November 3, 2008

Alexander Marion
Executive Director for Engineering
Nuclear Energy Institute
1776 I Street, NW, Suite 400
Washington, DC 20006-3708

SUBJECT: FEEDBACK ON INDUSTRY WHITE PAPERS ASSOCIATED WITH DIGITAL INSTRUMENTATION AND CONTROLS

Dear Mr. Marion:

In January 2007, the U.S. Nuclear Regulatory Commission (NRC) staff initiated a project to improve the regulatory predictability of licensing digital instrumentation and control (I&C) systems in new and existing power reactors. The NRC formed a Digital I&C Steering Committee that identified 20 high-priority issues, articulated them as problem statements in the Digital I&C Project Plan, and directed six task working groups to resolve them. Subsequently, a seventh task working group was developed to resolve five similar issues for fuel cycle facilities.

The task working groups were chartered to develop interim staff guidance (ISG) documents to clarify existing NRC policy and regulatory positions and, in the longer term, develop draft updates to NRC regulatory documents. The Commission directed the staff to promptly bring forward any policy issues the staff believed were necessary to resolve in support of its work regarding regulation of digital systems.

The task working groups held a series of public meetings with the Nuclear Energy Institute (NEI), other industry representatives, and public stakeholders to ensure that industry and the public had opportunities to provide input to the development of the ISG documents, and to ensure that the guidance was well understood. The draft ISG documents were posted on the NRC public web site for comment before being finalized. The majority of ISG documents have been completed for power reactor issues. The development of ISG documents regarding fuel cycle facilities is still in progress.

As part of the process, NEI provided their perspectives in a series of white papers, position papers, meeting presentations, and other documentation. The NRC staff has thoroughly reviewed and considered the suggestions put forth by NEI.

During the August 28, 2008, public meeting of the Digital I&C Steering Committee, NEI asked the NRC to provide timely feedback on the white papers. The majority of the white papers on power reactor issues had already been reviewed by the NRC staff and appropriately considered in the ISG documents. Several of the white papers go beyond the scope of the problem statements in the Digital I&C Project Plan, and beyond the intended scope of the ISG documents.

NRC policy on common cause failures (CCFs) in digital I&C systems expressed in Staff Requirements Memorandum 93-087 dated July 21, 1993, establishes the expectation that

diverse actuation systems be provided when a digital I&C system is susceptible to a CCF. The following industry white papers addressed this NRC policy:

- EPRI 1015312, "A Methodology to Determine the Acceptability of Manual Operator Actions Response Times for a BTP 7-19 Software Common Cause Failure," Revision E, July 2008;
- White Paper, "Common-Cause Failure Applicability," February 29, 2008;
- White Paper, "Echelons Discussion," February 29, 2008;
- White Paper, "U.S. Commercial Nuclear Power Plant Digital I&C System Operating Experience," Revision 0, June 13, 2008; and
- White Paper, "Benefits and Risks Associated with Expanding Automatic Diverse Actuation System Functions," May 16, 2008.

NEI summarized the goal of these white papers in a position paper that supported a March 18, 2008, public meeting. To paraphrase, the goal was to develop an alternative method of demonstrating adequate diversity and defense-in-depth against a common cause failure of a digital system, such that an automatic diverse actuation system is not needed for low frequency events. NEI proposed to accomplish this goal through a combination of design features, operator actions, and risk arguments. The staff has reviewed the above-listed white papers in the context of the March 18, 2008, position paper, and has determined that they do not provide sufficient justification to change the current NRC policy. More detailed comments on the white papers are included in the enclosure to this letter. NEI also requested additional guidance on crediting diversity attributes in digital systems. The staff is in the process of developing this guidance and plans to seek public comment on the draft guidance in Spring 2009.

In a public meeting with NEI on October 1, 2008, the NRC staff reiterated its intent to close the Project Plan problem statements associated with the above white papers because the completed ISG documents provide predictable approaches for licensing digital I&C systems. In that meeting, the staff discussed several options for pursuing alternate approaches to these items outside the task working groups. The staff is continuing its long-term research program, and the industry may wish to collaborate with the NRC Office of Nuclear Regulatory Research to further develop the basic knowledge in these technical areas. The staff is also preparing updates to regulatory documentation, such as the Standard Review Plan (NUREG-0800), and NEI may request changes to the NRC policy either during the comment period for updates to regulatory documents or in separate topical reports. In addition, individual applicants can request approval of alternatives to the positions established in the ISG documents, with adequate justification, based on the specific technology involved. The staff will review such requests on a case-by-case basis.

The NRC staff is in the process of updating the Digital I&C Project Plan to reflect a revised schedule for updating NUREG-0800 and other guidance documents, and to reflect closure of several problem statements. The updated Project Plan will be posted on the NRC public web site.

If you have any questions on the above items, please contact Stewart Bailey, Deputy Director for the Digital I&C Steering Committee, at 301-415-1321 or Stewart.Bailey@nrc.gov.

Sincerely,

/RA/

John A. Grobe, Chairman
Digital I&C Steering Committee

Enclosure:
As stated

If you have any questions on the above items, please contact Stewart Bailey, Deputy Director for the Digital I&C Steering Committee, at 301-415-1321 or Stewart.Bailey@nrc.gov.

Sincerely,

/RA/

John A. Grobe, Chairman
Digital I&C Steering Committee

Enclosure:
As stated

DISTRIBUTION:
RidsNrrAdes
RidsNroDe
RidsNrrDorl
RidsNsirDdrs
RidsResDe
RidsNmssFcssSptsd
RidsIsIcodItost
RidsNroDeIce2
RidsNrrDraApob
RidsNrrDeEicb
RidsNriDcipColp
RidsNrrDorlLpl3-1
RidsNmssFcssSptsdTsb
RidsNrrDe
RidsNrrOd
RidsNrrAdro
RidsAcrsAcnw_MailCTR Resource

ADAMS ACCESSION NO.: ML083020020

OFFICE	DI&C/DD	NRO/DE*	NSIR/DSP*	RES/DE*	NMSS/FCSS*	NRR/ADES
NAME	S.Bailey	M.Mayfield	S.Morris	M.Case	M.Bailey (T.Hiltz for)	J.Grobe
DATE	10/31/08	10/29/08	10/30/08	10/30/08	10/30/08	11/03/08

*concur by e-mail **OFFICIAL RECORD COPY**

COMMENTS ON INDUSTRY WHITE PAPERS
REGARDING NRC POLICY ON DIVERSITY AND DEFENSE IN DEPTH
FOR DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

BACKGROUND

The Digital Instrumentation and Control (I&C) Project was developed following the November 8, 2006, meeting of the Nuclear Regulatory Commission (NRC or Commission). The December 6, 2006, Staff Requirements Memorandum (SRM) entitled, "Briefing on Digital Instrumentation and Control," (Agencywide Documents Access and Management System, Accession No. ML063400033) and the January 12, 2007, memorandum from the Executive Director for Operations (ML063390606) chartered the Digital I&C Steering Committee to address specific issues related to digital I&C. The Steering Committee developed the Digital I&C Project Plan (ML080220448) and assigned task working groups (TWGs) to address the issues. The project plan was updated to reflect the Commission's SRM dated June 22, 2007, entitled, "Meeting with the Advisory Committee on Reactor Safeguards (ACRS)," (ML071730241) that directed the staff to include activities to support development of the final regulatory guidance on diversity and defense-in-depth (D3).

To support greater regulatory predictability, the Steering Committee issued interim staff guidance (ISG) documents that clarify existing NRC policy. The process of developing ISG documents included a series of public meetings to ensure that the guidance was understood and to solicit feedback from stakeholders. The ISG documents provide generically-applicable criteria the staff will use when reviewing digital I&C systems in new or existing reactors, or fuel cycle facilities. The ISGs represent one method that is acceptable to the staff and provides licensing certainty and predictability. The ISGs do not exclude the use of alternate methods that are submitted with sufficient justification.

The current NRC policy regarding D3 is promulgated in SRM 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs," dated July 21, 1993. To summarize, the policy is that common cause failures (CCFs) are credible in digital systems, and particularly in complex software driven systems, and that licensees should provide D3 to protect against CCFs for all design basis events in Chapter 15 of the Final Safety Analysis Report. Diverse actuation systems (DASs) shall be provided where systems are susceptible to CCFs. The policy is applicable to digital I&C safety systems in both new and existing reactors. Implementing guidance is provided in Standard Review Plan (SRP, NUREG-0800) Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems." The staff issued further clarification in ISG-2, "Interim Staff Guidance on Diversity and Defense-in-Depth Issues," (ML072540118) describing digital system designs that are sufficiently diverse that CCF is not credible, and stating that operator action can be credited as diversity for CCFs of the safety system if actuation is not needed for 30 minutes.

The discussions of D3 have continued following the issuance of ISG-2. The Nuclear Energy Institute (NEI) developed a series of white papers, position papers, and other documents to address the NRC policy on D3 and, in particular, the concern that the NRC policy and ISG guidance can lead to inclusion of an automatic DAS. The staff has provided feedback on these papers in several public meetings.

ENCLOSURE

DISCUSSION

The industry's goals for DAS were outlined in a March 18, 2008, meeting presentation (ML080920892). To summarize, industry was seeking guidance that would allow a licensee or applicant to: (1) take credit for operator action(s) to meet D3 policy; (2) take credit for defensive measures (design features that are intended to eliminate or restrict potential CCFs) and diversity attributes in determining adequate protection against CCFs; and (3) combine the results of the aforementioned items with the low probability of infrequent postulated accidents (such as large break loss of coolant accident (LOCA)) to justify adequate protection without dependence on a DAS. Industry's stated goal is to have the DAS, if required by the digital system design, protect against high-frequency events, including anticipated operational occurrences, and not infrequent design-basis accidents. The industry stated that adding a DAS increases complexity and can lead to spurious actuation or adverse interaction with the primary safety system. The industry's positions are: (1) designing DAS to address low frequency events does not provide a significant safety benefit, or could even result in a decrease in safety; and (2) defensive measures, diversity attributes, and operator actions provide adequate protection.

The staff notes that several of industry's meeting presentations and white papers have described the NRC policy on D3 to include an additional automatic DAS for digital I&C CCFs as an expansion of the requirements in Title 10 of the *Code of Federal Regulations* (10 CFR) Section 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants." This is an incorrect characterization. The requirement to consider a systematic, nonrandom, concurrent failure of a digital I&C system (e.g., software CCF) and its impact on the system's reliability, redundancy, and independence in accomplishing its safety function (e.g., D3) is not based on the ATWS rule, but rather it is based on Institute of Electrical and Electronic Engineers (IEEE) Std. 279, IEEE Std. 603, IEEE Std. 379, 10 CFR 50.55a(h), "Codes and standards," 10 CFR Part 50, App. A, "General Design Criteria," and the regulatory position provided by the SRM to SECY 93-087. Although it is recognized that systems installed to satisfy the ATWS rule can be an effective means to maintain D3 for specific digital I&C CCFs, the ATWS rule is not the regulatory basis for the D3 evaluations or the regulatory basis for adding a DAS to provide protection against CCFs. Therefore, contrary to industry's statements, the staff has not expanded the requirement for an automated DAS beyond previous guidance or regulation.

This enclosure provides the staff's feedback on the following NEI documents:

- EPRI 1015312, "A Methodology to Determine the Acceptability of manual Operator Actions Response Times for a BTP Software Common Cause Failure," Revision E, July 2008;

- White Paper, "Common-Cause Failure Applicability," February 29, 2008;

- White Paper, "Echelons Discussion," February 29, 2008;

- White Paper, "U.S. Commercial Nuclear Power Plant Digital I&C System Operating Experience," Revision 0, June 13, 2008; and

- White Paper, "Benefits and Risks Associated with Expanding Automatic Diverse Actuation System Functions," May 16, 2008.

These documents were developed to support various problem statements in TWG-2, “Diversity and Defense-in-Depth,” TWG-3, “Risk Informing Digital I&C,” and TWG-5, “Highly-integrated Control Room – Human Factors,” but focus directly or indirectly on the need for an automated DAS to satisfy the requirements for D3.

The staff appreciates the industry’s efforts to produce these white papers to address the D3 policy. However, the staff believes that further research and development of the technical issues is needed before changes to the Commission’s policy or the staff’s guidance are considered. It is the staff’s position that no revision to the current D3 policy is warranted. The staff has carefully reviewed the above papers in light of staff research, relevant domestic and international operating experience, international regulatory positions, and the licensing applications submitted to date, and has concluded that the ISGs are adequate to meet the intended purposes of providing technical positions that are acceptable to the staff and improving the predictability of staff reviews. Vendors, licensees, and applicants can submit approaches that do not follow the ISGs, with adequate justification, and the staff will review the submittals based on the technical merits.

COMMENTS ON SPECIFIC NEI DOCUMENTS

1. Unique Prompting Alarm Aspect of EPRI 1015312, “A Methodology to Determine the Acceptability of Manual Operator Actions Response Times for a BTP Software Common Cause Failure,” Revision E, July 2008

TWG-5 was tasked with developing methodologies for crediting manual actions as a diverse backup for CCF. TWG-5 Problem Statement 5 states, “Clarification is desired on the use of operator action as a defensive measure and corresponding acceptable operator action times. The NEI white paper on this subject, EPRI 1015312, has been reviewed and, where appropriate, addressed in the ISG on manual operator actions. The white paper included the concept of a unique prompting alarm, which was presented as a method of alerting the operator in the event of a safety actuation system CCF. The alarm would be designed to inform the operator that the safety system had not functioned as required, prompting the operator to take specific actions. The overall effect of a successful unique prompting alarm in the D3 analysis would be a reduction in the time required for an operator to recognize and diagnose the situation, and take appropriate action.

The staff’s view is that a unique prompting alarm may contribute to effective timely coping with CCF scenarios; however, the viability of this approach is expected to be highly dependent upon the design of the plant and its I&C systems. The feasibility of this alarm needs to be reviewed on a case-by-case basis to determine the viability of the alarm from an I&C perspective, and the human factors reviewers would need to review the operator’s ability to focus on this alarm (considering others that are likely to be sounding) and take appropriate actions. The EPRI report does not have sufficient information to support generic applicability of a unique prompting alarm; therefore, the staff did not include this aspect of EPRI 1015312 in the draft ISG. If a vendor, applicant, or licensee requests NRC approval to use a unique prompting alarm, the staff will review the request based on its technical merits. The schedule and level of resources needed to review the submittal would be based on the quality and technical adequacy of the information provided by the applicant.

2. White Paper, "Common-Cause Failure Applicability," February 29, 2008

This white paper provided industry's insights into using defensive measures to design digital systems such that they are less susceptible to CCFs or are better able to cope with CCFs if they occur. The white paper supports the TWG-2 problem statement, "Clarification is desired on identification of design attributes that are sufficient to eliminate consideration of CCFs (e.g., degree of simplicity)." The overall intent was to develop a method whereby defensive measures could be used to conclude that CCFs are non-credible for the purposes of the D3 analysis. In ISG-2, the staff stated that consideration of CCFs is not needed if the protection system has sufficient built-in diversity or if a system is fully testable and tested. ISG-2 does not specifically address defensive measures. In the white paper, NEI focuses on software or software-hardware interaction errors, and considers CCFs non-credible if overall failure probability is dominated by other failure modes.

The staff's position regarding the use of defensive measures is stated in BTP 7-19 as follows: "To defend against potential common-cause failures, 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 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" (emphasis added). Defensive measures alone have not been demonstrated to be sufficient to alleviate concerns about potential CCF in complex digital systems.

The white paper catalogs a set of defensive measures, and their applications, that have been employed or are available to the industry. Several of the defensive measures in the paper may have potential to reduce sources of, or to reduce the scope of, certain CCFs; however, the white paper lacks clear correlation between the defensive measures and the overall protection scheme against CCFs, as intended in BTP 7-19. Further, the white paper states it "does not provide a complete, detailed recipe and precise, quantified criteria against digital CCF that would be applicable for all situations," and there is no clear mapping of the applied defensive measures against the BTP 7-19 guidance and acceptance criteria. The white paper does not provide sufficient justification to support crediting defensive measures. The white paper further states that consideration of relevant operating experience or engineering judgment should be credited along with the defensive measures, particularly when the defensive measures alone may not be sufficient. The staff does not believe that this approach would provide the licensing certainty and predictability that are the goals of the ISG.

The white paper goes on to state that some components contribute little to the potential for CCFs. However, other components, particularly those more dependent on complex software programming (such as microprocessors and programmable logic devices) and those with increased interconnections among various devices and systems, are still of concern. Since the use of defensive measures listed in the white paper is up to the individual system designers, each submittal would need to be evaluated individually to verify that, in fact, no CCF consideration is needed. Additionally, since the white paper does not provide any detailed demonstrations of how specific defensive measures reduce the likelihood of, or effect of, specific CCFs, this will need to be done for each CCF that the proposed system may have. Based on the above, the staff concludes that, in order to rely on defensive measures, a licensee or applicant would need to provide rigorous technical justification to demonstrate that the specific

defensive measures make CCFs non-credible. This approach is not likely to provide licensing certainty and predictability.

Therefore, it is not clear to the staff how defensive measures can be used at this time in support of an adequate safety finding for digital systems, as discussed in the March 17, 2008, "Industry Goals for DAS" position paper.

The white paper also discusses the industry concern that a "diversity only" approach may overlook choices and may introduce problems, as complexity and risk of spurious actuation increase. The staff's position is that a well designed system should have a very low probability of spurious actuation. The staff notes the extremely low incidence of spurious actuation of the ATWS mitigation systems in current plants as relevant operating experience. The staff also notes that some vendors have already submitted designs for diverse systems that appear to successfully defend against both potential CCFs and spurious actuation.

Based on the above, the staff does not intend to revise ISG-2 regarding CCF applicability. The ISG is adequate to meet the objectives of the Digital I&C Steering Committee. If a licensee, vendor, or applicant submits a digital safety system for review that relies on defensive design features for protection against CCFs, the staff will review the submittal based on its technical merits and the current regulatory guidance. The schedule and resources needed to review the submittal would be based on the quality and technical adequacy of the information provided.

3. White Paper, "Echelons Discussion," February 29, 2008

The industry provided this white paper to describe their understanding of when reactor trip system (RTS) and engineered safety feature actuation system (ESFAS) may be combined into a single platform. This white paper was submitted to support discussions on the TWG-2 problem statement, ". . . Additional clarification is desired regarding how the echelons of defense for maintaining the above safety functions [listed in Project Plan] should factor into diversity and defense-in-depth analyses. . ." The staff's position, as discussed in ISG-2, is that RTS and ESFAS functions can be combined if the criteria of Positions 1 and 2 of ISG-2 are met. Industry proposed that RTS and ESFAS functions may be combined if the acceptance criteria of Section 3 of BTP 7-19 are met, arguing that the criteria in Positions 1 and 2 of ISG-2 are not appropriate nor required.

Echelon expectations are outlined in Guideline 4 of NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems." The guidance states that the instrumentation system should provide four echelons of defense-in-depth: control, reactor trip, engineered safety feature actuation, and monitoring and indication. Echelons are defined by their function. In general, the normal operational hierarchy for transients and accidents is that the second echelon (reactor trip) functions when the first (control) fails, and the third (ESFAS) and fourth (monitoring and indication) echelons support the first two. In the analysis method presented in NUREG/CR-6303, this order is sometimes reversed when non-Class IE echelons are allowed to compensate for CCFs in Class IE echelons. Also, ISG-2 states (from NUREG-0737, "Clarification of TMI Action Plan Requirements," Supplement 1) that sufficient information should be provided to the operators to monitor and thereby control certain plant safety functions and conditions.

The ISG provides an acceptable method of resolution of the D3 issues consistent with the purpose of the Digital I&C Steering Committee. The staff does not intend to change ISG-2 concerning combining RTS and ESFAS functions.

4. White Paper, "U.S. Commercial Nuclear Power Plant Digital I&C System Operating Experience," Revision 0, June 13, 2008

This white paper presents NEI's evaluation of digital system operating experience based on a search of NRC and INPO databases from 1987 to 2007. The review of operating experience was conducted to support long term actions for several problem statements in TWG-2. The white paper's focus was on D3 issues, so the "digital events" were evaluated for common defects that were significant with respect to actual or potential CCFs, and in particular software CCFs. The white paper treated 1E and non-1E systems separately, and did not indicate the overall rate of occurrence of events. The paper's overall findings were: (1) in 1E systems, most failures were identified through testing one or two cycles after the systems were placed in operation; (2) there were no instances in 1E systems where demand signal alone could have triggered CCF; (3) there were no instances where diverse platforms would have been effective in protecting against CCFs, indicating that the problem arose during specification development; and (4) current software development and testing practices, as well as design features, have been effective in keeping software a minor contributor to CCF.

The staff reviewed the white paper in light of its stated purpose and the staff's own reviews of operating experience. The staff draws different conclusions.

The staff's experience is that the digital systems being proposed are becoming increasingly complex, such that the operating experience reviewed by NEI may have limited applicability to new systems. The white paper states that most of the identified problems are in first-of-a-kind systems, and that higher levels of complexity make it increasingly difficult to specify system requirements "with high confidence that they are complete, correct, unambiguous, etc." The staff notes that most of the systems being proposed are first-of-a-kind and that, in some cases, the complexity is significantly increased over previous systems. Therefore, the trends noted in the white paper indicate the need to protect against CCFs.

It is also the staff's experience that there is little difference in the system lifecycle and design attributes (other than hardware separation) between 1E and high quality non-1E systems, such that the operating experience should not generally be differentiated along those lines. The staff believes a better method is to classify the operating experience by the software integrity level categorization, and the ACRS agrees on this approach. The data in the white paper indicates that the rates of failure (in percent) from the various causes (including software) are similar for 1E and non-1E systems. The white paper includes the conclusion that 1E systems are significantly better than non-1E systems in terms of CCFs, but the white paper does not include data that supports this conclusion.

The white paper notes that the rate of CCF (or potential CCF) from software is "no more problematic than other CCF contributors," and that design features such as defensive measures have been shown to be effective in limiting CCFs. The staff's evaluation of the data indicates that software accounts for approximately 15 percent of the total CCFs in 1E systems, and more in non-1E systems. While the white paper does not consider this significant, the staff interprets

15 percent to be a significant contribution. These rates do not support the general conclusions in the white paper on the effectiveness of defensive measures.

The white paper notes that most CCFs were found in the first one or two cycles of operation. The white paper attributes this to first-of-a-kind applications and notes that fixes have included addition of defensive measures, and there have been no instances of recurrence following corrective actions. The staff notes that the addition of defensive measures increases system complexity, which the general trends indicate would result in a higher potential for CCFs. Also, due to the time frame of the observations (up to 2006), it is not clear to the staff that the data supports the implication that there will not be recurrences. Further, in a typical system lifecycle, the operational testing is not routinely changed; therefore, the staff does not expect operational testing to identify CCFs. Potential CCFs should be identified and corrected in the unit and integration testing or factory acceptance testing. Therefore, the staff does not agree with the implication that corrective actions have resulted in digital systems that are free from potential CCFs.

The white paper states that plant design principles limit the potential effects of software defects, such that even if a defect takes out multiple redundancies of a safety system, it may not impact the overall safety function because other actuations would provide diversity. The staff notes that this is highly dependent on the designs of the reactor and the digital safety system. Not all safety functions have backups, and in highly-integrated digital safety systems, such as some of the systems being proposed, a CCF can disable several safety functions. Also, in the section on event overview, the white paper notes that two thirds of common defects resulted in subsystem or channel effects leaving the system available to perform its overall safety function by other means, such as functional or signal diversity. This implies that the system was not able to perform its safety function in one third of the cases.

The white paper also discusses the ability of operators to take corrective actions, such that the consequences of the CCFs were not significant. The staff does not consider this to be generically applicable to all CCFs, but highly dependent upon the design of the digital safety system, the particular CCF, and the reactor being protected.

The white paper considers that the industry design processes for digital I&C systems are well established. While the white paper did not discuss the “event” rate, making it difficult to draw conclusions on overall reliability, the staff does not believe the operating experience demonstrates across-the-board maturity in software design. The staff does not agree with the paper’s claim that the operating experience shows protection against software failures and CCFs is already at a “reasonable assurance level,” unless there is adequate D3. The claim is not supported by the information in the white paper.

The white paper provided three recommendations: (1) additional operating experience investigations; (2) modification of D3 ISG to endorse and credit methods that have proven effective in protecting against CCFs in 1E systems; and (3) industry focus on prevention of hardware failures and application of lessons learned. The staff agrees, in concept, on the recommendations with respect to continuing to evaluate operating experience and applying lessons learned. The accumulation of relevant experience and systematic compilation of the operating experience data is important in understanding failure modes, failure rates, and the effectiveness of various design and mitigation techniques. The staff expects that this will lead to improved design, operation, and maintenance of I&C systems, refinement of regulatory

guidance, and better understanding and application of digital system risks. The industry should carefully look into and assess the extensive data from (1) digital I&C deployed in other countries, (2) vendor experience, if applicable, and (3) experience in other industries. With regard to the recommendation to modify the D3 guidance to endorse and credit methods that have proven effective in protecting against CCFs in 1E systems, the staff does not agree with this recommendation, as it is not supported by the operating experience at this time.

The staff performed a study relevant to this area in response to the recommendations by the ACRS regarding digital operating experience and digital system inventory and classification. The results were provided in March 2008 (ML080590527). The staff's study came up with a set of findings that differ from the white paper. Even though there was a lack of high-quality data, The staff found that software CCFs are credible. In that study, the Office of Nuclear Regulatory Research stated that it intends to perform additional reviews of non-nuclear industry digital system failure data and will periodically review nuclear operating experience as these systems become more prevalent in the nuclear industry. The industry may wish to interact and cooperate in the area of operating experience.

In summary, the staff finds that some of this white paper's conclusions and observations are not well supported by the data. In concept, the staff concurs with the recommendations for continued attention to operating experience and application of lessons learned, but finds that the available operating experience is insufficient to justify revision of ISG-2. The staff expects that, domestically, at least several years of additional digital experience, especially with the plants with digital RPS and ESFAS, may be necessary to allow meaningful applications of the data in the regulatory arena.

5. White Paper, "Benefits and Risks Associated with Expanding Automatic Diverse Actuation System Functions," May 16, 2008

This white paper was submitted to support TWG-3 work under Problem Statement 2, "Using current methods for PRAs (Probabilistic Risk Assessments), NRC has not determined how or if risk-insights can be used to assist in the resolution of specific key digital system issues." The white paper used several plant PRAs in conjunction with a probabilistic risk screening analysis to evaluate the benefits of a DAS. The arguments are structured as a backfit analysis, and the conclusion is that proper operation of a DAS has only minor risk benefit for low frequency events, and addition of a DAS that protects against low frequency events may increase risk if spurious actuations are considered. The white paper suggests that a probabilistic risk screening approach should form the basis for eliminating the need for an automated DAS to mitigate the consequences of a safety system CCF during postulated medium to large LOCAs, or other low frequency design basis events.

The staff reviewed the white paper and concluded that it is not sufficient to support changes to NRC regulatory guidance regarding D3. As previously stated, the staff has not expanded the scope or applicability of the ATWS rule. The NRC policy on D3 is unrelated to the requirements of 10 CFR 50.62; therefore, it is incorrect to discuss this policy in terms of a backfit. Further, the use of the white paper's risk analysis to reduce D3 requirements would constitute a risk-based rather than a risk-informed approach, and does not adequately consider the significant uncertainties that may not be captured by parametric model uncertainties or sensitivity studies alone.

The staff has met with the ACRS on a number of occasions and with the Commission to discuss the draft ISG for TWG-3 (ML080570048) and supporting research for Tasks 2 and 3 of the TWG-3 project plan. As a result of these meetings, the staff received significant feedback on the overall TWG-3 charter of using current PRA methods to obtain risk insights, and on using these insights to help resolve specific issues unique to digital I&C. The comments and concerns raised by the Commission and ACRS (ML081510594, ML081050636, ML081610788, ML081610770, and ML081780761) during these meetings are applicable to the methods used in the white paper. The staff concludes that these comments and concerns are significant enough that the methodology used in the white paper does not provide the required rigor with respect to risk-informing D3 evaluations of DI&C systems (i.e., guidelines for DAS implementation).

The white paper includes significant assumptions regarding digital I&C system reliability. For example, the report assumes that software will be at least 99.99 percent reliable even during initiating events such as large LOCAs, for which there are no data. This assumption is referenced to an IEC (International Electrotechnical Commission) standard and is based on the assumption that a high-quality process and defensive measures are used in the design. However, insufficient relevant operating experience or failure mode data is provided to support the effectiveness of these claims (see staff comments in previous sections). In the white paper, the software is therefore treated as a black box. The report assumes that digital systems have improved reliability over their analog counterparts, and cites “defensive measures” and design attributes as providing enhanced reliability. The reliability improvement is not quantified in the study but assumed applicable for the very high reliability systems included in the study. Sensitivity studies were performed to show that the software failure probability is bounding to the conclusions of the white paper. However, the white paper did not substantiate the use of sensitivity studies to provide insights on the potential risks of digital I&C CCF when there is a substantial lack of knowledge of digital I&C failure modes or failure data. The white paper does not adequately justify the use of traditional PRA methods to support a comprehensive risk-informed evaluation of digital I&C risk. These and other assumptions drive the results that support the white paper conclusions.

The white paper conclusion that a DAS has little risk benefit is, in part, driven by the assumption that D3 is maintained by the independence of the plant design (mitigation systems) and the initiating events they are designed to mitigate. The report does not provide adequate justification that there are no dependencies between the initiating event and the mitigation system including a mitigation system digital I&C CCF. Operating experience has shown that these dependencies can exist, especially with regard to digital systems failure, maintenance, or operator input. The supporting analysis is limited to domestic plant PRAs (using analog I&C systems), reflects unsubstantiated data (i.e., limited consideration is given to the lack of knowledge of digital systems failure modes, failure data, and the conditional probability of a significant CCF), and uses sensitivity studies to establish a bounding result for all plant types.

Despite the statement in the white paper, the approach outlined does not conform to the guidance of Regulatory Guide (RG) 1.174, “An Approach for Using Probabilistic Risk-Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” such that risk-informed decisionmaking can be established for D3 evaluations. The report does not establish acceptance guidelines for implementing an automated DAS. The risk assessment results discussed in the report are a consequence of (1) assumed event frequencies, (2) the assumed high reliability of the mitigation systems evaluated, and (3) the methodology employed. However, significant issues, such as what are considered “credible or not credible events,” and

appropriate metrics (including what are adequate D3 acceptance guidelines) have not been addressed by the report. Additionally, the NRC staff notes that the proposed methodology's conformance to RG 1.200, "An Approach for Determining the Technical Adequacy of Risk Assessment Results for Risk-Informed Activities," is not discussed with regard to risk-informed decisionmaking.

The staff has traditionally considered the defense-in-depth philosophy when applied to reactor design and operation as providing multiple means to accomplish safety functions and prevent the release of radioactive material. The NRC staff also considers defense-in-depth to be an effective means to account for uncertainty in equipment reliability, human performance, and the likelihood of initiating events (e.g., large break LOCA). The staff has not endorsed a risk-based methodology using core damage frequency to establish a measure of defense-in-depth. RG 1.174 does note that a comprehensive risk analysis can aid in the evaluation of the appropriate extent of defense-in-depth with respect to maintaining a balance in core damage prevention, containment failure, and mitigation. However, based on the issues identified with digital I&C failure data, failure modes, and modeling of digital I&C using current PRAs, the use of traditional PRA methods to establish defense-in-depth insights cannot be considered "comprehensive" per RG 1.174. As such, the staff also finds the white paper to be inconsistent with the SRM to SECY-93-087 concerning digital I&C CCFs.

In summary, the staff concludes that the white paper does not provide justification for a change to NRC policy regarding D3. Given substantial feedback from the ACRS regarding the role of PRA in regulatory decision-making for digital I&C systems and additional staff concerns, the staff does not support use of the white paper to limit the scope of accidents that an automated DAS is designed to mitigate. The staff is continuing its long-term research program related to digital I&C, and the industry may wish to work with the Office of Nuclear Regulatory Research in the development of methods to evaluate the risk associated with digital I&C and apply the risk insights into regulatory decisionmaking.