclear plant safety through the benefits of digital technology. My remarks today represent my personal thoughts and not necessarily those of the Commission.

The common-cause failure theme of this conference is of great interest and importance to nuclear regulators throughout the world. Much thought and debate have been devoted to it for many years. I note and am encouraged that practical solutions have already been implemented to address it. However, the continuing advance of digital technology and the increasing world-wide interest in "all-digital" new nuclear plants have combined to make it imperative for us to continue constructive dialogue and the identification of practical and safe solutions. I believe that significant improvements to safety-system reliability can be gained through the use of digital technology, provided we don't lose focus on keeping the "safe" in new digital safety system designs.

II. Historical Perspective

Let me start with some Nuclear Regulatory Commission (NRC) history that I have found to be very insightful in understanding this issue. Software-based nuclear plant safety systems deployed in the U.S. in the 1980s, such as the Combustion Engineering Core Protection Calculators or CPCs, were considered safe by the NRC, largely due to being designed as a single digital component of a much

more extended analog safety system. Thus, every safety function initiated by these CPCs had at least one analog backup. The use of CPCs enabled more precise computations of plant operating parameters, thereby reducing uncertainties and allowing greater operational flexibility. Because the analog channel was diverse from the digital channel and could equally and redundantly fulfill the safety function when needed, the question of common-cause failure of the digital channels was not a significant concern.

In the early 1990s, the NRC began reviewing advanced reactor designs developed by General Electric, Combustion Engineering, and Westinghouse. At about the same time, the U.K. regulator was similarly reviewing the Sizewell B design. I understand that great debates took place among these regulators, their advisory committees, and the nuclear and computer software industries. Such debates were far ranging across a wide spectrum of issues. Questions included whether it would ever be possible to estimate the probability of common-cause and other design flaws leading to software failure that could impact reactor safety. Technical questions were debated, such as whether "hard-wire" or analog backup instruments and controls were needed to implement the concept of diversity, or whether diverse digital systems would suffice. To help resolve these debates, the NRC commissioned a study panel of the National Academies of Science and Engineering.

The 1997 report from this study panel supported the NRC staff's approach that common-cause software failures were credible, and it recommended maintaining diversity in digital safety systems. The panel recommended that the staff not rely heavily on techniques, such as different programming languages, different design approaches meeting the same functional requirements, different design teams, or using similar equipment from different vendors. The recommendation was that the staff should emphasize more robust techniques, such as the use of diverse inputs and processing algorithms, diverse hardware, and diverse real-time operating systems.

The panel also agreed with the NRC position that common-cause failures could be addressed using diversity in a number of different ways dependent upon plant-specific factors, including use of diverse digital systems. In fact, designs certified by NRC in the 1990s permitted the use of an added non-safety-grade diverse digital system to address the common-cause failure potential for important safety functions. To me, this seems a relatively straightforward approach to address the issue of digital-system common-cause failure.

As most of you are aware, international approaches to addressing common-cause failure in digital safety systems vary widely, but most are grounded in the application of varying degrees of diversity and independence to safety system components and functions. In fact, I am aware that at least one design certification application being prepared now plans to incorporate a diverse analog backup safety system to address common-cause failures of the primary digital safety system.

I believe that there are very real safety benefits that can be achieved through the use of digital systems in nuclear power plants, but to address persistent regulatory questions regarding some of the new approaches being taken, the Commission recently directed senior NRC managers to engage industry and establish a project plan to address these questions.

So I'd like to further discuss some of my initial thoughts on the application of independence and design techniques such as functional diversity in the application of the defense-in-depth philosophy to digital safety systems.

III. The Application of Defense-in-Depth Principles to Digital Systems

Digital safety and I&C systems have already demonstrated greater operational flexibility through (1) more precise calculations of plant parameters and safety margin and (2) greater reliability over analog systems by using features such as on-line diagnostics. However, ongoing advances in digital and human-machine interface technology can potentially lead to digital systems that more closely couple the various hardware components and software logic, thereby raising regulatory questions about the extent and adequacy of independence and diversity. In the U.S., the nuclear industry has argued that the familiar approaches to achieving defense-in-depth in electro-mechanical safety systems must be modified when they are applied to digital systems. I have considered that idea and offer the following thoughts.

First, we often use the term "diversity" and "defense-in-depth" as if they were two separate concepts. However, if defense-in-depth is viewed as the overarching objective, then diversity as well as redundancy and the implicit assumption of independence are three of its most important contributing elements.

We all know that traditional defense-in-depth concepts in the nuclear power industry often involve multiple and identical redundant electro-mechanical safety system trains, and in some cases, include additional diverse systems that can satisfy the same safety function, using alternative means. Inherent in these concepts of redundancy and diversity is the presumption of independence. Each train of each system that is capable of providing the safety function is designed to avoid being adversely influenced by the actions or failures of the other trains. Traditionally, for electro-mechanical systems, such independence has been achieved using separation: spatially, mechanically, electrically, and by utilizing separate sensors, communications, and controls. As redundant and/or diverse system components are designed to become more interconnected, and previously separate means of performing safety functions are combined into one system, it becomes increasingly important to understand the nature and effect of possible interactions between these components and to guard against unintended adverse outcomes. I believe the need to fully understand such effects is fundamental and, therefore, that it must also apply to digital safety systems.

The basic rule, as I see it, is that there are two determinations that need to be made. The first is to determine that the interconnections actually have a safety benefit. In some cases, designers may use interconnections for ease of installation or to avoid the need to redesign a commercially available system. Second, when two components of a system are designed to be more and more intertwined and coupled, greater and greater attention and effort must be paid to guarding against adversity while preserving the intended advantages of the coupling. From a regulator's point of view, we must continue to apply the fundamental concept of achieving defense-in-depth through, in part, independence of redundant and diverse safety system components. Independence and diversity are the key concepts, and there are presently no other safety concepts or approaches to take their place. 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 regulator must equally increase the scrutiny of how the designers have achieved the necessary independence and diversity to address common-cause and other failures.

I do not doubt that we can certify future digital I&C designs in which the treatment of common-cause failure may depart significantly from those designs already certified by the NRC, assuming full and proper attention is paid to the issues of independence and diversity, leading to adequate overall

defense-in-depth. The question for applicants today is one of whether at this point in time it is worth using significantly different digital-safety-system design concepts that raise new questions, which the designers, applicants, and regulators must ensure are addressed for adequate defense-in-depth. Although the NRC is actively working on updating our regulatory guidance in this area, current designers would do well to 'begin with the end in mind' and, at the very beginning, anticipate the regulatory safety case that must be made at the end.

I recognize that part of good regulation is being clear about the standard to be met. However, as standards become more precisely defined, they can often become more limiting. Given the continued rapid advance of digital technology, I worry about being an overly prescriptive regulator. Here I would emphasize that in setting its current standard, the NRC's definition of diversity can be applied at several levels, including at the component level of the digital safety system, or at the level of the mechanical systems that can provide the safety function, or even at the level of safety system functions themselves.

IV. The Big Picture

Common-cause failures are just one type of digital system failure. There are many more. So, I would like to turn to a discussion of the "Big Picture" view, encompassing the broadest definition of digital-system failure modes. We have found probabilistic risk assessments, or PRAs, to be a useful Big Picture tool, which are aimed at understanding overall system failure as a function of individual failures of system components following various initiating events. Such tools can help us better understand the risk of a system's operation in those cases in which it is impossible to test the overall system reliability. It is widely acknowledged that digital systems, beyond the simplest of designs, cannot be demonstrated as having achieved a minimum reliability standard through testing. So industry attention and NRC research is being devoted to examining whether it is possible to incorporate digital system failures into probabilistic risk assessment models.

A decade ago the great debate over this question was almost philosophical in nature. Today, the NRC is continuing to explore this question, and I cannot predict how it might be answered in the future. But I do know that in order to estimate the probability of failure of any system, digital or otherwise, for starters, you need to know <u>how</u> the various parts of the system can fail – individually, collectively, and synergistically. That is, each of the most basic elements of a probabilistic model must be defined before it can be given a failure probability or event likelihood. Such basic element failures are then logically connected to represent collective failures that could contribute to overall system failure. Synergistic failures must also be represented in the model and should include common-cause failures as well as consequential failures.

My point is that at the heart of these modeling assumptions is one fundamental assumption: that is, we assume that we have identified the basic failure causes, failure modes, and connections between failures. Given the complexity of digital systems, I believe that it might be helpful to create a catalogue of digital failures, organized to better enable industry and the NRC to systematically and methodically address each known failure mode, to coherently add to the knowledge base over time as operating experience accumulates, and, perhaps, to provide the basis for defense-in-depth evaluations, PRA models, or similar uses. At the highest level, such a catalogue might start with three broad categories of failure: hardware failure, software failure, and combined or synergistic hardware/software interactive failures. The message here is that a systematic approach to cataloging digital system functions and failures can be potentially very helpful to both the designer and the

regulator. This was also reinforced by the NRC's Advisory Committee on Reactor Safeguards, highlighting the need for an inventory and classification of digital software systems to support our analysis of the susceptibility of these systems to failures.

A second important Big Picture issue is the need for gathering, sharing, and using digital-system operating experience. The need to broadly share such experience was also emphasized by the advisory committee. Useful insights can even be obtained from experience with non-safety digital systems and from outside the nuclear industry. The U.S. stands to benefit from such international efforts as we move toward deployment of new plants. The U.S. should also provide increasing contributions to such a base of knowledge. The infrastructure for managing this sharing of experience is already beginning to take form, but must be managed to ensure we do not duplicate efforts and that we capture the most useful information. I am aware of the COMPSIS and OECD/NEA initiatives in this area and hope that as we move forward we continue to collaborate and stay coordinated. The Big Picture is that sharing operating experience becomes even more vitally important for systems where testing cannot be expected to "shake out" all the potential failure causes and modes. Thus, the NRC is working closely with other international regulatory bodies to learn and to share insights.

A third Big Picture issue for the NRC is that currently we are addressing the regulatory challenges of digital systems by using the test and analysis capabilities of our national laboratories, universities, and international research centers, as well as our own staff resources. The research through such varied contractor arrangements is conducted in a case-by-case fashion in which research topics are not always fully or efficiently integrated where appropriate. This approach has made regulatory improvements slower than we need them to be to keep up with advancing digital technology and the science of human-machine interface approaches. In addition, in a recent report prepared by the Idaho National Laboratory for the Department of Energy addressing the need for I&C and human-machine interface to support DOE's advanced nuclear energy programs, the lack of a national simulation facility to provide a test bed for the nuclear industry is discussed.

To close this gap, the Commission has directed its staff to begin a public dialogue on the potential benefits and challenges of a research, test, and evaluation facility in the U.S for digital safety system applications. My hope is that such an integrated facility would create synergies and efficiencies not evident in our current approach. Also, I believe this could better attract new graduates and experienced professionals in this highly competitive field. Possibilities include the participation of other government agencies and industries in examining issues, including hardware and software configuration, system requirements, maintenance approaches, normal and adverse environmental conditions, faulted condition performance, and a variety of human-machine interaction approaches, all evaluated under controlled conditions representative of those in nuclear facilities and in other safety-related applications outside of the nuclear industry.
I am pleased to announce that this dialogue will start with a public workshop to be held (tentatively) in Atlanta, Georgia, on September 6 and 7, 2007. More information is available from our NRC website at www.nrc.gov. I hope you will consider attending or at least letting your colleagues know about it.

V. Closing

So in closing, let me again emphasize my key points:

First, today's and tomorrow's digital technology can be put to good use in improving the effectiveness of human-machine interfaces and the precision by which we monitor and control reactor parameters to maintain safety at all times.

Second, reactor designers, and digital safety and I&C system designers in particular, must begin with the safety end in mind and recognize the fundamental regulatory principles that will ultimately need to be satisfied. These require achievement of adequate defense-in-depth based, in part, on independence of the means to satisfy each safety function. The goal to keep the "safe" in digital safety system design is absolute and must be met. To achieve this, we must find the appropriate ways to apply the concepts of redundancy, diversity, and independence with digital system designs.

Third, designers, researchers, and regulators need to be systematic, methodical, and thorough in identifying and cataloguing all the ways that digital systems can fail. We need to share these insights broadly, deriving them from design work as well as from our collective operating experience.

Finally, regulators should continue to improve the clarity and usefulness of regulatory requirements and standards for digital technology and must find better ways of evaluating these new designs, which will surely continue to evolve into the future.

I am pleased that the Commission is taking an active role in ensuring that adequate attention is being paid to addressing these issues. Thank you for your attention, and I hope you have a very informative and productive conference.

###