

Risk-Informed Evaluations of Nuclear Power Plant Digital Upgrades Technical and Regulatory Issues

Dave Blanchard
Applied Reliability Engineering
482 W Hamilton Ave. #255
Campbell, CA 95008

Ray Torok
EPRI
3412 Hillview Avenue
Palo Alto, CA 94304

KEYWORDS

Digital Upgrades, Risk-Informed Regulation, Defense-in-Depth and Diversity

ABSTRACT

When implementing a digital upgrade at a nuclear power plant, an area of technical and regulatory uncertainty is in the application of risk-informed techniques. All nuclear power plants now have plant-specific probabilistic risk assessments (PRAs) with which risk-informed analyses are routinely performed in support of the operation, maintenance and licensing of the plants. However, current regulatory guidance with respect to evaluation of digital upgrade design remains largely deterministic and does not yet take advantage of the PRAs. In this paper, the following questions will be addressed with respect to the use of risk insights in the implementation of a nuclear power plant digital upgrade:

- What technical issues are barriers to the use of PRA in the evaluation of the risks associated with a digital upgrade?
- What kinds of risk insights can be derived from a plant specific PRA using existing techniques that are useful in support of licensing a digital upgrade?

INTRODUCTION

Over the next few years, many nuclear stations will be initiating design changes to I&C systems using digital-based systems to replace obsolete aging analog instrumentation. In replacing this I&C, utilities wish to take advantage of the added reliability and operational capabilities available using digital technologies. When designing such a digital upgrade, licensees perform what is known as a defense-in-depth and diversity (D3) evaluation. The purpose of a D3 evaluation is to consider the effects from postulated digital or software related common mode failures that could be introduced by the digital

upgrade. These new common mode failures may have the potential to compromise the redundancy built into the mitigating systems into which the digital I&C is to be installed.

NRC guidance with respect to D3 evaluations is found in the Standard Review Plan. Developed prior to the completion of the plant specific PRAs, this regulatory guidance is largely deterministic in nature and strictly focuses on evaluating design basis events. Given this focus, accident scenarios that we now know from the PRAs could dominate risk are not considered. In addition, much effort is spent by licensees to evaluate and perhaps modify the design of the digital upgrade to address the effects of potential common mode failures on design basis events that have been demonstrated by the PRAs to be of limited safety significance. Finally, as evaluations are reviewed by the NRC, licensees are finding that acceptance criteria originally published as a part of current regulatory guidance may no longer be considered acceptable. This introduces significant licensing uncertainty and has had a chilling effect on plans to upgrade I&C at several plants.

In this paper, we introduce the use of PRA in the performance of D3 evaluations to limit scope as well as assure completeness in assessing adequate defense-in-depth and diversity in the design of a digital system. PRA is being applied successfully for a variety of other generic safety issues where the original regulatory guidance is recognized as being incomplete and/or overly burdensome without corresponding benefits in safety. The paper will discuss possible limitations of PRA in the evaluation of digital systems. Existing techniques for generating insights from PRA in the performance of D3 evaluations will be introduced. Finally, the advantages and limitations of PRA approaches vs. current regulatory approaches will be compared.

I Use of PRA to Address Regulatory Issues

All nuclear power plants have a plant specific PRA that has been performed to evaluate the potential for severe accident vulnerabilities [1]. These PRAs are being used successfully to identify risk insights and focus the scope of many regulatory related programs such as inservice testing, inservice inspection and quality assurance. In addition the PRAs are being used extensively in support of technical specification changes and inspection and enforcement activities. The industry and the NRC have identified numerous benefits to the use of PRA in its support of licensing actions, among them the evaluation of design modifications to the plant. A digital upgrade is considered to be such a design modification for which it may be useful to evaluate using the plant specific PRA.

Subsequent to development of the PRAs, the NRC published the PRA policy statement [2], in which the Commissioners stated that:

- Because PRA considers the frequency of a broad spectrum of initiating events and combines them with an assessment of the reliability of mitigating systems, including the potential for multiple and common cause failures, it is considered an extension and enhancement of traditional regulation.
- PRA techniques are most valuable when they serve to focus the traditional deterministic-based regulations and support the defense-in-depth philosophy.
- The PRA approach supports the NRC's defense in-depth philosophy by allowing quantification of the levels of protection, and by helping to identify and address weaknesses or overly conservative regulatory requirements applicable to the nuclear industry.

Consistent with these assertions, the Commissioners have instructed the NRC and encouraged the industry to increase the use of PRA:

- In all regulatory matters, to the extent supported by the state-of-the art in PRA methods and data, and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.
- In regulatory matters, where practical within the bounds of the state of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and NRC practices.

Given that the industry currently performs defense-in-depth and diversity evaluations in designing a digital upgrade and that NRC policy considers PRA to be an extension to traditional defense-in-depth philosophy, an obvious application of the plant specific PRAs would be in performing these D3 evaluations. The question is whether the state-of-the-art for current PRAs would support such an evaluation.

II Potential Limitations of PRA in Performing D3 Evaluations

In attempting to model digital systems within a PRA, it is important that analysts recognize that there are differences in the manner in which digital equipment "fails" as compared to the analog systems that they are replacing. Among these differences are:

The software in digital equipment is not a physical entity as would be the case for analog equipment and is not subject to wear out or random failure.

The failure modes of digital equipment, should it fail, may not be well defined.

Given the same inputs, software will produce the same outputs every time. As a result, the "probability of failure" of digital equipment and its software is related to the potential that the equipment will encounter conditions for which it was not designed and for which it will respond in a manner that is adverse to the function being performed by the system in which it is installed.

If digital equipment is to be incorporated into the logic models of the PRA, methods must be developed that differ from those used to model traditional analog systems. NRC staff has expressed the view that methods for identifying failure modes, modeling their effects and estimating failure probabilities of digital equipment have not yet been adequately demonstrated. To address these issues, NRC research is in the process of reviewing a variety of methodologies (e.g., Markov modeling, dynamic fault trees, etc.) to model the dynamic effects of potential digital failure modes. This review is part of a multi-year research plan that is to culminate in regulatory guidance with respect to how to incorporate digital equipment in PRA[3]. The NRC concludes that at this time the modeling methods needed to support current risk informed methods are not currently available[4].

III D3 EVALUATION INSIGHTS THAT CAN BE DERIVED FROM PRA

It is clear that methods for identification of digital equipment failure modes, modeling their effects and estimating their probabilities are still evolving. However, the results of recent EPRI investigations show that insights with respect to the acceptability of digital system design from a defense-in-depth and diversity perspective can still be derived from the plant-specific PRAs [5].

NRC RESEARCH PERSPECTIVE VS EPRI RESEARCH PERSPECTIVE

In deriving risk insights using current techniques, the PRAs must be examined from a slightly different perspective than is being investigated by NRC research. The following compares the perspectives of planned NRC research with investigations performed by EPRI

NRC Perspective	EPRI Perspective
Identify digital related failure mechanisms and associated failure modes	Identify what plant mitigating system failure modes should be avoided
Develop techniques for incorporating digital failure modes into PRA models	Identify existing modeling techniques that can be used to reflect undesired failure modes of the plant mitigating systems in the PRA
Establish methods for quantifying the reliability of digital failure modes	Establish what reliability target is needed (application-specific), and what "defensive measures" (design and process elements) should be used to provide reasonable assurance that this reliability will be achieved

Aside from its consideration of dynamic techniques, the NRC's approach to modeling digital equipment is similar to traditional approaches to performing risk evaluations for any plant modification. It is effectively a "bottom up" approach in which the changes to the plant (in terms of the digital system and its failure modes) are incorporated into the PRA and the consequences of these changes objectively determined through a regeneration of the PRA results. The EPRI analysis is more of a "top down" approach in which the objectives of what is to be achieved are first defined (in terms of the mitigating system failure modes to be avoided) and then design features that assure those objectives are met are determined. Both approaches have been used successfully in the past to implement risk-informed changes at nuclear power plants.

The NRC approach is expected to have the advantage of generating detailed knowledge of the important failure modes of various types of digital equipment, as well as producing more precision in terms of the likelihood of these failure modes. The EPRI approach carries with it more uncertainty

with respect to these failure modes and, hence, a higher likelihood of needing additional design features to deal with the uncertainties associated with these failure modes. However, it still offers improvement over the current regulatory approach.

The EPRI approach has the advantages of being available now and, given the use of commonly applied and accepted risk techniques, is capable of providing input to the design of near term digital upgrades before they are installed. If the NRC approach yields practical results, they will not come for several years, so they will have limited potential to influence those upgrades currently in the planning process.

EPRI RESEARCH ON THE APPLICATION OF PRA TO DIGITAL UPGRADES

The EPRI D3 project took a pragmatic approach, acknowledging that precise quantification of software reliability is a very difficult problem. The focus was instead on important engineering insights that can be gained through an understanding the role of the software in the broader context of the plant system and the plant itself. The remainder of this section will summarize this research and demonstrate that the current generation of PRAs are capable of generating a number of insights with respect to the design of digital systems.

In developing an approach for the performance of risk-informed D3 evaluations, EPRI recognized the need to exercise its guidance using actual PRAs. Five plant specific PRAs were obtained from participating utilities for these evaluations, including those for three Westinghouse plants of various vintage, a Combustion Engineering unit and a GE BWR. Some of the PRAs were used to perform simple sensitivity studies on the effects of digital failures at the system level, while others were used to test guidance for complete accident sequences. A general approach to modeling the effects of digital common cause failures evolved as a part of these exercises. The approach considers three factors as being important in the performance of a D3 evaluation using the plant specific PRAs:

Factor A: Reliability of a division of digital I&C (or, conversely, its failure probability).

Factor B: Potential for a redundant division of digital I&C to fail given the failure of the first division (or common cause β factor).

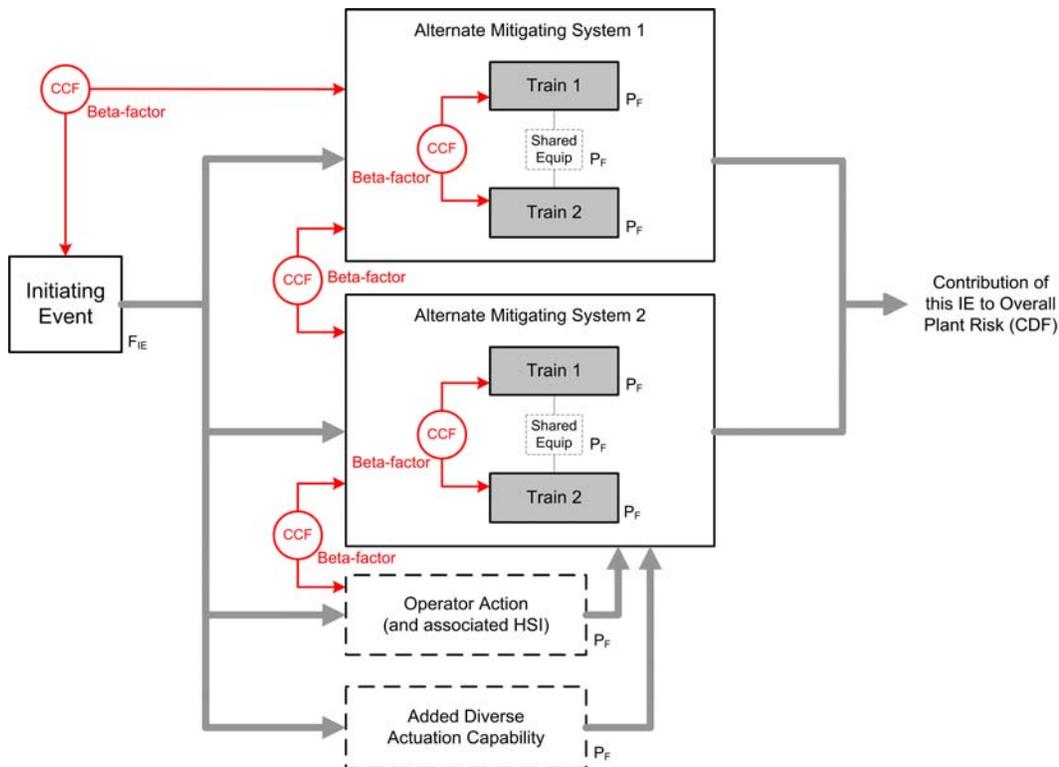
Factor C: Defense-in-depth and diversity between the mechanical and electrical trains of equipment into which the I&C is to be installed.

The reliability block diagram of Figure 1 conceptually illustrates the incorporation of these three factors into the models of a PRA for the evaluation of the possible effects of digital and software related common cause failures.

The product of Factors A and C is taken to represent the potential for common cause failure of the new digital I&C (represented by the common cause beta factors in Figure 1). The EPRI guidance has the analyst perform a review for susceptibilities to digital failures in estimating the probability of these two factors. This review identifies key design features of the digital upgrade which limit the potential for or effect of digital failure mechanisms. Such design features include fault tolerance, self diagnostics, data validation, etc.

Factor C recognizes that the new digital equipment is to be incorporated into mechanical and electrical mitigating systems that are available to respond to a spectrum of initiating events that may occur at the plant. These mechanical and electrical systems carry their own levels of defense-in-depth and diversity, which are desirable to maintain following the installation of the new I&C.

FIGURE 1 - INCORPORATING DIGITAL CCF IN PRA



The explicit consideration of defensive measures outlined by the EPRI guidance results in the identification of potential susceptibilities to digital failure as well as the evaluation of the dominant causes of digital failure and the potential for digital CCF. The consideration of the defense-in-depth and diversity in the existing mitigating systems that are to be controlled by the new I&C provides a determination of where defense-in-depth and diversity in the I&C itself is of value. Together, these factors allow for an integrated look at the effects of potential digital common cause failures on the plant as a whole and not just within the functions performed by the digital I&C itself.

Several general conclusions were reached as a part of the EPRI evaluations using the plant specific PRAs:

I&C as modeled in these PRAs does not typically dominate risk.

It is recognized that this conclusion has limited impact on determination of the risks associated with the final digital upgrade. Its implications, however, are that there is little room for improvement of current risks associated with the plant I&C. If the NRC or the licensee concludes that additional diversity is needed in a digital upgrade beyond that of the existing I&C, this implies that the new digital I&C is perceived to be less reliable than the analog system it is replacing.

The defense-in-depth and diversity of the mitigating systems dictates the level of defense-in-depth and diversity that is of value in the I&C.

In determining where defense-in-depth and diversity is of value in the digital upgrade, it should be kept in mind that this I&C does not itself mitigate an accident but is installed in mechanical and electrical systems that provide the needed mitigating functions in response to specific initiating events. These mechanical and electrical mitigating systems have an inherent level of defense-in-depth and diversity that is modeled explicitly in the plant specific PRAs. Where this existing mechanical and electrical system related defense-in-depth and diversity is important in keeping risk acceptably low, effort should be made not to introduce new common mode failures from the digital I&C that would compromise this defense-in-depth and diversity. What this suggests is that the existing defense-in-depth and diversity found in the mechanical and electrical systems in the plant should be an input to the design and licensing of the digital I&C, as it indicates where defense-in-depth and diversity is of value in the digital upgrade.

The reliability of a digital division of I&C needs only be similar to that of a comparable analog division.

With the recognition that the digital I&C should have similar defense-in-depth and diversity to the mechanical systems into which it is to be installed, it becomes obvious that the digital divisions of I&C need only be as reliable as the analog divisions of equipment that they are replacing. As noted earlier in this section, the EPRI guidance provides a listing of design features of digital equipment that are desirable in assuring that the reliability of the equipment equals or exceeds that of similar analog equipment. These design features are presented as defensive measures against the failure of digital systems and provide assurance that the digital equipment is at least as reliable as comparable analog trains.

IV COMPARISON OF THE CURRENT REGULATORY APPROACH FOR PERFORMING D3 EVALUATION WITH RISK-INFORMED METHODS

Regulatory guidance for the performance of a D3 evaluation is found in the Standard Review Plan under Branch Technical Position HCIB-19 (often referred to as BTP-19) [6]. The NRC's expectation is that a D3 evaluation will be performed for any digital upgrade that involves the reactor trip system (RTS) or engineered safeguards actuation system (ESFAS). As noted earlier, the NRC expects the licensee to reanalyze each event that is evaluated in the accident analyses of the FSAR for every postulated common cause failure that may exist in the new digital system to demonstrate adequate diversity in the design for each of these events. Acceptance criteria for the accident analysis in BTP-19 are as follows and are relaxed to the extent that they do not include traditional fuel and cladding limits:

1. radiological consequences of anticipated operational occurrences considered in the design basis should not exceed 10% of 10CFR100 limits
2. radiological consequences of accidents considered in the design basis shall not exceed 10CFR100 limits.

However, additional criteria are provided regarding the functional effects of common cause failures on RTS and ESFAS:

3. for common mode failures that affect both the control system and the RTS, a diverse means of actuating the RTS shall be provided
and
for common mode failures that affect both the control system and the ESFAS, a diverse means of actuating the ESFAS shall be provided.

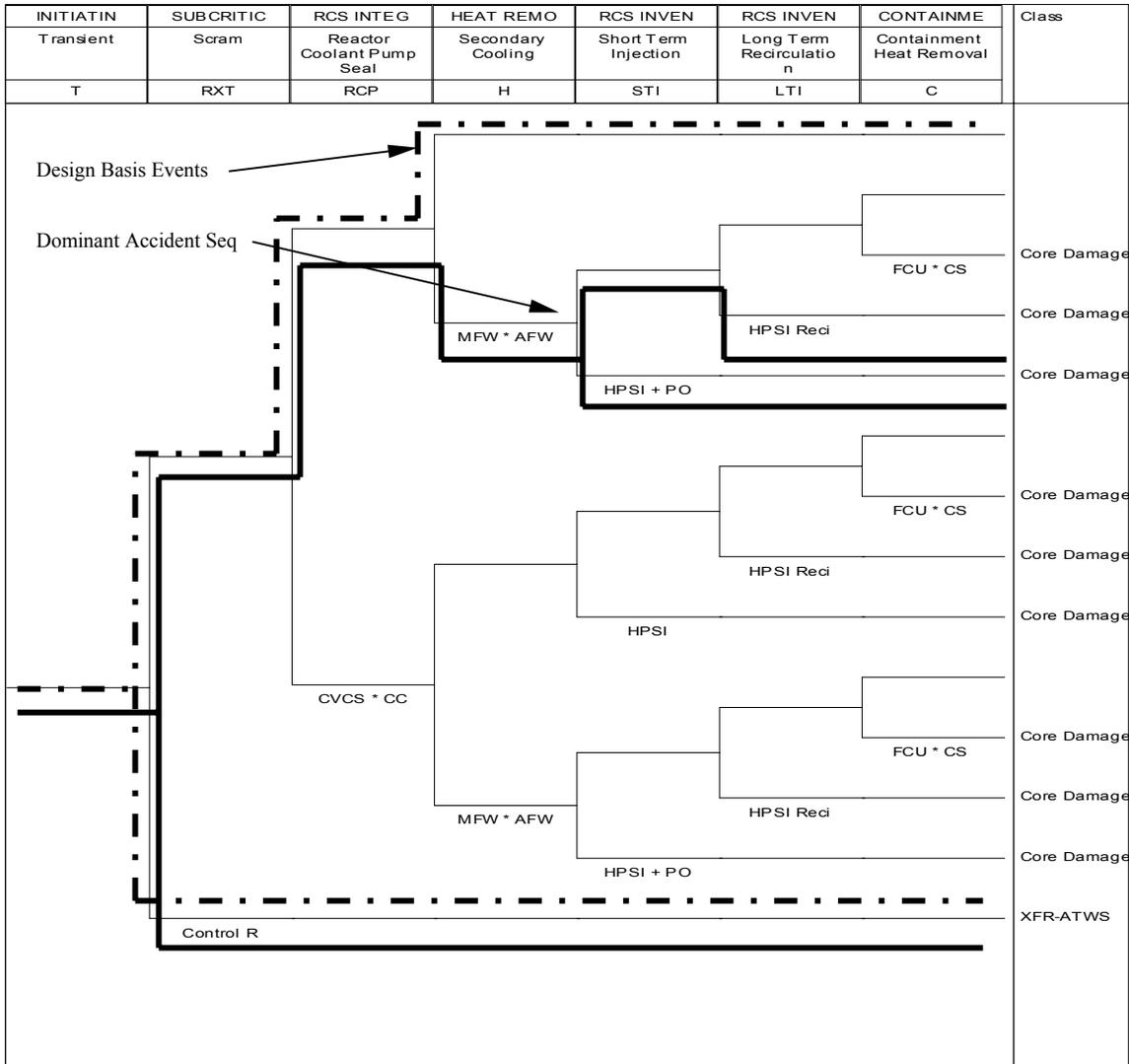
Interconnections between the RTS and ESFAS are permitted provided the requirements of the ATWS rule are met.

In considering risk-informed methods, there are obvious differences between the scope of accident sequences evaluated by BTP-19 and those that are considered in the PRA. Figure 2 illustrates these differences for one initiating event. In Figure 2, the accident sequences for a PWR loss of feedwater are presented. The accident sequences reflect the need for reactor trip and rod insertion, heat removal through secondary cooling and the initiation of feed and bleed operation in accordance with emergency operating procedures should secondary cooling be unavailable. The dominant accident sequences for a typical PWR PRA are noted on the figure.

The transient sequences considered in the accident analysis of the FSAR are also highlighted in Figure 2. It is noted that while the FSAR considers the need for reactor trip and secondary cooling following a loss of feedwater event, initiation of feed and bleed is not considered. As a result, the FSAR analysis (and, hence a D3 evaluation performed in accordance with BTP-19) will not consider loss of both secondary cooling and components that support feed and bleed. In other words, it is not clear that a BTP-19 D3 evaluation will consider the accident sequences that could dominate the PRA and, hence, there is a question as to its completeness in assuring the risks associated with potential software common cause failures have been addressed.

Risk-informed D3 evaluations using the plant-specific PRAs avoid this limitation of BTP-19 by considering accident sequences that go well beyond the design basis. In addition, for design basis events that are of limited safety significance, the plant specific PRAs are an efficient and logical means of identifying the reasons why these events are limited in their impact on safety, thereby providing a technically defensible alternative to the deterministic requirements of BTP-19.

FIGURE 2 - PRA ACCIDENT SEQUENCES



It is often the case that when there are differences in opinion regarding the adequacy of the design of power plant systems, the PRAs can be useful tools in providing insights with respect to the appropriate resolution. In this regard, it may be helpful for utilities to provide the NRC I&C branch results of plant-specific PRAs that clarify pros and cons of modifications to the design before implementing new design requirements that may not have the intended effect on plant safety.

V CONCLUSIONS

In response to obsolescence and increasing maintenance costs, nuclear plant operators are upgrading their existing instrumentation and control systems. Upgrade solutions often include digital technology due to its availability, operating flexibility and potential for performance and reliability improvements. Technical and licensing issues associated with the implementation of a digital upgrade include the need to consider the potential for new behaviors and failure modes caused by software or other digital system design flaws. Current regulatory guidance (BTP-19) directed at the evaluation of digital systems to assure adequate defense-in-depth and diversity against the occurrence of digital common cause failures are resource intensive, often result in added complexity to the plant that does not address safety and is potentially incomplete in addressing risk significant accident sequences.

To address the potential shortcomings of BTP-19, EPRI has developed guidance with respect to the performance of defense-in-depth and diversity evaluations that takes advantage of the existing plant specific PRAs to assure that the final design of the digital system as well as efforts in performing the D3 evaluations focus on areas most important to safety. The risk-informed framework provided by the EPRI guidance not only addresses potential adverse behaviors of digital equipment in risk-significant applications but is a significant improvement over the simple, but overly restrictive assumptions made with respect to software common-cause failure in current regulatory guidance.

Both the industry and the NRC recognize the potential for digital technology to enhance safety and reliability in nuclear power plant operation. However, uncertainty in licensing of digital upgrades based on current regulatory approaches is resulting in delays in the implementation of these systems and increased costs. As the need to replace existing I&C systems becomes more acute, a consensus approach to treating digital technology-related issues is needed to assure consistent and predictable licensing. Accordingly, it would be helpful to both utilities and regulators to consider the insights offered by plant-specific PRAs before implementing I&C upgrades and diverse backups that may not have the desired effect on safety. The EPRI guidance for the performance of D3 evaluations provides such an approach and is consistent with the risk-informed direction that is being taken in other areas of the operation and regulation of the nuclear power industry. EPRI is encouraging the NRC to endorse this guideline for widespread use by nuclear plant operators in the licensing of future digital upgrades.

VI REFERENCES

- 1 Generic Letter 88-20 "Independent Plant Examination for Severe Accident Vulnerabilities", USNRC, November 23, 1988
- 2 "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities", Federal Register Vol. 60 pg. 42622, August 16, 1995
- 3 Transcripts for the 527th Meeting of the ACRS, Digital Systems Research Plan, November 4, 2005
- 4 T. Aldemir, et. al., " Integration of Reliability Models for Nuclear Power Plant Digital Instrumentation and Control Systems into Probabilistic Risk Assessment Studies", PSA '05, International Topical Meeting on Probabilistic Safety Analysis, September 2005

- 5 EPRI 1002835, "Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades - Applying Risk-Informed and Deterministic Methods", December 2004
- 6 USNRC, Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems".