

Comparison of review guidelines from Draft ISG "Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments" with content of industry white paper entitled "Modeling of Digital I&C in Nuclear Power Plant Probabilistic Risk Assessments"

ISG		Industry White Paper	
Number	Guidance	Section	Discussion
A1	The level of review should be proportional to the use of the results and insights from the applicant's DI&C risk assessment.	Executive Summary	The paper discusses the level of modeling detail useful in incorporating I&C in PRA consistent with other applications of PRA, suggests that the required detail is dependent on the influence of the I&C on the overall results of the PRA.
		II. Current Industry Practice and the Resulting Sensitivity of PRA to Digital I&C	This paper outlines an approach to digital I&C modeling in PRA that can be used to confirm that the risk associated with digital I&C failures has been addressed adequately. By demonstrating that risks associated with digital failure are low and that this does not rely solely on the reliability of the digital system, but on redundant and diverse plant design features, it also is demonstrated that the PRA is not sensitive to the digital system modeling and that the level of detail is adequate.
A2	The modeling of DI&C systems should include the identification of how DI&C systems can fail and what their failure can affect.	III.A.1. Normal Plant control systems	The PRA should consider whether there are credible integrated control system failures that can cause an initiating event that is not included within one of the traditional initiating events already included in the PRA.

		<p>III.A.2. Mitigating Systems</p>	<p>For mitigating system digital I&C, it is important to capture the failure modes that may lead to the loss of the mitigating system function. The failure modes of individual components within the mitigating system itself dictate the level of detail needed in modeling the I&C. A bounding analysis may assume that the digital failure modes are such that the mitigating system components fail in the least convenient direction. Where such failure modes are excluded, an engineering rationale should be developed providing justification for their exclusion.</p>
<p>A2</p>	<p>Examine applicant documentation to ensure that the most significant failure modes of the DI&C risk assessment are documented with a description of the sequence of events that need to take place and how the failure modes can fail the system.</p>	<p>III.A.2. Mitigating Systems</p>	<p>For mitigating system digital I&C, it is important to capture the failure modes that may lead to the loss of the mitigating system function. The failure modes of individual components within the mitigating system itself dictate the level of detail needed in modeling the I&C. A bounding analysis may assume that the digital failure modes are such that the mitigating system components fail in the least convenient direction. Where such failure modes are excluded, an engineering rationale should be developed providing justification for their exclusion.</p>
		<p>III.B.2. Other Hardware Aspects of Digital I&C Systems</p>	<p>The PRA should consider the potential failure modes of a module’s digital output (fails on, fails off, fails as-is).</p>
		<p>III.B.2. Other Hardware Aspects of Digital I&C Systems</p>	<p>For the failure probability of a digital I&C system module, it is the analyst’s choice whether to parse out the failure probability by failure mode, or take a conservative “all-modes” approach.</p>

		<p>III.B.2. Other Hardware Aspects of Digital I&C Systems</p>	<p>Fault-tolerant design can be treated explicitly in the model, or it can be treated conservatively to reduce modeling complexity. For a digital I&C system with a high level of redundancy and diversity, a potentially conservative model is acceptable and can demonstrate that the risk is not sensitive to the digital I&C reliability or the level of modeling detail.</p>
<p>A4</p>	<p>Uncertainties in DI&C modeling and data should be addressed by at least performing a number of sensitivity studies that vary modeling assumptions, reliability data, and parameter values both at the component and system level.</p>	<p>V. Sensitivity of PRA to Digital I&C</p>	<p>A recommendation of the National Academy of Sciences report is the performance of sensitivity analyses to help the analyst assure that the results are not unduly dependent on parameters that are uncertain. Suggested sensitivity studies include:</p> <ul style="list-style-type: none"> ▫ Vary the probability of failure of the digital systems to determine <ul style="list-style-type: none"> ▪ What combinations of digital failure probability for a division of I&C and common cause failure would result in the PRA approaching the Safety Goals. ▪ What initiating events (and possibly the specific accident sequence characteristics) dominate the change in risk ▫ Where Safety Goals are not approached, a deterministic rationale for why risk remains low even in the presence of bounding digital failure probabilities is developed. Such a rationale may include: <ul style="list-style-type: none"> ▪ Diverse means of actuating the affected mitigating system or a redundant system, e.g., <ul style="list-style-type: none"> • Operator action (assurance should be provided that there is time to perform this action and the indications and controls needed to take this action are available given the presence of the postulated digital failure).

		<ul style="list-style-type: none">•Diverse actuation system (a description of the design features of the redundant actuation system should be provided with justification for why it is considered diverse).<ul style="list-style-type: none">▪Where no diverse actuation system is provided, identification of the of the accident sequence characteristics that keep the risk of digital system failure low is provided•Very low initiating event frequency (provide the plant design and operating characteristics that result in such a low frequency)•Confirmation that the initiating event frequency is not influenced by digital system failures▫Where Safety Goals are approached, then the reliability of the digital system itself plays an important role in managing safety. A deterministic basis for concluding that the failure probability of the digital system is relatively low is needed. Such a rationale may include:<ul style="list-style-type: none">▪An assessment of diversity attributes and defensive measures that keep one or both P_{df} and b_{cc} low.▪Design, operational, maintenance and monitoring activities that assure the identified diversity attributes and defensive measures will continue to be maintained.
--	--	--

<p>A4</p>	<p>If a risk outlier challenges the Safety Goals, the reviewer should document this and submit it to the reviewer's management.</p>	<p>V. Sensitivity of PRA to Digital I&C</p>	<p>Vary the probability of failure of the digital systems to determine</p> <ul style="list-style-type: none"> o What combinations of digital failure probability for a division of I&C and common cause failure would result in the PRA approaching the Safety Goals. o What initiating events (and possibly the specific accident sequence characteristics) dominate the change in risk. o Where Safety Goals are not approached, a deterministic rationale for why risk remains low even in the presence of bounding digital failure probabilities is developed. o Where Safety Goals are approached, then the reliability of the digital system itself plays an important role in managing safety. A deterministic basis for concluding that the failure probability of the digital system is relatively low is needed.
<p>A7</p>	<p>Evaluate the acceptability of how the failure of control room indication is modeled</p>	<p>III.A.4. MCR Instrumentation Systems</p>	<p>The diversity and redundancy of instrumentation is usually sufficient that its failure is an insignificant contributor to the HRA, and its reliability can be included in the HRA, if this is not the case. Symptom-based EOPs often provide appropriate guidance irrespective of the availability of specific instrumentation, further reducing the significance of modeling operator informational I&C in the performance of human reliability analysis.</p>
<p>A8</p>	<p>A DI&C defensive measure may have the downside of causing spurious trips or spuriously failing functional capabilities. The licensee should describe the segregation process that prevents this from occurring.</p>	<p>III.A.3. Supporting Control Systems</p>	<p>The consequence of failure is easily modeled as a failure mode of the final controlled device(s). However, like the protection system and other mitigating control systems, these separate control functions may share common hardware, software, or support systems and the dependencies should be resolved in the PRA.</p>

		IV.A. Operating System	There are features used in SR digital I&C, such as strictly cyclic operation, static memory allocation, and constant bus loading, that are used to ensure reliable and predictable performance of the OS and behavior that is free of interference from the application program.
A9	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.	III.A.4. MCR Instrumentation Systems	Main control room (MCR) instrumentation systems are typically not modeled explicitly in the PRA. This includes implicit modeling of instrumentation dependencies in the HRA if there are dependencies upon the initiating event. The diversity and redundancy of instrumentation is usually sufficient that its failure is an insignificant contributor to the HRA, and its reliability can be included in the HRA, if this is not the case.
A9	If recovery actions are modeled, they should consider loss of instrumentation and the time available.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems. The protection system performs the functions of reactor trip and actuation of engineered safety features, and should be a primary I&C focus for the PRA.
A10	Verify that a method for quantifying the contribution of software failures to DI&C system reliability was used and documented.	IV. Software Failure Probabilities for PRA	For the purposes of determining the sensitivity of plant risk to digital I&C reliability and driving corresponding design decisions, the industry approach is to portray the probability of software failure as a random event. This is consistent with the National Academy of Sciences findings.

		<p>IV. Software Failure Probabilities for PRA</p>	<p>With respect to application software, it is assumed that there is a quality software development life cycle process, including an independent verification and validation (IV&V) methodology to provide assurance that the application software is adequately specified, designed, implemented, tested, and controlled. Design errors may nonetheless occur, and it is important that the system design have adequate functional diversity, as well as defensive measures to prevent application software errors from defeating the OS.</p>
		<p>IV. Software Failure Probabilities for PRA</p>	<p>Good industry design practice includes features in SR digital I&C systems to minimize the impact of CCF. Values and methods used to estimate the software failure probability need to account for these defensive measures that are implemented in the design.</p>
		<p>IV. Software Failure Probabilities for PRA</p>	<p>For estimation of software failure probability, the recommended analysis distinguishes between the OS and the application software.</p>
<p>B1</p>	<p>Verify that physical and logical dependencies were identified and their bases provided in the DI&C PRA.</p>	<p>III.A.2. Mitigating Systems</p>	<p>Non safety related mitigating systems also are considered in the PRA. Where these systems share dependencies with initiating systems or other mitigating systems, these dependencies are generally developed in the PRA.</p>

B1	The probabilistic model should encompass all the relevant dependencies of a DI&C system on its support systems.	III.A.1. Normal Plant control systems	The normal plant control systems are generally pre-initiating event functions and are not of much interest to the PRA post-trip. A few normal plant controls (such as for MFW) may be given limited post-trip credit in some PRAs; however this credit is rarely extensive, and never solely relied upon. A minimum amount of fault tree modeling of initiating events may be necessary to capture dependencies (e.g., shared components or support systems), and the purpose of these models is to ensure that credit is not given post-trip for a system or component that was involved in the initiating event.
		III.A.2. Mitigating Systems	Non safety related mitigating systems also are considered in the PRA. Where these systems share dependencies with initiating systems or other mitigating systems, these dependencies are generally developed in the PRA.
B1	If the same DI&C hardware is used for implementing several DI&C systems that perform different functions, a failure in the hardware, software, or system of the DI&C platform may adversely affect all these functions. Should these functions be needed at the same time, they would be affected simultaneously.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems. The protection system performs the functions of reactor trip and actuation of engineered safety features, and should be a primary I&C focus for the PRA.
		III.A.2. Mitigating Systems	Non safety-related mitigating systems also are considered in the PRA. Where these systems share dependencies with initiating systems or other mitigating systems, these dependencies are generally developed in the PRA.

B1	The DI&C system probabilistic model should be fully integrated with the probabilistic model of other systems.	I. Introduction and Purpose	The purpose of this white paper is to describe a method for incorporating digital instrumentation and control (I&C) system models in nuclear power plant (NPP) probabilistic risk assessments (PRA).
		II. Current Industry Practice and the Resulting Sensitivity of PRA to Digital I&C	In selecting methods for modeling of digital I&C in PRA, it is important to recognize the context of the digital I&C with respect to the functions it provides in the overall plant design, not only including the quality of the software and hardware but considering the effect of these defense-in-depth and diversity related design practices as well.
B3	Based on the results of this evaluation, D&IC software and/or hardware/software dependent CCFs may need to be applied in several areas within subsystems (e.g., logic groups), among subsystems of the same division, across divisions or trains, and across systems.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems.
B3	An important expectation is that the applicant included sufficient equipment in the CCF groups. The evaluation should address why various channels, trains, systems, etc. were or were not placed in each CCF group. The justification should discuss common software/hardware among the equipment considered and the level(s) of dependency among them.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems. The protection system performs the functions of reactor trip and actuation of engineered safety features, and should be a primary I&C focus for the PRA.

B3	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.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems.
		III.A.1. Normal Plant Control Systems	A minimum amount of fault tree modeling of initiating events may be necessary to capture dependencies (e.g., shared components or support systems), and the purpose of these models is to ensure that credit is not given post-trip for a system or component that was involved in the initiating event.
B3	The CCF events are to be identified and modeled by the applicant.	III.B.1. Physical and Functional Characteristics	The level of detail of the PRA model should be appropriate to resolve physical and functional dependencies.
B3	The CCF probabilities and their bases should be evaluated and provided by the applicant based on an evaluation of coupling mechanisms (e.g., similarity, design defects, external events, and environmental effects) combined with an evaluation of design features meant to protect against CCF (e.g., separation, operational testing, maintenance, diagnostics, self-testing, or fault tolerance).	I.V.C. Estimating Beta Factors	See Examples 8 through 11.

B3	If the safety functions of a DI&C system (and/or the redundancy within safety functions) use common software, dependency should be assumed for software faults. That is, when common software is used for different safety functions (or in the redundancy within a safety function) it may fail each function.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems. The protection system performs the functions of reactor trip and actuation of engineered safety features, and should be a primary I&C focus for the PRA.
		III.B. Level of Detail of PRA Model for Mitigating System Digital I&C	The CCF probabilities will consider the case of hardware that shares common software, whether it be common operating system (OS) or application software.
B3	Hardware CCF between different safety functions using the same hardware should be modeled.	III.A.3. Supporting Control Systems	The consequence of failure is easily modeled as a failure mode of the final controlled device(s). However, like the protection system and other mitigating control systems, these separate control functions may share common hardware, software, or support systems and the dependencies should be resolved in the PRA.
B3	Dependencies between hardware and software should be identified.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems. The protection system performs the functions of reactor trip and actuation of engineered safety features, and should be a primary I&C focus for the PRA.

		III.B. Level of Detail of PRA Model for Mitigating System Digital I&C	The software and hardware are coupled, and should be treated together. The approach is to attach the software CCF probability to the hardware upon which it resides.
		III.B. Level of Detail of PRA Model for Mitigating System Digital I&C	The CCF probabilities will consider the case of hardware that shares common software, whether it be common operating system (OS) or application software.
B3	The applicant should provide the rationale for the degree of dependency assumed for DI&C CCF.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems. The protection system performs the functions of reactor trip and actuation of engineered safety features, and should be a primary I&C focus for the PRA.
B3	The reviewer should work with the I&C reviewer to evaluate the applicant's justifications.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems. The protection system performs the functions of reactor trip and actuation of engineered safety features, and should be a primary I&C focus for the PRA.

B4	<p>If the design features (e.g., fault tolerance, diagnostics, self testing, DAS) are relied upon to help keep the probability of the DI&C system failure low, including DI&C CCF, then an implementation and monitoring program should address how the applicant will assure that the design features continue to support the assumed reliability of the systems and components in the future.</p>	<p>III.A.2. Mitigating Systems</p>	<p>It is important that the PRA capture the dependencies and potential CCF contributions while simultaneously crediting the design features of redundancy and diversity that (per industry consensus design standards and practices) provide reliable and robust performance.</p>
		<p>III.B.2. Other Hardware Aspects of Digital I&C Systems</p>	<p>Fault-tolerant design can be treated explicitly in the model, or it can be treated conservatively to reduce modeling complexity. For a digital I&C system with a high level of redundancy and diversity, a potentially conservative model is acceptable and can demonstrate that the risk is not sensitive to the digital I&C reliability or the level of modeling detail.</p>
		<p>IV.A. Operating System</p>	<p>There are features used in SR digital I&C, such as strictly cyclic operation, static memory allocation, and constant bus loading, that are used to ensure reliable and predictable performance of the OS and behavior that is free of interference from the application program.</p>
	<p>Design features such as fault tolerance, diagnostics, and self testing are intended to increase the availability and reliability of DI&C systems, and therefore are expected to have a positive effect on the system's reliability.</p>	<p>III.A.2. Mitigating Systems</p>	<p>It is important that the PRA capture the dependencies and potential CCF contributions while simultaneously crediting the design features of redundancy and diversity that (per industry consensus design standards and practices) provide reliable and robust performance.</p>

B4	However, these features also may have a negative impact on the reliability of DI&C systems if they are not designed properly or fail to operate appropriately. The potentially negative effects of these features should be included in the probabilistic model.	III.B.2. Other Hardware Aspects of Digital I&C Systems	Fault-tolerant design can be treated explicitly in the model, or it can be treated conservatively to reduce modeling complexity. For a digital I&C system with a high level of redundancy and diversity, a potentially conservative model is acceptable and can demonstrate that the risk is not sensitive to the digital I&C reliability or the level of modeling detail.
B4	The PRA should account for the possibility that after a failure is detected, the system may fail to re-configure properly, may be set up into a configuration that is less reliable than the original one, fail to mitigate the failure altogether, or the design feature itself may contain a fault.	III.B.2. Other Hardware Aspects of Digital I&C Systems	The PRA should consider the potential failure modes of a module's digital output (fails on, fails off, fails as-is).
		III.B.2. Other Hardware Aspects of Digital I&C Systems	Fault-tolerant design can be treated explicitly in the model, or it can be treated conservatively to reduce modeling complexity. For a digital I&C system with a high level of redundancy and diversity, a potentially conservative model is acceptable and can demonstrate that the risk is not sensitive to the digital I&C reliability or the level of modeling detail.
B4	Care should be taken to ensure that design feature intended to improve the availability and reliability are modeled correctly	IV. Software Failure Probabilities for PRA	For the purposes of determining the sensitivity of plant risk to digital I&C reliability and driving corresponding design decisions, the industry approach is to portray the probability of software failure as a random event. This is consistent with the National Academy of Sciences findings.

B4	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.	III.A.2. Mitigating Systems	For mitigating system digital I&C, it is important to capture the failure modes that may lead to the loss of the mitigating system function. The failure modes of individual components within the mitigating system itself dictate the level of detail needed in modeling the I&C. A bounding analysis may assume that the digital failure modes are such that the mitigating system components fail in the least convenient direction. Where such failure modes are excluded, an engineering rationale should be developed providing justification for their exclusion.
		III.B.2. Other Hardware Aspects of Digital I&C Systems	For the failure probability of a digital I&C system module, it is the analyst's choice whether to parse out the failure probability by failure mode, or take a conservative "all-modes" approach.
		III.B.2. Other Hardware Aspects of Digital I&C Systems	Fault-tolerant design can be treated explicitly in the model, or it can be treated conservatively to reduce modeling complexity. For a digital I&C system with a high level of redundancy and diversity, a potentially conservative model is acceptable and can demonstrate that the risk is not sensitive to the digital I&C reliability or the level of modeling detail.
B4	It should be noted that how fault coverage is measured and defined should be provided by the applicant.	III.B.2. Other Hardware Aspects of Digital I&C Systems	Fault-tolerant design can be treated explicitly in the model, or it can be treated conservatively to reduce modeling complexity. For a digital I&C system with a high level of redundancy and diversity, a potentially conservative model is acceptable and can demonstrate that the risk is not sensitive to the digital I&C reliability or the level of modeling detail.

B5	If a DI&C system shares a communication network with others, the effects on all systems due to failures of the network should be modeled jointly.	III.B. Level of Detail of PRA Model for Mitigating System Digital I&C	The software and hardware are coupled, and should be treated together. The approach is to attach the software CCF probability to the hardware upon which it resides.
		IV.A.1. Operating Systems, Crediting Operating Experience	Since the OS and the computer processor are highly coupled in terms of design and operating history, failure of the OS may be considered a failure mechanism (or CCF mechanism) of the processor. The PRA can incorporate the OS failure probability using either a fixed probability or a beta factor against the hardware failure probability. A review of the failure history should determine what portion of the computer processor failures is attributable to hardware failures versus OS.
B5	The impact of communication faults and their effects on the related components or systems should be evaluated, and any failure considered relevant should be included in the probabilistic model.	III.B. Level of Detail	Therefore the computer processor hardware (with appropriate CCF factors) provides a good surrogate for PRA modeling of the software. The processor may exist at the signal processing, communications or logic level within the digital system. Alternately the functional effects of the software failure can be represented at the component, train or system level.
B7	Confirm that the data used in the PRA are appropriate for the hardware and/or software version being modeled, or that adequate justification is provided.	IV.A.1. Operating Systems, Crediting Operating Experience	The manufacturer is a good source of failure data for the digital system components and embedded operating. However, care must be taken in applying failure data derived from operating experience.

B8a	Confirm that...the data are obtained from the operating experience of the same equipment as that being evaluated, and preferably in the same or similar applications and operating environment. Uncertainty bounds should be appropriately reflect the level of uncertainty. (both component-specific and generic data)	IV.A.1. Operating Systems, Crediting Operating Experience	The manufacturer is a good source of failure data for the digital system components and embedded operating. However, care must be taken in applying failure data derived from operating experience.
B8e	Confirm that...data for CCF meet the above criteria in 8d. (If the system being modeled is qualified for its environment but the data obtained are not drawn from systems qualified for that environment, the data should account for the differences in application environments.)	IV.A.2. Operating Systems, Crediting Defensive Measures	In lieu of operating experience for the specific I&C platform, a conservative CCF probability for the OS may be determined from subjective judgment based upon consideration of its design features.
B8f	Confirm that...Data for fault coverage meet the above criteria in 8d. (both component specific and generic data)	III.B.2. Other Hardware Aspects of Digital I&C Systems	“Coverage” is an important concept, as it determines the percentage of failures that are self-monitored (i.e., self-revealing) versus non-self-monitored (or test-revealed). This failure mode breakdown will vary between I&C designs and between different types of digital components. It has an important role in the PRA analysis, as it drives which mathematical unavailability model (repair-time model, test-interval model, or both) is used for each component.
B9	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.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems.

In comparing the content of the draft ISG and the industry's white paper, it was noted that many of the review guidelines from the ISG were not explicitly discussed in the white paper, as the white paper concentrated on issues unique to DI&C rather than general PRA issues. Thus, many aspects of standard PRA practice, such as modeling support system dependencies, performing uncertainty analysis, and documenting assumptions, were not discussed in the industry's white paper. The industry is considering referencing the ASME PRA standard in future papers on the topic to reinforce the expectation that PRA quality requirements from the standard should be met. The industry believes that, if the ASME PRA standard were referenced, the following review guidelines from the ISG would be addressed by the industry white paper:

A1	Perform all the normal aspects of a PRA review including evaluation of the quality of the PRA
A5	The reviewer should confirm that DI&C system equipment is capable of meeting its safety function for the environment assumed in the PRA.
A6	The reviewer should confirm that the impact of external events (i.e., seismic, fire, high winds, flood and others) has been addressed with regard to DI&C.
A8	Verify that the assumptions made in developing the reliability model and probabilistic data are realistic, and the associated technical justifications are sound and documented.
B7	The guidelines in Subsection 4.5.6, "Data analysis," of the ASME standard for PRA for nuclear power plant applications should be satisfied consistent with the clarifications and qualifications of RG 1.200.
B7	Determine if the manner in which basic event probabilities were established is acceptable and if the rates seem reasonable.
B7	Check the assumptions made in calculating the probabilities of basic events (unavailabilities).
B8b	Confirm that...the sources for raw data or generic databases are provided. (both component-specific and generic data)
B8c	Confirm that...the method used in estimating the parameters is documented, so that the results can be reproduced. (component-specific data)
B8d	Confirm that...if the system being modeled is qualified for its environment but the data obtained are not so subject, the data should account for the differences in application environments. (both component-specific and generic data)

B8g	Confirm that...documentation is included on how the basic event probabilities are calculated in terms of failure rates, mission times, and test and maintenance frequencies. (both component-specific and generic data)
-----	---

Comparison of criteria listed in Draft NUREG "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems" with content of industry white paper entitled "Modeling of Digital I&C in Nuclear Power Plant Probabilistic Risk Assessments"

Draft NUREG			Industry White Paper	
Number	Section	Criteria	Section	Discussion
1.1	Level of Detail of the Probabilistic Model	A reliability model of a digital system should be developed to a level of detail that captures the design features affecting the system's reliability, and that provides the output needed for risk-informed decision-making.	III.A.1. Normal Plant control systems	Detailed modeling of normal (non-safety-related, NSR) plant control systems in the PRA should be avoided. Success for these systems is more often a function of plant response and performance, rather than a function of either hardware or software reliability. In the PRA, the failure of these systems at power is generally included in the initiating event frequency. For these systems, the important failure mode of the I&C is reflected at the system functional level, regardless of how the digital system itself may fail. A PRA that relies upon traditional initiating event frequencies, with a plan to update the frequencies when plant-specific data are available, will be conservative.
2.1	Identification of Failure Modes of the Components of a Digital System	A systematic method should be applied for identifying failure modes of the basic components of the digital system and their impact on the system.	III.B.2. Other Hardware Aspects of Digital I&C Systems	The PRA should consider the potential failure modes of a module's digital output (fails on, fails off, fails as-is).

<p>2.2</p>	<p>Identification of Failure Modes of the Components of a Digital System</p>	<p>Supporting analysis should be carried out to determine how specific features of a design, such as communication, voting, and synchronization, could affect system operation. It should determine whether the specific design features could introduce dependent failures that should be modeled.</p>	<p>III.A.1. Normal Plant Control Systems</p>	<p>Hence the PRA should consider whether there are credible integrated control system failures that can cause an initiating event that is not included within one of the traditional initiating events already included in the PRA. A failure modes and effects analysis (FMEA), such as is typically performed by the design activity, is a good tool for making this determination.</p>
			<p>III.A.2. Mitigating Systems</p>	<p>For mitigating system digital I&C, it is important to capture the failure modes that may lead to the loss of the mitigating system function. The failure modes of individual components within the mitigating system itself dictate the level of detail needed in modeling the I&C. A bounding analysis may assume that the digital failure modes are such that the mitigating system components fail in the least convenient direction. Where such failure modes are excluded, an engineering rationale should be developed providing justification for their exclusion.</p>
<p>2.3</p>	<p>Identification of Failure Modes of the Components of a Digital System</p>	<p>Failure modes that have occurred. in the operating experience should be examined and their applicability to the digital system being studied should be considered.</p>	<p>IV.A.1. Operating Systems (OS), Crediting Operating Experience</p>	<p>Unlike the application software, which may be one of a kind, the OS will usually have some applicable operating history...An operating history coupled with robust design and defensive features will minimize the uncertainty associated with OS failure probability. This should allow estimation of a best estimate failure probability or a bounding value for sensitivity study purposes.</p>

			IV.A.2. Operating Systems (OS), Crediting Defensive Measures	Other SR I&C systems may not have the experience cited in the preceding example. In lieu of operating experience for the specific I&C platform, a conservative CCF probability for the OS may be determined from subjective judgment based upon consideration of its design features.
2.4	Identification of Failure Modes of the Components of a Digital System	The probabilistic model of the digital system should account for the possibility that the system may fail due to incorrect design requirements, or due to correct requirements that are not implemented into the system.	IV. Software Failure Probabilities for PRA	With respect to application software, it is assumed that there is a quality software development life cycle process, including an independent verification and validation (IV&V) methodology to provide assurance that the application software is adequately specified, designed, implemented, tested, and controlled. Design errors may nonetheless occur, and it is important that the system design have adequate functional diversity, as well as defensive measures to prevent application software errors from defeating the OS.
			IV.B. Application Software	Application software failures occur because of design errors, and they cannot be completely ruled out.
3.1	Modeling of software failures	Software failures should be accounted for in the probabilistic model.	III.B. Level of Detail of PRA Model for Mitigating System Digital I&C	The software and hardware are coupled, and should be treated together. The approach is to attach the software CCF probability to the hardware upon which it resides.

<p>3.2</p>	<p>Modeling of software failures</p>	<p>The model of the software should include the "application software" and the "support software."</p>	<p>IV. Software Failure Probabilities for PRA</p>	<p>For estimation of software failure probability, the recommended analysis distinguishes between the OS and the application software.</p>
<p>3.3</p>	<p>Modeling of software failures</p>	<p>Modeling of software failures should be consistent with the basis of how they occur (see Appendix C); that is, software failures happen when triggering events occur.</p>	<p>IV.A. Operating System</p>	<p>There are features used in SR digital I&C, such as strictly cyclic operation, static memory allocation, and constant bus loading, that are used to ensure reliable and predictable performance of the OS and behavior that is free of interference from the application program.</p>
			<p>III.B. Level of Detail of PRA Model for Mitigating System Digital I&C</p>	<p>The software and hardware are coupled, and should be treated together. The approach is to attach the software CCF probability to the hardware upon which it resides.</p>
			<p>III.B. Level of Detail of PRA Model for Mitigating System Digital I&C</p>	<p>The functional effects of the software failure can be represented at the component, train or system level.</p>

			IV. Software Failure Probabilities for PRA	For the purposes of determining the sensitivity of plant risk to digital I&C reliability and driving corresponding design decisions, the industry approach is to portray the probability of software failure as a random event. This is consistent with the National Academy of Sciences findings.
3.4	Modeling of software failures	Modeling of software failures should account for the context/boundary condition in which a software is used.	III.B. Level of Detail of PRA Model for Mitigating System Digital I&C	The software and hardware are coupled, and should be treated together. The approach is to attach the software CCF probability to the hardware upon which it resides.
			III.B. Level of Detail of PRA Model for Mitigating System Digital I&C	The CCF probabilities will consider the case of hardware that shares common software, whether it be common operating system (OS) or application software.
			III.B.1. Physical and Functional Considerations	The chosen level of detail needs to address the effects of the functional or other diversity not only within the I&C but the plant systems in which the I&C resides.
4.1.1	Modeling of dependencies	Inter-system failure propagation should be addressed, and modeled appropriately.	III.A.2. Mitigating Systems	It is important that the PRA capture the dependencies and potential CCF contributions while simultaneously crediting the design features of redundancy and diversity that (per industry consensus design standards and practices) provide reliable and robust performance.

			III.B.1. Physical and Functional Considerations	The level of detail of the PRA model should be appropriate to resolve physical and functional dependencies. Since the computers may perform multiple functions, a level of detail at the computer processor module is appropriate to resolve these dependencies. However, a higher level of detail, such as subsystem or train, may be appropriate if failure rate data is available or can be estimated at that level.
4.1.2	Modeling of dependencies	Inter-channel failure propagation should be addressed, and modeled appropriately.	III.A.2. Mitigating Systems	It is important that the PRA capture the dependencies and potential CCF contributions while simultaneously crediting the design features of redundancy and diversity that (per industry consensus design standards and practices) provide reliable and robust performance.
			III.B.1. Physical and Functional Considerations	The level of detail of the PRA model should be appropriate to resolve physical and functional dependencies. Since the computers may perform multiple functions, a level of detail at the computer processor module is appropriate to resolve these dependencies. However, a higher level of detail, such as subsystem or train, may be appropriate if failure rate data is available or can be estimated at that level.
4.1.3	Modeling of dependencies	Intra-channel failure propagation should be addressed, and modeled appropriately.	III.A.2. Mitigating Systems	It is important that the PRA capture the dependencies and potential CCF contributions while simultaneously crediting the design features of redundancy and diversity that (per industry consensus design standards and practices) provide reliable and robust performance.

			III.B.1. Physical and Functional Considerations	The level of detail of the PRA model should be appropriate to resolve physical and functional dependencies. Since the computers may perform multiple functions, a level of detail at the computer processor module is appropriate to resolve these dependencies. However, a higher level of detail, such as subsystem or train, may be appropriate if failure rate data is available or can be estimated at that level.
4.2.1	Modeling of dependencies	Loss of power to safety related digital systems should be modeled appropriately. It is important to note that there may be cases where loss of power generates an actuation signal, i.e., the system of component fails safe. If this is the case, then loss of electric power should not be modeled as a cause of failure on demand of the system or component. Instead, it should be modeled for the generation of a spurious signal.	III.B.1. Physical and Functional Considerations	The chosen level of detail needs to address the effects of the functional or other diversity not only within the I&C but the plant systems in which the I&C resides.
			III.B.2. Other Hardware Aspects of Digital I&C Systems	The PRA should consider the potential failure modes of a module's digital output (fails on, fails off, fails as-is).
4.2.2	Modeling of dependencies	If dependencies on HVAC are relevant, they should be modeled.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems. The protection system performs the functions of reactor trip and actuation of engineered safety features, and should be a primary I&C focus for the PRA.

			III.B.1. Physical and Functional Considerations	The chosen level of detail needs to address the effects of the functional or other diversity not only within the I&C but the plant systems in which the I&C resides.
4.2.3	Modeling of dependencies	Other potential dependencies on support systems should be considered, and modeled as appropriate.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems. The protection system performs the functions of reactor trip and actuation of engineered safety features, and should be a primary I&C focus for the PRA.
			III.A.2. Mitigating Systems	Non safety related mitigating systems also are considered in the PRA. Where these systems share dependencies with initiating systems or other mitigating systems, these dependencies are generally developed in the PRA.
			III.B.1. Physical and Functional Considerations	The chosen level of detail needs to address the effects of the functional or other diversity not only within the I&C but the plant systems in which the I&C resides.

4.3.1	Modeling of dependencies	The digital systems of a plant should be examined to determine if there are dependencies due to sharing of digital hardware. Any relevant dependencies should be modeled.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems. The protection system performs the functions of reactor trip and actuation of engineered safety features, and should be a primary I&C focus for the PRA.
			III.A.3. Supporting Control Systems	The consequence of failure is easily modeled as a failure mode of the final controlled device(s). However, like the protection system and other mitigating control systems, these separate control functions may share common hardware, software, or support systems and the dependencies should be resolved in the PRA.
4.3.2	Modeling of dependencies	The effect of sensor failures on the digital system and on other components or systems of the plant should be evaluated and included in the probabilistic model.	III.A.3. Supporting Control Systems	The consequence of failure is easily modeled as a failure mode of the final controlled device(s). However, like the protection system and other mitigating control systems, these separate control functions may share common hardware, software, or support systems and the dependencies should be resolved in the PRA.
4.3.3	Modeling of dependencies	The failures of devices that process the output of redundant channels of a system should be modeled.	III.A.3. Supporting Control Systems	The consequence of failure is easily modeled as a failure mode of the final controlled device(s). However, like the protection system and other mitigating control systems, these separate control functions may share common hardware, software, or support systems and the dependencies should be resolved in the PRA.

4.3.4	Modeling of dependencies	Failure of a digital system may trigger an initiating event with possible additional failures of mitigation features. This dependency also should be included in the model, as applicable.	III.A.1. Normal Plant control systems	The PRA should consider whether there are credible integrated control system failures that can cause an initiating event that is not included within one of the traditional initiating events already included in the PRA.
4.4.1	Modeling of dependencies	The deterministic analysis of the digital system should identify those failure modes of a component that the fault-tolerant features can detect and the system is able to reconfigure itself to cope with the failure. The probabilistic model should only credit the ability of these features to automatically cope with these specific failure modes. It should consider that all the remaining failure modes cannot be automatically tolerated.	III.B.2. Other Hardware Aspects of Digital I&C Systems	Fault-tolerant design can be treated explicitly in the model, or it can be treated conservatively to reduce modeling complexity. For a digital I&C system with a high level of redundancy and diversity, a potentially conservative model is acceptable and can demonstrate that the risk is not sensitive to the digital I&C reliability or the level of modeling detail.
4.4.2	Modeling of dependencies	When applying a value of "fault coverage" to the probabilistic data of a component, the types of failures that were employed in the testing used to derive this value should be known. No credit for fault coverage should be given to those failure modes that were not included in the testing. This also would apply when using a value of fault coverage from a generic database or the literature.	III.B.2. Other Hardware Aspects of Digital I&C Systems	Fault-tolerant design can be treated explicitly in the model, or it can be treated conservatively to reduce modeling complexity. For a digital I&C system with a high level of redundancy and diversity, a potentially conservative model is acceptable and can demonstrate that the risk is not sensitive to the digital I&C reliability or the level of modeling detail.

4.4.3	Modeling of dependencies	Information from a generic database about a specific probabilistic datum of a component, such as a failure rate, should be reviewed to assess whether it was adjusted for the contribution of fault coverage. If so, this datum may be used in a probabilistic model, but no additional fault coverages should be applied to this component, unless it can be shown that the two fault coverages are independent.	III.B.2. Other Hardware Aspects of Digital I&C Systems	“Coverage” is an important concept, as it determines the percentage of failures that are self-monitored (i.e., self-revealing) versus non-self-monitored (or test-revealed). This failure mode breakdown will vary between I&C designs and between different types of digital components. It has an important role in the PRA analysis, as it drives which mathematical unavailability model (repair-time model, test-interval model, or both) is used for each component.
4.4.4	Modeling of dependencies	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 relevant components, but not in both.	III.B.2. Other Hardware Aspects of Digital I&C Systems	Fault-tolerant design can be treated explicitly in the model, or it can be treated conservatively to reduce modeling complexity. For a digital I&C system with a high level of redundancy and diversity, a potentially conservative model is acceptable and can demonstrate that the risk is not sensitive to the digital I&C reliability or the level of modeling detail.
			IV. Software Failure Probabilities for PRA	Good industry design practice includes features in SR digital I&C systems to minimize the impact of CCF. Values and methods used to estimate the software failure probability need to account for these defensive measures that are implemented in the design.

4.4.5	Modeling of dependencies	The probabilistic model should account for the possibility that a fault-tolerant feature may fail to detect and/or fix a failure mode that it was designed to catch.	III.B.2. Other Hardware Aspects of Digital I&C Systems	Fault-tolerant design can be treated explicitly in the model, or it can be treated conservatively to reduce modeling complexity. For a digital I&C system with a high level of redundancy and diversity, a potentially conservative model is acceptable and can demonstrate that the risk is not sensitive to the digital I&C reliability or the level of modeling detail.
			IV. Software Failure Probabilities for PRA	Good industry design practice includes features in SR digital I&C systems to minimize the impact of CCF. Values and methods used to estimate the software failure probability need to account for these defensive measures that are implemented in the design.
4.4.6	Modeling of dependencies	If the detection of a failure of a component depends on other components e.g., a watchdog timer, then the dependency must be modeled.	IV.A.2. Operating Systems (OS), Crediting Defensive Measures	In lieu of operating experience for the specific I&C platform, a conservative CCF probability for the OS may be determined from subjective judgment based upon consideration of its design features.
4.4.7	Modeling of dependencies	The probabilistic model 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.	III.B.2. Other Hardware Aspects of Digital I&C Systems	Fault-tolerant design can be treated explicitly in the model, or it can be treated conservatively to reduce modeling complexity. For a digital I&C system with a high level of redundancy and diversity, a potentially conservative model is acceptable and can demonstrate that the risk is not sensitive to the digital I&C reliability or the level of modeling detail.

			IV. Software Failure Probabilities for PRA	Good industry design practice includes features in SR digital I&C systems to minimize the impact of CCF. Values and methods used to estimate the software failure probability need to account for these defensive measures that are implemented in the design.
4.5	Modeling of dependencies	The probabilistic model should address Type I and Type II interactions.	III.A.1. Normal Plant Control Systems	The normal plant control systems are generally pre-initiating event functions and are not of much interest to the PRA post-trip. A few normal plant controls (such as for MFW) may be given limited post-trip credit in some PRAs; however this credit is rarely extensive, and never solely relied upon. A minimum amount of fault tree modeling of initiating events may be necessary to capture dependencies (e.g., shared components or support systems), and the purpose of these models is to ensure that credit is not given post-trip for a system or component that was involved in the initiating event.
			III.A.3. Supporting Control Systems	The consequence of failure is easily modeled as a failure mode of the final controlled device(s). However, like the protection system and other mitigating control systems, these separate control functions may share common hardware, software, or support systems and the dependencies should be resolved in the PRA.

4.6.1	Modeling of dependencies	Intra-system hardware CCF. Hardware CCF parameters should be estimated using applicable data and information associated with the possible causes of hardware CCF.	III.A.2. Mitigating Systems	It is important that the PRA capture the dependencies and potential CCF contributions while simultaneously crediting the design features of redundancy and diversity that (per industry consensus design standards and practices) provide reliable and robust performance.
			IV.C. Estimating Beta Factors	Intra-system beta-factors are often assigned a value of 1, even when the channels benefit from design, equipment or software diversity.
4.6.2	Modeling of dependencies	Intra-system software CCF. 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.	III.A.2. Mitigating Systems	It is important that the PRA capture the dependencies and potential CCF contributions while simultaneously crediting the design features of redundancy and diversity that (per industry consensus design standards and practices) provide reliable and robust performance.
			III.B. Level of Detail of PRA Model for Mitigating System Digital I&C	The functional effects of the software failure can be represented at the component, train or system level.
			IV.A.2. Operating Systems, Crediting Defensive Measures	In lieu of operating experience for the specific I&C platform, a conservative CCF probability for the OS may be determined from subjective judgment based upon consideration of its design features.

<p>IV.A.2. Operating Systems, Crediting Defensive Measures</p>	<p>Examples of factors to consider when estimating OS CCF probabilities include the following:</p> <ul style="list-style-type: none"> ▪Rigorous development and modification processes. ▪Focus on safety, avoidance of non required components and capabilities. ▪No generic susceptibilities (e.g., no management of time and date). ▪Deterministic behavior. ▪Static Memory Allocation ▪Invariability of software during operation ▪Validation of inputs prior to further processing. ▪No process driven interrupts ▪Cyclic functioning. ▪Asynchronous Operation (e.g., redundant channels not tied to a common clock or time) ▪Single-tasking. ▪Non- software watchdogs (failure of the digital system or channel to periodically reset a watchdog results in a specified safe action within a specified time frame). ▪Surveillance of short and long term memory. Defensive programming. ▪Rigorous operational procedures for operator requests (one channel at a time, only when absolutely necessary). ▪“Dissociation” of Operating System from Application Software. ▪Constant bus loading ▪Transparency of Operating System to plant transients. ▪Further decomposition of Operating System into dissociated modules
<p>IV.C. Estimating Beta Factors</p>	<p>Intra-system beta-factors are often assigned a value of 1, even when the channels benefit from design, equipment or software diversity.</p>

			IV.C. Estimating Beta Factors	For different platforms implementing different functions, the likelihood of CCFs may be considered negligible.
4.6.3	Modeling of dependencies	Inter-system hardware CCF. Hardware CCF between different systems using the same hardware should be modeled.	III.A.2. Mitigating Systems	It is important that the PRA capture the dependencies and potential CCF contributions while simultaneously crediting the design features of redundancy and diversity that (per industry consensus design standards and practices) provide reliable and robust performance.
			III.A.3. Supporting Control Systems	The consequence of failure is easily modeled as a failure mode of the final controlled device(s). However, like the protection system and other mitigating control systems, these separate control functions may share common hardware, software, or support systems and the dependencies should be resolved in the PRA.
			IV.C. Estimating Beta Factors	With appropriate defensive measures, most types of functional specification faults are either very unlikely or unlikely to be causally related in diverse functional specifications in a manner that would cause digital CCFs. There is a reasonable assurance that the likelihood of inter-system digital CCF is at least an order of magnitude less than the digital failure probability.

4.6.4	Modeling of dependencies	Inter-system software CCF. Use of similar support software in different digital systems should be modeled as CCF, and a complete dependence should be assumed for software failures.	III.A.2. Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems. The protection system performs the functions of reactor trip and actuation of engineered safety features, and should be a primary I&C focus for the PRA.
			III.A.3. Supporting Control Systems	The consequence of failure is easily modeled as a failure mode of the final controlled device(s). However, like the protection system and other mitigating control systems, these separate control functions may share common hardware, software, or support systems and the dependencies should be resolved in the PRA.
			III.B. Level of Detail of PRA Model for Mitigating System Digital I&C	The functional effects of the software failure can be represented at the component, train or system level.
			III.B. Level of Detail of PRA Model for Mitigating System Digital I&C	The CCF probabilities will consider the case of hardware that shares common software, whether it be common operating system (OS) or application software.

--	--	--

<p>IV.A.2. Operating Systems, Crediting Defensive Measures</p>	<p>Examples of factors to consider when estimating OS CCF probabilities include the following:</p> <ul style="list-style-type: none"> ▪Rigorous development and modification processes. ▪Focus on safety, avoidance of non required components and capabilities. ▪No generic susceptibilities (e.g., no management of time and date). ▪Deterministic behavior. ▪Static Memory Allocation ▪Invariability of software during operation ▪Validation of inputs prior to further processing. ▪No process driven interrupts ▪Cyclic functioning. ▪Asynchronous Operation (e.g., redundant channels not tied to a common clock or time) ▪Single-tasking. ▪Non- software watchdogs (failure of the digital system or channel to periodically reset a watchdog results in a specified safe action within a specified time frame). ▪Surveillance of short and long term memory. Defensive programming. ▪Rigorous operational procedures for operator requests (one channel at a time, only when absolutely necessary). ▪“Dissociation” of Operating System from Application Software. ▪Constant bus loading ▪Transparency of Operating System to plant transients. ▪Further decomposition of Operating System into dissociated modules
--	--

			<p>IV.A.2. Operating Systems, Crediting Defensive Measures</p>	<p>In lieu of operating experience for the specific I&C platform, a conservative CCF probability for the OS may be determined from subjective judgment based upon consideration of its design features.</p>
			<p>IV.C. Estimating Beta Factors</p>	<p>With appropriate defensive measures, most types of functional specification faults are either very unlikely or unlikely to be causally related in diverse functional specifications in a manner that would cause digital CCFs. There is a reasonable assurance that the likelihood of inter-system digital CCF is at least an order of magnitude less than the digital failure probability.</p>
5.1.1	<p>Probabilistic data (w/component-specific data available)</p>	<p>The data should be obtained from the operating experience of the same component as that being evaluated, and preferably in the same or similar application and operating environment.</p>	<p>IV.A.1. Operating Systems, Crediting Operating Experience</p>	<p>The manufacturer is a good source of failure data for the digital system components and embedded operating. However, care must be taken in applying failure data derived from operating experience.</p>
			<p>IV.B.2. Applications Software, Crediting Defensive Measures.</p>	<p>A number of regulatory agencies have accepted the use of a failure probability of 10⁻⁴ for digital equipment qualified for use in safety applications. This should be applicable in estimating the probability of digital failure of channels that use pre-qualified platforms with applications and configurations developed following current industry and regulatory guidance.</p>

			IV.B. Application Software	The quality of the software development and its life cycle is equally important. Therefore, the failure data from digital software in standard applications have no relevance to SR I&C systems.
5.1.5	Probabilistic data (w/generic data)	It should be verified that the generic data were collected from components that were designed for applications similar to those in nuclear power plants.	IV.A.1. Operating Systems, Crediting Operating Experience	Unlike the application software, which may be one of a kind, the OS will usually have some applicable operating history. If there is operating history in similar SR applications for the computer processor hardware, then it probably includes the OS.
			IV.B.1. Application Software, Operational Experience from Other Industries	Unlike operating systems, unique applications may not have as great amount of operating history on which to draw. Therefore, if operating experience is to be used, it may be necessary to consider that from other industries. Statistical evidence on the operational experience of comparable digital systems is a factor that may provide indication of bounding or practical estimates of digital failure probabilities for use in risk-informed evaluations.
5.1.8	Probabilistic data (component specific and generic)	Data for common cause failures should also meet the above criteria.	IV. Software Failure Probabilities for PRA	Good industry design practice includes features in SR digital I&C systems to minimize the impact of CCF. Values and methods used to estimate the software failure probability need to account for these defensive measures that are implemented in the design.

			<p>IV.A.2. Operating Systems, Crediting Defensive Measures</p> <p>In lieu of operating experience for the specific I&C platform, a conservative CCF probability for the OS may be determined from subjective judgment based upon consideration of its design features.</p>
			<p>IV.A.2. Operating Systems, Crediting Defensive Measures</p> <p>Examples of factors to consider when estimating OS CCF probabilities include the following:</p> <ul style="list-style-type: none"> ▪Rigorous development and modification processes. ▪Focus on safety, avoidance of non required components and capabilities. ▪No generic susceptibilities (e.g., no management of time and date). ▪Deterministic behavior. ▪Static Memory Allocation ▪Invariability of software during operation ▪Validation of inputs prior to further processing. ▪No process driven interrupts ▪Cyclic functioning. ▪Asynchronous Operation (e.g., redundant channels not tied to a common clock or time) ▪Single-tasking. ▪Non- software watchdogs (failure of the digital system or channel to periodically reset a watchdog results in a specified safe action within a specified time frame). ▪Surveillance of short and long term memory. Defensive programming. ▪Rigorous operational procedures for operator requests (one channel at a time, only when absolutely necessary). ▪“Dissociation” of Operating System from Application Software. ▪Constant bus loading ▪Transparency of Operating System to plant transients. ▪Further decomposition of Operating System into dissociated modules

5.1.9	Probabilistic data (component specific and generic)	Data for "fault coverage" should also meet the above criteria.	III.B.2. Other Hardware Aspects of Digital I&C Systems	“Coverage” is an important concept, as it determines the percentage of failures that are self-monitored (i.e., self-revealing) versus non-self-monitored (or test-revealed). This failure mode breakdown will vary between I&C designs and between different types of digital components. It has an important role in the PRA analysis, as it drives which mathematical unavailability model (repair-time model, test-interval model, or both) is used for each component.
5.2.1	Probabilistic data (for software)	A method for quantifying the contribution of software failures to digital system unreliability should be used and documented.	IV. Software Failure Probabilities for PRA	For the purposes of determining the sensitivity of plant risk to digital I&C reliability and driving corresponding design decisions, the industry approach is to portray the probability of software failure as a random event. This is consistent with the National Academy of Sciences findings.
			IV. Software Failure Probabilities for PRA	Good industry design practice includes features in SR digital I&C systems to minimize the impact of CCF. Values and methods used to estimate the software failure probability need to account for these defensive measures that are implemented in the design.
6.3	Uncertainty	Key assumptions of the model should be identified, and a discussion of the associated model uncertainty provided, including the effects of alternative assumptions.	V. Sensitivity of PRA to Digital I&C	A recommendation of the National Academy of Sciences report is the performance of sensitivity analyses to help the analyst assure that the results are not unduly dependent on parameters that are uncertain. Sensitivity analyses have been performed by the reactor vendors as well as EPRI in the assessment of the risk associated with digital systems.

7.1	Integration of the digital system model with a PRA model	For full effectiveness of the digital system reliability model, it should be possible to integrate it into the plant PRA model; the process for integration should be verifiable.	I. Introduction and Purpose	The purpose of this white paper is to describe a method for incorporating digital instrumentation and control (I&C) system models in nuclear power plant (NPP) probabilistic risk assessments (PRA).
			II. Current Industry Practice and the Resulting Sensitivity of PRA to Digital I&C	In selecting methods for modeling of digital I&C in PRA, it is important to recognize the context of the digital I&C with respect to the functions it provides in the overall plant design, not only including the quality of the software and hardware but considering the effect of these defense-in-depth and diversity related design practices as well.
7.2	Integration of the digital system model with a PRA model	If a model of a digital system has been integrated with a PRA model, all the dependencies related to the system should be properly accounted for. They are the dependencies of the digital system on other systems (such as its support systems), and of other systems on the digital system.	III.A.1. Normal Plant control systems	The normal plant control systems are generally pre-initiating event functions and are not of much interest to the PRA post-trip. A few normal plant controls (such as for MFW) may be given limited post-trip credit in some PRAs; however this credit is rarely extensive, and never solely relied upon. A minimum amount of fault tree modeling of initiating events may be necessary to capture dependencies (e.g., shared components or support systems), and the purpose of these models is to ensure that credit is not given post-trip for a system or component that was involved in the initiating event.

7.2	Integration of the digital system model with a PRA model	If a model of a digital system has been integrated with a PRA model, all the dependencies related to the system should be properly accounted for. They are the dependencies of the digital system on other systems (such as its support systems), and of other systems on the digital system.	III.A.2 Mitigating Systems	Dependencies between these mitigating systems considered in the PRA include not only shared equipment but, where digital systems are used, common software between redundant systems. The protection system performs the functions of reactor trip and actuation of engineered safety features, and should be a primary I&C focus for the PRA.
			III.A.3 Supporting Control Systems	The consequence of failure is easily modeled as a failure mode of the final controlled device(s). However, like the protection system and other mitigating control systems, these separate control functions may share common hardware, software, or support systems and the dependencies should be resolved in the PRA.
			III.B.1. Physical and Functional Considerations	The chosen level of detail needs to address the effects of the functional or other diversity not only within the I&C but the plant systems in which the I&C resides.
8.1	Human errors	Human errors during upgrade of hardware and software should be modeled.	III.A.4. MCR Instrumentation Systems	Main control room (MCR) instrumentation systems are typically not modeled explicitly in the PRA. This includes implicit modeling of instrumentation dependencies in the HRA if there are dependencies upon the initiating event. The diversity and redundancy of instrumentation is usually sufficient that its failure is an insignificant contributor to the HRA, and its reliability can be included in the HRA, if this is not the case.

<p>8.2</p>	<p>Human errors</p>	<p>Human errors due to poor design of HSI should be modeled.</p>	<p>III.A.4. MCR Instrumentation Systems</p>	<p>Main control room (MCR) instrumentation systems are typically not modeled explicitly in the PRA. This includes implicit modeling of instrumentation dependencies in the HRA if there are dependencies upon the initiating event. The diversity and redundancy of instrumentation is usually sufficient that its failure is an insignificant contributor to the HRA, and its reliability can be included in the HRA, if this is not the case.</p>
<p>9.3</p>	<p>Documentation and results</p>	<p>The dominant failure modes of the reliability model should be documented with a description of the sequence of events that need to take place and how the failures propagate to fail the system. The sequence of events should realistically represent the system's behavior at the level of detail in the model.</p>	<p>V. Sensitivity of PRA to Digital I&C</p>	<p>Vary the probability of failure of the digital systems to determine</p> <ul style="list-style-type: none"> o What combinations of digital failure probability for a division of I&C and common cause failure would result in the PRA approaching the Safety Goals. o What initiating events (and possibly the specific accident sequence characteristics) dominate the change in risk. o Where Safety Goals are not approached, a deterministic rationale for why risk remains low even in the presence of bounding digital failure probabilities is developed. o Where Safety Goals are approached, then the reliability of the digital system itself plays an important role in managing safety. A deterministic basis for concluding that the failure probability of the digital system is relatively low is needed.

In comparing the content of the draft NUREG and the industry's white paper, it was noted that many of the criteria from the NUREG were not explicitly discussed in the white paper, as the white paper concentrated on issues unique to DI&C rather than general PRA issues. Thus, many aspects of standard PRA practice, such as modeling support system dependencies, performing uncertainty analysis, and documenting assumptions, were not discussed in the industry's white paper. The industry is considering referencing the ASME PRA standard in future papers on the topic to reinforce the expectation that PRA quality requirements from the standard should be met. The industry believes that, if the ASME PRA standard were referenced, the following criteria from the NUREG would be addressed by the industry white paper:

5.1.3	Probabilistic data (w/component-specific data available)	The method used in estimating the parameters should be documented, so that the results can be reproduced.
5.1.6	Probabilistic data (w/generic data)	The sources of the generic database should be given.
5.1.7	Probabilistic data (component specific and generic)	If the system being modeled is subject to an adverse environment and the data are obtained from systems that are not subject to a similarly adverse environment, then the data should be modified to account for the corresponding impact of the specific environment on the reliability of the system components.
5.1.10	Probabilistic data (component specific and generic)	Documentation of basic event calculations should include how the basic event probabilities are calculated in terms of failure rates, mission times, and test and maintenance frequencies.
6.1	Uncertainty	Uncertainties associated with the probabilistic data for hardware and software should be estimated.
6.2	Uncertainty	Data uncertainty throughout the PRA model should be propagated such that the uncertainty characteristics of risk measures, such as CDF, can be determined.
9.1	Documentation and results	Key assumptions made in developing the reliability model and probabilistic data should be documented.

9.2	Documentation and results	Assumptions made in developing the reliability model and probabilistic data should be realistic, and the associated technical justifications should be sound and documented.
-----	---------------------------	--