

DRAFT

**GUIDANCE ON REVIEWING RISK ASSESSMENTS AND
RISK-INFORMED DECISIONS FOR ADVANCED REACTOR DIGITAL
INSTRUMENTATION AND CONTROL SYSTEMS**

Executive Summary

Digital instrumentation and control (DI&C) systems are complex combinations of hardware components and software (i.e., computer programs). Although computer software does not wear out, excitation of residual design errors can cause significant problems. If one could eliminate all design errors before a software product is put into operation, it would work perfectly forever. However, it is impossible to be certain that a software product is error free. Experience shows there are always residual faults in complex software that can cause a software failure when the program is exposed to an environment for which it was not designed or tested. Exposure to such an environment for nuclear power plants is possible because there are a large number of possible states and inputs for the software programs.

Comment [vka1]: Suggest rewording.

Comment [vka2]: Suggest changing to "frequently."

Comment [vka3]: For safety systems, there are generally only two possible end states. Suggest removing this sentence.

To limit these errors, comprehensive deterministic guidance was developed by the NRC and industry. The deterministic guidance is based, in part, on digital system development processes recognized for producing quality software and known to limit errors, including those leading to DI&C software CCF. Other parts of the process include use or development of highly reliable hardware. Although development processes and methods are designed to result in high quality and high reliability digital systems, the potential for a common cause failure (CCF) remains, and the effects of a CCF on event mitigation may be significant. The Nuclear Regulatory Commission (NRC) and industry recognize that not all failures, including software CCF, can be eliminated. In addition, digital system development processes and methods do not readily lend themselves to measurable acceptance guidance or metrics to judge a digital system's overall quality or reliability (including software.)

Comment [vka4]: The use of a quality software development process is only one way to prevent CCF failures from having significant impact. Others include being fault tolerant and having defense in depth, diversity, and redundancy.

Comment [vka5]: This is not unique to digital I&C, and does not need to be restated in this document. Suggest removing this statement.

The deterministic guidance is designed to help assure that adequate defense-in-depth is maintained such that the propagation of digital system CCF to other channels, divisions, or trains is adequately 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.

Comment [vka6]: Please provide examples of the propagation of CCF failures from channel to channel since the basis for including this type of failure seems to be dated historic experience which is no longer applicable. Currently channels do not share information in such a way to cause these type of errors on safety related controls.

The methodology and acceptance guidance for a deterministic defense-in-depth evaluation are provided in SECY-93-87 and expanded by NUREG-0800, Chapter 7, Branch Technical Position 19 (BTP-19). The methodology uses a single failure review method, but with relaxed assumptions and acceptance guidelines modified to evaluate CCFs of digital systems. Therefore, in addition to the traditional single failure criterion evaluation to determine adequate DI&C redundancy, the methodology addresses digital system CCF by including an independence and diversity assessment.

The NRC and industry recognize that current PRA methods can provide some useful 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). Regulatory Guide (RG) 1.200 provides guidance on evaluating the technical adequacy of PRAs. However, RG 1.200 only provides limited guidance on how to model and evaluate

DRAFT

DI&C systems. It does not address completeness issues, level of modeling detail needed, or how to address the uncertainties associated with digital system modeling and data.

Comment [vka7]: The intent of RG 1.200 is not to provide system-specific modeling guidance. These statements are not unique to digital I&C, but would apply to any specific system. Suggest removing this sentence.

Once risk insights have been obtained, they may be used to help make risk-informed decisions. The NRC has identified a process by which regulatory decisions can be risk informed. This process is outlined in RG 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Revision 1, dated November 2002. The process has been used many times by the NRC as a model for making risk-informed decisions. A major underlying consideration of the process is that in making a risk-informed decision, the applicant must perform both traditional and probabilistic engineering assessments that are appropriately robust for the decision to be made. It is not enough merely to consider risk insights, because they are subordinate to traditional engineering evaluations.

Comment [vka8]: RG 1.174 directly applies to CLB changes, not regulatory decisions.

Regulatory Guide 1.174 provides five basic principles that the Commission expects will be followed in making risk-informed decisions:

1. The proposed change meets the current regulations or an exemption is requested.
2. The proposed change is consistent with the defense-in-depth philosophy.
3. The proposed change maintains sufficient safety margins.
4. When proposed changes result in an increase in CDF or risk, the increases should be small and consistent with the intent of the safety goal policy statement.
5. The impact of the proposed change should be monitored using performance measurement strategies.

In addition, in implementing the principles, the guidance calls for the following to be accomplished:

- The scope, level of detail, and technical acceptability of the engineering analyses (traditional and probabilistic) should be appropriate for the application.
- The plant-specific PRA should be subject to Quality Assurance methods.
- Uncertainties should be appropriately handled.
- The acceptability of the proposed application should be evaluated in an integrated fashion that ensures that all principles mentioned above are met.
- Data, methods, and assessment criteria must be well documented and available for public review.

Further, the guidance notes that it is expected in a risk-informed application "that the risk from significant accident sequences will not be increased and that the frequencies of the lower ranked contributors will not be increased so that they become significant contributors

DRAFT

to risk. It is expected that no significant new sequences or cutsets¹ will be created” and “risk should be considered in addition to likelihood.”

The NRC performed reviews of the DI&C systems modeled in the PRAs for advanced plants such as the Advanced Boiling Water Reactor (ABWR), AP600, and AP1000 designs. A brief summary of how these evaluations were performed is provided in this paper. The modeling of DI&C in the AP600 and AP1000 PRAs received a more detailed NRC review than did the modeling of the ABWR DI&C design in its PRA. This guidance document provides greater detail of and relies more on the AP600/AP1000 DI&C PRA review than of the ABWR review.

Based on the higher level of detail provided for the AP600 and AP1000 DI&C systems, the NRC performed a more thorough, although still high level, PRA review in that area. As with the ABWR PRA evaluation, the evaluations of the AP600 and AP1000 DI&C systems in the respective PRAs concluded that failures of individual instrumentation and control components interfacing with or making use of digital information were not particularly significant, but concluded that CCFs of DI&C systems were significant (i.e., had high risk achievement worth importance function values.)

The NRC review of the DI&C portion of the AP600/1000 PRA² was a small but integrated part of the overall PRA review. The NRC performed all the normal aspects of a PRA review including evaluation of the quality of the PRA. The review of the DI&C portion of the PRA was made difficult by the lack of design details, including lack of detail for some interfacing areas such as the control room design. The NRC’s review relied on use of sensitivity studies to determine the extent to which the insights and findings of the PRA would vary if different assumptions were made about failure modes, failure rates, and CCF for the DI&C design.

Despite the limitations, NRC’s reviews produced important lessons learned and insights, including the following:

- * 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,
- * risk assessment modeling of DI&C systems has significant uncertainties,
- * data for digital component failure rates have high uncertainties,
- * CCF rates of DI&C software have high uncertainties,
- * assumptions about how software CCFs propagate can influence CDF and risk insights, and

Comment [vka9]: Define

Comment [vka10]: The risk assessment modeling of DI&C has no larger uncertainties risk assessment modeling for other systems. This includes CCF of DI&C which has similar uncertainty as to other uncertainties. Consequences of the failure are not part of the uncertainty.

Comment [vka11]: Define

Comment [vka12]: Data for digital failures are no more uncertain than other failure rates used in the PRA, including CCF.

Comment [vka13]: This is also the case for many of the CCF-modeled components in the PRA.

Comment [vka14]: This statement is difficult to understand and should be reworded.

¹ A “cutset” is a set of conditions (such as failures of specific components) whose collective satisfaction causes the undesired outcome.

² Although the AP600 and AP1000 each had a PRA performed for it, in reviewing the AP1000 PRA, the NRC relied significantly on the similarities between the AP1000 and AP600 designs to reduce the review effort, which allowed the use of the AP600 PRA as a starting point. From this point forward throughout this guidance document, only the AP1000 design and PRA will be referenced unless a comment only applies to AP600.

DRAFT

* importance measure values for CCF of DI&C system components often are very large.

Due to data limitations³ and the lack of appropriate modeling tools, the assessment of DI&C system risk for new plants essentially 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. These limitations make it difficult to develop robust risk insights about DI&C systems. For the advanced reactor risk assessments performed to date and reviewed by the NRC, the inclusion in the design of a diverse actuation system (DAS) has been found to positively affect PRA safety insights (i.e., a diverse backup system provides assurance that certain safety functions will be performed given a failure of the DI&C systems) and to satisfy the defense-in-depth acceptance guidance of BTP-19 and SECY 93-87. The result, for both operating plants and yet to be built advanced reactors, is that full deterministic assessments as set forth in BTP-19 and SECY 93-87 must continue to be performed and their criteria met.

General guidance is provided to clarify how NRC will review near-term DI&C system risk assessments for advanced reactors, including comparisons to Safety Goals. This guidance is based on previously accepted reviews performed on advanced reactor DI&C system designs.

Purpose

The primary purpose of this document is to provide clear guidance on how NRC reviewers should evaluate digital instrumentation and control system PRAs, including addressing common cause failure modeling and uncertainty analysis associated with digital systems for design certification and combined operating license (COL) applications.

Introduction

When nuclear power plants were designed and built from the 1950s to the 1980s, they used analog hardware to provide the instrumentation and control (I&C) needed to operate the plants. The potential for common cause failures (CCFs) was believed not to be present because it usually was assumed that CCF, if it did occur, was due to slow processes such as corrosion or premature wear-out. Today, with I&C manufacturers' lack of support for analog systems and the realization that digital systems can offer unique design and functional capabilities, the nuclear industry is in the process of replacing aging analog I&C systems in operating plants and developing DI&C systems for advanced reactor designs. The use of digital devices in I&C systems of nuclear facilities has the potential to improve safety and operational performance. However, the assumption of CCF due to slow processes is no longer true for systems containing software.

Although DI&C systems are intended to be at least as reliable as the analog systems they replace, digital systems have unique failure modes. Of significant concern are DI&C system CCF that can propagate to multiple safety channels, divisions, or trains, thereby defeating the defense-in-depth and diversity (D3) that was considered adequate for an analog I&C

Comment [vka15]: For the PRA that includes digital system model, the digital models will participate significantly in the list. However, so will many of the other highly reliable components in the plant such as the reactor vessel.

Comment [vka16]: The supporting references for this assertion need to be more robust. The current reference is subjective.

Comment [vka17]: The lack of appropriate modeling tools is not established in this document and is a point of debate among many risk analysts.

Comment [vka18]: This phrase lacks clarity and needs to be removed or better explained.

Comment [vka19]: The positive effects of inclusion of a DAS, if they exist, need to be more robustly discussed in this document. There should be a more balanced discussion of the risk impact of the DAS, with acknowledgement of potential downsides.

Comment [vka20]: Use of the word "must" implies a regulatory requirement. Reword or cite a reference to 10 CFR supporting its use.

Comment [vka21]: In order to be consistent with the problem statement, this phrase should be placed directly after "PRAs" in this paragraph.

Comment [vka22]: This statement is not always correct. Many types of CCF, such as maintenance errors, are not slow processes.

Comment [vka23]: Suggest deleting, as other types of CCF are not slow processes.

³ There appear to be too few hours of applicable data to make robust statistical estimates of software failure rates at the very low failure rates assumed in the risk assessments. There also is uncertainty associated with how appropriate it is to combine data from hardware or software that are used in similar but different applications.

DRAFT

system. Since digital systems play an increasingly important role in nuclear facility control and safety systems, particularly for advanced reactor designs, the need for risk assessment methods appropriate to DI&C systems is evident. Historically, analog I&C systems could be modeled to the level necessary for a PRA to support risk-informed decision-making. However there are significant challenges in modeling DI&C systems in PRAs and the available data to populate these models is limited.

This guidance document provides general guidance on how NRC should perform reviews of future DI&C system advanced reactor risk assessments (including comparisons to Safety Goals). It discusses the background of DI&C review guidance and the U.S. Nuclear Regulatory Commission's (NRC's or Commission's) expectations about how risk-informed decisions are to be made. This document also provides a summary of methods used by the NRC to evaluate risk associated with DI&C systems in previously approved design certifications (DCs) and it identifies the currently available risk insights for DI&C systems.

Background

Digital I&C systems are designed as complex combinations of hardware components and software (i.e., computer programs). Although computer software does not wear out as hardware does, it can fail as a result of the excitation of residual design errors when a particular combination of inputs occurs. If one could eliminate all design errors before a software product is put into operation, it would work perfectly forever. However, it is impossible to be certain that a software product is error free. On the contrary, experience shows that there are always residual faults in complex software that do not manifest themselves. They cause a software failure when the program is exposed to an environment for which it was not designed or tested, or for which it was not effectively designed to respond. Exposure to such an environment for nuclear power plants is possible because there are a large number of possible states and inputs for the software programs. It is extremely difficult for software designers to perfectly comprehend program requirements and implementation in power plants. It also is difficult to test all possible input combinations during development. When trying to estimate software reliability, it must be remembered that each software product is unique, and extrapolation of statistical data from other products is not necessarily meaningful.

Because software does not fail the way hardware fails, the commonly used hardware redundancy techniques do not improve software reliability. It is difficult to assure that one has high reliability when common software is used in two or more channels (or divisions) at the same time. It generally is accepted that high reliability can be achieved for software by following formal and disciplined methods during the development process, combined with a testing program based on expected use.

Comment [vka24]: This assertion needs a citation or background information to be supported.

Although development processes and methods are designed to result in high-quality and reliable digital systems, the potential for a common cause failure (CCF) remains, and the effects of a CCF on event mitigation may be significant. The NRC and industry recognize that not all failures, including CCF, can be eliminated. To address this, 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 digital system software, specifically common cause digital system failures. Digital system CCFs were recognized as having the potential to propagate across channels, divisions, or trains. These failures could negate the defense-in-depth features assumed adequate in the traditional analog systems

DRAFT

they are replacing. The deterministic guidance is based, in part, on digital system development processes recognized for producing quality software and known to limit errors in the development and implementation of digital systems, including those leading to DI&C software CCF. Other parts of the process include use or development of highly reliable hardware. However, digital system development processes and methods do not readily lend themselves to measurable acceptance guidance or metrics to judge a digital system's overall quality or reliability (including software).

The deterministic guidance is designed to help assure that adequate defense-in-depth is maintained such that the propagation of digital system CCF to other channels, divisions, or trains is adequately 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.

The methodology and acceptance guidance for a deterministic defense-in-depth evaluation are provided in SECY-93-87 and expanded by NUREG-0800, Chapter 7, Branch Technical Position 19 (BTP-19). The methodology uses a single failure review method, but with relaxed assumptions and acceptance guidelines modified to evaluate CCFs of digital systems. Therefore, in addition to the traditional single failure criterion evaluation to determine adequate DI&C redundancy, the methodology addresses digital system CCF by including an independence and diversity assessment. Attributes of the above guidance and methodology include Commission policy, conclusions, and direction that

Comment [vka25]: The meaning of this term is unclear. Would this mean that CCF is viewed as a single failure? What is the regulatory basis for this?

- (1) A DI&C system CCF (i.e., particularly software), although possible, is expected to be a relatively rare event.
- (2) Software CCF is considered a beyond design basis event.
- (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.

Experience with implementation of the above deterministic guidance has shown that reviews have involved significant NRC effort in the evaluation of whether D3 are adequate. Although issues have been identified with both operating reactor and new reactor 10 CFR 52 DC and combined operating license (COL) applications, the review of digital 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 review guidance.

Comment [vka26]: When has this result occurred? As no operating plants have been approved for upgrades at this point, it is unclear what the basis for this sentence is.

DRAFT

Unlike operating reactors, 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 deterministic guidance and Chapter 19 risk-informed guidance. However, due to data limitations⁴ and the lack of appropriate 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. These limitations make it difficult to develop robust risk insights about DI&C systems. For the advanced reactor risk assessments performed to date and reviewed by the NRC, the inclusion in the design of a diverse actuation system (DAS) has been found to positively affect PRA safety insights (i.e., a diverse backup system provides assurance 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 guidance of BTP-19 and SECY 93-87. The result, for both operating plants and yet-to-be-licensed advanced reactors, is that full deterministic assessments as set forth in BTP-19 and SECY 93-87 must continue to be performed and their criteria met.

Comment [vka27]: Data availability and PRA modeling techniques are always evolving; this does not mean that one cannot glean risk insights from a PRA.

Comment [vka28]: The DAS system has not been fully designed, and human actions and recovery actions have not been fully addressed or quantified in the risk model. Perhaps the language is more appropriately directed to diversity.

The first of the advanced 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. It was recognized that an advance in the state-of-the-art was needed to permit a comprehensive risk-informed decisionmaking framework in licensing reviews of DI&C systems for future and current reactors.

Comment [vka29]: The crux of the challenge that faces this TWG is how to model the software. Reliability models for digital hardware are not particularly challenging, and are routine among digital I&C vendors. Advancing the "state-of-the-art" for predicting software failure probability is not so easy. The computer related industries have failed to produce a viable method for predicting software failure probability despite years of trying. This TWG should not delay the opportunity to use risk insights in order to wait for advancement in quantitative software reliability methodology that may not be possible.

Despite the limitations, NRC's reviews produced important lessons learned and insights, including the following:

- 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.
- Risk assessment modeling of DI&C systems has significant uncertainties.
- Data for digital component failure rates have high uncertainties.
- CCF rates of DI&C software have high uncertainties.

The SR computer industry has moved beyond this difficulty by focusing on reducing the probability and consequences of software failure, rather than on quantification of its precise probability. This is done by designing multi-legged defenses against SWCCF. Standards written by the industry encourage a defense that includes not only the quality of the software development process, but also operating system features that limit the likelihood of failure triggers, features to cope with SW failure when it occurs, and diversity.

⁴ 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 software can be used for a different software.

DRAFT

- Assumptions on the extent software CCFs propagate can influence CDF and risk insights.
- Importance measure values for CCF of DI&C system components often are very large.

Making risk-informed decisions about DI&C systems has been suggested as a means to address some of the industry concerns with the current deterministic NRC digital review guidance and process. However, for this to be effective, at a minimum, risk assessment methods must be developed that accurately characterize the risk associated with DI&C systems in nuclear power plants. The NRC currently has a long-term project to attempt to determine if such methods exist or can be developed. The methods normally employed when performing PRAs have not been demonstrated to be adequate for the purpose of making comprehensive risk-informed decisions for DI&C.

Comment [vka30]: This is not necessarily correct, as bounding methods could be used to make decisions.

Comment [vka31]: This statement is not supported in this document. A reference or supporting discussion should be given, or the statement should be removed.

In spite of this, the NRC and industry recognize that current PRA methods can provide some useful 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). Regulatory Guide (RG) 1.200 provides guidance on evaluating the technical adequacy of PRAs. However, RG 1.200 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 digital system modeling and data. Guidance as to what risk metrics are appropriate for evaluating the acceptability of DI&C systems in operating reactors and in DC and COL PRAs also may be needed.

Comment [vka32]: New risk metrics are not needed, as CDF and LERF are the risk metrics already in use.

The NRC established the Risk-Informing Digital Instrumentation and Control Task Working group (TWG # 3) to address issues related to the risk assessment of digital systems, with particular emphasis on risk-informing digital system reviews for operating plants and new reactors. The TWG # 3 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."

The TWG # 3 task is to evaluate the feasibility of risk-informing the DI&C system evaluations. The intent is to improve the effectiveness and efficiency of the digital system review process while adhering to the five key principles of risk-informed decisionmaking including adequate D3 when implementing a DI&C system either as a retrofit or new reactor installation. 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 digital systems in PRAs for design certificate applications or COL applications under Part 52. The issue includes addressing CCF modeling and uncertainty analysis associated with digital systems.

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

DRAFT

Use of Risk Insights in Risk-Informed Decisionmaking for Advanced Reactor DI&C Systems

Risk insights may be determined by various means, including systematic evaluation of the area of interest or observation. Although risk insights may be quantitative, they need not be (e.g., a failure modes and effects analysis). Risk insights from a nuclear power plant PRA might include the following:

- the plant's estimated core damage frequency (CDF)
- containment conditional failure probability
- the high confidence, low probability of failure estimate of the seismic capacity of the plant (HCLPF)
- a list of dominant accident sequences
- a determination of where the containment is most likely to fail after a severe accident
- the ranking of the most important plant equipment modeled in the PRA
- a list of assumptions made in the PRA that if different would significantly alter the PRA results or insights.

Risk insights can range from being very robust to being based on less well-grounded reasoning and data. How risk insights should influence a decision depends on the decision to be made, the importance of the decision, and the robustness of the insights.

When reviewing a risk-informed decision, it is important to first determine the proposed uses or implications of the decision. This is because the necessary sophistication, scope, and detail of the evaluation or review depend on the proposed applications. The greater the potential for a significant effect on risk, the greater the need for a broader scope and an increased level of detail.

The NRC has identified a process by which regulatory decisions can be risk informed. This process is outlined in RG 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Revision 1, dated November 2002. The process outlined in this RG has been used many times by the Commission as a model for making risk-informed decisions. A major underlying consideration of the process is that in making a risk-informed decision, the applicant must perform both traditional and probabilistic engineering assessments that are appropriately robust for the decision to be made. It is not enough merely to consider risk insights, because they are subordinate to traditional engineering evaluations.

Regulatory Guide 1.174 provides five basic principles that the Commission expects will be followed in making risk-informed decisions:

- (1) The proposed change meets the current regulations or an exemption is requested.

DRAFT

- (2) The proposed change is consistent with the defense-in-depth philosophy.
- (3) The proposed change maintains sufficient safety margins.
- (4) When proposed changes result in an increase in CDF or risk, the increases should be small and consistent with the intent of the safety goal policy statement.
- (5) The impact of the proposed change should be monitored using performance measurement strategies.

In addition, in implementing the principles, the guidance calls for the following to be accomplished:

- The scope, level of detail, and technical acceptability of the engineering analyses (traditional and probabilistic) should be appropriate for the application.
- The plant-specific PRA should be subject to Quality Assurance methods.
- Uncertainties should be appropriately handled.
- The acceptability of the proposed application should be evaluated in an integrated fashion that ensures that all principles mentioned above are met.
- Data, methods, and assessment criteria must be well documented and available for public review.

Further, the guidance notes that it is expected in a risk-informed application “that the risk from significant accident sequences will not be increased and that the frequencies of the lower ranked contributors will not be increased so that they become significant contributors to risk. It is expected that no significant new sequences or cutsets will be created” and “risk should be considered in addition to likelihood.”

Therefore, a reviewer of a risk-informed decision influenced by DI&C would be expected to examine the areas above to determine if the applicant has fully addressed the listed areas and has correctly made use of risk insights in making a risk-informed decision. For example, particular attention should be paid to assuring that sufficient defense-in-depth has been retained or achieved with implementation of the DI&C systems and a DAS. Defense-in-depth is primarily required to address the existence of uncertainties. Additional details on making risk-informed decisions can be found in RG 1.174, Revision 1.

Summary of Risk Assessment Methods Used to Evaluate DI&C Systems in Advanced Reactor Designs (ABWR, AP600, AP1000)

The NRC performed reviews of the DI&C systems modeled in the PRAs for advanced plants such as the Advanced Boiling Water Reactor (ABWR), AP600, and AP1000 designs. A brief summary of how these evaluations were performed is provided below. The modeling of DI&C in the AP600 and AP1000 PRAs received a more detailed NRC review than did the modeling of the ABWR DI&C design in its PRA. This guidance document provides greater detail of, and relies more on, the AP600/AP1000 DI&C PRA review than of the ABWR review.

Comment [vka33]: The fact that recoveries were not credited in this evaluation should be noted more prominently in the document. It should be noted that this could have a profound effect on the results. Although the PRA can give some insights given this limitation care must be taken when making decisions to ensure that all the underlying assumptions and inputs are understood.

DRAFT

ABWR REVIEW. As discussed in the Background, the methods currently available to model DI&C systems in a PRA and the statistical size and applicability of data currently available to estimate hardware and (especially) software failure rates are limited. The ABWR, developed by the General Electric Company (GE), was the first advanced plant design submitted to the NRC under 10 CFR 52 that made extensive use of DI&C. In order not to constrain future design capabilities (since it was expected that the state-of-the-art in instrumentation and control would advance significantly over time), GE provided only limited information about the DI&C design, and instead worked with the NRC to define attributes that the future design must have. These high-level attributes (primarily Design Acceptance Criteria (DAC) attributes that were identified during the DC process) were modeled in the ABWR PRA (in particular for the multiplex transmission network, trip logic units, remote multiplexing units, digital trip modules, and system logic units). Based on the assumptions in the PRA, individual failures of these systems or components were found not to be significant contributors to CDF or risk, but CCFs were determined to be very significant (as determined by importance measure values in the ABWR PRA). The NRC performed a very limited review of the ABWR DI&C PRA analysis. The NRC found a limited evaluation acceptable because (1) the DI&C design details would not be available until the COL application, (2) the NRC intended to review the DI&C design details and the plant-specific PRA at the COL stage, and (3) it was premature to perform a detailed review since the NRC's experience has been that most of the important PRA insights come out of detailed modeling of systems and components. The NRC documented its expectation in its Final Safety Evaluation Report on the ABWR DC that a detailed review of the DI&C system risk assessment would be performed at the COL application stage, when the "essentially complete design" was expected to be submitted to the NRC.

AP600/AP1000 REVIEW. The application for the Westinghouse AP600 DC was submitted shortly after the ABWR and was followed a number of years later by submittal of the AP1000 application. The AP600 application provided more information on DI&C than did the ABWR application. The AP1000 DC submittal was similar to that of the AP600 in the area of DI&C, and built on the information submitted for AP600. While more detailed than the ABWR submittal, significant details of the DI&C design still were not available at the time the AP1000 design was submitted for certification. Based on the higher level of detail provided for the AP600 and AP1000 DI&C systems, the NRC performed a more thorough, although still high-level, PRA review in that area. As with the ABWR PRA evaluation, the evaluations of the AP600 and AP1000 DI&C systems in the respective PRAs concluded that failures of individual instrumentation and control components interfacing with or making use of digital information were not particularly significant, but concluded that CCFs were significant with respect to risk (i.e., they had high risk achievement worth importance function values.)

The NRC review of the DI&C portion of the AP600/1000 PRA⁵ was a small but integrated part of the overall PRA review. The NRC performed all the normal aspects of a PRA review including evaluation of the quality of the PRA. The review of the DI&C portion of the PRA was made difficult by the lack of design details, including lack of detail for some interfacing areas such as the control room design. The NRC's review relied on use of sensitivity studies

⁵ Although the AP600 and AP1000 each had a PRA performed for it, in reviewing the AP1000 PRA, the NRC relied significantly on the similarities between the AP1000 and AP600 designs to reduce the review effort, which allowed the use of the AP600 PRA as a starting point. From this point forward throughout this guidance document, only the AP1000 design and PRA will be referenced unless a comment only applies to AP600.

DRAFT

to determine the extent to which the insights and findings of the PRA would vary if different assumptions were made about failure modes, failure rates, and CCF for the DI&C design.

Sensitivity studies were performed by the NRC, using the applicant's PRA models and results, to assess the effect on PRA results and insights gathered from uncertainty in the mean value of software failure probabilities. Sensitivity studies were performed under the following three scenarios:

- (1) Increase software failure probability by an order of magnitude and evaluate the change in CDF compared to the base case.
- (2) Increase software failure probability by an order of magnitude, while simultaneously assuming that all non-safety-related defense-in-depth systems become unavailable, and assuming the plant continues to operate at power. Evaluate the change in CDF and compare it to the base case.
- (3) Increase software failure probability by an order of magnitude, while simultaneously assuming that all non-safety-related defense-in-depth systems become unavailable with the exception of the diverse actuation system, and assuming the plant continues to operate at power. Evaluate the change in CDF and compare it to the base case.

Comment [vka34]: These sensitivity study scenarios appear to be rather extreme.

In addition to sensitivity studies, NRC reviewers evaluated the modeling of the DI&C systems. Fault trees in the AP1000 PRA were developed to model the following scenarios:

- (1) actuation failure of each component credited in the PRA that is required to be actuated by either automatic or manual means via the DI&C systems.
- (2) automatic and manual failure of the reactor trip and reactor coolant pump trip.

The failure modes of DI&C systems are often identified by the performance of Failure Modes and Effects Analysis (FMEA) studies. Reviewers evaluated the FMEA and determined whether the effects on failures of electromagnetic interference have been properly considered. They evaluated how the failure of control room indication is modeled in the fault trees (in AP1000 it was treated by incorporating a "failure of all indication" event from all three DI&C systems in the fault trees in parallel with human action failure events).

The NRC examined how software failures were modeled in the fault trees. Software failures were explicitly modeled in the AP1000 fault tree logic in parallel with hardware failures. Failures of software modules that are common across multiple applications were considered (e.g., common function modules used to store and retrieve information from memory buffers that are common between the protection and safety monitoring system (PMS) and plant control system (PLS)). Hardware failures, including CCF, were explicitly modeled in the fault trees using the same modular approach employed for other systems modeled in the PRA.

The reviewers examined how the PRA success criteria were affected by DI&C failures. In the AP1000 PRA, DI&C systems were assumed not to affect PRA success criteria (for systems and operator actions). This was considered to be a reasonable assumption because the PRA success criteria are minimum requirements of operation, which are independent of any system failures. Any impact of DI&C system failures on the performance of front-line systems was addressed through the AP1000 PRA fault tree models.

DRAFT

Below are listed nine important scope, boundary, level of detail, and modeling assumptions made in developing fault trees for the AP1000 DI&C systems:

- (1) The level of modeling detail for the DI&C systems was carried to the circuit board or line replaceable unit level. The diverse actuation system was modeled as a "black box" (i.e., a detailed fault tree was not developed) and was allocated reliability values based on the system design goals (its failure is assumed to be 1E-2 per demand, which is considered to be a conservative estimate).
- (2) Power supply to each DI&C cabinet subsystem was explicitly modeled.
- (3) Loss of cooling to DI&C equipment was considered. For the DI&C equipment in the AP1000 PRA, only the PMS equipment was determined to accommodate, by design, a loss of the normal heating, ventilation, and air conditioning. Other digital systems were assumed to fail on loss of cooling.
- (4) Wiring and cable failures were assumed negligible compared to the failure rates of circuit boards or their failures were incorporated in the failures of the receiving and transmitting hardware (associated circuit boards).
- (5) Failures of sensors and sensor taps were explicitly modeled.
- (6) Computer bus failures, including failures of directly connected cards to the bus, were modeled in the fault trees.
- (7) Failure of the automatic tester subsystem was not modeled. Benefits of the tester subsystem were credited in estimating card failure probabilities. This assumption could be problematic for other designs.
- (8) No contribution due to random software failure was modeled, as software failure was assumed to fall solely under the category of common cause design failures.
- (9) No test and maintenance unavailability events were modeled because the systems are run to failure and then replaced. DI&C systems are assumed to be able to respond appropriately even if in the testing mode.

No recovery actions were considered in the AP1000 PRA logic models (fault trees and event trees) for DI&C functions (except for using the manual option of a function once the automatic option of that function fails).

Physical and logical dependencies in DI&C systems were captured in the DI&C fault trees. The DI&C system fault trees were fully integrated with the fault trees of other systems. The following is a list of three important assumptions made in the AP1000 PRA regarding the treatment of dependencies:

- (1) Loss of cabinet cooling to the PMS cabinet subsystems was not modeled for AP1000 because the PMS is designed to withstand a loss of the normal HVAC. Loss of cabinet cooling for other DI&C systems was assumed to result in their failure.
- (2) Failure of sensors was explicitly modeled in the fault trees.

DRAFT

- (3) Power supply to each I&C cabinet subsystem is explicitly modeled.

The identification of areas where CCF should be modeled and the estimation of CCF probabilities for the three DI&C systems modeled in the AP1000 PRA (i.e., PMS, PLS, and DAS) were based on evaluation of coupling mechanisms (e.g., similarity, design defects, and environmental effects) combined with an evaluation of defense mechanisms against CCF (e.g., separation, operational testing, maintenance, and ability to detect failures immediately through on-line diagnostics). It was important to evaluate the level of confidence claimed regarding the credit that should be given for defense mechanisms. The level of modeling detail was carried to the circuit board or line replaceable unit level. Two CCF types were identified: (1) hardware CCFs (mainly to address CCF of the same type of boards in several subsystems and same type of sensors), and (2) software CCFs. Both CCFs of components within a DI&C system (e.g., PMS) and across two or more DI&C systems (e.g., across both PMS and PLS) were considered.

The following are 10 examples of where CCFs were modeled in the AP1000 PRA:

- (1) CCF of all sources of indication (this is considered a bounding assumption; CCF assumed among PMS and PLS, and diverse DAS indication)
- (2) CCF of the same type sensors (e.g., pressure transmitters) across all four sensor groups for both automatic protection functions and indication were modeled in each of the three DI&C systems
- (3) CCF of hardware portions of the engineered safety feature (ESF) input logic groups
- (4) CCF of software portions of ESF input logic groups
- (5) CCF of software portions in the ESF Actuation Cabinets. This CCF fails all functions performed in all four cabinets (i.e., all automatic ESF actuations fail)
- (6) CCF of software portions of the output logic inputs/outputs
- (7) CCF of output driver cards (hardware) across all divisions for each I&C system
- (8) CCF of software in the multiplexer cabinets
- (9) CCF of software across the four divisions of communications subsystems.
- (10) CCF of common software elements (common functions software) among the reactor trip and ESF functions and other DI&C functions

Hardware CCF probabilities were estimated using the multiple Greek letter method or the beta factor method. The NRC performed an audit of these calculations.

NRC review identified the following areas as having significant uncertainty in the AP1000 PRA:

DRAFT

1. Potential design errors in "common functions" software (i.e., software controlling fundamental processor functions, such as input/output, processing, and communications). Because such functions and their associated software are repeated across all major subsystems of PMS and PLS, such software design errors could affect the reactor trip and ESF portions of PMS, as well as all the PLS functions, and fail both their automatic and manual functions.
2. Potential design errors in "application" software (i.e., software controlling the actual algorithms, protective functions, and actuating functions that the PMS is designed to provide).

The DI&C failure data for the AP1000 microprocessor-based components were derived from Westinghouse data. The component failure rates used in the data development were derived from a combination of operational data, estimated component reliability based on Military Handbook calculations, and specified component reliability. The NRC considered the appropriateness of this data and audited the calculation notes during the AP600 DC review.

The following three assumptions were made in the AP1000 PRA in calculating the probabilities of basic events (unavailabilities):

- (1) All sensors were assumed to be non-repairable at power (repair was assumed to take place at refueling).
- (2) The repair time (i.e., replacement time) for all DI&C components (except sensors) was assumed to be four hours.
- (3) Systems self-diagnostics in the AP1000 DI&C systems were assumed to be automatically completed at a set period. The effectiveness of these diagnostics in detecting failures was assumed to be in excess of 90% for most functions.

Propagation of parameter uncertainties associated with basic events related to the DI&C systems was performed in the uncertainty analyses for CDF and large early release frequency (LERF). It should be noted that some of the assumed parameter uncertainties were subjective estimates based on engineering judgment.

Guidance for NRC Review of DI&C Systems in Advanced Reactor Probabilistic Risk Assessments

The significant difficulties and limitations associated with performing a risk assessment of DI&C systems are discussed in the Background section of this guidance document. The DI&C risk assessment methods have the potential to disclose design problems in DI&C systems that are significant. However, it is not expected that any such deficiencies will exist, given the rigorous and comprehensive process associated with DI&C design in nuclear power plants. The level of uncertainty associated with DI&C risk assessment results and insights (in part due to PRA modeling limitations and limited applicable data) restricts the use of digital system risk information in nuclear power plant design decisions and licensing actions. 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.

DRAFT

To date, risk assessments can provide 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 advanced reactor DI&C system PRA reviews (i.e., the reviews of the risk assessments for the ABWR, AP600, and AP1000 designs).

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 the DI&C system design. Potential problems that might be identified include the following:

- 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, or
- 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 advanced reactor DI&C systems, the following review guidelines are provided (note that review areas are not listed in order of importance):

- A. The review should include the following 27 steps:
- (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 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 insufficiency in current modeling techniques for determining the risk significance of the DI&C system.
 - (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. 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 should be reviewed include the following:
 - a. Increase the software failure probability and evaluate the change in CDF compared to the base case.

DRAFT

- b. Increase the software failure probability while simultaneously assuming that all non-safety-related defense-in-depth systems become unavailable, and the plant continues to operate at power. Evaluate the change in CDF and compare it to the base case.
 - c. Increase the software failure probability while simultaneously assuming that all non-safety-related defense-in-depth systems become unavailable with the exception of the diverse actuation system, and the plant continues to operate at power. Evaluate the change in CDF and compare it to the base case.
 - d. Ensure the propagation of CCF properly reflects the system architecture, connections, and software failure modes. If it does not, increase the span of propagation in a sensitivity study.
 - e. Increase the CCF rate of the DI&C system and evaluate the change in CDF compared to the base case.
 - f. Increase the CCF rate, increase the associated human error rates, and evaluate the change in CDF compared to the base case.
- (3) Verify the adequacy of propagation of parameter uncertainties for DI&C systems in the uncertainty analyses for CDF and LERF.
 - (4) 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 software failure modes because they occur in many different 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 and ensure it is complete.
 - (5) Ensure that environmental effects on the DI&C systems are properly modeled in the PRA. The PRA should consider the effects of environmental conditions such as electromagnetic interference, radio frequency interference, pressure, external events, fires, smoke, temperature, and humidity.
 - (6) Evaluate the acceptability of how the failure of control room indication is modeled in the DI&C system fault trees. For example, in AP1000 it was treated by incorporating a "failure of all indication" event for all three DI&C systems in the fault trees in parallel with human action failure events.
 - (7) Evaluate how software failures are modeled in the fault trees. It is acceptable at this time to model software failures explicitly in fault tree logic in parallel with hardware failures. Failures of software modules that are common across multiple applications should be considered (e.g., look at CCF of common function modules used to store and retrieve information from memory buffers.)
 - (8) Evaluate how PRA success criteria are affected by DI&C system failures. In the AP1000 PRA, DI&C systems were assumed not to affect PRA success criteria (for systems and operator actions). This may or may not be a reasonable assumption for other designs and as the state-of-the-art becomes better

Comment [vka35]: Is it physically possible for the plant to remain at power under these conditions? If not, what is the meaning of this sensitivity study? Are separate acceptance criteria for sensitivity studies being developed?

Comment [vka36]: Some note must be included to indicate what these results mean. Are there reasonable human action recoveries that might mitigate the results of this sensitivity? These have not been modeled in some or all of the applications. This may be difficult for some CF designs – but this should be considered before taking action on this sensitivity.

Comment [vka37]: PRAs do not normally do this.

Comment [vka38]: This criterion portrays the use of software functional blocks as a negative thing, rather than as the benefit that it is. The use of simple reusable software (functional blocks that are completely tested and rigorously controlled) improves the reliability of application-specific software. Restricting application software in safety-related applications to exclusive use of software functional blocks reduces software design errors. The current state-of-the-art in safety-related software design does not allow "programmers" to write individual customized lines of computer code.

Comment [vka39]: It appears that "in series" would be appropriate here, as hardware and software are likely not redundant.

DRAFT

defined, other models may be more appropriate. Evaluate how the PRA considers the loss of displays, controls, and specific systems.

- (9) Verify that physical and logical dependencies were captured adequately in the DI&C fault trees. The probabilistic model should encompass all the relevant dependencies of a digital system on its support systems. If the same digital hardware is used for implementing several digital systems that perform different functions, a failure in the hardware or software of the digital 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 fault trees should be fully integrated with the fault trees of other systems.
- (10) 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. See examples in the AP1000 DI&C system review. 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. DI&C models in PRAs often assume that multiple functions (e.g., on one chip) can be segregated in such a manner as to prevent the failure of one function from affecting another or the failure of one function from propagating to other chips. The degree to which this can be accomplished should be considered by a reviewer. The reviewer should carefully evaluate the reasoning given by the applicant.
- (11) Ensure that spurious actuation of the DAS was considered adequately.
- (12) 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. It should be noted that no recovery actions were considered in the AP1000 PRA logic models (fault trees and event trees) for DI&C functions (except for using the manual actions to implement a function once the automatic actions of that function fail). If recovery actions are modeled, they should consider loss of instrumentation and the time available. Recovery actions should not credit equipment potentially subject to the same CCF.
- (13) 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, CCFs (both hardware and software) may need to be applied in several areas within subsystems (e.g., logic groups), among subsystems of the same division, across divisions, and across systems. For example, CCF assignments of DI&C components and systems in the

Comment [vka40]: These criteria require complete dependence to be assumed between failures of different systems that use the same operating system (OS) or platform. This assumption is extremely unrealistic and ignores the principle that software CCF needs not just a common latent defect, but also a common trigger in the input data trajectory. Even for a relatively unreliable OS, such as that used in office computers, it is unlikely for all of the computers in the same office lockup at exactly the same time.

The SR I&C systems used in nuclear power plants have much more reliable OS than office computers. The proposed criteria ignores features that vendors of SR digital I&C platforms have built into their products to prevent exactly this kind of dependency. It is a fundamental objective of these OS designs that a failure in the execution of application software code cannot cause failure of the OS. Features such as deterministic program execution, cyclic processing, asynchronous operation, and constant bus loading, are designed to reduce failure triggers and prevent failures that do occur from propagating through the OS. To do a realistic PRA analysis of digital I&C, these features must be understood and valued by the analyst. Even if this value is difficult to quantify, it does not make the value of the features any less real. The PRA must attempt to model these failures realistically so that it does not artificially raise the importance of some failure modes and mask the importance of others.

Comment [vka41]: There should be discussion elsewhere in this document of DAS spurious actuation for low frequency events, and potential risk offsets.

Comment [vka42]: What does this phrase mean? Inter-system CCF is not normally considered in the PRA.

Comment [vka43]: Why do CCFs need to be applied across systems? This is generally not done in the PRA.

DRAFT

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 the AP1000 PRA should not be considered as the current state-of-the-art.

- (14) Ensure that CCF events were identified and modeled properly, and that CCF probabilities were estimated based on an evaluation of coupling mechanisms (e.g., similarity, design defects, external events, and environmental effects) combined with an evaluation of defense mechanisms against CCF (e.g., separation, operational testing, maintenance, and ability to detect failures by on-line diagnostics or self-testing). If the channels of a digital system (and/or the redundancy within a channel) use similar software, a complete dependence should be assumed for software failures. That is, similar software in different channels (and or in the redundancy within a channel) should be assumed to fail together. Hardware CCF between different systems using the same hardware should be modeled. Use of similar support software in different digital systems should be modeled as CCF, and a complete dependence should be assumed for software failures.
- (15) Fault-tolerance design features are intended to increase the availability and reliability of digital systems, so they 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 digital 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 fault-tolerant feature detects a failure, the system may fail to re-configure properly, or may be set up into a configuration that is less reliable than the original one. The benefits of these features also may be included. Care should be taken to ensure that both are modeled correctly (e.g., ensuring that the beneficial impacts of these features are only credited for appropriate failure modes).

Comment [vka44]: The basis for suggesting this kind of assumption is not clear. Suggest removing this sentence.

Comment [vka45]: What constitutes "similar" software?

Comment [vka46]: This criterion requires complete dependence for application software, if it is "similar." For modeling application software in a PRA this might be an acceptable assumption to make, under some circumstances (such as software that has identical inputs, algorithms, and function). However, extending this assumption to software that is merely "similar" ignores the generally recognized premise that software failure requires both a programming defect and a trigger in the input data trajectory. The proposed criterion of complete dependence recognizes only the contribution of the software defect and not that of the data trajectory. Use of different inputs and data trajectories is a recognized characteristic of functional diversity, which is an accepted defense against SWCCF. The PRA should make an attempt to judge the degree of coupling between similar but different functions. Assuming complete dependence is not realistic in all circumstances.

An issue with including a fault-tolerant feature of a digital system in a PRA model is that its design may be such that it only can detect, and hence fix, 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 repair. The PRA model should only give credit to the ability of these features to automatically repair their specific failure modes; it should consider that all remaining failure modes cannot be automatically tolerated.

A very important characteristic of fault coverage is that it expresses 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. 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.

DRAFT

- (16) It is important to evaluate the level of confidence in claims by applicants regarding the credit that should be given for defense mechanisms. If the defense mechanisms (e.g., self-test diagnostics or design diagnostics) are relied upon to help keep the probability of failure low (this is especially important when making risk-informed decisions), then 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.
- (17) If a digital system shares a communication network with others, the effects on all systems due to failures of the network should be modeled jointly. The propagation of failures through communication devices and their effects on the related components or systems should be evaluated, and any effect considered relevant should be included in the probabilistic model.
- (18) If hardware and software 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.
- (19) 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. 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). Carefully examine assumptions about the efficacy of system self-diagnostics in detecting failures.
- (20) If component-specific data are available, they confirm that they 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.
 - b. The sources of raw data are provided.
 - c. The method used in estimating the parameters is documented, so that the results could be reproduced.
- (21) If component-specific data are not available, confirm that the generic data used meets the following:
- a. The data of the same generic type of component are used and wide uncertainty bounds are used.
 - b. The generic data were collected from components that were designed for applications similar to those in nuclear power plants.

Comment [vka47]: These programs are not necessary; monitoring is the approach of RG 1.174.

Comment [vka48]: What are wide uncertainty bounds? Uncertainty bounds should be based on the same methods as the rest of the PRA.

DRAFT

- c. The sources of the generic database are given.
- (22) Verify that both component-specific and generic data meet the following:
- a. If the system being modeled is subject to an adverse environment and the data obtained are not so subject, the data should be modified to account for the corresponding impact.
 - b. Data for CCF meet the above criteria in (22)a.
 - c. Data for fault coverage meet the above criteria in (22)a.
 - d. Documentation is included on how the basic event probabilities are calculated in terms of failure rates, mission times, and test and maintenance frequencies.
- (23) 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 fault coverage. 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 digital system can be explicitly included either in the logic model or in the PRA data, but not both.
- (24) Verify that a method for quantifying the contribution of software failures to digital system reliability was used and documented.
- (25) 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 digital system (e.g., communication between different components, multi-tasking, multiplexing, etc.).
- The reviewer should examine how these dynamic interactions have been addressed in the PRA model for DI&C systems or should evaluate the rationale for not modeling them.
- (26) Examine how the DI&C failure data was determined and if it is appropriate. Evaluate the adequacy and appropriateness of the basis for applying the data to the systems involved.
- (27) 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 propagate to fail the system. The sequence of events should realistically represent the system's behavior at the level of detail of the model.

Comment [vka49]: This is not common practice for analog equipment, and digital equipment should not be treated differently.

Comment [vka50]: This should be clarified to indicate that subjective probability estimates are an acceptable alternative. A probability can be assigned subjectively using qualitative attributes of the systems design, the platform, and the software development life cycle, as opposed to detailed analysis of the specific application software. Coupled with sensitivity or uncertainty analysis, this can be an appropriate way to proceed.

There should not be a criterion asking for a quantitative methodology when none exists and it may not even be possible. As stated in this document, there is no generally agreed upon method to estimate the reliability of complex application-specific software. In spite of years of exhaustive research by the software and computer industries, a method to estimate software failure probability has been elusive. It would be a mistake to delay the use of PRA-based risk insights, and possibly the installation of digital I&C itself, waiting for development of a software reliability quantification method that may never come. It is more important for the PRA analyst to understand the factors that affect software reliability, than to be able to quantify the precise failure probability.

Comment [vka51]: The dynamic interactions (as discussed in NUREG/CR-6901 and 6942) are primarily issues that involve complex control systems in the non-safety-related part of the plant. These issues are of limited interest to PRA because their impact is mostly limited to the initiating event. It has not been shown that these failure modes are applicable to the safety-related systems that comprise the bulk of the typical PRA. In addition, as the research clearly indicates, it is difficult to probabilistically model the performance of complex integrated control systems, either digital or analog. The modeling methods discussed in NUREG/CR-6901 and 6942 may have some use for stand-alone control system studies; however their practicality and usefulness for modeling of PRA initiating event frequencies is unproven.

DRAFT

- B. 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 result in unacceptable risk, 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.
- C. If the applicant has indicated it is making risk-informed decisions with input from the DI&C risk assessment, the reviewer should ensure that the principles of RG 1.174, Revision 1 are met. For example, the reviewer should evaluate the base case and sensitivity studies to see if the use of a DI&C design might introduce significant new failure modes not previously analyzed, might increase the frequency of significant accident sequences, or might increase the frequencies of lower-ranked contributors so that they become significant contributors to risk.
- D. The reviewer should document risk insights drawn from the DI&C system risk assessment.
- E. 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 DAS (if necessary) and DI&C systems should be clearly explained. Coordinate this review with NRC staff evaluating the DI&C system's D3 capabilities.

Comment [vka52]: Sensitivity study results are not required to comport to the LERF and CDF subsidiary objectives. The LERF and CDF subsidiary objectives contain margin to the actual safety goal (QHO) and are used with realistic analysis.

Comment [vka53]: By design, sensitivity studies will increase frequencies of significant accident sequences of lower-ranked contributors. This should be done with realistic analyses, not sensitivities.

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

The following are general insights drawn from previously reviewed advanced 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.

Comment [vka54]: Subjective judgment should not be used to assign levels of uncertainties to the insights. A better basis is necessary.

Comment [vka55]: This statement is an important observation, and should be discussed more prominently in the document.

DRAFT

- (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 Risk Achievement Worth (RAW,) (i.e., 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 importance measure values for CCF of DI&C components are extremely high (i.e., the RAW values for DI&C CCFs are often the highest of all structures, systems, and components modeled in the PRA). 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 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 advanced 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 important 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 CDF and risk.

Comment [vka56]: It is misleading to compare importance values for CCFs to SSCs, as this involves comparing a two-train failure to a single train failure. Comparing CCF importance values to those for other CCFs, however, is acceptable.

Comment [vka57]: This statement is vague, and may not universally be true for low-frequency initiators.

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

- (1) The use of two redundant and diverse actuation systems with automatic and manual actuation capability (one is safety related) 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 DAS appears to be less reliable and cannot 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

Comment [vka58]: Are two redundant DASs used?

Comment [vka59]: Does the DAS have to be treated as safety-related?

DRAFT

- 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 to be highly reliable (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 are significant contributors to the estimated 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

Comment [vka60]: It is unclear how many recoveries were considered in the AP1000. This statement may be true, but a more detailed evaluation may show that they have significant time for recoveries that are not credited due to lack of knowledge on actual configurations and procedures.

Comment [vka61]: The use of "significant" here may be misleading. A "significant" contributor, by the ASME standard, can be 1% of the overall risk. Here, the overall risk is 1E-7. Therefore, it is possible to cite a 1E-9 event as "significant." The absolute values should be cited.

DRAFT

- 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).

DRAFT

Acronyms

ABWR	Advanced Boiling Water Reactor
AP600	a Westinghouse designed 600 MWe passive nuclear power plant
AP1000a	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
I&C	instrumentation and control
LERF	large early release frequency
LRF	large release frequency
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+	an advanced nuclear reactor design from the former Combustion Engineering Company
TWG-3	Task Working Group # 3
MWe	megawatt electric

DRAFT

References

SECY-93-87

NUREG-0800, Chapter 7, Branch Technical Position 19 (BTP-19)

NUREG/CR-6850

10 CFR 52

Safety Goal Policy Statement

Regulatory Guide 1.200

PRA Policy Statement on Pg. 5

RG 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis", Revision 1, dated November 2002.

AP1000 PRA

ABWR PRA

AP1000 FSER

ABWR FSER

ASME standard for PRA

DRAFT

Glenn Kelly
11/05/07
Version 7a