U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-03

Task Working Group #3:
Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments

Interim Staff Guidance
Draft

(Issued for Review and Comment)

January 31, 2008

ML080350109

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-03

Task Working Group #3: Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments

Interim Staff Guidance

Draft
(Issued for Review and Comment)

IMPLEMENTATION

This Interim Staff Guidance (ISG) provides acceptable methods for evaluating digital instrumentation and control system risk assessments. The primary purpose of this document is to provide clear guidance on how NRC reviewers should evaluate digital instrumentation and control (DI&C) system probabilistic risk assessments (PRAs), including addressing inclusion of common cause failures in PRAs and uncertainty analysis associated with new reactor digital systems. This guidance is consistent with current NRC regulations (10CFR52) on performance of risk assessments for new reactors, and NRC policy on Safety Goals and PRAs, and is not intended to be a substitute for NRC regulations, but to clarify how a licensee or applicant may satisfy those regulations and policies.

This ISG also clarifies the criteria the staff would use to evaluate whether a digital system design is consistent with Safety Goal guidelines. The staff intends to continue interacting with stakeholders to refine digital instrumentation and control ISGs and to update associated guidance and generate new guidance where appropriate.

Except in those cases in which a licensee or applicant proposes or has previously established an acceptable alternative method for complying with specified portions of NRC regulations, the NRC staff will use the methods described in this ISG to evaluate compliance with NRC requirements.

1. There is common mis-conception that SW CCF is only about quality of the software development process. This is only one leg of a multi-legged defense. The second leg is an operating system that reduces failure triggers. The third leg of defense is to limit the consequence of application software failures. This is accomplished by forbidding the use of features that may halt the execution of or interfere with other programs on the same computer or system. The last leg of defense is functional diversity, which is effective if operated on a system containing the other three legs of defense. By focusing this discussion primarily upon the probability of a SW fault, important opportunities to affect DI&C reliability are being missed.

1. SCOPE

This interim staff guidance document provides general guidance on how NRC should perform reviews of future DI&C system risk assessments for new reactors (portions may be applicable to operating reactors). It discusses the background of DI&C review guidance and also identifies currently available risk insights for DI&C systems (see Appendix A). The interim staff guidance document is not intended to provide guidance on the scope, level of detail, and technical acceptability of DI&C system risk assessments for plant basis changes, for current or new reactors. This is beyond the scope of this ISG and will be addressed in future regulatory guidance.

2. RATIONALE

In order to prepare this interim staff guidance document, the NRC primarily relied upon the following:

(1) Regulatory Guide 1.200, Revision 1, January 2007, which addresses the technical adequacy of PRAs;

(2) The Commission policy statement on the use of PRA methods in nuclear regulatory activities;

(3) Regulatory Guide 1.174, Revision 1 on using PRA in making risk-informed decisions;

(4) Final Safety Evaluation Report (FSER) of the AP1000 Standard Design;

(5) FSER of the Advance Boiling Water Reactor Design

3. BACKGROUND

DI&C systems are complex combinations of hardware components and software (i.e., computer programs). This combination of complex hardware and software can result in the presence of faults and failure modes unique to DI&C systems. For DI&C systems, failures arise from the combination of a fault in the system in conjunction with a set of circumstances (e.g., a plant transient or accident) that satisfies the conditions required for the fault to be exercised. When exercised, the fault may result in a DI&C system failure. Although software does not wear out over time, excitation of system faults can cause significant system failures. The nuclear industry has purposed to design and implement DI&C systems in new reactors that have a low probability of containing significant faults. In particular, the designers have attempted to reduce the likelihood of DI&C common cause failure (CCF). There is uncertainty as to the actual CCF rate in these DI&C systems, and the NRC considers it prudent to be cautious as it is extremely difficult to either accurately predict or verify such failure rates. If one could eliminate all software errors before a system is put into operation, the software would work perfectly. However, experience shows that one cannot ensure that faults do not continue to exist in complex DI&C systems that can cause a system failure when the system is exposed to an operating environment or profile for which it was not designed, tested, or used. Exposure to such an operating environment or profile for nuclear power plants is

2. Suggest rewording to "The nuclear industry has proposed to design and implement DI&C systems in new reactors that have a low probability of containing significant faults, that reduce the probability of failure triggers, that limit failure propagation, and contain appropriate functional diversity. In particular, the designers have attempted to reduce the likelihood and consequence of DI&C common cause failure (CCF). ... However, experience shows that one cannot ensure that faults do not continue to exist in complex DI&C systems that can cause a system failure when the system is exposed to an operating environment or profile for which it was not designed, tested, or used. Therefore designers also attempt to eliminate untested software paths and reduce the sensitivity of their systems to failure triggers in the operating environment."

possible because there are a large number of possible states and inputs for a DI&C system. When trying to estimate DI&C system reliability, it must be remembered that each DI&C system, including software, is unique, and extrapolation of statistical data from other systems may not necessarily be meaningful. Likewise, extrapolation of statistical data from the same system being used in a different operating environment or profile is not necessarily meaningful.

Systems consisting of hardware and software may not fail the way hardware fails due to wear-out. Therefore, commonly used hardware redundancy techniques may not improve software reliability. It generally is accepted that high reliability can be achieved for DI&C systems by following formal and disciplined methods during the system development process, combined with a testing program based on expected use and by controlling operational use.

3. Suggest adding, "In addition, hardware and operating system designs that reduce failure triggers and limit failure propagation are important to DI&C reliability."

Although the industry has made an effort to reduce the probability of significant faults, the NRC and industry recognize that not all failures, including CCF, can be eliminated in complex DI&C systems. To address this issue, comprehensive deterministic guidance was developed by the NRC and industry for new as well as operating nuclear power plants to address the unique failure modes of DI&C systems, specifically common cause DI&C system failures. DI&C system CCFs were recognized as having the potential to simultaneously and independently affect systems, channels, divisions, or trains. These failures could negate the defense-in-depth (D3) features assumed adequate in the traditional analog systems the DI&C systems are replacing. The deterministic guidance is based, in part, on digital system development processes and methods recognized for producing quality software and known to avoid, remove, detect, or tolerate the effects of faults including those leading to DI&C software CCF. Other parts of the process include the use or development of highly reliable hardware. Because these processes and methods have not been shown to be fully effective, acceptance guidance or metrics are needed to establish a DI&C system's overall quality and reliability. A project is underway by the NRC Office of Nuclear Regulatory Research to develop a set of metrics for evaluating the quality of a digital system development processes.

4. Probability and consequence

5. Suggest deleting, as this is an oxymoron - CCFs are not independent.

6. Change to: of highly reliable hardware and operating systems.

The deterministic guidance is designed to help assure that adequate defense-in-depth is maintained such that the effects of a DI&C system CCF are appropriately limited. Adequate defense-in-depth is judged to occur if additional means remain available to perform required reactor trip and engineered safety features functions for each event evaluated in the accident analysis.

7. Suggest replacing the highlighted text with "if the acceptance criteria of BTP-19 is met."

The current methodology for a deterministic defense-in-depth and diversity assessment uses an approach similar to a single failure analysis but with the difference that a DI&C system CCF is analyzed as a beyond the design basis event and therefore not subject to a traditional single failure analysis. Consequently, the assessment uses relaxed assumptions and acceptance criteria to evaluate the effect of each single postulated CCF, coincident with each design basis accident and anticipated operational occurrence. Therefore, in addition to a traditional single failure criterion evaluation to determine adequate redundancy, the staff addresses DI&C system CCFs by also including an assessment of independence and diversity to establish whether (1) adequate diversity has been provided, (2) adequate defense-in depth has been provided, and (3) displays and manual controls for critical safety functions initiated by operator action are diverse from the DI&C system used for the automatic protection system. Attributes of the above guidance and methodology include Commission policy, conclusions, and direction that:

8. Change to "failure modes and effects analysis."

9. Change to "and therefore are not required to be included as a part of a traditional single failure analysis."

10. This does not accurately reflect the four points of BTP-19 or its acceptance criteria.

(1) A DI&C system CCF (i.e., particularly software), although possible, is expected to be a relatively rare.

(2) DI&C system CCF are analyzed as beyond design basis events.

(3) The assessment may be performed using realistic methods.

(4) For a postulated DI&C system CCF that could disable a safety function, a diverse means to accomplish the safety function (i.e., a method unlikely to be subject to the same CCF) shall be required.

(5) The diverse means may be a different function and may be performed by a non-safety system of sufficient quality to perform the function.

(6) A set of independent and diverse displays and controls are to be provided in the control room for manual system-level actuation and monitoring of critical safety functions. These displays also may be non-safety related.

11. Suggest deleting

Experience with implementation of the above deterministic guidance has shown that reviews have involved significant NRC effort in the evaluation of whether D3 is adequate. Although issues have been identified with operating reactor and new reactor 10 CFR 52 design certification (DC) and combined operating license (COL) applications, the review of DI&C systems is more challenging for operating reactors. The main reason is that with a DI&C retrofit of an operating plant, the same degree of defense-in-depth may not be available for each event in the safety analysis that was provided prior to the retrofit by the analog system. This has tended to result in licensees providing additional hardware, software, procedures, or commitments so that the operating plant retrofit fully meets NUREG-0800, Chapter 7 deterministic acceptance criteria.

12. It is not clear that the additional commitments are required by regulation. It is also not clear why this is here given that the guidance is for DC/COL PRAs.

New reactors licensed under 10 CFR 52 are required to have a PRA (a design-specific PRA at the DC stage as well as site-specific PRA at the COL stage) and are reviewed to both Chapter 7, NUREG-800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," deterministic guidance and Chapter 19, NUREG-800 guidance. However, due to data limitations[1] and the lack of consensus modeling tools, the assessment of DI&C system risk for new plants has been limited to examining assumptions, performing sensitivity studies, and evaluating importance measure values. The resulting plant risk then is assessed against the Commission's Safety Goals. In general, these limitations make it difficult to develop robust risk insights about DI&C systems. For the new reactor risk assessments performed to date and reviewed by the NRC, the inclusion in the design of a diverse backup system has been found to positively affect PRA safety insights (i.e., a diverse backup system provides assurance

13. The industry disagrees with much of this material. Significant insights have been generated regarding digital systems using PRA. It is not clear why the staff is attempting to justify the need for diverse actuation systems in guidance that is supposed to be directed at reviewing DC/ COL PRAs.

[1] Software is normally developed by a team of people who implement the software's design requirements. Specific software is tailored to those specific requirements, and thus, it is functionally and structurally different to any other software. Accordingly, if a technically sound method or process was employed to obtain a probabilistic parameter of a software, such as its probability of failure, in general this probability cannot be applied to any other software. Therefore, substantial technical justification must be given for assuming a probabilistic parameter from one set of software can be used for different software.

that certain safety functions will be performed given a failure of the DI&C systems) (1) by limiting the uncertainties inherent in DI&C including software and (2) by satisfying the defense-in-depth acceptance criteria of branch technical position (BTP) 7-19 and SECY 93-87.

The first of the new reactor designs submitted limited information about their DI&C systems in part because the DI&C technology was changing rapidly and it was determined that it was not prudent to freeze the DI&C designs years prior to plant construction. The DI&C designs for the Advanced Boiling Water Reactor, System 80+, AP600, and AP1000 reactors were submitted to the NRC so it could complete the DC reviews. Each of the vendors also developed design-specific PRAs that modeled the DI&C systems at a high level. High-level modeling was necessary since DI&C design details were postponed until the COL stage. In addition, an acceptable state-of-the-art method for detailed PRA modeling of DI&C systems has not been established within the technical community. It was recognized that while a variety of methods might be acceptable for some applications, the NRC is not yet confident in how specific decisions should be mapped to levels of PRA detail. While bounding PRA analyses may provide needed insights in very specific cases, the Commission has made it clear that it believes that realistic risk assessments should be performed whenever possible since bounding analyses may mask important safety insights and can distort a plant's risk profile and bounding analysis may not adequately address unique digital system failure modes. An advance in the state-of-the-art may be needed to permit a comprehensive risk-informed decision-making framework in licensing reviews of DI&C systems for future and current reactors.

Despite the limitations, NRC's reviews of DI&C risk assessments performed to date produced important lessons learned and insights, including the following:

(1) As modeled in the risk assessments, the DI&C contributions to CDF and risk were relatively insensitive to moderate changes in failure rates assumed for individual DI&C components,

(2) risk assessment modeling of DI&C systems has significant uncertainties,

(3) data for digital component failure rates have high uncertainties,

(4) CCF rates of DI&C software have high uncertainties,

(5) assumptions concerning DI&C CCF, (e.g., inter-channel, inter-system, inter-train) can influence CDF and substantially affect risk insights and,

(6) RAW importance measures for CCF of DI&C system components often are very large.

There is a lack of consensus in the technical community that methods normally employed when performing PRAs are adequate for the purpose of making comprehensive risk-informed decisions for DI&C. In spite of this, the NRC and industry recognize that current PRA methods can provide useful, high-level risk information about DI&C systems (e.g., insights on what aspects of, or assumptions about, the DI&C systems are most important, and approximation of the degree to which the risk associated with operation of these systems is sensitive to failure rate assumptions). The

14. The deterministic D3 assessment (discussed one page back) is itself such a "bounding analysis" that may mask important safety insights. By assuming the worst case CCF, it drives the design towards separate backup systems (aka DAS), and diverts focus from the main DI&C system and its features, and ensuring that it is designed well in the first place. Therefore, since this is a PRA document, it would be useful to add a paragraph after this one to caution that the PRA should not blindly adopt the bounding CCF assumptions made in the deterministic D3 assessment, and should instead attempt to be realistic in assigning the probability and scope of CCFs.

15. These methods have been established, but have not been accepted by the NRC. Suggest replacing "acceptable state-of-the-art" with "a consensus."

16. This does not mean that PRA cannot be used for this purpose now.

17. This insight, as well as number 1, is the product of bounding analysis assumptions (which were derived from the deterministic D3 process) that is cautioned against in the last paragraph.

18. EPRI believes it is possible to design a DI&C system for which this is not the case.

NRC Office of Regulatory Research has a long-term project to determine if risk assessment methods are available or can be developed to appropriately model DI&C risk.

Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," provides guidance on evaluating the technical adequacy of PRAs. As noted in Element 1.1 of Table A-1 in Appendix A to Regulatory Guide 1.200, special emphasis should be placed on PRA modeling of novel and passive features in the design, as well as addressing issues related to those features, such as DI&C , explosive (squib) valves, and the issue of thermal-hydraulic uncertainties. The regulatory guide (RG), itself, only provides limited guidance on how to model and evaluate DI&C systems. It does not address completeness issues, level of modeling detail needed, or how to address the uncertainties associated with DI&C system modeling and data. Guidance as to what risk metrics are appropriate for evaluating the acceptability of DI&C systems also may be needed. See also RG 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)'," Section C,I.19.5 Technical Adequacy.

19. Regulatory guide 1.206 is likely the correct reference.

The NRC established the Risk-Informing Digital Instrumentation and Control Task Working group (TWG # 3) to address issues related to the risk assessment of DI&C systems. The TWG # 3's efforts are to be consistent with the NRC's policy statement on PRA, which states in part that the NRC supports the use of PRA in 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." One aspect of the charter of TWG # 3 is to resolve the following problem statement:

> Existing guidance does not provide sufficient clarity on how to use current methods to properly review models of DI&C systems in PRAs for design certificate applications or COL applications under Part 52. The issue includes addressing CCF modeling and uncertainty analysis associated with DI&C systems.

This guidance document provides clear direction on how NRC reviewers should evaluate new reactor DI&C risk assessments.

4. STAFF POSITION

The difficulties and limitations associated with performing a risk assessment of DI&C systems are discussed in the Background section of this guidance document. It is expected that a PRA reviewer will need to interface with a DI&C reviewer on many areas of the PRA review. The DI&C risk assessment methods have the potential to disclose design problems in DI&C systems that are significant. The level of uncertainty associated with DI&C risk assessment results and insights (in part due to a lack of consensus in the technical community over acceptable PRA models for DI&C risk assessments and limited applicable data) is high. The uncertainties currently are large enough to reinforce the need for diversity, defense-in-depth, adequate safety margins, and the deterministic requirements designed to assure their continued existence.

20. Nobody is advocating the removal of diversity, defense-in-depth, or safety margins. We only object to whether the said deterministic requirements are the best way to provide them.

To date, the reviews of risk assessments for the ABWR, AP600, and AP1000 designs and more recent work conducted by the NRC Office of Regulatory Research have

provided limited but important insights into DI&C systems, in particular in the area of identifying assumptions and parameters that must be assured to be valid in the as-built, as-operated nuclear power plant. To ensure confidence in the validity of the insights drawn from PRAs, the NRC normally evaluates the PRA against the guidance outlined in RG 1.200. However, RG 1.200 provides limited information on how to perform or review the portion of the PRA modeling the DI&C system. As a result, the NRC has developed guidance on how to review DI&C system risk assessments based on the lessons learned from previously accepted new reactor DI&C system PRA reviews.

The attributes outlined here should help a reviewer identify the areas of the DI&C design and operation that require additional regulatory attention and they should help identify if there are high-level, risk-significant problems in a DI&C system. Potential problems that might be identified include the following:

(1) Installation of the system would raise the frequency of low risk contributors to an unacceptable level,

(2) Installation of the system would introduce significant new failure modes not previously analyzed, or

(3) It would become apparent that areas of the DI&C system design (i.e., hardware or software) are in need of additional regulatory attention (e.g., coverage under Technical Specifications, enhanced treatment, or improved reliability goals under the Maintenance Rule).

Based on PRA reviews the NRC has previously performed on new reactor DI&C systems and recent research activities, the following review guidelines are provided:

A. The review should consider the following steps, as applicable, to ensure that the risk contributions from DI&C, including software, are reflected adequately in the overall plant risk results:

(1) Review the DI&C portion of the PRA as an integrated part of the overall PRA review. Perform all the normal aspects of a PRA review including evaluation of the quality of the PRA. The level of review of the DI&C portion of the PRA may be limited due to limitations such as the lack of design details, lack of applicable data, and the lack of consensus in the technical community regarding acceptable modeling techniques for determining the risk significance of the DI&C system. The level of review should be proportional to the use of the results and insights from the DI&C risk assessment.

(2) Uncertainties in DI&C modeling and data should be addressed in the DI&C risk assessment. It is expected that the DI&C risk assessment will address uncertainties by at least performing a number of sensitivity studies that vary modeling assumptions, reliability data, and parameter values both at the component and system level. The reviewer should evaluate the sensitivity studies performed by the applicant on the PRA models and data to assess the effect of uncertainty on CDF, risk, and PRA insights. Sensitivity study scenarios that may be appropriate and if provided should be reviewed include the following:

a. Increase all software failure probabilities (for each types of software employed including application, platform, and support) and evaluate the change in CDF compared to the base case.

b. Increase all software failure probabilities (including application, platform, and support software) while simultaneously assuming that all non-safety-related defense-in-depth systems become unavailable with the exception of diverse backup systems, while the plant continues to operate at power. Evaluate the change in CDF and compare it to the base case.

c . Increase all software failure probabilities (including application, platform, and support software) while simultaneously assuming that all non-safety-related defense-in-depth systems (including diverse backup systems) become unavailable, and the plant continues to operate at power. Evaluate the change in CDF and compare it to the base case.

d. Ensure the effect of DI&C system CCF assumptions properly reflects the system architecture, connections, and hardware and/or software failure modes. If it does not, increase the CCF scope in a sensitivity study.

e. Increase the DI&C CCF rates including software (for each type of software employed including application, platform, and support software) of the DI&C system and evaluate the change in CDF compared to the base case.

f. Increase the DI&C CCF rates, including software (including application, platform, and support software) and increase the associated human error rates, and evaluate the change in CDF compared to the base case.

(3) The reviewer should confirm that DI&C system equipment is capable of meeting its safety function for the environment assumed in the PRA.

(4) The reviewer should confirm that the impact of external events (i.e., seismic, fire, high winds, flood and others) has been addressed with regard to DI&C.

(5) Evaluate the acceptability of how the failure of control room indication is modeled.

(6) Important scope, boundary condition, and modeling assumptions need to be determined and evaluated. Verify that the assumptions made in developing the reliability model and probabilistic data are realistic, and the associated technical justifications are sound and documented. The reviewer should pay attention to assumptions about the potential effects from failure of an automatic tester system. Such a system may have the downside of causing spurious trips or spuriously failing functional capabilities. In a typical microprocessor-based system, the functions are in a single program such that a failure caused by one function will prevent the other functions from being performed. The licensee should describe the segregation process that prevents this from occurring. The reviewer should work with the DI&C reviewer to evaluate the reasoning given by the applicant.

21. This sentence is simply not true for today's systems. It is a fundamental design principle of some platform designs that failure of an application software function not be allowed to propagate to other functions. A better wording of this sentence would be: "In some microprocessor-based systems the functions may be in a single program such that failure caused by one function may prevent the other functions from being performed."

(7) The reviewer should evaluate the acceptability of the recovery actions taken for loss of DI&C functions referring to RG 1.200 and HRA Good Practices NUREGs for additional guidance. Coordinate the review with staff evaluating areas such as main control room design, and minimum alarms and controls inventory requirements. If recovery actions are modeled, they should consider loss of instrumentation and the time available.

(8) Ensure that CCF events are identified and modeled properly, and that CCF probabilities are estimated based on an evaluation of coupling mechanisms (e.g., similarity, design defects, external events, and environmental effects) combined with an evaluation of design features meant to protect against CCF (e.g., separation, operational testing, maintenance, diagnostics, self-testing, or fault tolerance). Failures of system modules common across multiple applications should be considered (e.g., look at CCF of common function modules.) If the safety functions of a DI&C system (and/or the redundancy within safety functions) use common software, a degree of dependency should be assumed for software faults. That is, when common software is used for different safety functions (and or in the redundancy within a safety function), it should be assumed to fail in each function. Hardware CCF between different safety functions using the same hardware should be modeled. Dependencies between hardware and software should be modeled. The DI&C dependency should represent both the presence of a DI&C software fault and the conditions required for the fault to be exercised (i.e., associated trigger mechanism). In determining the dependence of common software, its similarity should be considered in determining the extent of dependency (It has been demonstrated by Knight and Leveson and others that it is not possible to develop redundant software (with common specifications) that does not have any dependencies or determine how two software designs will differ in their failure behavior.). The applicant should provide the rationale for the degree of dependency assumed for DI&C CCF.

An important expectation is that the reviewer will evaluate whether the applicant included the appropriate equipment in the CCF groups. The reviewer should work with the I&C expert and review the applicant's justifications. The discussion should also address why or why not various channels, trains, systems, etc. were placed in each CCF group. It is expected that the justification would discuss common software/hardware among the equipment considered and the level(s) of dependency among them. CCF analysis methods available in SRP Chapter 7, BTP 7-19 and NUREG/CR-6303 provide information on functional diversity and design features believed to reduce the likelihood of CCF.

(9) It is important to evaluate the level of confidence in claims by applicants regarding the credit that should be given for defensive design features. If the design features (e.g., fault tolerance, diagnostics or self testing) are relied upon to help keep the probability of the DI&C system failure low, then an implementation and monitoring program should address how the applicant will assure that the design features continue to support the assumed reliability of the systems and components shown to have high risk importance by PRA sensitivity studies.

(10) Verify that a method for quantifying the contribution of software failures to DI&C system reliability was used and documented.

(11) Examine applicant documentation to assure the dominant failure modes of the DI&C risk assessment are documented with a description of the sequence of events that need to take place and how the failure modes can fail the system. The sequence of events should realistically represent the system's behavior at the level of detail of the model.

(12) The reviewer should evaluate the sensitivity study results to determine if the DI&C system would challenge the ability of the design to meet the Commission's Safety Goal Policy. Once sensitivity studies have been performed, the applicant is expected to compare the resulting risk results (e.g., CDF, large release frequency (LRF)) to the NRC's Safety Goals. It is not expected that the sensitivity studies will show that the risk results associated with DI&C systems will exceed the Safety Goals. Rather, it is expected that the sensitivity studies will show there is adequate margin to the Safety Goals. However, if sensitivity studies identify systems or components that would significantly increase CDF or risk due to changes in DI&C failure probabilities (including software), the reviewer should document these results for consideration of what, if any, actions should be taken. As with any risk assessment, a reviewer should determine if the applicant has performed a balanced review and has considered the need to increase requirements or regulatory attention to aspects of the design or operation based on the sensitivity studies and other risk insights. If a balance has not been met, the reviewer should document this and submit it to the reviewer's management. Note, just because the results of a specific sensitivity study may challenge the Safety Goals does not necessarily imply that additional requirements or regulatory attention are necessary, since the particular sensitivity study may involve a very unlikely scenario or set of failure events.

(13) Systems and components necessary to assure that the DI&C system remains highly reliable should be in a monitoring program.

(14) Verify that key assumptions from the DI&C PRA are captured under the applicant's design reliability assurance program (D-RAP), which is described in SRP Chapter 17, Section 17.4. The applicant should describe adequately where and how the D-RAP captures the DI&C system key assumptions. Target reliability and availability specifications should be described adequately for the operational phase of D-RAP (details of the operational phase are provided in SRP Section 17.6). If the PRA lacks sufficient quantitative results to determine target values, the applicant should describe adequately how expert judgment will establish reliability and availability requirements. These specified values should be defined to help ensure that no safety conclusions based on review of the risk analysis of the DI&C are compromised once the plant is operational. How the licensee will carry out performance monitoring for diverse backup systems (if necessary) and DI&C systems should be clearly explained. Coordinate this review with NRC staff evaluating the DI&C system's D3 capabilities. An implementation and monitoring program should address how the

applicant will assure that the design continues to reflect the assumed reliability of the systems and components during plant operation.

B. The review also should include the following additional steps, as applicable, if a more detailed review is needed (e.g., through field audits):

(1) The modeling of DI&C systems should include the identification of how DI&C systems can fail and what their failure can affect. The failure modes of DI&C systems are often identified by the performance of failure modes and effects analyses (FMEA). It is difficult to define DI&C system failure modes because they occur in various ways depending on specific applications. Also, failure modes, causes, or effects often are intertwined or defined ambiguously, and sometimes they overlap or even are contradictory. The reviewer should review the depth of the FMEA or other hazard analysis techniques employed by the applicant and ensure they are complete.

(2) Verify that physical and logical dependencies were captured adequately in the DI&C PRA as needed. The probabilistic model should encompass all the relevant dependencies of a DI&C system on its support systems. If the same DI&C hardware is used for implementing several DI&C systems that perform different functions, a failure in the hardware, software, or system of the DI&C platform may adversely affect all these functions. Should these functions be needed at the same time, they would be affected simultaneously. This impact should be explicitly included in the probabilistic model. The DI&C system probabilistic model should be fully integrated with the probabilistic model of other systems.

(3) Ensure that spurious actuations of diverse backup systems or functions are evaluated and the overall risk impact documented.

(4) Common cause failures can occur in areas where there is sharing of design, application, or functional attributes, or where there is sharing of environmental challenges. Review the extent to which the DI&C systems were examined by the applicant to determine the existence of such areas. Each of the areas found to share such attributes should be evaluated in the DI&C analysis to determine where CCF should be modeled and to estimate their contribution. Based on the results of this evaluation, D&IC software and/or hardware/software dependent CCFs may need to be applied in several areas within subsystems (e.g., logic groups), among subsystems of the same division, across divisions or trains, and across systems. For example, CCF assignments of DI&C components and systems in the AP1000 PRA were based on similarity in design and function of component or system modules, including software. The level of modeling detail was carried to the circuit board or line replaceable unit level. Recognize that there is on-going research into how to best model DI&C CCFs (including software CCF) in PRAs, and that the CCF modeling in new reactor PRAs prior to 2008 should not be considered state of-the-art.

(5) Design features such as fault tolerance, diagnostics, and self testing are intended to increase the availability and reliability of DI&C systems, and

therefore are expected to have a positive effect on the system's reliability. However, these features also may have a negative impact on the reliability of DI&C systems if they are not designed properly or fail to operate appropriately. The potentially negative effects of these features should be included in the probabilistic model. The PRA should account for the possibility that after a failure is detected, the system may fail to re-configure properly, or may be set up into a configuration that is less reliable than the original one, fail to mitigate the failure altogether, or the design feature itself may contain a fault. The benefits of these features also may be credited in the PRA. Care should be taken to ensure that design feature intended to improve the availability and reliability are modeled correctly (e.g., ensuring that the beneficial impacts of these features are only credited for appropriate failure modes and the limitations including failure of the design feature itself is considered in the model).

An issue with including a design feature such as fault-tolerance in a DI&C system modeled in a PRA is that its design may be such that it only can detect, and hence mitigate, certain types of failures. A feature may not detect all the failure modes of the associated component, but just the ones it was designed to detect. The PRA model should only give credit to the ability of these features to automatically mitigate these specific failure modes; it should consider that all remaining failure modes cannot be automatically tolerated. Those failure modes that were not tested should not be considered to be included in the fault coverage, but should be included explicitly in the logic model.

When a specific datum from a generic database, such as a failure rate of a digital component, is used in a DI&C risk assessment, the reviewer should assess whether the datum was adjusted for the contribution of design features specifically intended to limit postulated failures. If so, the failure rate may be used in the PRA, but no additional fault coverage should be applied to the component, unless it is demonstrated that the two fault coverages are independent. Otherwise, applying the same or similar fault coverages would generate a non-conservative estimate of the component's failure rate. A fault-tolerant feature of a DI&C system can be explicitly included either in the logic model or in the PRA data, but not both.

With respect to the above design features, the concept of fault coverage is used to express the probability that a failure will be tolerated for the types of failures that were tested. Fault coverage is a function of the failures that were used in testing. It is essential to be aware of the types of failures that were used in testing to apply a value of fault coverage to a PRA model.

It should be noted that how fault coverage is measured and defined should be provided by the applicant and evaluated by the reviewer in conjunction with the DI&C reviewer.

(6) If a DI&C system shares a communication network with others, the effects on all systems due to failures of the network should be modeled jointly. The impact of communication faults and their effects on the related components or systems should be evaluated, and any failure considered relevant should

be included in the probabilistic model.

(7) If hardware, software, and system CCF probabilities are treated together in the PRA, they could be estimated using the multiple Greek letter method, alpha factor method, or beta factor method. An NRC audit of these calculations may be warranted.

(8) The data for hardware failure rates (including CCF) probably will be more robust than the software failure data. NRC audits of data calculations may be warranted. Data are a weak link in the evaluation of risk for DI&C systems. The guidelines in Subsection 4.5.6, "Data analysis," of the ASME standard for PRA for nuclear power plant applications should be satisfied consistent with the clarifications and qualifications of RG 1.200. Determine if the manner in which basic event probabilities were established is acceptable and if the rates seem reasonable. Check the assumptions made in calculating the probabilities of basic events (unavailabilities). Confirm that the data used in the PRA are appropriate for the hardware and/or software version being modeled, or that adequate justification is provided.

Note, a fault-tolerant feature of a DI&C system (or one of its components) can be explicitly included either in the logic model or in the probabilistic data of the components in the model. It should not be included in both because this would result in double-counting the feature's contribution.

(9) Confirm data meet the following:

a. The data are obtained from the operating experience of the same equipment as that being evaluated, and preferably in the same or similar applications and operating environment. Uncertainty bounds should be appropriately reflect the level of uncertainty. (both component-specific and generic data)

b. The sources for raw data or generic databases are provided. (both component-specific and generic data)

c. The method used in estimating the parameters is documented, so that the results can be reproduced. (component-specific data)

d. If the system being modeled is qualified for its environment but the data obtained are not so subject, the data should account for the differences in application environments. (both component-specific and generic data)

e. Data for CCF meet the above criteria in 9d. (both component-specific and generic data)

f. Data for fault coverage meet the above criteria in 9d. (both component-specific and generic data)

g. Documentation is included on how the basic event probabilities are calculated in terms of failure rates, mission times, and test and maintenance frequencies. (both component-specific and generic data)

(10) The use of DI&C systems in nuclear power plants raises the issue of dynamic interactions, specifically

a. the interactions between a plant system and the plant's physical processes, i.e., the values of process variables, and

b. the interactions within a DI&C system (e.g., communication between different components, multi-tasking, multiplexing, etc.).

The reviewer should confirm that interactions have been addressed in the PRA model for DI&C systems or should evaluate the rationale for not modeling them.

5. ACRONYMS

ABWR	Advanced Boiling Water Reactor
AP600	a Westinghouse designed 600 MWe passive nuclear power plant
AP1000	a Westinghouse designed 1000 MWe passive nuclear power plant
ATWS	anticipated transient without scram
CCF	common cause failure
CDF	core damage frequency
CFR	Code of Federal Regulations
COL	combined operating license
DAC	design acceptance criteria
DAS	diverse actuation system
DC	design certification
DI&C	digital instrumentation and control
ESF	engineered safeguards feature
FMEA	failure modes and effects analysis
GE	General Electric Company
HRA	human reliability assessment
I&C	instrumentation and control
LERF	large early release frequency
LRF	large release frequency
MWe	megawatt electric
NRC	Nuclear Regulatory Commission
PLS	plant control system
PMS	protection and safety monitoring system
PRA	probabilistic risk assessment
RAW	risk achievement worth
RG	regulatory guide
RTNSS	regulatory treatment of non-safety systems
SYSTEM 80+	a new nuclear reactor design from the former Combustion Engineering Company
TWG-3	Task Working Group # 3

6. REFERENCES

1. U.S. Nuclear Regulatory Commission, "Policy, Technical, and licensing issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," Commission Paper SECY 93-87, April 2, 1993 and the associated Staff Requirements Memorandum, July 21, 1993.

2. U.S. Nuclear Regulatory Commission, "Standard Review Plan," "Guidance for the Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," NUREG-0800, Chapter 7, Branch Technical Position 7-19, Revision 5 (BTP-19), March 2007.

3. U.S. Nuclear Regulatory Commission, "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities," Volumes 1 and 2, NUREG/CR-6850, September 2005.

4. U.S. Nuclear Regulatory Commission, "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments," NUREG/CR-6901, February 2006.

5. *U.S. Code of Federal Regulations*, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," Part 52, Title 10, "Energy."

6. U.S. Nuclear Regulatory Commission, Safety Goals for the Operation of Nuclear Power Plants; Policy Statement, 51 FR 300028; August 21, 1986.

7. U.S. Nuclear Regulatory Commission, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," Regulatory Guide 1.200, Revision 1, January 2007.

8. U.S. Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Policy Statement", *Federal Register*, Vol. 60, No. 158, pp. 42622-42629, August 16, 1995.

9. U.S. Nuclear Regulatory Commission, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis", Regulatory Guide 1.174, Revision 1, November 2002.

10. U.S. Nuclear Regulatory Commission, "Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design," NUREG-1793, September 2004.

11. U.S. Nuclear Regulatory Commission, "Final Safety Evaluation Report Related to the Certification of the Advance Boiling Water Reactor Design," NUREG-1462, August 1994.

12. U.S. Nuclear Regulatory Commission, "Final Safety Evaluation Report Related to the Certification of the AP600 Standard Design," NUREG-1512, September 1998.

13. U.S. Nuclear Regulatory Commission, "Final Safety Evaluation Report Related to the Certification of the System 80+ Design, Docket No. 52-002," NUREG-1503, July 1994.

14. U.S. Nuclear Regulatory Commission, “Digital Computer Systems for Advanced Light Water Reactors,” Commission Paper SECY-91-292, September 16, 1991.

15. John C. Knight and Nancy G. Leveson. An experimental evaluation of the assumption of independence in multi-version programming. IEEE Transactions on Software Engineering, SE-12(1):96-109, January 1996.

16. National Research Council, “Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues”, National Academy Press, 1997.

17. S.A. Arndt, N.O. Siu, and E.A. Thornsbury, "What PRA Needs From a Digital Systems Analysis," Probabilistic Safety Assessment and Management , E.J. Bonano, A.L. Camp, M.J. Majors and R.A. Thompson (Eds.), 1917-1922, Elsevier Science Publishing Co., New York (2001).

18. S. Arndt, "Development of Regulatory Guidance for Risk-Informing Digital System Reviews," Proceedings of the 5th ANS International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, November 2006.

19. N. Storey, “*Safety-Critical Computer Systems*,” Addison Wesley Longman (1996).

20. Hoang Pham, “*Software Reliability*,” Springer-Verlag Singapore Pte. Ltd. (2000).

21. U.S. Nuclear Regulatory Commission, “Combined License Applications for Nuclear Power Plants (LWR Edition),” Regulatory Guide 1.206, June 2007.

22. U.S. Nuclear Regulatory Commission, “Method for Performing Defense-In-Depth and. Diversity Analyses of the Reactor Protection System". NUREG/CR-6303, December 1994.

23. U.S. Nuclear Regulatory Commission, “Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments,” NUREG/CR-6901, February 2006.

24. U.S. Nuclear Regulatory Commission, “Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments,” NUREG/CR-6942, October 2007.

APPENDIX A

Insights from Risk Assessments Performed for New Reactor DI&C Systems

The following are general insights drawn from previously reviewed new reactor DI&C system risk assessments. Subjective judgment was used to assign levels (low, medium, high) of uncertainty to these seven insights:

(1) The absolute value of the contribution to CDF and risk from failure of DI&C systems is low. The uncertainty of this insight is at the medium level.

(2) The estimated CDF is not very sensitive to reasonable changes in single DI&C component failure probabilities or in initiating event frequencies. This was confirmed for previously reviewed designs when DI&C system components had their importance measure functions assessed. Measures evaluated included Fussell-Vesely, a measure that looks at how the CDF or risk would change if the particular component or system were always available, and RAW, a measure that looks at how the CDF or risk would change if the particular component or system were always unavailable. The uncertainty of this insight is medium.

(3) The RAW values for CCF of DI&C components are very high (i.e., the RAW values for DI&C CCFs reported by reactor vendors in their PRAs are often the highest of all structures, systems, and components (SSCs) modeled in the PRA). Similar RAW values would be found for other high reliability SSCs (e.g., a reactor vessel) that have no additional layers of defense and whose failure would directly cause core damage. This insight has implications for the development of reliability assurance programs, emergency procedures, and other areas. The uncertainty of this insight is low.

(4) The inclusion of a diverse backup system (e.g., DAS) to automatically and manually actuate selected safety systems appears to compensate for the uncertainties in DI&C system CCF rates. The uncertainty in this insight is low.

(5) In new reactor designs, most of the dominant contributors to CDF and risk normally found in a risk assessment for operating reactors have been designed away. One result of this is that human errors associated with DI&C system failures have become more important as contributors to CDF, although the absolute numerical value of these failures is low. The uncertainty in this insight is low.

(6) There are significant uncertainties in the modeling of DI&C systems in PRAs and therefore the insights from the assessment have uncertainties.

(7) There are significant uncertainties in the data used to estimate DI&C system contributions to CDF and risk.

For the AP1000 design, the following six important insights were gained from the risk assessment performed for the DI&C systems:

(1) The use of two redundant and diverse backup systems with automatic and manual actuation capability (one is safety related and the other non-safety-related, e.g., DAS) minimizes the likelihood of actuation failures, including common-cause actuation failures. The non-safety-related DAS is a reliable system capable of initiating automatic and manual reactor trip using the motor-generator sets when the reactor fails to trip via the PMS. At operating reactors, the diverse actuation system (i.e., DAS) appears to be less reliable and in some cases, may not automatically initiate a reactor trip. The redundant and diverse actuation capabilities help reduce the risk associated with anticipated transient without scram (ATWS) events in the AP1000 design.

(2) The DI&C-related systems and components with the highest RAW values are as follows:

a. Software for the PMS and PLS logic cards

b. PMS ESF software components, such as input logic software, output logic software, and actuation logic software

c. PMS ESF manual input multiplexer software

d. PMS ESF hardware components, such as output drivers and input logic groups

e. PMS reactor trip logic hardware.

(3) No CCF of software has high Fussell-Vesely importance measure values (i.e., a measure of how much the CDF could be improved if the software were made perfectly reliable) in the AP1000 PRA because software was assumed to be highly reliable. When the NRC's review performed sensitivity studies, it became clear that these assumptions were very important. Requirements were imposed on the AP1000 design to help ensure that software will be built with processes recognized to result in highly reliable software. (i.e., at least as highly reliable as assumed in the sensitivity studies.)

(4) Major contributors to uncertainty associated with CCF of DI&C include the following:

a. CCF probability of hardware in the PMS ESF input logic groups

b. CCF probabilities of several sensor groups

c. CCF of the automatic reactor trip portion of the PMS (hardware and software)

d. failure probabilities of the automatic DAS function (hardware and software).

(5) The plant risk is sensitive to the "hot short" failure assumptions in the fire risk analysis. Guidance on hot shorts can be found in NUREG/CR-6850. The AP1000 design incorporates features to minimize the consequences of hot

shorts. Examples include the use of a valve controller circuit that requires multiple hot shorts to occur to change valve position, physical separation of potential hot short locations (e.g., routing of Automatic Depressurization System (ADS) cables in low-voltage cable trays and the use of “arm” and “fire” signals from separate PMS cabinets), and provisions for operator action to remove power from the fire zone to prevent spurious actuation of the ADS valves.

(6) DAS reduced uncertainties (for the decision of what equipment should go into regulatory treatment of non-safety systems (RTNSS)) by providing reactor trip backup for ATWS by tripping motor-generator set breakers.

The AP1000 PRA shows that the AP1000 design is significantly less dependent on human actions for assuring safety than are operating reactors. Even so, because the estimated CDF for the AP1000 design is so low and the risk from so many initiating events has been designed away, certain operator errors become significant contributors relative to the estimated AP1000 CDF from internal events. These errors include the following:

- failure of the operator to manually actuate safety systems through DAS, given failure to do so through PMS
- failure of the operator to manually actuate containment sump recirculation (when automatic actuation fails)
- failure of the operator to manually trip the reactor via PMS or DAS within one minute (given automatic trip failed).

Glenn Kelly
01/31/08
Version 8a