



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-07-040

August 29, 2007

The Human Factor in Nuclear Safety

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

Joint IEEE Conference on Human Factors and Power Plants and
Workshop on Human Performance - Root Cause - Trending -
Operating Experience - Self Assessment

Monterey, California

August 27, 2007

Introduction

I welcome all of you to this first joint meeting between IEEE's conference on human factors and power plants and the human performance, root cause, trending, operating experience, and self-assessment workshop (HPRCT). There is clearly an extensive range of topics being explored this week, but the two groups that have joined together for this meeting also appear to share many similar objectives. I commend all of you for taking this mutual step, for I strongly believe that opportunities such as this can promote great synergism in information exchanges and help us all to better achieve nuclear plant safety now and into the future. As usual, I must preface my remarks today with the statement that they represent my personal thoughts and not necessarily those of the Commission.

Optimizing the Human Factor

The title of my speech today begins with "The Human Factor," and is meant to emphasize the importance of the human element. I did not use the term "Human Factors" since that term is often used as a label for a long list of interrelated research areas. I am taking this approach today because of a fascinating discussion I had recently with one of the operators who was at the controls of Three Mile Island Unit 2 on the night of the accident that became a defining event for this industry and for the NRC. Although I had already read with great interest the official reports of that event, hearing it and re-living it through the personal story of one of the actual operators made me profoundly aware of the nature of the relationship between operator and machine. That relationship seems to be defined by a constant tension between what might be called "oneness" and "separateness."

For example, there is often a certain sense of connection between operator and machine. The former TMI operator discussed his need to feel this connection through the controls and instruments of the

plant, and he expressed his own concern that such a feeling could be lost in an all-digital, control-room environment. I think most of us can relate to such a feeling, for example, as we drive our cars and “feel” that connection through all of our senses as well as the instrument panel. I can imagine that race car drivers and airplane pilots are even more attuned to this feeling of connection to their machines and the environment in which they operate.

Popular movies often examine the degree of connection between computers and humans as the means to explore our relationship with machines. Such stories can be entertaining, but nuclear professionals need to deal with the reality of the Human Factor, that is, the question of “what is the optimal degree of connectedness, both physical and cognitive, that should exist between operators and the plants they operate?” I suspect that many of you here today have made professional careers out of answering this and associated questions.

For the designers and regulators of nuclear power plants, I submit that the “optimal” degree of connectedness should relate predominantly to overall plant safety. I probably wouldn’t get any argument on that point, but I also acknowledge that the devil is always in the details. I believe that digging into those details means staying well-grounded in real operational environments. Designers, engineers, researchers, scientists, and regulators must stay grounded in the details of reality by putting themselves in the shoes of real operators and in their real environments and experience their world through their senses. Or, as one Human Factors pundit once said, “Humans are infinitely creative when it comes to making mistakes.”

Although I am using cognitive and physical operator interfaces as the example here, this question of what is the optimal degree of human connectedness might also apply more broadly to areas such as safety culture, organizational performance, root cause analysis, fitness for duty, and knowledge management. In these cases, the answer might be different than for the control room example. For example, in the case of safety culture, the concept of optimum human connectedness might have far more to do with optimizing the questioning attitude of plant personnel. My point is that these broader areas of interest are also vitally important to understand, and my message to you is the same: you must stay well grounded with the real people, doing the real jobs, in their real environments.

A Human Factor Taxonomy

The history of our technological advances is replete with examples of how the Human Factor has contributed to countless events and accidents, both large and small, serious and minor. Stories and anecdotes can help convey the sense of its potential importance, but we still need a taxonomy of some kind to systematically organize and sort all the aspects of the Human Factor that should be considered in the design of a machine, a technical enterprise, an industrial facility, or a nuclear power plant. Those of you who are specialists in human performance and reliability or in organizational factors may already use various taxonomies in your work.

However, let me offer a simple one - one that applies very broadly to all human enterprise in general. It has only two categories: first is the ways in which accidents have happened before, and second is the ways in which accidents could happen in the future but that have not happened yet. The first category provides us with lessons that we must apply so those particular failures and accidents do not happen again. The second category requires both creative and systematic thinking about how things can possibly go wrong that have never happened before. Complicating this is the relentless advance of technology. How we go about understanding what went wrong in the past and predicting what could go wrong in the future must constantly change as the underlying technologies change and evolve. The advent of computer-based safety systems and highly integrated control rooms is a clear example.

Category 1 - Learning Lessons

Let me briefly examine each of these two categories of my Human Factor taxonomy in more detail, starting with the first category involving learning from experience. Broadly sharing and using operating experience is really the only means to address this category and to avoid repeat problems. To help accomplish this, the NRC is working with other international regulatory bodies in countries in which highly advanced computerized control rooms were put into operation during a time when the U.S. was experiencing a hiatus of new nuclear plant construction. However, during this same time, several U.S. vendors developed digital I&C systems for use abroad, so our industrial expertise in this area was clearly advancing, even if the systems weren't in use here.

As the U.S. now prepares for potential new plant construction, we are fully leveraging this international experience to help gain the safety benefits we seek. The NRC's research in this area also looks to industries beyond nuclear power. Specifically, we have been seeking insights in areas such as aerospace, transportation, petrochemical applications, medical devices, and the military. In utilizing these insights, we are being careful to fully understand the differences in their safety functions and the degree to which they are relied upon to control hazards.

The U.S. stands to significantly benefit from international experience and, to the extent that advanced nuclear plant designs are licensed, we will also be providing increasing contributions to the international knowledge base. The infrastructure for managing this sharing of experience is already beginning to take form, and we must be careful to capture the most useful information and not to duplicate efforts. For example, the international Organization for Economic Co-operation and Development (OECD), through its Nuclear Energy Agency (or NEA) recently became the Secretariat for an initiative originated by NRC. Known as the Multi-National Design Evaluation Program (or MDEP), 10 countries are currently participating in this initiative to standardize worldwide nuclear power plant designs, regulatory reviews, and quality assurance standards, to improve regulatory efficiency, and to promote international safety and security. A first stage effort is for NRC to collaborate with the Finnish and French regulators on reviews of the AREVA EPR design. The NRC is actively engaged in discussions with the Finnish regulator on its 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.

Also, I'm very pleased with the NEA's development of a new database, named Computer Systems Important to Safety, or COMPSIS, to collect digital system operating experience information to support improved operation and regulation of digital systems and its continued sponsorship of workshops on human and organizational factors. The NRC encourages and supports these efforts.

Examples

As I've noted, specific examples of past problems can be useful as anecdotes that remind us of the importance of the Human Factor. It is in that light that I would like to offer the following examples based on my recent readings that have struck me as particularly noteworthy. They range from the amusing to the deadly serious. My purpose in presenting them is not to minimize the significant improvement in safe operations that have resulted from carefully designed systems, but to call attention to the pitfalls that await anyone who does not thoroughly confront the challenges of designing human-machine interfaces and digital controls.

One example of bad human interface design was the cockpit control panels of the B-17 bombers in WWII. It was cheaper and faster to design and build the panels using a series of closely spaced toggle switches. Unfortunately, two of these adjacent switches were the flaps and the landing gear. When they were initially deployed, it was not uncommon for a just-landed and taxiing B-17 to suddenly belly-flop onto the concrete when the pilot mistakenly hit the landing gear toggle instead of the one for the flaps.

Another example of poor human interface design was the modification made to many U.S. police cars in the 1990s that coupled the brake lights to the roof flashing lights so that the brake lights would flash on and off with the roof lights. Unfortunately, in many vehicle models the brake lights were part of the interlock circuit that prevents the shift lever from moving out of park unless the brakes are engaged. This, of course, is intended to be a safety interlock. However, on these modified police cars this safety interlock was actually turning on and off with the flashing lights. This came to light in 1999 only in an accident investigation for a tragedy in which a parked police car was shifted into gear at full throttle, hitting several parade-goers. This can serve as an example of the problems that can happen from connecting safety systems together, either inadvertently or by design, without careful analysis of all the implications.

These are just two of many examples in a fascinating book I recently read entitled “Inviting Disaster - Lessons from the Edge of Technology,” by James Chiles. I encourage you to read it, as it is one of the most informative that I have seen on the subject.

In the medical field, the NRC noted that through the 1980s to mid-1990s the number of misadministrations from computerized radiation therapy machines was increasing. Its review determined that nearly half of the events studied involved interface deficiencies that included cryptic or misleading error messages and problems in the data entry routines. One of the most thoroughly studied of medical misadministration events was the THERAC-25 radiation therapy machine that caused significant overdoses of radiation in six known accidents in the late 1980s. These accidents involved serious injuries and death. There were a number of contributing factors involving software design flaws. In one of these, depending on the sequence and timing of the operator’s data entry at the keyboard, the software could incorrectly set the intensity of the beam, without any indication to the operator.

Similar data entry problems have caused lock-ups and failures of computer-based systems at nuclear power plants. These have included multiple instances of loss of control room alarm functions and another instance involving the failure of an ATWS mitigation system. Such issues highlight the importance of careful design of human-machine interfaces to minimize potential data entry issues.

Examples of digital system failures continue to come across my desk. For example, last summer a scram at Browns Ferry Unit 3 occurred when a digital network controlling the reactor recirculation pumps experienced a ‘data storm’ of excessive traffic due to malfunction of one of the components on the network. It seems there was no ‘limiter’ designed into the network to ensure that the data flow remained within the physical capability of the network.

Then earlier this summer, the Honeywell uranium hexafluoride conversion plant digital control system power supply failed and placed plant components into a start-up configuration while the plant was operating. Operators were able to bypass the failed power supply and restore power to the work stations and communications network. However, when communications were re-established with the plant controllers, the controllers reinitialized as designed. This reconfigured the production equipment for a “cold start,” which shut a number of valves. However, because the plant was operating and ‘hot,’ the valve closure caused some of the process tanks to begin increasing their pressure. The operators noted the increasing pressures and shut the plant down safely.

Although these last two problems were more design-related and not operator interface issues, it remains true that the root cause was the Human Factor.

Category 2 - Predicting Problems

Turning now to the second category of my Human Factor taxonomy, which involves failures that have never happened before, but could. In my view, research is one of the best ways to address this second category, that is, to identify and anticipate the possible problems that have not yet actually occurred.

Early in my term as a Commissioner, I visited the OECD Halden Reactor Project and observed the digital I&C and human-machine interface research being done there. The NRC contributes support for much of this work, which 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 regulatory 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, the humans that operate and maintain them, and information to enhance human reliability analyses.

The NRC sponsors domestic research predominately through individual contractor arrangements in a case-by-case fashion. However, to improve our ability to make regulatory improvements that keep up with rapidly advancing digital technology and the science of human-machine interfaces, the NRC will begin a public dialog on the potential benefits and challenges of a research, test, and evaluation facility in the U.S for digital safety system and advanced control room applications. My hope is that such an integrated facility, if approved by the Commission, 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, such as 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. I am pleased to announce that this dialog will begin with a public workshop to be held in Atlanta, Georgia, on Sept. 6 and 7, 2007, and continue in Rockville, Md. on Sept. 11. More information is available from our NRC website at www.nrc.gov. I hope you will consider attending or advising your colleagues about it.

All of our research in the digital system area is integrated within our 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 six categories: 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.

Near-Term NRC Challenges For Review of New Plant Applications

In addition, earlier this year the NRC formed a senior management steering group and several specific task working groups with industry to focus on specific problems related to our upcoming reviews of digital I&C systems in new power plant applications and replacement systems for existing plants, as well as certain materials licensees. The NRC expects to receive up to seven applications for new plants later this year, with up to 11 more next year. The working groups have held over 25 public meetings to develop near-term interim regulatory guidance to provide greater clarity and predictability to our reviews of these expected applications. Specific areas of focus include diversity and defense-in-depth, highly integrated control room communications and human factors, cyber-security, risk-informed approaches, and the licensing process. Most of the interim staff guidance is due to be finished later this year, but work will continue to further refine and capture this guidance into formal regulatory guides

and standards, for instance, IEEE standards developed by the subcommittee that sponsors this conference.

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 to that 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 as you are doing this week.

Human Resources and Technical Expertise

From all indications, we see a coming surge of new plant applications, and the NRC is getting ready to meet this significant new challenge. I see a need for both NRC and industry to attract new people to reemerging work in nuclear power in order to build and maintain the necessary pool of talent to be successful in an environment of 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 and human factors 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 access 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 human-machine interfaces in our power reactors will certainly enhance the interest and recruitment of the next generation of students to the nuclear industry. But unfortunately, as I visit university 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, human factors, advanced control rooms, and regulatory requirements. Part of this will have to be accomplished through strong knowledge management programs, since so many of the NRC and industry staff are nearing retirement age.

Closing

In my travels, I've visited several facilities that incorporate advanced control room and computer-based safety and control systems 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 that uses 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, and the fully modern digital systems of the research reactors at the OPAL facility in Australia and at Tsinghua University in China. I was 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.

As a technical person and a safety regulator, I'm drawn to the potential safety benefits of computer-based technology, but I'm also sobered by the challenge of the many failure possibilities that must be addressed for its intended safety-related uses. Nevertheless, I am an optimist that we can achieve improved human-machine interfaces and overall safety performance, provided that the failure vulnerabilities are thoroughly identified, understood, and mitigated. As a regulator, the potential for enhanced safety motivates NRC's ongoing efforts to refine the regulatory requirements that enable such enhancements.

Building on a wealth of experience from other industries as well as the nuclear power industry, the NRC is considering human information gathering and cognitive processes to a greater extent than ever before in the design of advanced and highly integrated nuclear plant control rooms, aided by ongoing and extensive research.

In closing, I will reemphasize my key point: Digital I&C and safety systems offer the potential for improved human-machine interfaces and safety performance, provided that the Human Factor and other 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 ensuring 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, 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 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 improving the methods to achieve defense-in-depth and diversity, 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 will reside in the multitude of details that must be considered. Therefore, success will require a great and constant discipline to master the complexity to ensure it serves only the cause of safety.

Thank you.