



DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-03

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

Interim Staff Guidance

Draft

(Issued for Review and Comment)

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

Draft

(Issued for Review and Comment)

IMPLEMENTATION

This Interim Staff Guidance (ISG) provides acceptable methods for evaluating digital instrumentation and control system risk assessments. This guidance is consistent with current NRC regulations (10CFR52) on performance of risk assessments for new reactors, and NRC policy on Safety Goals and PRAs, and is not intended to be a substitute for NRC regulations, but to clarify how a licensee or applicant may satisfy those regulations and policies.

This ISG also clarifies the criteria the staff would use to evaluate whether a digital system design is consistent with Safety Goal guidelines. The staff intends to continue interacting with stakeholders to refine digital I&C ISGs and to update associate 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

GUIDANCE ON REVIEWING NEW REACTOR RISK ASSESSMENTS OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

Executive Summary

The Nuclear Regulatory Commission (NRC or Commission) and the nuclear industry realize that digital instrumentation and control (DI&C) systems (usually partial replacement of analog equipment in operating plants and full DI&C systems for new reactor designs) have the potential to improve reliability and reduce risk. DI&C systems are complex combinations of hardware components and software (i.e., computer programs). Although computer software does not wear out and therefore is not subject to some of the failure modes of analog systems, excitation of residual software design errors can cause significant problems. For digital systems, failure of software comes from the combination of a defect in the software in conjunction with a set of circumstances (e.g., a plant transient or accident) that causes an unusual set of inputs to the software that result in the residual error being accessed.

The nuclear industry has purposed to design and implement DI&C systems in new reactors that have a low probability of containing significant software errors. In particular, the designers have attempted to reduce the likelihood of common cause failures (CCFs). Still, there is significant 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 estimate or verify such failure rates. If one could eliminate all design errors before a software product is put into operation, it would work perfectly. However, experience shows that one cannot ensure that residual faults do not continue to exist 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 internal input states and inputs for the software programs.

To limit hardware and software errors and to deal with the uncertainty of common cause failures, comprehensive deterministic guidance was developed by the NRC and industry. The deterministic guidance is based, in part, on robust digital system development/design 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 specifically to result in high quality and high reliability digital systems, the potential still remains for a CCF, and the effects of a CCF on event mitigation may be significant. The NRC recognizes that not all failures, including software CCF, can be eliminated from complex systems. 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.) A research project is underway to develop a set of metrics for evaluating the quality of a digital system development process.

The industry believes that there are reasonable ways to estimate and bound the risks associated with digital systems. Further, although there is significant research ongoing for digital system modeling, it does not include a focused review of what the NRC has noted as the dominant factor of software common cause.

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

DRAFT

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 variation of the single failure review method, but with relaxed assumptions and acceptance guidelines modified to evaluate the effect of postulated CCFs in digital systems. In addition to the traditional single failure criterion evaluation to determine adequate DI&C redundancy, the methodology addresses digital system CCFs by including an independence and diversity assessment.

The NRC and industry recognize that current probabilistic risk assessment (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). However, there currently is no guidance for NRC reviewers on evaluating DI&C system risk assessments.

The NRC performed reviews of the DI&C systems modeled in the PRAs for new designs such as the Advanced Boiling Water Reactor (ABWR), AP600, and AP1000. A brief summary of how these evaluations were performed is provided in Attachment 1 to 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. The guidance herein provides greater detail of and relies more on the AP600/AP1000 DI&C PRA review than of the ABWR review. In operating reactor PRAs, the analog instrumentation and control (I&C) systems are normally "black-boxed". They are modeled as highly reliable with low probabilities of CCF. The reactor protection system, which is potentially subject to common cause failure, has a diverse backup system to help reduce the uncertainties associated with CCF probability.

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 of the DI&C systems. 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 (RAW) importance function values.)

The NRC review of the DI&C portion of the AP600/1000 PRA¹ 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 overall 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

¹ 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.

The assessment of independence is performed in accordance with IEEE Standard 603 or 279 depending on the date of the operating license, not BTP-19.

Although there are some unique aspects to digital R.G. 1.200 provides sufficient guidance for what standards must be met.

Other than the reactor protection system, I&C modeling in PRA is not normally black boxed nor was it at the time of the IPEs. Where technical difficulties exist in modeling systems such as the reactor protection system, accepted practice has been to model the system as a supercomponent, assigning quantitative values based on expert judgment supported by operating experience. Other potentially safety significant I&C systems (particularly , ESFAS) are generally modeled in significant detail. This statement is not correct. In many cases the industry does model these systems in detail. Further, NFPA 805 requirements are causing more of these systems to be modeled in detail to allow fire impacts to be modeled.

DRAFT

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 core damage frequency (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 CCFs propagation (e.g., inter-channel, inter-system, inter-train) can influence CDF and substantially affect risk insights), and
- * RAW values for CCF of DI&C system components due to software failures often are very large.

As noted in this document, detailed configurations are unknown and recoveries were not modeled. Assuming no recoveries in advanced plants, where many of the initiators will have very long time frames to core uncoveries, is obviously extremely conservative. There will be some low frequency events that require a more rapid response, but these will not have the same impact on RAW. Given this uncertainty and the very small overall CDF of the advanced plants, it may be unreasonable to make judgments regarding the results until more realistic assessments can be made.

Due to data limitations² and the lack of consensus 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. There have been no risk-informed DI&C system submittals from industry for operating reactors. For the new reactor risk assessments performed to date and reviewed by the NRC, the inclusion in the design of a diverse backup system (e.g., a diverse actuation system (DAS)) has been found to reduce the uncertainties about startup of important equipment in the plant following a significant transient or accident (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 new reactors, is that full deterministic assessments as set forth in BTP-19 and SECY 93-87 should continue to be performed and their criteria met.

A reviewer should keep in mind that while uncertainties may be large regarding failure rates and appropriate modeling techniques for DI&C systems, new reactor PRAs consistently have calculated low expected CDF rates on the order of 1E-7 per year for internal event initiators. The new reactor vendors appear to have designed away or significantly limited many of the dominant contributors to risk found in operating plants.

Much of this risk importance noted here is not related to the initiators that BTP-19 is designed to protect against. The majority of this RAW is almost certainly from anticipated transients, not from rare events.

² 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

The NRC's concerns regarding DI&C risk are a measure of the prudence it exercises in guarding the health and safety of the public.

General guidance is provided to clarify how NRC will review near-term DI&C system risk assessments for new reactors, including comparisons to Safety Goals. This guidance is based on previously accepted reviews performed on new reactor DI&C system designs. Portions of this guidance may apply to operating reactors DI&C submittals because partial analog I&C system replacements may not require as robust a review, may only have portions of the guidance pertinent, or may engender different issues than those raised in the new reactor, full DI&C 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 inclusion of common cause failures in PRAs and uncertainty analysis associated with new reactor digital systems.

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 needed to operate the plants. The potential for CCFs was believed not to be present or to have an extremely low probability because it usually was assumed that CCF, if it did occur, was due to slow processes such as corrosion or premature wear-out. This assumption was further supported by the use of aggressive vendor inspection activities by the NRC to assess the quality of components used in the safety system designs. In addition, other CCFs whose occurrence could immediately make the system incapable of performing its function(s) important to safety, such as maintenance errors, were assumed to be detectable by scheduled testing. The software failures of concern to the NRC and which are believed probably to be of low probability are assumed not to be detectable by testing.

Today, with I&C manufacturers' lack of support for analog systems and the realization that digital systems can offer unique, beneficial design and functional capabilities, the nuclear industry is in the process of replacing portions of aging analog I&C systems in operating plants and is developing full DI&C systems for new 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 CCFs being due to slow processes or being discovered by scheduled testing may no longer be true for systems containing complex software.

DI&C systems are intended to be at least as reliable as the analog systems they replace. However, the integrated aspects of digital system designs result in the possibility of unique failure modes when compared to analog systems. Of significant concern to the NRC and industry is the possibility that DI&C system CCF 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 system. In addition, it is very difficult to determine the failure rates associated with CCF for such systems. It is to this end that industry has engaged in an effort to reduce the likelihood of CCF.

The sentence implies that digital I&C systems somehow have greater importance than other plant systems. As statements to this effect can be made of any number of plant systems, the purpose of this sentence is not clear. It is suggested that the sentence be deleted.

Suggest revising this paragraph to reflect the ISG's role in demonstrating that the digital I&C system meets the intent of the Commission's safety goals.

It is not clear why it should be the case that current plants pose any more difficult an analysis problem than new plants.

It is the industry's position that if the system is a highly qualified system, not only the probability that the fault will occur low, but there is also a low probability of a set of inputs that would actuate this fault.

DRAFT

Since digital systems play an increasingly important role in nuclear facility control and safety systems, particularly for new reactor designs, the need for risk assessment methods appropriate to DI&C systems is evident. However there are significant challenges³ 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 risk assessments for new reactors (portions may be applicable to operating reactors). It discusses the background of DI&C review guidance and also provides a summary of methods used by the NRC to evaluate risk associated with DI&C systems in previously approved design certifications (DCs). The document identifies the currently available risk insights for DI&C systems.

Background

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. The nuclear industry has purposed to design and implement DI&C systems in new reactors that have a low probability of containing significant errors. In particular, the designers have attempted to reduce the likelihood of CCF. There is uncertainty as to the actual CCF rate in these DI&C systems, and the NRC considers it prudent to be cautious as it is extremely difficult to either accurately predict or verify such failure rates. If one could eliminate all design errors before a software product is put into operation, it would work perfectly. However, experience shows that one cannot ensure that residual faults do not continue to exist 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. 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. Likewise, extrapolation of statistical data from the same product being used in a different operational environment is not necessarily meaningful.

Because software does not fail the way hardware fails due to wear-out, the commonly used hardware redundancy techniques do not improve software reliability. 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.

Although development processes and methods are designed to result in high-quality and reliable digital systems, the potential for a CCF remains, and the effects of a CCF on event mitigation may be significant. Although the industry has made an effort to reduce the probability of significant software errors, the NRC and industry recognize that not all failures, including CCF, can be eliminated in complex software. 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

³ See NUREG/CR-6901, S. Arndt (2001), S. Arndt (2006), and National Research Council (1997)

DRAFT

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 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) such that they can be integrated into a PRA.

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.

This statement implies that quality and reliability of digital systems cannot be assessed in a manner that permits integration into a PRA. This statement is inconsistent with the National Academy of Sciences report on digital I&C systems in nuclear power plants which concludes that bounded estimates for software failure probabilities can be obtained by processes that include valid random testing and expert judgment as in other PRA computations. Furthermore, international standards (e.g. IEC 61226) suggest that reliability estimates can be based on meeting referenced quality criteria. It is requested that the statement be modified to recognize that even without precise knowledge of digital system reliability, qualitative risk insights can contribute to the estimation of CCF that will support decision making in an appropriate manner.

See comment regarding second paragraph on P. 4

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 variation of the 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

- (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 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

DRAFT

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.

Suggest deleting this phrase, as operating reactors have PRAs that can be used for the purpose of generating risk insights regarding digital I&C systems similar to new plants.

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 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. In general, these limitations make it difficult to develop robust risk insights about DI&C systems. For the new reactor risk assessments performed to date and reviewed by the NRC, the inclusion in the design of a diverse backup system has been found to positively affect PRA safety insights (i.e., a diverse backup system provides assurance 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 new reactors, is that full deterministic assessments as set forth in BTP-19 and SECY 93-87 should continue to be performed and their criteria met.

Suggest replacing this statement with "due to the evolving nature of PRA."

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

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 set of software can be used for different software.

DRAFT

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 CCF propagation can influence CDF and substantially affect risk insights.
- RAW values for CCF of DI&C system components often are very large.

The NRC currently has a long-term project to attempt to determine if risk assessment methods exist or can be developed to appropriately model DI&C system risk. There is no consensus in the technical community that methods normally employed when performing PRAs are adequate for the purpose of making comprehensive risk-informed decisions for DI&C.

In spite of this, the NRC and industry recognize that current PRA methods can provide useful, high-level risk information about DI&C systems (e.g., insights on what aspects of, or assumptions about, the DI&C systems are most important, and approximation of the degree to which the risk associated with operation of these systems is sensitive to failure rate assumptions). Regulatory Guide 1.200 provides guidance on evaluating the technical adequacy of PRAs. As noted in Element 1.1 of Table A-1 in Appendix A to Regulatory Guide 1.200, special emphasis should be placed on PRA modeling of novel and passive features in the design, as well as addressing issues related to those features, such as digital instrumentation and control, explosive (squib) valves, and the issue of T-H uncertainties. The regulatory guide, 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 digital system modeling and data. Guidance as to what risk metrics are appropriate for evaluating the acceptability of DI&C systems also may be needed.

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. 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 digital systems in PRAs for design certificate applications or COL applications under Part 52. The issue includes

DRAFT

addressing CCF modeling and uncertainty analysis associated with digital systems.

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

Guidance for NRC Review of New Reactor DI&C System Probabilistic Risk Assessments

Suggest changing to "potential," as the staff has not yet demonstrated that the difficulties and limitations are significant.

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. It is expected that a PRA reviewer will need to interface with a DI&C expert 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. 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 lack of consensus in the technical community over acceptable PRA models for DI&C risk assessments and limited applicable data) is high. The uncertainties currently are large enough to reinforce the need for diversity, defense-in-depth, adequate safety margins, and the deterministic requirements designed to assure their continued existence.

Suggest deleting, as insights regarding digital I&C generated by PRA are already influencing digital system designs.

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 new 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).

DRAFT

Based on PRA reviews the NRC has previously performed on new reactor DI&C systems, the following review guidelines are provided⁵:

- A. The review should consider the following steps, as applicable, to ensure that the risk contributions from DI&C are reflected adequately in the overall plant risk results:
- (1) Review the DI&C portion of the PRA as an integrated part of the overall PRA review. Perform all the normal aspects of a PRA review including evaluation of the quality of the PRA. The level of review of the DI&C portion of the PRA may be limited due to limitations such as the lack of design details, lack of applicable data, and the lack of consensus in the technical community regarding acceptable modeling techniques for determining the risk significance of the DI&C system. The level of review should be proportional to the use of the results and insights from the DI&C risk assessment.
 - (2) Uncertainties in DI&C modeling and data should be addressed in the DI&C risk assessment. It is expected that the DI&C risk assessment will address uncertainties by at least performing a number of sensitivity studies that vary modeling assumptions, reliability data, and parameter values. The reviewer should evaluate the sensitivity studies performed by the applicant on the PRA models and data to assess the effect of uncertainty on CDF, risk, and PRA insights. Sensitivity study scenarios that may be appropriate and if provided should be reviewed include the following:
 - a. Increase the software failure probability and evaluate the change in CDF compared to the base case.
 - 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 diverse backup systems, 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.

The purpose of the proposed sensitivity studies and the issues that the staff is intending to investigate are not stated. Also, items A (2) and (3) would not appear to provide meaningful insights, as the plants may not even be able to operate under the assumed conditions.

⁵ A reviewer should not expect that a model of DI&C systems will exactly follow the guidance discussed for every area.

DRAFT

Suggest combining with (7)

(3) The reviewer should confirm that DI&C system equipment is qualified for the environment to which it might be subject. For example, the reviewer should confirm if the equipment is qualified for the following environments:

a. electromagnetic interference

b. radio frequency interference

c. pressure

d. external events

More than seismic qualification?

e. fires

Not explicitly required as a qualification attribute by RG 1.209. What is intended by the confirmation that equipment is qualified for these environments?

f. smoke

g. temperature

h. humidity.

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

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

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

(7) 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 design features meant to protect against CCF (e.g., separation, operational testing, maintenance, diagnostics, self-testing, or fault tolerance) If the safety functions of a digital system (and/or the

DRAFT

redundancy within safety functions) use common software, a degree of dependency should be assumed for software failures. That is, when common software is used for different safety functions (and or in the redundancy within a safety function), it should be assumed to fail together. Hardware CCF between different safety functions using the same hardware should be modeled. Dependencies between hardware and software failures should be modeled. The DI&C dependency should represent both the presence of a DI&C fault and its associated trigger mechanism. In determining the dependence of common software, its similarity should be considered in determining the extent of dependency (It has been demonstrated by Knight and Leveson that it is not possible to develop redundant software that does not have any dependencies). Whenever dependence is assumed in the evaluation (or should be assumed), the reviewer should expect that the applicant has provided rationale for the degree of dependency assumed.

The referenced work was predicated on redundant software being developed from the same functional specification. This statement should be put in its correct context or removed.

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

- (8) It is important to evaluate the level of confidence in claims by applicants regarding the credit that should be given for design features. If the design features (e.g., self-test diagnostics or design diagnostics) are relied upon to help keep the probability of failure low, 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.
- (9) Verify that a method for quantifying the contribution of software failures to digital system reliability was used and documented.
- (10) 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 propagates to fail the system. The sequence of events should realistically represent the system's behavior at the level of detail of the model.
- (11) 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 guidance should be modified to reflect a need for a monitoring program only if the results of the PRA are sensitive to the system in question.

DRAFT

Note that the existence of specific sensitivity study results that may challenge the Safety Goals do not necessarily imply that additional requirements or regulatory attention are necessary, since the particular sensitivity study may involve a very unlikely scenario or set of failure events. Specifically, care must be taken when directing the PRA reviewers to require additional DAS systems based on sensitivity study results. There are obvious insights that can be obtained, but the foundation of the PRA must be considered in regulatory decisions.

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. Note, just because the results of a specific sensitivity study may challenge the Safety Goals does not necessarily imply that additional requirements or regulatory attention are necessary, since the particular sensitivity study may involve a very unlikely scenario or set of failure events.

- (12) The reviewer should document risk insights drawn from the DI&C system risk assessment.
 - (13) Verify that key assumptions from the DI&C PRA are captured under the applicant's design reliability assurance program (D-RAP), which is described in SRP Chapter 17, Section 17.4. The applicant should describe adequately where and how the D-RAP captures the DI&C system key assumptions. Target reliability and availability specifications should be described adequately for the operational phase of D-RAP (details of the operational phase are provided in SRP Section 17.6). If the PRA lacks sufficient quantitative results to determine target values, the applicant should describe adequately how expert judgment will establish reliability and availability requirements. These specified values should be defined to help ensure that no safety conclusions based on review of the risk analysis of the DI&C are compromised once the plant is operational. How the licensee will carry out performance monitoring for diverse backup systems (if necessary) and DI&C systems should be clearly explained. Coordinate this review with NRC staff evaluating the DI&C system's D3 capabilities. An implementation and monitoring program should address how the applicant will assure that the design continues to reflect the assumed reliability of the systems and components during plant operation.
- B. The review also should include the following additional steps, as applicable, if a more detailed review is needed (e.g., through field audits):
- (1) Verify the adequacy of propagation of parameter uncertainties for DI&C systems in the uncertainty analyses for CDF and large early release frequency (LERF).
 - (2) 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.

DRAFT

- (3) Evaluate how software failures are modeled in the fault trees, if needed. It is acceptable at this time to model software failures explicitly in the fault trees. 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.)
- (4) Evaluate how PRA success criteria are affected by DI&C system failures. In at least one new reactor 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 defined, other models may be more appropriate. Evaluate how the PRA considers the loss of displays, controls, and specific systems.
- (5) Verify that physical and logical dependencies were captured adequately in the DI&C fault trees, as needed. 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.
- (6) Ensure that spurious actuations of diverse backup systems or functions are evaluated and the overall risk impact documented.
- (7) 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 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.
- (8) Design features such as fault tolerance, diagnostics, and self testing are intended to increase the availability and reliability of digital 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 digital systems if they are not designed properly or fail to operate appropriately. The potentially negative effects of these features should be

The assertion that hardware CCF should be incorporated across systems is inconsistent with the manner in which CCF is modeled in PRA. A rationale should be provided in the guidance as to why digital I&C is unique in this regard, or the guidance should be deleted.

DRAFT

included in the probabilistic model. The PRA should account for the possibility that after a fault is detected, the system may fail to re-configure properly, or may be set up into a configuration that is less reliable than the original one, fail to mitigate the fault altogether, or the design feature itself may introduce 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 failure of the design feature itself is considered in the model).

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

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. 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.

It should be noted that how you measure and define fault coverage needs to be clearly defined by the applicant and evaluated by the reviewer in conjunction with the DI&C expert.

- (9) 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.
- (10) 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.
- (11) 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). Confirm that the data used in the PRA is appropriate for the hardware

DRAFT

and/or software version being modeled, or that adequate justification is provided.

Note, a fault-tolerant feature of a digital 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.

- (12) If component-specific data are available, 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 can be reproduced.
- (13) 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 uncertainty bounds appropriately reflecting the level of uncertainty are used.
 - b. The generic data were collected from components that were designed for applications similar to those in nuclear power plants.
 - c. The sources of the generic database are given.
- (14) Verify that both component-specific and generic data meet the following:
 - a. If the system being modeled is qualified for its environment but the data obtained are not so subject, the data should account for the differences in application environments.
 - 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.
- (15) When a specific datum from a generic database, such as a failure rate of a digital component, is used in a DI&C risk assessment, the reviewer should assess whether the datum was adjusted for the contribution of design features specifically intended to limit postulated failures. If so, the failure rate may be used in the PRA, but no additional fault coverage should be

DRAFT

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.

- (16) 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 confirm that interactions have been addressed in the PRA model for DI&C systems or should evaluate the rationale for not modeling them.

- (17) 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.

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

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

- (1) The absolute value of the contribution to CDF and risk from failure of DI&C systems is low. The uncertainty of this insight is at the medium level.
- (2) The estimated CDF is not very sensitive to reasonable changes in single DI&C component failure probabilities or in initiating event frequencies. This was confirmed for previously reviewed designs when DI&C system components had their importance measure functions assessed. Measures evaluated included Fussell-Vesely, a measure that looks at how the CDF or risk would change if the particular component or system were always available, and RAW, a measure that looks at how the CDF or risk would change if the particular component or system were always unavailable. The uncertainty of this insight is medium.
- (3) The RAW values for CCF of DI&C components are very high (i.e., the RAW values for DI&C CCFs reported by reactor vendors in their PRAs are often the highest of all structures, systems, and components (SSCs) modeled in the PRA). **Similar RAW values would be found for other high reliability SSCs (e.g., a reactor vessel) that have no additional layers of defense and whose failure would directly cause core damage.** This insight has implications for the development of reliability assurance programs, emergency procedures, and other areas. The uncertainty of this insight is low.

This paragraph suggests that advanced plants in which a single digital CCF can lead directly to core damage are being designed and licensed. We do not believe this is the case and suggest the paragraph be deleted.

DRAFT

- (4) The inclusion of a diverse backup system (e.g., DAS) to automatically and manually actuate selected safety systems appears to compensate for the uncertainties in DI&C system CCF rates. The uncertainty in this insight is low.
- (5) In new reactor designs, most of the dominant contributors to CDF and risk normally found in a risk assessment for operating reactors have been designed away. One result of this is that human errors associated with DI&C system failures have become more important as contributors to CDF, although the absolute numerical value of these failures is low. The uncertainty in this insight is low.
- (6) There are significant uncertainties in the modeling of DI&C systems in PRAs and therefore the insights from the assessment have uncertainties.
- (7) There are significant uncertainties in the data used to estimate DI&C system contributions to CDF and risk.

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

- (1) The use of two redundant and diverse backup systems with automatic and manual actuation capability (one is safety related and the other non-safety-related, e.g., DAS) minimizes the likelihood of actuation failures, including common-cause actuation failures. The non-safety-related DAS is a reliable system capable of initiating automatic and manual reactor trip using the motor-generator sets when the reactor fails to trip via the PMS. At operating reactors, the diverse actuation system (i.e., DAS) appears to be less reliable and in some cases, may not automatically initiate a reactor trip. The redundant and diverse actuation capabilities help reduce the risk associated with anticipated transient without scram (ATWS) events in the AP1000 design.
- (2) The DI&C-related systems and components with the highest RAW values are as follows:
 - a. software for the PMS and PLS logic cards
 - b. PMS ESF software components, such as input logic software, output logic software, and actuation logic software
 - c. PMS ESF manual input multiplexer software
 - d. PMS ESF hardware components, such as output drivers and input logic groups
 - e. PMS reactor trip logic hardware.
- (3) No CCF of software has high Fussell-Vesely importance measure values (i.e., a measure of how much the CDF could be improved if the software were made perfectly reliable) in the AP1000 PRA because software was assumed to be highly reliable. When the NRC's review performed sensitivity studies, it became

DRAFT

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 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).

DRAFT

Acronyms

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

DRAFT

References

SECY-93-87

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

NUREG/CR-6850

NUREG/CR-6901

10 CFR 52

Safety Goal Policy Statement

Regulatory Guide 1.200

PRA Policy Statement

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

Knight and Leveson

National Research Council, "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues", National Academy Press (1997)

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).

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.

DRAFT

Attachment 1

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

The NRC performed reviews of the DI&C systems modeled in the PRAs for new 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.

ABWR REVIEW. As discussed in the Background, there is no consensus in the technical community about the PRA methods that are acceptable for modeling 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 new 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 RAW 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

DRAFT

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 RAW importance function values.)

The NRC review of the DI&C portion of the AP600/1000 PRA⁶ 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. The staff noted that because of the limited consensus on the appropriate methodologies or metrics and the lack of data pertaining to software failures, the probability distribution functions for software were subjective point estimates.

To address this, 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. The goal of the sensitivity study was to determine if the CDF was sensitive enough to changes in software failure probability to influence the PRA conclusions about the design including diverse backup capability. 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.

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.

⁶ 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

- (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.

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.

DRAFT

- (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 were assumed to be able to respond appropriately even if in the testing mode.
- (10) No operator recover of DI&C systems was assumed if the system failed. Operator actions to manually operate equipment or otherwise perform recovery actions were modeled. That is, 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.
- (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 design features that protect 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 design features. 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:

DRAFT

- (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:

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.

DRAFT

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 LERF. It should be noted that some of the assumed parameter uncertainties were subjective estimates based on engineering judgment.

DRAFT

Glenn Kelly
11/29/07
Version 7d