POLICY ISSUE
INFORMATION

April 14, 2009 SECY-09-0061

FOR: The Commissioners

FROM: R. W. Borchardt
Executive Director for Operations

SUBJECT: STATUS OF THE NUCLEAR REGULATORY COMMISSION STAFF EFFORTS TO IMPROVE THE PREDICTABILITY AND EFFECTIVENESS OF DIGITAL INSTRUMENTATION AND CONTROL REVIEWS

PURPOSE:

To provide the Commission with information on recent staff efforts and accomplishments designed to improve the predictability and effectiveness of the review process for digital instrumentation and control (I&C) systems and to provide the Commission with information on decisions that the staff has made regarding certain industry proposals in this area. This paper does not address any new commitments or resource implications.

SUMMARY:

This paper provides information on how the staff has improved the licensing review process for digital I&C through development of improved regulatory guidance. In response to Commission direction, the staff initiated a project to improve the regulatory efficiency and predictability of the licensing of digital systems in new and existing power reactors. Over the past 2 years, the staff developed and has begun using five interim staff guidance (ISG) documents that provide improvements in the efficiency and predictability of the staff licensing reviews for digital

CONTACT: Steven A. Arndt, NRR/DE
(301) 415-6502

systems. The staff took advantage of significant stakeholder input as well as experience gained by other industries and countries to aid in the development of the ISGs. The staff plans to revise the standard review plan (SRP), regulatory guides, and other staff guidance as it gains experience with the use of the ISGs. As digital I&C technology evolves and new information becomes available, the staff will continue to update regulatory guidance in this area. Industry stakeholders provided valuable input during the development of the ISGs. The staff incorporated the input into the ISGs where appropriate. The staff does not support the industry's recommendation to allow the use of defensive measures to show that digital systems are not susceptible to common cause failures and does not support the industry's recommendation to use risk insights to relax deterministic regulatory policy.

BACKGROUND:

In SECY-91-292, "Digital Computer Systems for Advanced Light-Water Reactors," dated September 16, 1991, the staff described its positions regarding the use of digital I&C in evolutionary and advanced light water reactors (ALWR). The staff concluded that digital I&C systems could provide additional capabilities and reliability over comparable analog systems if properly designed and implemented. However, with these new capabilities also came added complexities and new failure modes. Of concern was the added potential for software common cause failure (CCF) and the need to ensure digital system communications issues were properly addressed. In SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to [ALWR] Designs," dated April 2, 1993, the staff presented its recommendations for addressing the potential for CCFs in digital safety systems. To summarize, the staff informed the Commission that it intended to require an adequate level of diversity and defense-in-depth to protect against CCF. The staff proposed to require, in part, that (1) applicants assess the diversity and defense-in-depth of the proposed I&C system to demonstrate that potential CCFs have been adequately addressed; (2) each postulated CCF be analyzed for each event that is evaluated in the accident analysis section of the safety analysis report (SAR); (3) if a postulated CCF could disable a safety function, a diverse means that is unlikely to be subject to the same CCF shall be provided; and (4) a set of displays and controls, diverse from the safety system and located in the main control room, shall be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The staff also stated that manual actions from the control room are acceptable for diversity if adequate time and information are available to the operators. In the Staff Requirements Memorandum (SRM) to SECY-93-087 dated July 21, 1993, the Commission approved a revised position clarifying, in part, that since the CCF is considered beyond design basis, the accident analysis should use best estimate or realistic assumptions.

These Commission positions were incorporated into the 1997 revision of Chapter 7, "Instrumentation and Controls," of the SRP, NUREG-0800, including Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems." Using the guidance in Chapter 7 and the associated regulatory guides, the staff was able to license a number of digital systems. In March 2007, Chapter 7 was updated based on experience in licensing digital systems to reference more current industry standards and regulatory guides.

In January 2007, in response to a November 8, 2006, Commission meeting and the December 6, 2006, SRM (ADAMS Accession No. ML0634000331), the U.S. Nuclear Regulatory Commission (NRC) staff initiated a project to improve the regulatory efficiency and predictability of licensing digital I&C systems in new and existing power reactors. During the November 8, 2006, Commission meeting, the industry panel, including the Nuclear Energy Institute (NEI), expressed concerns over the ability to license digital I&C safety systems and implement certain NRC policies regarding digital I&C. NEI stated that additional improvements were needed to NRC guidance to facilitate the nuclear industry's needed retrofits of aging analog systems in operating reactors and orders for new reactor simulators.

Also in response to the SRM from the November 8, 2006, Commission meeting; the staff established the Digital I&C Steering Committee, which identified high priority issues, articulated them as problem statements in a Digital I&C Project Plan, and directed six task working groups (TWG) to resolve them. Subsequently, a seventh TWG was formed to resolve similar issues for fuel cycle facilities. The TWGs were chartered to develop ISG documents and, in the longer term, develop draft updates to NRC regulatory documents.

RECENT ACCOMPLISHMENTS:

The Digital I&C Steering Committee and the TWGs have prepared ISG documents for all high priority technical issues associated with licensing digital I&C for power reactors. The ISG documents were developed with significant input from external stakeholders through a series of public meetings, and draft versions were posted on the NRC web site for public comment. The TWGs have addressed the technical issues of cyber security (TWG-1), diversity and defense-in-depth (TWG-2), review of new reactor digital I&C probabilistic risk assessments (PRA) (TWG-3), highly-integrated control room-communications (TWG-4), and highly-integrated control room - human factors (TWG-5). The staff is using the ISG documents to conduct ongoing reviews, and the feedback from licensees and staff who have utilized the ISG documents has been positive. The TWGs are translating the ISGs into updates to regulatory documents such as SRP Chapters, Regulatory Guides, and NUREGs. Updates to these regulatory documents are long-term actions in the project plan.

TWG-6 and TWG-7 are still developing guidance on the licensing process for operating power reactors and fuel cycle facilities, respectively. For the licensing process, TWG-6 is providing additional guidance on the scope and conduct of the review of digital retrofits to operating plant safety systems. The staff is incorporating lessons learned from ongoing reviews and anticipates completing the draft ISG for comment in the summer of 2009. For fuel cycle facilities, TWG-7 is addressing many of the same technical and licensing questions but with consideration of the significant differences in licensing requirements and consequences of digital system failures.

DISCUSSION:

As part of the development of the ISGs, the nuclear industry provided recommendations for consideration by the staff in the form of industry white papers, reports, and input at public meetings. In many cases, after careful consideration of the issues and the technical bases for the industry's recommendations, the staff was able to address the industry's technical positions in the ISGs. However, there were two areas where the staff could not support the industry's recommendations:

- the industry's desire to use defensive measures to demonstrate that digital systems are not susceptible to CCFs and

- the industry's desire to use risk insights to relax deterministic regulatory policy.

The staff recognizes the need for further development and refinement of regulatory guidance on diversity attributes and the use of risk evaluations of digital systems. However, the staff has concluded that, at this time, sufficient technical information is not available to refine guidance in these areas beyond that endorsed in the ISGs.

Defensive Measures

The industry describes an alternative method in their white papers for demonstrating adequate diversity and defense-in-depth against a CCF of a digital system such that an automatic diverse actuation system is not needed for low frequency common cause events. The industry proposed to accomplish this goal through a combination of design features (defensive measures), operator actions, and risk insights.

The industry's white paper on "Common-Cause Failure Applicability" dated February 29, 2008 (ADAMS Accession No. ML080700390), suggests that using defensive measures to design digital safety systems make them less susceptible to CCFs and/or better able to cope with CCFs should they occur. The industry's intent was to develop a method whereby defensive measures could be used to conclude that CCFs are not credible for the purposes of the diversity and defense-in-depth analysis. In the white paper, the industry focuses on software or software-hardware interaction failures and considers CCFs non-credible if overall failure probability is dominated by other failure modes. The white papers requested that the staff credit defensive measures and diversity attributes in determining adequate protection against CCFs. The industry wishes to combine the results of the aforementioned items with infrequent postulated accidents to justify adequate protection without meeting the diversity requirements provided in SRM-SECY-93-087 and the implementing guidance provided in Chapter 7 of the SRP.

The staff acknowledges that the use of defensive measures in the design of digital safety systems may reduce the likelihood of CCFs. However, at this time, sufficient knowledge regarding the effectiveness of specific defensive measures as described by the industry is not available to provide reasonable assurance that CCFs would not occur. The staff's position regarding the use of defensive measures is stated in SRP BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," as follows:

> To defend against potential CCFs, the staff considers high quality system designs, including the use of defensive design measures[;] to avoid or tolerate faults and to cope with unanticipated conditions[;] and D3 (diversity and defense-in-depth) to be key elements in digital system design. High-quality software and hardware reduce failure probability. However, despite high quality of design and use of defensive design measures, software errors may still defeat safety functions in redundant[] safety-related channels.

The staff finds that a technical basis for the use of defensive measures as described by the industry to alleviate the staff's concerns about potential CCFs in complex digital systems has not been sufficiently demonstrated. As a result, additional technical information needs to be collected or developed to determine how, and under what circumstances, credit could be given for the use of advanced design features in conjunction with, or in lieu of, diversity and defense-in-depth.

Relaxation of Digital Safety System Policy Based on Risk Information

The industry's white paper on "Benefits and Risks Associated with Expanding Automatic Diverse Actuation System Functions" dated May 16, 2008 (ADAMS Accession No. ML090860465), argues that the inclusion of a diverse actuation system has only minor risk benefit for low frequency events and that the addition of a diverse actuation system to a digital safety system that is not sufficiently diverse may increase the risk of spurious actuations. The industry used several current generation PRAs in conjunction with a probabilistic risk screening analysis to evaluate the risk impacts of using a diverse actuation system to meet the NRC guidance for digital safety system diversity and defense-in-depth. The white paper suggests that a probabilistic risk screening approach should form the basis for eliminating the policy requiring diversity and defense-in-depth for a digital safety system during postulated medium to large loss of coolant accidents (LOCA), or other low frequency design basis events provided in SRM-SECY-93-087 and the implementing guidance provided in Chapter 7 of the SRP.

The industry analysis includes significant assumptions regarding digital I&C system reliability. However, insufficient operating experience and failure mode data have been provided to support these assumptions. The staff has evaluated the industry's white paper and has concluded that there is insufficient knowledge of digital I&C failure modes and reliability data at this time to support a recommendation that the Commission modify its policy on the need for diversity and defense-in-depth. The staff has based this decision on inputs from the Advisory Committee on Reactor Safeguards, its own research program in this area, and the preponderance of the technical literature in this field. The current state-of-the-art and available data are insufficient to support risk-informed digital I&C licensing actions at this time.

The staff communicated these positions and the rationale for them to the industry in a November 3, 2008, letter to the Nuclear Energy Institute (ADAMS Accession No. ML083020020). Nonetheless, the staff continues to perform research in these areas. The staff is completing a number of research activities including (1) the quantification of diversity attributes (e.g., how much diversity is enough to provide protection against CCFs) and the lessons learned from operating experience and (2) the evaluation of digital system failure modes and the development of methods to evaluate the risk associated with digital I&C systems that may provide risk insights into regulatory decision-making.

Interactions with Other Industries and Countries

Digital I&C systems are used in other industries and, in some cases, in the nuclear industry in other countries. In the area of digital system safety requirements in other industries, the staff reviewed those requirements to determine if more effective and efficient methods to ensure safety can be implemented in the U.S. nuclear industry. The staff found that the differences in regulatory structure and oversight between industries are predominately due to the nature of the use of digital systems in the industry in question and the potential consequences of system

failures. In the area of requirements associated with nuclear power plants in other countries, the staff has engaged our regulatory counterparts throughout the world to better understand the situation.

The staff has found, based on a number of interactions with its counterparts in other countries, that the requirements associated with digital system design development are not greatly different. Some differences in specific criteria may exist between countries to address differences in the licensing approach and regulatory requirements. However, all countries recognize the need for (1) effective cyber security, (2) defense-in-depth and diversity against potential common cause software failure, (3) development of an effective means to address digital I&C system risk, (4) proper interchannel communication independence, and (5) guidance to ensure appropriate human-system interfaces in a highly integrated control room.

As digital technology has advanced, so has the staff guidance particularly in the area of defense-in-depth and diversity. While some countries require fully diverse analog backup capability to deal with postulated common cause software failures, the U.S. has been able to refine its position on this issue based on extensive interaction with other countries, other industries, and the U.S. nuclear industry. This has permitted U.S. licensees and applicants to avail themselves of a broader range of options (as discussed in ISG-2) in this key technical area while maintaining a reasonable assurance of safety. The staff will continue its international interactions in order to learn from the experiences of the other countries as digital technology becomes more common in nuclear power plants. The U.S. has, since the early 1990s, laid an effective foundation for this technology. This foundation has evolved as the technology has evolved, including the development of the ISGs, and will continue to take advantage of information gained from domestic and international operating experience and interactions with other industries and countries on issues of common concern.

As one part of the staff's efforts to learn from other industries and nations, the staff has been actively participating in the digital I&C aspects of the Multinational Design Evaluation Programme (MDEP). Specifically, the staff has been participating in the design-specific working groups for evolutionary power reactors (EPR) and advanced passive (AP) 1000s, and the staff also chairs the digital I&C issue-specific working group. These activities not only facilitate sharing of valuable knowledge and experience among member countries but also support the staff safety review of the proposed new reactor designs.

NEXT STEPS:

The staff will continue to engage the industry and other external stakeholders through the Digital I&C Steering Committee, TWGs, and established regulatory processes to complete the project plan and provide an effective path forward to improve the digital I&C review process. As the staff gains experience with the use of the ISGs through current reviews; the SRP, regulatory guides, and other guidance will be revised to incorporate the ISGs and lessons learned. Additionally, the staff will carry out research in this area to develop additional technical bases for new methods.

As digital I&C technology evolves and new information becomes available, there will be further opportunities to update guidance in this area. The development of new information and technical bases should be conducted by both the industry and the NRC. The staff has informed industry of opportunities for collaboration to develop the knowledge and technical basis in this

area. The current Memorandum of Understanding (MOU) between the NRC and the Electric Power Research Institute on cooperative nuclear safety research, for example, specifically identifies digital I&C risk methods as a potential area of cooperation. The staff is working with industry to develop another addendum to include additional specific digital I&C and human factors research activities. This MOU will provide the necessary vehicle for the timely exchange of information on planned and ongoing research activities and for conducting jointly-sponsored cooperative projects.

COORDINATION:

The Office of the General Counsel has reviewed this paper and has no legal objection.

/RA Bruce S. Mallett for/

R. W. Borchardt
Executive Director
for Operations