

DRAFT



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

Revision 0

(Initial Issue for Use)

DRAFT



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

Revision 0

(Initial Issue for Use)

OFFICE	DI&C/TWG3	DI&C/DD	OGC/NLO	NRO/DE	NSIR/DSP
NAME	MFranovich	SBailey	PMoulding	MMayfield	SMorris
DATE					
OFFICE	RES/DFERR	NMSS/FCSS	NRR/ADES		
NAME	JUhle	JGitter	JGrobe		
DATE					

DRAFT

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

Revision 0

(Initial Issue for Use)

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 (10 CFR Part 52) on performance of risk assessments for new reactors, and NRC policy on Safety Goals and PRAs, and is not a substitute for NRC regulations, but rather clarifies how a licensee or applicant may satisfy those regulations and policies.

This ISG also clarifies the criteria the staff will 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.

DRAFT

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 from the Advanced Boiling Water Reactor (ABWR) and the AP1000 design certification reviews (see Appendix A).

The interim staff guidance document ~~does not support nor is it~~ intended to provide guidance on the scope, level of detail, and technical acceptability of DI&C system risk assessments for risk-informed **regulatory decisionmaking** (i.e., risk-informed plant licensing basis changes), either for current or new reactors. ~~The staff considers it premature to risk-inform DI&C regulatory matters. The use of risk-informed decisionmaking in matters, such as reducing or eliminating accident prevention or mitigation features provided as defense-in-depth measures, is beyond the scope of this ISG and may be addressed in future regulatory guidance.~~

Insert: is not

These statements should not be included in this ISG that addresses Problem Statement #1. The issue surrounding the use of risk-informed insights should be addressed in the ISG for Problem Statement #2.

2. RATIONALE

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

- A. Regulatory Guide 1.200, Revision 1, January 2007, which addresses the technical adequacy of PRAs.
- B. The Commission policy statement on the "Use of PRA Methods in Nuclear Regulatory Activities; Final Policy Statement." [*Federal Register*, Vol. 60, No. 158, pp. 42622-42629, August 16, 1995]
- C. Regulatory Guide 1.174, Revision 1, on using PRA in making risk-informed decisions.
- D. Final Safety Evaluation Report (FSER) of the AP1000 Standard Design.
- E. FSER of the Advanced 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 necessary for the fault to be exercised. When exercised, the fault may result in a DI&C system failure. Excitation of these system faults can cause significant system failures. For new reactors, the nuclear industry has purposed to design and implement DI&C systems 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

Suggest changing to "software-based DI&C systems." Much of the discussion below addresses failure modes unique to digital systems. The only unique failure modes that differentiate digital from analogue systems are for software-based systems.

The words "regulatory decisionmaking" are objectionable. Suggest using just the parenthetical words "licensing basis changes." The PRA is a decision-making tool and is being used as such in regulatory decision-making. It is not a question of if, but rather a question of whether the scope of the PRA is commensurate with the decisions being made from it, and vice versa. Some of these "regulatory decisions" are in this very document: uncertainties are large enough to reinforce need for D3, DRAP requirements, etc.

DRAFT

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. 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, nor is it possible to determine how two software designs will differ in their failure behavior. Experience shows that one cannot eliminate all faults 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 is possible for nuclear power plants 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 one system to another may not necessarily be meaningful. Likewise, extrapolation of statistical data of the same system used in a different operating environment or profile is not necessarily meaningful.

Systems consisting of combined hardware and software may not fail the way hardware alone 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 by utilizing software and hardware design techniques known to limit digital system failures combined with a testing program based on expected use, and by controlling operational use.

To reduce the probability and consequences of significant faults, 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 failures and their effects on DI&C systems. DI&C system CCFs were recognized as having the potential to simultaneously 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 process.

See comment on software-based DI&C systems on page 2.

Current deterministic guidance is designed to ensure adequate defense-in-depth such that the effects of a DI&C system CCF are appropriately limited. Defense-in-depth is judged to be adequate if the acceptance criteria of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Chapter 7, "Instrumentation and Controls," BTP 7-19 are met.

The current methodology for a deterministic defense-in-depth and diversity assessment considers a DI&C system CCF as a beyond design basis event, and, therefore, DI&C CCFs are not required to be included as part of a traditional single failure analysis. Consequently, the assessment uses best estimate analysis and acceptance criteria to

DRAFT

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, the staff evaluates DI&C system defense-in-depth and diversity with respect to beyond design basis DI&C system CCFs. Attributes of the above guidance and methodology include Commission policy, conclusions, and direction that:

- A DI&C system CCF (particularly of software), although credible, is expected to be relatively rare.
- DI&C system CCFs are analyzed as beyond design basis events.
- The assessment may be performed using best-estimate (realistic assumptions) analyses.
- 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.
- The diverse means may be a different function and may be performed by a non-safety system of sufficient quality to perform the necessary function under the associated event conditions.
- A set of displays and controls independent and diverse from the computer-based safety systems shall be provided in the control room for manual actuation and monitoring of critical safety functions. These displays need not be safety related.

Experience with implementation of the above deterministic guidance during reviews has shown that significant NRC effort has been necessary in the evaluation of whether D3 is adequate. Although issues have been identified with operating reactors as well as with 10 CFR Part 52 new reactor design certification (DC) and combined operating license (COL) applications, the review of DI&C systems is more challenging for operating reactors. One of the main reasons for the additional challenge 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 for the DI&C system that was provided by the analog system prior to the retrofit.

New reactors licensed under 10 CFR Part 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, "Severe Accident," and Section 19.0, "Probabilistic Risk Assessment and Severe Accident evaluation for New Reactors," guidance. However, due to data limitations¹ and the lack of consensus in the technical community on appropriate

¹ Software normally is 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 from 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

DRAFT

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.

The first 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. 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 because 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. NRC reviewers should be aware that bounding analyses may alter or cover up safety insights in areas such as importance measure values and sequences identified as dominant and may not be capable of modeling or bounding unique digital 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.

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. 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, which states, "... that 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, including but not limited to digital I&C system hardware and software, explosive (squib) valves, and the issue of thermal hydraulic (T-H) uncertainties."

Although there is a lack of consensus in the technical community on whether methods normally employed when performing PRAs are adequate for the purpose of making comprehensive risk-informed decisions for DI&C, 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 NRC Office of Nuclear

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.

This sentence is at odds with D3 (BTP 7-19). Uniformly requiring backups for all designs masks the features that distinguish good designs from bad designs.

Suggest removing this sentence, as it is not clear what this statement has to do with reviewing new reactor PRAs.

DRAFT

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.

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.

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 warrant additional regulatory attention and should help identify whether there are high-level, risk-significant problems, including the existence of risk outliers in a DI&C system. Potential challenges that might be identified include the following three examples:

DRAFT

- Installation of the system would raise the frequency of low risk contributors to an unacceptable level.
- Installation of the system would introduce significant new failure modes not previously analyzed.
- 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 12 review guidelines are provided. 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 results and insights from the applicant's DI&C risk assessment.
2. The modeling of DI&C systems should include the identification of how DI&C systems can fail and what these failures 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 especially for software 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 to ensure the process employed is systematic and comprehensive in its identification of failure modes. The reviewer should work with the DI&C reviewer to evaluate the methodology and results provided by the applicant. Examine applicant documentation to ensure that the most significant 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.
3. The DI&C CCF events are to be identified by the applicant and the bases provided for grouping of CCFs. Review the discussion of how the applicant determined the probabilities associated with CCFs. The reviewer should work with the I&C reviewer to evaluate the applicant's justifications.

DRAFT

This sentence presupposes the answer. Suggest removing.

4. The uncertainties associated with DI&C system risk assessments 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. 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 studies may be particular helpful in assessing the effectiveness of design attributes such as a diverse actuation system or defensive measure in limiting DI&C uncertainties including that of software.

As with any risk assessment, a reviewer should determine if the applicant has performed a balanced assessment of prevention and mitigation, and has considered the need to increase regulatory attention to aspects of the design or operation based on the sensitivity studies and other risk insights. If a risk outlier challenges the Safety Goals, 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 is necessary, since the particular sensitivity study may involve a very unlikely scenario or set of failure events

Suggest replacing "support" with "address"

Although this ISG does not support risk-informed decisionmaking, additional support for the review and treatment of uncertainties is provided by NUREG-1855, "Guidance on the Treatment of Uncertainties Associated With PRAs in Risk-Informed Decisionmaking," dated November 2007.

See comment on page 2 regarding the use of the term "decisionmaking."

5. The reviewer should confirm that DI&C system equipment is capable of meeting its safety function for the environment assumed in the PRA.
6. 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. A specific concern would be the impact of fire on DI&C.
7. Evaluate the acceptability of how the failure of control room indication is modeled. Coordinate with the DI&C reviewer.
8. 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 that the associated technical justifications are sound and documented. The reviewer should pay attention to assumptions about the potential

DRAFT

The term "defensive measures" is misused here. The items listed in the footnote should simply be listed here explicitly.

effects from failure of defensive measures². A DI&C defensive measure may have the downside of causing spurious trips or spuriously failing functional capabilities. The licensee should describe the segregation process that prevents this from occurring. The reviewer should work with the DI&C reviewer to evaluate the process discussed by the applicant.

"DI&C defensive measure" should be replaced with "DAS," as this sentence refers to complications associated with a DAS, which is not a defensive measure.

9. 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. If recovery actions are modeled, they should consider loss of instrumentation and the time available.
10. Verify that a method for quantifying the contribution of software failures to DI&C system reliability was used and documented.
11. Systems and components necessary to ensure that the DI&C system remains highly reliable should be in a monitoring program. It is important to evaluate claims by applicants regarding the credit that should be given for defensive design features. 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, such as how future software and hardware modifications will be handled to assure high reliability continues over the life of the plant.
12. Resources expended to review an applicant's claims regarding data should be proportional to the use to be made of the PRA results. If limited use is made, limited review is required.

Additional Steps:

The following 10 additional steps, as applicable, are included if a more detailed review is needed (e.g., through field audits):

1. Verify that physical and logical dependencies were identified and their bases provided in the DI&C PRA. The probabilistic model should encompass all 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. Coordinate with the DI&C reviewer.

² e.g., automatic tester system, fault tolerance, diagnostics, DAS

The footnote is incomplete if "defensive measures" is not replaced with "DAS." Most importantly, "defensive measures" include many features to prevent software failures by removing the common software failure triggers. Examples of such features include: constant bus loading (eliminates network traffic overload), static memory allocation (eliminates memory conflicts), asynchronous operation (removes clock interference), deterministic program execution (one path through software, no untested software paths), strictly cyclic processing (transparency of OS to external interference). To define defensive measures only in terms of those defenses that perform after the fact is incorrect.

DRAFT

2. Ensure that spurious actuations of diverse backup systems or functions are evaluated and the overall risk impact documented.
3. 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 should be based on similarity in design and function of component or system modules, including software. Recognize that there is on-going research into how to best model DI&C CCFs (including software CCF) in PRAs, and there is no consensus yet as to how they should be modeled.

Add to examples: independence, OS design.

The CCF events are to be identified and modeled by the applicant. The CCF probabilities and their bases should be evaluated and provided by the applicant 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., CCF of common function modules). If the safety functions of a DI&C system (and/or the redundancy within safety functions) use common software, dependency should be assumed for software faults. That is, when common software is used for different safety functions (or in the redundancy within a safety function) it may fail each function. Hardware CCF between different safety functions using the same hardware should be identified. Dependencies between hardware and software should be identified. The applicant should provide the rationale for the degree of dependency assumed for DI&C CCF.

An important expectation is that the applicant included sufficient equipment in the CCF groups. The evaluation should address why various channels, trains, systems, etc. were or were not placed in each CCF group. The justification should discuss common software/hardware among the equipment considered and the level(s) of dependency among them. The reviewer should work with the I&C reviewer to evaluate the applicant's justifications.

repetitive to A. 11.

4. It is important to evaluate claims by applicants regarding the credit that should be given for defensive design features. If the design features (e.g., fault tolerance, diagnostics, self testing, DAS) are relied upon to help keep the probability of the DI&C system failure low, including DI&C CCF, then an implementation and monitoring program may be required to address how the applicant will assure that the design features continue to

DRAFT

support the assumed reliability of the systems and components in the future. 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, may be set up into a configuration that is less reliable than the original one, may 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 features 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 that 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 can only 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, and 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 risk analyst, in conjunction with the DI&C 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.

DRAFT

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.

5. 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.
6. DI&C system CCFs are difficult to model. If hardware, software, and system CCF probabilities are treated together in the PRA and if the applicant uses standard methods such as the multiple Greek letter method, alpha factor method, or beta factor method to model DI&C system CCFs, an NRC audit of these calculations, their bases, and the modeling assumptions may be warranted.
7. The data for hardware failure rates (including CCF) probably will be more robust than the software failure data. Review of applicant claims regarding data should be proportional to the use to be made of the PRA results. If limited use is made, limited review is required. If the applicant claims extremely low CCF rates, an NRC audit 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, ASME RA-S-2002 and Addenda, for nuclear power plant applications should be satisfied consistent with the clarifications and qualifications of RG 1.200. Determine if the process used to determine basic event probabilities is 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.

Suggest replacing "are" with "could be."

Note, that 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.

8. If the values of the data used appear to be skewed and use of different values might change the insights drawn from the DI&C risk assessment, confirm that the data meet the following criteria:
 - 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 appropriately reflect the level of uncertainty. (Applies to both component-specific and generic data)
 - b. The sources for raw data or generic databases are provided. (Applies to both component-specific and generic data)

DRAFT

- c. The method used in estimating the parameters is documented, so that the results can be reproduced. (Applies to component-specific data)
 - d. If the system being modeled is qualified for its environment but the data obtained are not drawn from systems qualified for that environment, the data should account for the differences in application environments. (Applies to both component-specific and generic data)
 - e. Data for CCF meet the above criteria in 9d. (Applies to both component-specific and generic data)
 - f. Data for fault coverage meet the above criteria in 9d. (Applies to 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. (Applies to both component-specific and generic data)
9. 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 value 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.

10.

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 goals. How the applicant will carry out performance monitoring for diverse backup systems (if necessary) and DI&C systems should be clearly explained. 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. 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 ensure that the design continues to reflect the assumed reliability of the systems and components during plant operation.

Repetitive. Seems similar to A.11. and B.4.

DRAFT

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
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

DRAFT

6. REFERENCES

- A. 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.
- B. 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.
- C. U.S. Nuclear Regulatory Commission, "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities," Volumes 1 and 2, NUREG/CR-6850, September 2005.
- D. 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.
- E. *U.S. Code of Federal Regulations*, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," Part 52, Title 10, "Energy."
- F. U.S. Nuclear Regulatory Commission, Safety Goals for the Operation of Nuclear Power Plants; Policy Statement, 51 FR 30028; August 21, 1986.
- G. 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.
- H. 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.
- I. 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.
- J. U.S. Nuclear Regulatory Commission, "Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design," NUREG-1793, September 2004.
- K. U.S. Nuclear Regulatory Commission, "Final Safety Evaluation Report Related to the Certification of the Advance Boiling Water Reactor Design," NUREG-1462, August 1994.
- L. U.S. Nuclear Regulatory Commission, "Final Safety Evaluation Report Related to the Certification of the AP600 Standard Design," NUREG-1512, September 1998.

DRAFT

- M. 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.
- N. U.S. Nuclear Regulatory Commission, "Digital Computer Systems for Advanced Light Water Reactors," Commission Paper SECY-91-292, September 16, 1991.
- O. 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.
- P. National Research Council, "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues", National Academy Press, 1997.
- Q. S.A. Arndt, N.O. Siu, and E.A. Thornsby, "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).
- R. 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.
- S. N. Storey, "*Safety-Critical Computer Systems*," Addison Wesley Longman (1996).
- T. Hoang Pham, "*Software Reliability*," Springer-Verlag Singapore Pte. Ltd. (2000).
- U. U.S. Nuclear Regulatory Commission, "Combined License Applications for Nuclear Power Plants (LWR Edition)," Regulatory Guide 1.206, June 2007.
- V. U.S. Nuclear Regulatory Commission, "Method for Performing Defense-In-Depth and Diversity Analyses of the Reactor Protection System". NUREG/CR-6303, December 1994.
- W. 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.
- X. American Society of Mechanical Engineers (ASME), "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," ASME RA-S-2002 and Addenda A to this standard (ASME RA-Sa-2003 and ASME-Sb-2005)
- Y. U.S. Nuclear Regulatory Commission, "Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decisionmaking," NUREG-1855, November 2007.
- Z. U.S. Nuclear Regulatory Commission, Commission Staff Requirements Memorandum (SRM) dated June 26, 1990, to SECY-90-016.

DRAFT

- AA. U.S. Nuclear Regulatory Commission, "Good Practices for Implementing Human Reliability Analysis," NUREG-1792, April 2005.
- AB. U.S. Nuclear Regulatory Commission, "Evaluation of Human Reliability Analysis Methods Against Good Practices," NUREG-1842, September 2006.

DRAFT

DI&C-ISG-03 Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments

APPENDIX A

Insights from Risk Assessments Performed for the ABWR and AP1000 DI&C Systems

The following are insights drawn from previously reviewed new reactor DI&C system risk assessments (i.e., from the ABWR and AP1000 design certification reviews).

1. The absolute value of the contribution to CDF and risk from failure of DI&C systems is low for these designs, as modeled.
2. The estimated CDF is not very sensitive to changes in single DI&C component failure probabilities or in initiating event frequencies.
3. The Risk Achievement Worth (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 were the highest of all structures, systems, and components modeled in the PRA). Note that high RAW values may be driven by other assumptions used in the sensitivity assessment.
4. The inclusion of a diverse backup system (e.g., DAS) in the AP1000 design (which automatically or manually actuates selected safety systems) is intended to reduce the probability of a severe accident resulting from a postulated DI&C CCF coincident with a postulated transient or accident. The DAS helps compensate for uncertainties in DI&C system CCF assumptions (i.e., failure rates and failure modes and their effects), especially software.
5. Most of the dominant contributors to CDF and risk normally found in a risk assessment for operating reactors have been designed away for these designs. One result of this is that human errors associated with DI&C system failures have become more important contributors to CDF, although the expected frequency of these failures leading to core damage is low.
6. There are significant uncertainties in the data used to estimate DI&C system contributions to CDF and risk.

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

1. The use of two redundant and diverse systems with automatic and manual actuation capability (one is safety related and the other non-safety related, e.g., DAS) reduces the likelihood of actuation failures, including beyond design basis DI&C common-cause DI&C failures. The non-safety-related DAS is

DRAFT

- projected to be a reliable system capable of providing a reactor trip and engineered safeguards features (ESF) actuation along with operator indications that are all diverse from the protection and safety monitoring system (PMS). The DAS also provides manual reactor trip and manual ESF capabilities. The DAS receives signals directly from dedicated sensors and uses redundant signal processing units that use hardware and software diverse from the PMS. The redundant and diverse actuation capabilities reduce the probability of a severe accident that potentially results from the unlikely coincidence of postulated transients and postulated DI&C CCF 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 plant control system (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 important a failure is including its likelihood of occurrence, or a measure of the importance of a component being down including its likelihood of being down) 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. The AP1000 design incorporates features to minimize the consequences of hot shorts. Examples include the use of a valve controller

DRAFT

circuit for which multiple hot shorts need to occur before a valve position will change, 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. Current guidance on hot shorts can be found in NUREG/CR-6850.

6. DAS reduced uncertainties for the decision of what equipment should go into regulatory treatment of non-safety systems (RTNSS).

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).