الهيئة الإتحادية للرقابة النووية
FEDERAL AUTHORITY FOR NUCLEAR REGULATION

Regulatory Guide

Probabilistic Risk Assessment:
Scope, Quality and Applications
FANR-RG-003

Version 0

Table of Contents

Basic Principle of Regulatory Guides

Regulatory Guides are issued to describe methods and/or criteria acceptable to the Authority for meeting and implementing specific requirements in the Authority's regulations. Regulatory Guides are not substitutes for regulations, and compliance with them is not required. Methods of complying with the requirements in regulations different from the guidance set forth by the Regulatory Guide can be acceptable if the alternatives provide assurance that the requirements are met.

Definitions

Article (1)

For purposes of this regulatory guide, the following terms shall have the meanings set forth below.

Basic Event (BE)	An event in a fault tree model that requires no further development because the appropriate limit of resolution has been reached. This event typically represents the failure likelihood (unreliability or unavailability) of a System, Structure or Component (SSC) function or human action.
Core Damage Frequency (CDF)	The likelihood of Accidents that would cause damage to a reactor core; the sum of the frequencies of those Accidents that result in uncovery and heat-up of the reactor core to the point at which prolonged oxidation and severe fuel damage are anticipated and involving enough of the core, resulting into fission products release from the fuel that if released to the environment would result in offsite public health effects.
Country-of-Origin (CoO)	The country whose regulatory body approved the nuclear power plant Design being proposed for the State.
Cutset (CS)	A representation of the combination of Basic Events that can lead to a fault trees top event. The fault tree top event can represent a subsystem, system, plant function or an overall risk metric.
Defence-in-Depth	A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of Anticipated Operational Occurrences and to maintain the effectiveness of physical barriers placed between a Radiation Source or Radioactive Material and workers, members of the public or the environment, in Operational States and, for some barriers, in Accident Conditions

Fault Tree A deductive logic diagram that depicts how a particular undesired event can occur as a logical combination of other undesired events.

Functional Event Sequence (FS) A group of similar Accident sequences into an event class. Similar Accident sequences are those that have similar initiating events and display similar Accident behaviour in terms of system failures and/or phenomena and lead to similar end states. Similar Accident sequences are likely to have the same systems, structures and components credited for Accident prevention and/or mitigation.

Fussell-Vesely (FV) Importance Measure For a specified Basic Event, Fussell-Vesely importance is the fractional contribution to the total of a selected figure of merit for all Accident sequences containing that Basic Event. For PRA quantification methods that include non-minimal Cutsets and success probabilities, the Fussell-Vesely importance measure is calculated by determining the fractional reduction in the total figure of merit brought about by setting the probability of the Basic Event to zero.

Items Important to Safety An item that is part of a Safety Group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public, including:

- Those SSCs whose malfunction or failure could lead to undue radiation exposure of site personnel or members of the public;
- Those SSCs that prevent anticipated operational occurrences from leading to Accident Conditions;
- Those features that are provided to mitigate the consequences of malfunction or failure of SSCs.

Large Release Frequency (LRF) The sum of the frequencies of those Accidents leading to unmitigated release of airborne fission products from the Containment to the environment such that there is the potential for health effects (such Accidents generally include releases associated with Containment failure, Containment bypass events, or loss of Containment isolation).

PRA Peer Review An examination or review of commercial, professional or academic efficiency, competence, etc., by others in the same occupation.

Probabilistic Risk Assessment (PRA)	PRA is a comprehensive, structured approach to identifying failure scenarios constituting a conceptual and mathematical tool for deriving numerical estimates of risk. Level 1 comprises the assessment of failures leading to the determination of the frequency of core damage. Level 2 constitutes the assessment of Containment response and leads to the determination of frequency of Containment failure resulting in release to the environment of a given percentage of the reactor core's inventory of radionuclides.
Risk Achievement Worth (RAW) Importance Measure	For a specified Basic Event, Risk Achievement Worth importance reflects the increase in a selected figure of merit when an SSC is assumed to be unable to perform its function due to testing, Maintenance, or failure. It is the ratio or interval of the figure of merit, evaluated with the SSC's Basic Event probability set to one, to the base case figure of merit.
Safety Significance / Safety Significant	Any System, Structure, Component or human action whose failure can cause a change in PRA results that exceed predefined risk criteria.
Severe Accident Mitigation	Termination of or reduction in consequences of core melt Accidents.
Severe Accident Prevention	Prevention of reactor core from melt. Correction measures to any imbalance and disorder that may lead to melt the nuclear reactor core".

Background

Article (2)

1. As stated by the International Atomic Energy Agency (IAEA) in its "General Safety Requirements on Safety Assessment for Facilities and Activities", IAEA Safety Standard Series No. GSR, Part 4 (2009): "the objectives of a probabilistic Safety Assessment (PSA)", (henceforth referred to as a Probabilistic Risk Assessment (PRA)) "are to determine all significant contributing factors to the radiation risks arising from a Facility or Activity, and to evaluate the extent to which the overall Design is well balanced and meets probabilistic Safety criteria where these have been defined. In the area of reactor Safety, probabilistic Safety analysis uses a comprehensive, structured approach to identify failure scenarios. It

constitutes a conceptual and mathematical tool for deriving numerical estimates of risk. The probabilistic approach uses realistic assumptions whenever possible and provides a framework for addressing many of the uncertainties explicitly. Probabilistic approaches may provide insights into systems performance, reliability, interactions and weaknesses in the Design, the application of Defence-in-Depth, and risks, that it may not be possible to derive from a deterministic analysis."

2. Accordingly, Nuclear Facility Operators have performed PRAs to identify and understand key plant vulnerabilities. As a result of the availability of these PRA studies, there is a desire to use them to enhance plant Safety and security, and to operate the Nuclear Facilities in the most efficient manner. PRA is an effective tool for this purpose as it assists the applicant/Licensee to target resources where the largest benefit to plant Safety can be obtained. However, any PRA which is to be used in this way must have a credible and defensible basis. Thus, it is very important to have a high quality PRA. Since an application to construct and operate a Nuclear Facility in the State is based upon a Design approved by a regulatory body in another country (i.e., Country-of-Origin: CoO), this guide is intended to be compatible with the PRA associated with that Design. Specifically, if this guide is being applied to a PRA with regulatory approval in its CoO, then credit can be taken for what was done in the CoO, provided the PRA methods and quality are in conformance with nationally or internationally recognised standards.

Objective

Article (3)

The objective of this guide is to provide guidance for implementation of the requirements in FANR-REG-05, Regulation for the Application of PRA at Nuclear Facilities, Ref (1).

Scope

Article (4)

This guide applies to the conduct of a PRA for application to Nuclear Facility Siting, Design, Construction and Operation. It addresses PRA scope, quality, application, Maintenance and documentation. This guide is written for application to a light water Nuclear reactor.

PRA Scope and Quality

Article (5)

The PRA should be of high quality and represent the Design and site specific features of the Facility. Seven key PRA attributes associated with high quality are identified below and are addressed in this guide.

1. **Scope:** The scope of the PRA should include all initiating events that challenge the Facility and address all the Systems, Structures, Components, human actions and modes of Operation that can affect the Safety of the Facility. Therefore, the PRA should include all internal and external initiating events and hazards and address all the modes of Operation of the Facility, including low power and shutdown conditions. The PRA should include Level 1 (Core Damage Frequency) and Level 2 (Large Release Frequency) analysis.

2. **Level of detail:** The PRA level of detail should be sufficient to model the SSCs and human actions that affect CDF, LRF and the form, content, quantity of radionuclides and the time they are released to the environment.

3. **Technical quality:** The methods used in the analysis should be consistent with the state of the art and current best practices as documented in nationally or internationally recognised PRA standards and guidance.

4. **Programme quality:** The PRA should be based on a structured and traceable process in which all details of the PRA, including Design information, data, explicit and implicit assumptions, models, and modelling techniques, etc. are fully checked and documented.

5. **Uncertainty:** The analyses and interpretation of results and insights should include appropriate consideration of uncertainty. This includes quantitative and qualitative considerations, including the use of sensitivity studies. Such consideration should include uncertainties associated with parameters and analytical models used in the PRA and identification of areas or phenomena not modelled in the PRA.

6. **PRA Peer Review:** The PRA should be peer reviewed by qualified personnel according to an established process that compares the PRA against a set of desired characteristics and attributes, documents the results and identifies both strengths and weaknesses of the PRA.

7. **PRA maintenance:** The PRA should be updated on a regular basis or when significant changes occur in plant Operation, Maintenance or Design, or there is an improved understanding of thermal-hydraulic or Accident phenomenology, new information or advances in analytical techniques that could significantly impact PRA results. PRA Maintenance should include a monitoring and feedback programme on key SSC and human performance to reflect operating experience.

PRA Applications

Article (6)

The PRA should be used as much as practical to support the Design, Construction and Operation of the Facility. This support should be directed toward optimising and confirming the Safety of the Facility in the areas where PRA can model and assess the performance of SSCs and humans. As a minimum, the areas that should be supported by the PRA and discussed in the application are those listed in Table 1.

Table 1 - PRA Applications

Application Category	Specific Application
Design	• Assess the Safety Significance of new information, issues and changes to the Country of Origin approved Facility Design. • Complement the selection of Safety Significant SSCs. • Complement the treatment of Severe Accidents. • Complement the identification of SSC EQ needs and methods, based upon their Safety Significance and service conditions. • Complement the application of quality assurance for SSCs based upon their Safety Significance. • Establish performance goals for Safety Significant SSCs that are to be monitored over the life of the Facility. • Demonstrate how the Facility risk compares with the Authority’s probabilistic Safety targets, including conformation that no single SSCs or human action contributes disproportionately to risk.
Construction	• Prioritise Construction Inspection and testing activities. • Assess the Safety Significance of Construction errors.
Start-up/ Operation	• Confirm that Emergency and Accident management procedures address the most Safety Significant event sequences and Licensee actions. • Confirm that the Licensee training programme addresses the most Safety Significant event sequences and Operator actions. • Confirm that the technical specifications address the most Safety Significant SSC, plant configurations and consider risk implication in setting allowable outage times and surveillance intervals. • Inform the configuration control programme regarding the Safety Significance of plant configurations.

	• Confirm that ageing management focuses on the most Safety Significant SSCs. • Confirm that Maintenance, surveillance, in-service Inspection and in-service testing programmes focus on the most Safety Significant SSCs. • Evaluate the Safety Significance of operating events, plant modifications, Inspection findings, and new Safety issues.
Safety and Security Interfaces	• Assess the impact of Physical Protection measures/changes on plant Safety. • Assess the impact of Design or operational changes or Maintenance outages on Physical Protection.

Reliance on Country-of-Origin PRA

Article (7)

1. In the event the Design proposed for the State has an existing PRA, the CoO PRA may be used provided it can be shown that the CoO PRA meets Authority requirements or deviations are adequately justified. Specifically, where the CoO PRA is to be relied upon, the following should be demonstrated:

   a) the PRA scope, level of detail and quality is consistent with the Authority's requirements (e.g., conducted in accordance with nationally or internationally recognised standards); and

   b) confirmation that no Design or operational changes have been made from what was modelled in the CoO PRA.

2. Where the CoO PRA does not reflect State unique conditions or Design or site specific features, the CoO PRA should be modified, consistent with Authority requirements, to reflect the Design and site specific conditions. This can be done in a phased fashion as discussed in Article (10).

PRA Scope

Risk Characterization

Article (8)

1. The Level 1 and Level 2 PRA should consist of the major technical elements shown in Table 2.

Table 2 - Technical Elements of the PRA

Analysis	Technical Benefits	
Level 1	• Initiating event analysis • Success criteria analysis • Accident sequence analysis • System analysis	• Parameter estimation analysis • Human reliability analysis • Quantification
Level 2	• Plant damage state analysis • Accident progression analysis	• Quantification • Source term analysis

2. The technical elements should encompass the following:

   c) **Initiating event analysis** should identify and characterise the events that both challenge normal plant Operation during power or shutdown conditions and require successful mitigation by Facility equipment and personnel to prevent core damage from occurring. Events that have occurred at the Facility and those that have a reasonable probability of occurring should be identified and characterised. Grouping of the events, with the groups defined by similarity of system and Facility responses (based on the success criteria), may be performed to manage the large number of potential events that challenge the Facility.

   d) **Success criteria analysis** which determine the minimum requirements for each function (and ultimately the systems used to perform the functions) to prevent core damage (or to mitigate a release) given an initiating event. The requirements defining the success criteria should be based on acceptable engineering analyses that represent the Design and Operation of the Facility.

   e) **Accident sequence analysis** which model chronologically (to the extent practical), the different possible progressions of events (i.e., Accident sequences) that can occur from the start of the initiating event to either successful mitigation or core damage release. The Accident sequences should account for the systems that are used (and available) and Operator actions performed to mitigate the initiator based on the defined success criteria and plant operating procedures (e.g., plant Emergency and abnormal operating procedures) and training.

f) **Systems analysis** which identify the various combinations of failures that can prevent the system from performing its function as defined by the success criteria. The model representing the various failure combinations includes, from an as-built and as-operated perspective, the system hardware and instrumentation (and their associated failure modes) and human failure events that would prevent the system from performing its defined function. The Basic Events representing equipment and human failures should be developed in sufficient detail in the model to account for dependencies among the various systems and to distinguish the specific equipment or human events that have a major impact on the system's ability to perform its function.

g) **Parameter estimation analysis** which quantify the frequencies of the initiating events, as well as the equipment failure probabilities and equipment unavailabilities of the modelled systems. The estimation process should include a mechanism for addressing uncertainties and have the ability to combine different sources of data in a coherent manner, including the actual operating history and experience of the Facility, as well as applicable generic experience.

h) **Human reliability analysis** which identify and provide probabilities for the human-induced failure events that can negatively impact normal or Emergency Operations. The human-induced failure events associated with normal Operation include the events that leave the system (as defined by the success criteria) in an unrevealed, unavailable state. The human-induced failure events associated with Emergency plant Operation represent those human actions that, if not performed, do not allow the needed system to function. Quantification of the probabilities of these human-induced failure events should be based on Facility and Accident specific conditions, where applicable, including any dependencies among actions and conditions.

i) **Quantification** which provides an estimation of the CDF and LRF given the Design and/or Operation of the plant (depending whether the Facility is in the Design or operating stage). Regardless of the stage, the CDF/LRF should be based on the summation of the estimated CDF/LRF from each Accident sequence for each initiator group. If truncation of Accident sequences and Cutsets are applied, truncation limits should be set so that the overall model results are not impacted in such a way that significant Accident sequences or contributors are eliminated. Therefore, the truncation value should be selected so that the required results are stable with respect to further reduction in the truncation value.

j) **Facility damage state analysis** which group similar core damage scenarios together to allow a practical assessment of the severe Accident progression and Containment response resulting from the full spectrum of core damage Accidents identified in the

Level 1 analysis. The Facility damage state analysis defines the attributes of the core damage scenarios that represent boundary conditions to the assessment of severe Accident progression and Containment response that ultimately affect the resulting radionuclide releases.

The dependencies between the Containment systems modelled in the Level 2 analysis with the core damage Accident sequence models should be modelled to fully account for mutual dependencies. Core damage scenarios with similar attributes should be grouped together to allow for efficient evaluation of the Level 2 response.

k) **Accident progression analysis** which models the different series of events that challenge Containment integrity for the core damage scenarios represented in the Facility damage states. The Accident progressions should account for interactions among severe Accident phenomena and system and human responses to identify credible Containment failure modes, including failure to isolate the Containment. The timing of major Accident events and the subsequent loadings produced on the Containment should be evaluated against the capacity of the Containment to withstand the potential challenges. The Containment performance during the severe Accident should be characterised by the timing (e.g., after vessel breach), size (e.g., catastrophic versus bypass), and location of any Containment failures.

l) **Source term analysis** which characterise the radiological release to the environment resulting from each Severe Accident sequence leading to Containment failure or bypass. The characterisation includes the time, elevation, and energy of the release and the amount, form, and amount of Radioactive Material that is released to the environment. The source term analysis should be sufficient to determine whether a large release occurs. A large release is one involving the unmitigated release of airborne fission products from the Containment to the environment such that there is the potential for early health effects.

Plant Challenges

Article (9)

The PRA should include internal and external events analysis. Internal events refer to Accidents resulting from internal causes in the Facility initiated by hardware failures or Operator actions, and internal fires and floods. External events refer to Accidents resulting from causes initiated outside of the Facility.

1. Internal Events

   a) **Internal Hardware Failures and Operator Actions**

      - The PRA models, system success criteria, and data should be developed for the analysis of internal events Accident initiators. Internal event initiators generally include items such as loss of power, pipe breaks, equipment malfunctions, etc. Loss of off-site power is generally considered an internal event, even though the cause may occur off-site. Internal hardware failures and Operator actions should be assessed for all modes of Operation.

b) **Internal Flood Analysis**

- An internal flood analysis generally utilises the models generated for internal initiators modified to include consideration of the type of flood initiator, the potential for flood propagation, and the impact of flooding environments on both the equipment located in the flooded areas and on the Operator actions. An internal flood analysis must include internal floods initiated during all modes of Facility Operation. Internal flooding initiators that can adversely affect sources of radioactivity other than the core should also be analysed. Internal flood analysis should include:

  - Identification of flood sources;

  - Identification of flood areas (i.e., flood area partitioning);

  - Identification of flood scenarios (e.g., propagation paths, mitigation measures, equipment failure mechanisms, etc.); and

  - Flood scenario quantification (e.g., success criteria, human actions, estimation of CDF/LRF, etc.)

c) **Internal Fire Analysis**

- An internal fire analysis generally utilises the PRA models generated for internal initiators modified to include consideration of the fire initiator, the potential for fire and smoke propagation, and the impact of fire on both the equipment located in the areas and on the Operator actions. Of specific concern is the impact of the fire on cables leading to the potential for spurious component Operation, loss of motive power, or loss of the ability to initiate a component. As is the case for other internal initiators, an internal fire analysis includes fires during all modes of Operation. Fire analysis should include:

  - identification of equipment and cables to be modelled;

  - identification of SSC failures that result from fires;

  - development of a logic model that represents the plant response to fires (e.g., equipment failures, circuit failures, etc.);

  - identification of fire scenarios (e.g., ignition sources, fire growth and propagation, detection suppression);

  - fire scenario quantification (e.g., success criteria, human actions, estimation of CDF/LRF); and

    - seismic / fire interaction-qualitative assessment.

- If an alternative approach to conducting a fire PRA is proposed (e.g., fire hazards analysis, screening analysis), then it must be demonstrated capable of identifying the most Safety Significant SSCs, human actions, fire scenarios and demonstrate the effectiveness of the fire protection measures. If a risk-informed, performance-based approach to fire protection is to be applied to an existing Design (e.g., CoO Design), the guidance contained in US NRC Regulatory Guide 1.205 (Reference 14) is acceptable for use.

2. External Events

   a) The potential for external events (e.g., earthquakes, high winds, hurricanes, aircraft impacts (other than those stemming from hostile acts), and external flooding) occurring at the Facility should be reviewed and those that are important included in the PRA. The external event PRA includes consideration of random failures and the impact of the external events on SSCs and on Operator actions. As is the case for internal initiators, external events are evaluated for all modes of Operation. External event analysis should include:

   - hazard analysis;

   - fragility analysis; and

   - Facility response analysis for seismic, high winds, Sandstorms, precipitation and any other relevant external events.

   b) If an alternative approach to conducting a full scope external events PRA is proposed (e.g., seismic margins analysis), then it must be demonstrated capable of identifying the most Safety Significant SSC and human actions.

3. Common cause failures

   Common cause failure should be considered in both internal events and external events analysis.

PRA Development - Phased Completion

Article (10)

1. The PRA should reflect the as-designed, as-sited, and as-operated Facility (Plant) to the degree possible consistent with the life-cycle phase of Facility (i.e., Design, Siting, Construction and Operation).

2. It is recognised that the level of detail and the scope of the PRA will increase as the plant progresses from the Design phase to Siting, Construction and Operation. It is also recognised that the PRA developed in the CoO may not reflect the State unique or site specific aspects of the Facility. In some areas, interfacing assumptions may have been

made (e.g., external events) and in other areas the PRA may not be complete at the time of the Construction license application (e.g., human reliability). Ultimately, to support Operations the PRA should be complete. However, the PRA may be completed in a phased fashion, consistent with the various stages of Design and Construction.

3. In completing the PRA in a phased fashion, the following must be considered:

   a) State Site specific conditions: At the Construction License stage it should be demonstrated that the PRA bounds the hazards of the proposed site. For seismic, this would include demonstration that the soil-structure interactions and the component and structure fragilities are applicable. If it can be demonstrated that the hazards are bounded by the PRA, then this would be sufficient for the Construction Licence. At the operating license stage, key interfaces (e.g., seismic) should be updated to reflect actual site conditions.

   b) Completeness of the PRA Model: At the Construction Licence stage, the completeness issue addresses the limitations of performing a PRA on a plant that is yet to be built. These limitations include:

      - Incomplete Elements or Sub-elements of the Design: areas of the Design not modelled or bounded using simplified assumptions should be identified.

      - Human Reliability: the lack of operating procedures and training details (these are two key inputs used in determining the human action failure rates). Without these inputs, the estimation of the human failures rates will contain much greater uncertainty.

      - Equipment Availability and Reliability: the unavailability and failure rates used for the PRA Basic Events (e.g., pump fails to start) may not reflect plant specific Maintenance practices (which will likely need to be developed) and may not reflect the ultimate equipment reliability due to differences in the environment and Maintenance practices.

   c) At the Construction Licence stage, the PRA should identify the limitations related to completeness. At the Operating Licence stage, as-designed and as-built information should be reviewed and walk-downs conducted as necessary to confirm that the assumptions used in the PRA remain valid with respect to factors such as external events, internal flooding and fire events (routings and locations of pipe, cable and conduit), and human reliability analyses (HRA) (i.e., development of operating procedures, Emergency operating procedures and Severe Accident Management guidelines and training).

   d) Quality: Ideally, a PRA Peer Review (see Articles 33 to 35) should be conducted at the Construction Licence stage. Such a review increases confidence in the quality of the analysis and can be used to support compliance with recognised PRA standards (see Article II). Without a PRA Peer Review, the Construction Licence submitted should emphasise the measures used to ensure quality, as described in Part 4 of this chapter. At the Operating Licence stage, a formal PRA Peer Review should be conducted.

PRA Technical Quality

Consensus Standards

Article (11)

1. One acceptable means of achieving acceptable technical quality is to use internationally recognised PRA standards that address PRA scope and quality for the applications listed in Table 1. USNRC Regulatory Guide 1.200 (Reference 8) recognises the standards listed below and provides guidance on their application.

2. Generally recognised PRA standards include:

   a) ASME/ANS RA-Sa-2009, "Standard for Level 1 / Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Applications," Addendum A to RA-S-2008, ASME, New York, NY, American Nuclear Society, LaGrange Park, Illinois, February 2009.

   b) Previous revisions and addenda:

      - ASME RA-S-2002, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," ASME, New York, NY, April 5, 2002.

      - ASME RA-Sa-2003, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," Addendum A to ASME RA-S-2002, ASME, New York, NY, December 5, 2003.

      - ASME RA-Sb-2005,"Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," Addendum B to ASME Ra-S-2002, ASME, New York, NY, December 30, 2005.

      - ASME-RA-Sc-2007,"Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," Addendum C to ASME RA-S-2002, ASME New York, NY, July 6, 2007.

      - ASME/ANS RA-S-2008,"Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," Revision 1 RA-S-2002, ASME, New York, NY, April 2008.

   c) NEI 00-02,"Probabilistic Risk Assessment Peer Review Process Guidance," Revision A3, Nuclear Energy Institute, Washington, DC, March 20, 2000.

d) Updates

- Nuclear Energy Institute, Letter from Anthony Pietrangelo, Director of Risk- and Performance-Based Regulation Nuclear Generation, Nuclear Energy Institute, to Mary Drouin, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC, "NEI 00-02, "Probabilistic Risk Assessment Peer Review Process Guidance," Revision 1, May 19, 2006.

- Nuclear Energy Institute, Letter from Biff Bradley, Manager of Risk Assessment, Nuclear Energy Institute, to Mary Drouin, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC, "Update of Appendix D to revision 1 of NEI 00-02, "Probabilistic Risk Assessment Peer Review Process Guidance," November 15, 2006.

- NEI 05-04, "Process for Performing Follow-On PRA Peer Reviews Using the ASME PRA Standard," Revision 2, Nuclear Energy Institute, Washington, DC, November 2008.

- NEI 07-12, "Fire Probabilistic Risk Assessment (FPRA) Peer Review Process Guidelines," Draft Version H, Revision 0, Nuclear Energy Institute, Washington, DC, November 2008.

- National Fire Protection Association Standard 805, "Performance-Based Standard for Fire Protection for Light-Water Reactor Electric Generating Plants," 2001 Edition, Quincy, MA.

3. Compliance with USNRC RG 1.200 is sufficient to meet the technical quality discussed in Chapter 4, Parts 1 and 6, of this Regulatory Guide. In addition, the IAEA has recently issued Safety standards on the development and application of level 1 and level 2 PRAs (references 9 and 10) which contain additional supplemental information related to PRA quality that may be useful.

Assumptions and Inputs

Article (12)

Models, assumptions and inputs used in the PRA should be realistic and defensible with their basis and application clearly documented. They should not be overly conservative or optimistic and expert judgment should only be used in those situations in which there is a lack of available information regarding the condition or response within the PRA, or a lack of analytical methods upon which to base a prediction of a condition or response. The models, assumptions and inputs also should not take credit for SSCs beyond rated or Design capabilities or heroic human actions that have a small probability of success. All models, assumptions and inputs should be traceable to a clearly identified source and consistent with the proposed Design.

Analytical Methods

Article (13)

The analytical methods used should be sufficiently detailed as to their purpose, basis, assumptions, input, references and units such that a person technically qualified in the subject can review and understand the analysis and verify the adequacy of the results without recourse to the originator. Where possible, analytical methods should be consistent with available codes and standards and checked for reasonableness and acceptability. Method-specific limitations and features that could impact the results should be identified.

Analytical Tools

Article (14)

PRA quantification software, thermal/hydraulic codes, structural codes, radionuclide transport codes, human reliability models, common cause models, etc. are typically used in the PRA quantification process. These models and codes should have sufficient capability to model the conditions of interest and provide results representative of the Facility. They need to be used only within their limits of applicability. As errors in such programmes may significantly impact the results, it is necessary that the development and application of the computer programmes, spreadsheets or other calculation methods exhibit a high level of reliability as ensured through a documented verification and validation process. In addition, users should demonstrate the appropriateness of the models or codes selected for a specific application and of the way in which these programmes are combined and used to produce the needed results.

Success Criteria

Article (15)

Success criteria are used to distinguish the path between success and failure for components, human actions, trains, systems, structures and sequences. In all cases, the success criteria should be fully defensible and biased such that issues of manufacturer or Construction variability, code limitations and other uncertainties are unlikely to result in a failure path being considered a success path.

PRA Programme Quality

General

Article (16)

The PRA should be based on a secure and traceable process in which all details of the PRA, including explicit and implicit assumptions, modelling techniques, etc. are fully checked and documented. The methods, resources, controls, procedures, and responsibilities affecting the quality of a PRA should be carried out in accordance with FANR-REG-01, Regulation for Management Systems for Nuclear Facilities, Ref (2).

Procedures

Article (17)

The programme should be based upon procedures, work instructions, and assessment (audit) and review specifications which are to be used in the development of the PRA. The technical instructions are detailed directives on how general or specific activities are to be performed. They delineate the explicit methods and processes to be used to ensure that the work performance and results will comply with requirements. The procedures for any part of the PRA programme should be issued prior to the commencement of any work on that part of the programme and should be subject to review and approval before issue.

Responsibilities

Article (18)

The functions, authority, responsibilities and accountabilities of units and individuals within the organisation for the implementation of the PRA programme should be documented. It should include the lines of reporting to higher management and communication with other organisational units. It also should include the interactions among the groups involved in the PRA and other groups, i.e., the review organisations.

Interfaces

Article (19)

The PRA programme should have defined interfaces between the constituent parts of the analysis. It should establish controls for source information used by the PRA and output information provided from the PRA to ensure transparency and version control.

Qualifications

Article (20)

The PRA programme should have defined requirements for staff training and special expertise required to achieve the appropriate quality for each PRA activity. It should include measures to provide for training and qualification of personnel performing PRA related activities to ensure suitable technical proficiency and quality is achieved and maintained.

Technical Reviews

Article (21)

The PRA programme should have defined processes for evaluating the PRA work in relation to completeness, consistency and accuracy. It should identify the reviews needed at the various levels and stages of the work performed.

Audits

Article (22)

The PRA programme should have defined frequency and types of quality audits in order to verify compliance with task instructions.

Software Quality

Article (23)

The PRA programme should have requirements for software Quality Assurance. Requirements should include the verification and validation of all computer codes. Computer codes that are purchased commercially should be verified and validated by the code developer. For software that is not commercially procured, verification, validation and Quality Assurance processes should be performed.

Non-Conforming Items

Article (24)

Systematic control should be maintained over the identification, documentation and disposition of non-conforming items. The handling of nonconforming work should be controlled in accordance with applicable procedures and working instructions. Once the cause of a deficiency is identified, corrective action should be taken.

PRA Documentation

Article (25)

The PRA analysis and calculations should be documented. This should include documentation of input data, assumptions, criteria and calculations, including exclusion criteria or screening analyses, performed. The models, data, assumptions and calculations should be documented in sufficient detail such that other PRA practitioners could reproduce the results. Articles (54) and (55) provide further discussion on documentation.

PRA Configuration Management

Article (26)

Controls should be established to assign and track the identification of the models, data and documentation including their revision. Logs and records should be maintained relating to the distribution, inventory, configuration control and status accounting for all received and deliverable items. All PRA inputs should be identified and identifiable. Provision should be made for informing the PRA programme of the latest changes in the PRA information. PRA updates should be subject to Quality Assurance that is equivalent to the one applied during the development phase.

Appropriate procedures should be put in place to ensure that Facility changes are reported to the PRA group. This includes changes such as permanent configuration changes, hardware changes, changes to the operating procedures, Maintenance procedures, etc. Other changes such as those resulting from review of operating data, advances in techniques, availability of new information, or experience feedback (e.g. real events not properly represented by the PRA) also need to be reported.

Uncertainties

General

Article (27)

The PRA should model uncertainties to the extent supported by available data. The PRA should model the effect of data uncertainties. However, uncertainties associated with success criteria and modelling are typically not quantified. Uncertainties associated with modelling issues are dealt with by making specific assumptions, adopting specific models or performing sensitivity analysis.

Approach

Article (28)

The three different types of uncertainties described below should be addressed.

1. **Parameter uncertainty.** Parameter uncertainty relates to the uncertainty in the data used in the computation of the input parameter values used to quantify the probabilities of the events in the PRA logic model. Examples of such parameters are initiating event frequencies, component failure rates and probabilities, and human error probabilities. These uncertainties can be characterised by probability distributions that relate to the analysts' degree of belief in the values of these parameters (which could be derived from simple statistical models or from more sophisticated models).

2. **Model uncertainty.** Model uncertainty arises because different approaches may exist to represent certain aspects of Facility response and none is clearly more correct than another. An example would be the model used to estimate the leakage from a reactor coolant pump seal. Uncertainty with regard to the PRA result is then introduced because uncertainty exists with regard to which model appropriately represents that aspect of the Facility being modelled. In addition, a model may not be available to represent a particular aspect of the Facility. Uncertainty with regard to the PRA results is again introduced because there is uncertainty with regard to a potentially significant contributor not being considered in the PRA.

3. **Completeness uncertainty.** Completeness uncertainty relates to failure modes, phenomena or other risk contributors that are not in the PRA model. These types of uncertainties either are ones that are known but not included in the PRA model or ones that are not known and, therefore, not in the PRA model.

Parameter Uncertainty

Article (29)

Parameter uncertainty should be addressed by propagating the parameter uncertainty using a Monte Carlo method, or similar means, through the PRA model. The estimate of parameter uncertainty should include the following steps:

1. **Uncertainty.** Determine the parameter uncertainty for each Basic Event using actual data, such as failure rates, or expert elicitation.

2. **Identify and group correlated events.** Identify and group correlated events to address the dependency of parameters that are based on the same state of knowledge. For example, for all components of a certain type, if their failure rate is evaluated from the same data set, the Basic Events for these components are correlated. If the failure rates for subgroups are determined using different data sets, the Basic Events for these components are correlated within the subgroups, but not across the subgroups.

3. **Propagate parameter uncertainty.** The uncertainty should be evaluated using Monte Carlo or Latin Hypercube Sampling methods. The number of samples used should be such that the sampling distribution obtained converges to the true distribution of the risk metric.

Model Uncertainty

Article (30)

Model uncertainty should be addressed using the following steps:

1. **Identification of sources of model uncertainties and related assumptions of the base PRA.** Both generic and Facility specific sources of model uncertainty and related assumptions of the base PRA should be identified and characterised.

2. **Identification of sources of model uncertainties and related assumptions relevant to the application.** Identify the sources of model uncertainty and related assumptions that are relevant to the application. This identification may be performed with a qualitative analysis. This analysis should be based on an understanding of how the PRA is used to support the application and the associated acceptance criteria or guidelines. In addition, new sources of model uncertainty and related assumptions may be introduced by the application.

3. **Screening for key sources of model uncertainties and related assumptions for the application.** The sources of model uncertainty and related assumptions that are key to the

application are identified. Qualitative analyses of the importance of the sources of model uncertainty and related assumptions identified in the previous steps are performed in the context of the acceptance guidelines for the application. The analyses are used to identify any reasonable alternative modelling hypotheses that could impact the decision. These hypotheses are used to identify which of the sources of model uncertainty and related assumptions are key.

Completeness Uncertainty

Article (31)

1. Uncertainties not included in the PRA models could have a significant impact on the predictions of the PRA. Examples of sources of these types of incompleteness include the following:

    a) The scope of the PRA does not include some classes of initiating events, hazards, or models of Operation.

    b) The analysis may have omitted phenomena, failure mechanisms, or other items, because their relative contribution is believed to be negligible.

    c) State-of-the-art PRA techniques do not exist to model certain phenomena and effects (e.g., organisation influences).

2. When a PRA is used to support an application, its scope and level of detail needs to be examined to determine if they match what is required for the risk-informed application. If the scope or level of detail of the existing base PRA is incomplete, then either the PRA is updated to include the missing piece(s), or it is demonstrated using conservative or bounding-type analyses that the mission elements are not significant risk contributors or the fact that the analysis does not consider certain factors is identified so that the decision-makers are aware of the limitations of the analysis.

Output

Article (32)

In developing an approach to take into account uncertainties, it has to be decided how the numerical results are to be compared with acceptance guidelines, i.e., whether to use the mean value of the probability distribution on the numerical result to compare with a guideline, or whether to compare some percentile of that distribution. Therefore, the PRA needs to discuss the treatment of uncertainties and present data consistent with decision criteria to be used. Furthermore, since not all the uncertainties are represented in the probability distribution, the PRA needs to identify what uncertainties are not quantified.

Peer Review

General

Article (33)

1. The PRA should be peer reviewed by qualified personnel according to an established process that compares the PRA against a set of desired characteristics and attributes, based on Articles (8) through (32) of this guide, documents the results and identifies both strengths and weaknesses of the PRA. In addition to reviewing the methods used in the PRA, the PRA Peer Review determines whether the application of those methods was done correctly. The PRA models are compared against the plant Design and procedures to validate that they reflect current Facility Design and operational information. Key assumptions are reviewed to determine if they are appropriate and to assess their impact on the PRA results. The PRA results are checked for fidelity with the model structure and for consistency with the results from PRA's for similar facilities based on the peer reviewer's knowledge. Finally, the PRA Peer Review examines the procedures or guidelines in place for updating the PRA to reflect changes in Facility Design, Operation, or experience.

2. Ideally, the PRA should be peer reviewed at the Construction Licence and Operating Licence stages. If a PRA Peer Review is not performed at the Construction Licence stage, a complete description of the process used to ensure quality (addressing the items in Part 4 of the chapter) needs to be provided. At the Operating Licence stage, a PRA Peer Review should be performed. Following the initial PRA Peer Review, if the PRA is upgraded (e.g., incorporation of new methodologies, changes in scope, expanded analysis capability such as new Accident sequences) a new PRA Peer Review should be performed. However, routine PRA Maintenance activities (e.g., updated equipment failure rate information) do not need a new PRA Peer Review.

Peer Reviewer Qualifications

Article (34)

Peer Reviewer qualifications determine the credibility and adequacy of the PRA Peer Review. To avoid any perception of a technical conflict of interest, the PRA Peer Reviewers should not have performed any actual work on the PRA. Each member of the PRA Peer Review team should have technical expertise in the PRA elements he or she reviews, including experience in the specific methods that are used to perform the PRA. This technical expertise includes experience in performing (not just reviewing) the work in the element assigned for review. Knowledge of the key features specific to the Facility Design and Operation is essential. Finally, each member of the Peer Review Team should be knowledgeable in the PRA Peer Review process, including the desired characteristics and attributes used to assess the adequacy of the PRA.

Peer Review Process

Article (35)

The PRA Peer Review process should include a documented procedure used to direct the team in evaluating the adequacy of a PRA. The PRA Peer Review process should be consistent with the standards listed in Article (11).

PRA Maintenance

Article (36)

1. The PRA should be updated on a regular basis or when significant changes occur in Facility Operation, Maintenance or Design or there is an improved understanding of thermal-hydraulic or Accident phenomenology, new information, or advances in analytical techniques that could significantly impact PRA results.

2. Accordingly, the impact of any modification (Design, procedures, operating practices, licensing bases, etc.) on the PRA should be assessed in order to check its continuing validity and to identify any need for updating.

3. The PRA should be updated as frequently as necessary to ensure that the model remains an accurate representation of the Safety of the Facility. Modifications that significantly impact the PRA results may require an immediate updating of the PRA. However, even if this type of modification does not arise for a longer period, it is still suggested that the updating process be performed every three years and the PRA formally amended at that time.

4. The same PRA quality programme used in the development of the initial PRA should continue in force for the updating process.

PRA Applications

General

Article (37)

As stated in Ref (1), the applicant/Licensee is expected to use the PRA to complement the Design, Construction and Operation of the Facility. The expected applications are shown in Table 1 and guidance with respect to each of these applications is provided in following Articles. Applications beyond those listed in Table 1 may be proposed along with their supporting basis.

Design Applications

Assessment of New Information, Safety Issues and Design Changes

Article (38)

PRA information can complement decision-making by providing a perspective on the significance of new information, Safety issues and proposed changes to the Design or Operation. Guidance for using PRA information in decision-making is contained in an INSAG report, “A Framework for Integrated Risk-Informed Decision-making Process” (Reference 3) Guidelines for using risk-information in this process are as follows:

1. The risk impact of the Safety issue, plant modification or item under consideration should be determined. The risk impact can generally be considered small if:

   a) A balanced Design is still maintained such that the item under consideration does not make a disproportionately large contribution to the overall risk, and defence in depth is maintained.

   b) The change in risk is small. Increases in risk less than one percent of the Authority’s probabilistic Safety targets for CDF, or LRF are considered small. Mean values should be sued in the assessment.

   c) The cumulative impact of changes in risk is considered and overall Facility probabilistic Safety targets are met.

   d) Uncertainties are considered in the analysis, described in the assessment and accounted for in the decision. Uncertainties could include the potential for new failure modes, phenomena or aging mechanisms with the potential for reduced Safety margins.

Classification of Safety Significant SSCs

Article (39)

1. The use of risk insights provide a broader perspective on the importance of the SSCs and can complement the deterministic SSC Safety classification based on risk. Accordingly, Article (11), item 2, of FANR-REG-03, “Regulation for the Design of Nuclear Power Plants”, Ref (4), requires that both deterministic and probabilistic methods be used for classifying the Safety Significant of SSCs.

2. The risk-informed Safety classification process endorsed by the United States Nuclear Regulatory Commission Regulatory in Guide 1.201, Ref (5), is an acceptable way to use PRA information to complement a deterministic Safety classification process. Application of this process will result in binning SSCs into one of four categories, called Risk-Informed

Safety Categories (RISC). In this process, the selection of Safety Significant SSCs starts with a deterministic selection process and then overlays a probabilistic process that modifies the deterministic Safety classification to reflect risk insights.

3. In the deterministic approach, SSCs are generally categorised as either “Safety-related” or “non-Safety-related” (U.S. NRC terminology) or "Items Important to safety" or "not Items Important to safety" (IAEA terminology) based upon their role in preventing and/or mitigating Design Basis Accidents. Figure 1 depicts a deterministic (important-to-Safety vs. not important-to-Safety) SSC categorisation scheme, as shown by the vertical line, with an overlay of a risk-informed (Safety-significance) categorisation derived from the PRA. Risk insights can be used to identify SSCs as being either “Safety Significant” or “low Safety Significance” as shown by the horizontal line in the figure. This results in SSCs being grouped into one of four categories, as represented by the four boxes in the figure. SSCs in RISC categories 1 and 3 are those selected via deterministic methods as important-to-Safety. SSCs in RISC categories 1 and 2 are those selected using risk insights as Safety Significant.

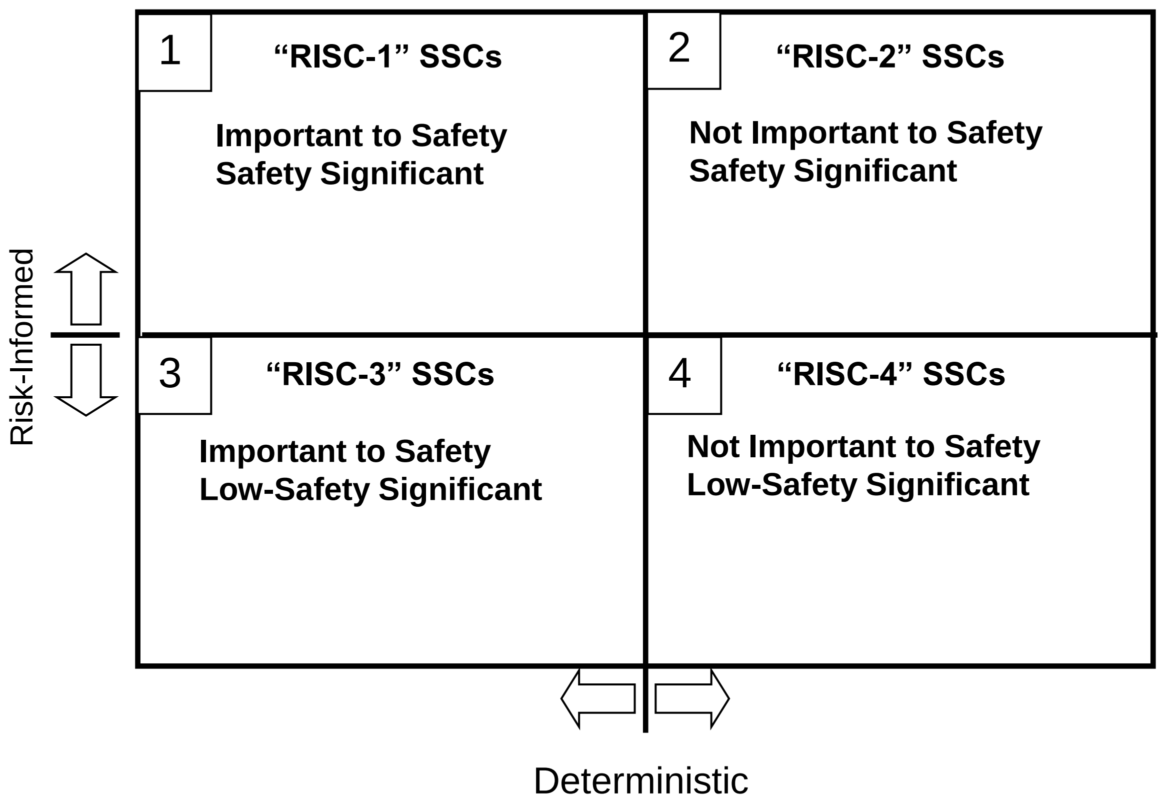

Figure 1 - Risk

a) **RISC-1** SSCs are those Items Important-to-Safety SSCs that the risk-informed categorisation process determines to be significant contributors to plant Safety. Their Safety Significant functions may go beyond the functions defined as Items Important-to-Safety for which credit is taken in the deterministic categorisation process (e.g., the SSC may be Safety Significant for more than Design Basis Accidents).

b) **RISC-2** SSCs are those SSCs that are defined as not important-to Safety, although the risk-informed categorisation process determines that they are significant contributors to plant Safety on an individual basis. The focus for RISC-2 SSCs is on the Safety Significant functions for which credit is taken in the PRA.

c) **RISC-3** SSCs are those SSCs that are defined as Items Important-to-Safety, although the risk-informed categorisation determines that they are not significant contributors to plant Safety.

d) **RISC-4** SSCs are those SSCs that are defined as not important-to-Safety, and that the risk-informed categorisation process determines are not significant contributors to plant Safety.

e) In using a risk-informed Safety classification process, SSCs should be identified as RISC-1, 2, 3 or 4. The risk-informed Safety classification can then be useful in determining the nature of the special treatment (e.g., quality) needed for each SSC to ensure it performs as assumed in the Safety analysis. The more risk significant an SSC is, the more assurance is desired that it will reliably perform its function as assumed in the Safety analysis.

Complement the Treatment of Severe Accidents

Article (40)

The PRA should be used to assess and confirm that the Severe Accident preventive and mitigative measures described in FANR-RG-004 (Reference 6) are adequate to prevent and/or mitigate the phenomena and conditions associated with the more likely Severe Accident scenarios (i.e., functional event sequences with a mean frequency of $\geq 10^{-7}$/yr) consistent with the Authority's probabilistic Safety targets and Containment performance target (see Article 44). If a Severe Accident scenario is found that causes the probabilistic Safety targets and/or the Containment performance target to be exceeded, corrective action should be taken to provide additional prevention or mitigation measures such that the Authority's targets are met.

Graded Equipment Qualification

Article (41)

1. Equipment qualification requirements have generally been determined on a deterministic basis, which represent an acceptable mean to meet the Authority's regulation. Equipment qualification approved by the regulatory body of the Country of Origin (CoO) will be sufficient provided it conforms to internationally accepted codes or standards and accounts for the impact of State unique factors. A graded EQ approach could be used to complement the deterministic approach, using the PRA and RISC categories discussed in Article (39) above.

2. Establishing EQ needs includes defining the conditions under which the equipment must operate as well as defining acceptable qualification methods. If a graded EQ is adopted by the applicant/Licensee, the plant PRA should be used as input to defining the appropriate environmental conditions for each RISC category, and associated acceptance criteria for qualification tests (i.e., testing, analysis, operating experience, or a combination of these methods). The impact of State unique environmental conditions on EQ needs should be considered and the need for any additional qualification beyond what was done in the CoO determined. General guidance on a graded approach to establishing EQ needs and methods for each of the RISC categories is discussed below.

   a) **RISC-1** SSCs perform Safety Significant functions (that is, the functions credited in the Design basis and assumed in the PRA). The qualification requirements for RISC-1 SSCs should, to the greatest extent practicable, be based on testing under the most demanding environmental and dynamic loading conditions associated with Design Basis Accidents and selected Severe Accidents for which the particular SSC is relied on to mitigate the consequence of the Accident. When necessary, qualification by analysis can be used to account for any lack of testing under the required environmental and loading conditions, provided a technical basis is established. EQ approved by RBCoO will be sufficient for SSCs categorised as RISC-1 provided it conforms to internationally accepted codes or standards and is not impacted by State unique factors. Additional attention may be needed for any SSCs classified as Safety Significant as a result of their importance to the prevention or mitigation of Severe Accidents to ensure it will function as assumed in the PRA.

   b) **RISC-2** SSCs perform Safety Significant functions although deterministically, they are considered not important-to-Safety. The qualification requirements for RISC-2 SSCs should focus on the Safety Significant functions for which credit is taken in the PRA. The qualification requirements for RISC-2 SSCs that are intended to ensure additional attention is given to those SSCs classified as not important-to Safety that are Safety Significance and should rely to the greatest extent practical on qualification testing under the most demanding environmental and dynamic loading conditions for which the particular SSC is relied upon to mitigate the consequence of the Accident. When necessary, qualification by analysis can be used to account for any lack of testing under the required environmental and loading conditions, provided a technical basis is established. SSCs categorised as RISC-2 should be reviewed to ensure their EQ is consistent with and supports their Safety Significant function. RISC-2 SSCs qualified in the CoO for their Safety Significant functions using internationally accepted codes or standards will be sufficient provided it is not impacted by State unique factors.

   c) **RISC-3** SSCs are not significant contributors to plant Safety, although they are identified as important-to Safety. Functional performance of RISC-3 SSCs should be adequate considering CoO EQ requirements resulting from their important-to-Safety classification. The qualification requirements for RISC-3 SSCs can put greater reliance on analyses to extrapolate qualification testing for the environmental and dynamic loading conditions associated with their service conditions. When necessary, qualification by operating experience can be used to account for any lack of testing or analysis under the required environmental and loading conditions.

d) **RISC-4** SSCs are not significant contributors to plant Safety. RISC-4 SSCs can be adequately maintained with commercial-grade qualification standards and appropriate record keeping. It is expected that the EQ approved in the CoO would be sufficient for SSCs categorised as RISC-4.

3. As discussed above, test, analysis, operating experience and combinations of these methods may be applied to establish qualification. Prescriptive application of the methods specified in Design codes and qualification standards, based on defined methodologies and criteria provides an acceptable approach that can be used for qualification. Where SSC EQ is changed from that approved by the regulatory body in the CoO, the acceptability of change should be justified.

Graded Quality Assurance (QA)

Article (42)

The risk significance of SSCs may be used to determine the degree of Quality Assurance needed. Therefore, the RISC categories discussed in Article (39) above can be used to help decide on the appropriate Quality Assurance requirements. If it is proposed to apply Quality Assurance in a graded fashion, based upon risk insights, the approach and criteria to be used should be provided to Authority for review.

Performance Goals

Article (43)

1. In conducting the PRA, assumptions are made regarding equipment and human performance (e.g., reliability, availability) and the frequency and type of initiating events. These assumptions are incorporated into the risk calculations and, to varying degrees, impact the results of the PRA. Since results from the PRA are used to complement the deterministic licensing process and are to be used in support of Operations (e.g., configuration control, see article 49), it is important that steps are taken to verify that the key assumptions made in the PRA remain valid over the life of the Facility and, if not, that corrective action is taken. Accordingly, performance goals should be established and monitored for key equipment and human actions consistent with the performance assumptions in the PRA. The performance goals may be established on an individual component, subsystem or system basis and should be sufficiently conservative such that, if not met, there is no immediate Safety concern. A comprehensive set of goals should be

established such that the performance of all Safety functions and Safety Significant systems and human actions can be monitored. The Safety Significant functions are those required for reactor shutdown, decay heat removal and the Containment of Radioactive Material. The Safety Significant SSCs are those identified using the risk-informed Safety classification process described in Article (39).

2. The process for establishing the goals should have the following attributes:

   e) Be based upon observable characteristics that provide measures of Safety performance.

   f) Use measures of Safety performance associated with the desired outcomes as directly as possible. (Sometimes, it may be necessary to use proxy measures. For example, if the monitoring of a performance goal calls for an analysis, the results of the analysis may be one of the measures.)

   g) Be sufficiently comprehensive so as to capture the effect of human and equipment performance.

   h) Be at as high a level as practical.

   i) Account for uncertainties in the PRA and in monitoring techniques.

   j) Ensure that the goal is not in a region of highly unstable or non-linear behaviour (so-called "cliff effects"), such that there is an opportunity to take corrective action if performance is lacking prior to reaching Safety limits.

3. A monitoring programme should be established to collect and analyse data over the life of the Facility sufficient to determine whether or not the goals are being met, including trending of the data. The data used should be from actual operating experience, including that data associated with in-service testing and equipment surveillance programmes. In addition to monitoring the performance of Safety Significant SSC and human actions, the number and nature of initiating events which affect normal Operation (power or shutdown) should be monitored (i.e., what caused the event) for comparison to assumptions in the PRA. The results from the monitoring programme should be fed back into the PRA as part of maintaining the PRA up to date (see Article (36)) and, where necessary, provide the basis for corrective action.

Comparison to Probabilistic Safety Targets

Article (44)

The PRA results should be compared to the probabilistic Safety targets and Containment performance target defined in FANR-RG-004 (Reference 6).

Construction

Article (45)

Risk insights from the PRA should be used during the Construction period to complement the Construction Inspection and testing programme such that:

1. Priority is given to those Construction Inspection and testing activities associated with the most risk and Safety Significant SSCs (as determined by importance measures such as risk achievement worth and Fussell-Vesely). The extent and nature (i.e., type) of Construction Inspection and testing should be commensurate with the risk and Safety Significance of the SSCs to ensure high confidence that the as built SSCs will perform their Safety functions, and

2. Construction errors and programmatic deficiencies found during the Construction period are assessed with respect to their potential Safety and risk implications and the resulting risk insights are factored into decisions regarding the extent, nature and timing of corrective actions to be taken.

Operation

Procedures

Article (46)

Risk insights from the PRA should be factored into the development of plant operating, Emergency and Accident management procedures. Specifically, procedures should be developed that cover all initiating events assessed in the PRA and reflect insights from the analysis associated with each of the initiating events. This would include ensuring that the procedures emphasize those steps (i.e., equipment functions and human actions) that are most likely to result in successful termination of the event (i.e., PRA success paths which correspond to those sequences leading to successful termination of the off-normal event) and consider plant conditions (e.g. environmental) at each stage of the event.

Operator Training

Article (47)

Risk insights from the PRA should be factored into the Operator training programme such that emphasis is placed on those initiating events that are most likely to occur, those actions (human and equipment) that are most likely to lead to successful termination of the event and those event sequences that are the most risk significant. Emphasis should also be placed on Communication protocol and the language used. In addition, the training programme should reflect the Facility and environmental conditions associated with the event sequences modelled in the PRA.

Technical Specifications

Article (48)

1. Risk insights from the PRA should be used in the development of the Facility technical specifications. This would include ensuring that:

    a) the technical specifications include all risk and Safety Significant SSCs as determined using a risk-informed Safety classification process (See Article (39).),

    b) allowable equipment outage times specified in the technical specifications result in only a small incremental increase in risk (NEI-06-09), and

    c) surveillance intervals associated with checking the operability and/or performance of technical specification equipment are established (NEI-04-10) to detect equipment in a condition not capable of performing its Safety function before a period of time elapses that would represent more than a small increase in risk.

2. The guidance contained in US NRC Regulatory Guide 1.177 (Reference 7) is acceptable for use in evaluating a risk-informal approach to technical specifications and for determining appropriate acceptance criteria.

Configuration Control

Article (49)

Prior to placing the Facility into a configuration involving removing normally operable equipment from service (e.g., for Maintenance), the risk impact should be assessed. This would include assessing the change in CDF and LRF associated with the configuration change and establishing criteria for judging the acceptability of the configuration. The guidelines for assessing and managing risk before conducting Maintenance activities contained in US NRC RG 1.182 (Reference 11) are acceptable for use. The provisions for this article do not apply to changes in plant configurations necessary for power Operation (e.g., transition from low power to full power) or those plant configurations allowed by technical specifications.

Aging Management

Article (50)

Risk insights from the PRA should be used to complement programmes and actions taken to manage Facility aging. Specifically, risk insights should be used to ensure that:

1. Surveillance for and actions to manage aging mechanisms are applied to the most Safety Significant SSCs; and

2. The risk impact of age related degradation is assessed and used in decisions regarding the extent, nature and timing of corrective actions to be taken.

Maintenance, Inspection and Testing

Article (51)

1. Risk insights from the PRA should be used to complement the development and implementation of Facility Maintenance, surveillance, Inspection and testing programmes, such that:

   a) The risk implications of performing Maintenance (e.g., at what intervals, under what plant conditions and configurations, for what duration) are considered in developing and implementing the Maintenance programme so as to minimise risk while performing Maintenance and maintaining the Facility SSCs in a condition consistent with the assumptions in the PRA;

   b) Surveillance, Inspection and testing intervals are set to limit the potential for problems to go undetected for periods of time that could result in large increases in risk; and

   c) The nature of the surveillance, Inspection and testing is consistent with the risk significance of the SSC.

2. The guideline contained in USNRC RG 1.182 (reference 11) is acceptable for use in assessing and managing risk prior to performing Maintenance activities. The guidance contained in US NRC RGs 1.175 (Reference 12) and 1.178 (Reference 13) is acceptable for use in evaluating a risk-informed approach to in-service testing and in-service Inspection of piping and for determining appropriate acceptance criteria.

Operational Assessments

Article (52)

1. A programme should be established, implemented and maintained for using the PRA to assess the risk significance of operational events and Safety issues over the life of the Facility. This should include assessing the risk significance of:

    a) Inspection findings (e.g. inoperable equipment);

    b) operational events (i.e. model the actual sequence of events to determine conditional CDF/LRF); and

    c) newly identified Safety issues.

2. The risk information from these assessments should be factored into decisions regarding the scope, nature and priority of corrective actions needed.

3. In addition, the PRA should be used to assess proposed modifications to the Facility Design or Operation with respect to its impact on risk (e.g., change in CDF/LRF and an estimate of the uncertainty). The information should be used as input to an integrated risk-informed decision process (such as described in Reference 3) for assessing the acceptability of proposed Facility modifications.

Safety and Security Interface

Article (53)

1. Safety and security need to be considered together, such that the impacts of one upon the other can be accounted for. Accordingly, the assumptions used in the PRA, particularly with respect to human actions, should reflect the impact of security measures on access to equipment and the performance of required actions. Over the life of the Facility, the impact of changes in security measures on plant risk should be assessed whenever such changes are made and compared to the probabilistic Safety targets contained in Reference (6) and the integrated decision criteria contained in Reference (3).

2. Similar to the above, changes in Facility Design, Operation or configuration (e.g., Maintenance) should be assessed with respect to their impact on the effectiveness of the security measures. To the extent that the PRA has been used to demonstrate the effectiveness of the Facility security measures, revised risk information reflecting the changes in Design, Operation or configuration should be used to confirm the continued effectiveness of the security measures.

Documentation

Archival Documentation

Article (54)

As stated in Article (25), the models, assumptions, data and calculations used in the PRA should be documented. This documentation should be maintained and available for audit by the Authority. The archival documentation should include:

1. Description of the Level 1 internal events (except internal fires) PRA.

   a) Describe the methodology used to develop the Level 1 PRA model (e.g., fault tree linking, large event tree and small fault tree approach, etc.).

   b) List the internal initiating events (including internal floods) that are addressed.

   c) List the success criteria used to delineate Accident sequences, discuss how they were determined, and identify any thermal-hydraulics (T-H) and Severe Accident codes used.

   d) Summarise the Accident sequences modelled.

   e) List the plant systems and associated functions that are included in the PRA model, and identify their interdependencies. One acceptable way to provide dependency information is to include a system dependency matrix that includes front line to front line, front line to support and support to support dependencies.

   f) Identify the source of all numerical data (initiating event frequencies, component failure rates, equipment unavailabilities due to test or Maintenance, human error probabilities, common-cause failure parameters, etc.), especially for numerical data that is based on expert judgement or expert elicitation.

   g) Identify the PRA software platform used to construct the model.

   h) State the truncation frequency used to solve the PRA model.

2. Description of the Level 2 PRA

   a) Discuss the interface with the core damage evaluation (Level 1 PRA).

   b) Describe the Severe Accident physical processes / phenomena and modelling.

   c) List the success criteria used to delineate Accident sequences, discuss how they were determined, and identify any T-H and severe Accident codes used.

   d) Define the Accident classes / release categories.

   e) Characterise the Containment ultimate pressure capacity, and explain how it was determined, and identify any computer codes used.

f) List the plant systems and associated functions that are included in the Level; 2 PRA model, and identify their interdependencies. One acceptable way to provide dependency information is to include a system dependency matrix.

3. Description of the seismic risk evaluation

   a) Describe the seismic analysis methodology and approach, including any screening and bounding analysis (e.g., seismic margins analysis).

   b) Describe the site-specific seismic hazards analysis, and identify the source(s) of information used.

   c) Describe the SSC fragility analysis, including the use of information about similar components and information developed from expert opinion or expert elicitation.

   d) Describe the seismic risk Accident sequence and system modelling, and identify any computer codes used.

4. Description of other external hazards (e.g., high wind) Risk Evaluation

   a) Describe the analysis methodology and approach, including any screening and bounding analysis.

   b) Describe the site-specific hazards analysed and identify the source(s) of information used.

   c) Describe the Accident sequence and system modelling, and identify any computer codes used.

5. Description of the internal fire risk evaluation

   a) Describe the internal fire analysis methodology and approach, including the use of any screening or bounding analyses.

   b) Explain how the fire initiation frequencies were estimated.

   c) Describe the propagation of fires, and identify any computer codes used.

   d) Describe the fire damage modelling, and identify fire-induced failures considered in the evaluation, including:

      - Cable failures
      - Hot shorts
      - Smoke

   e) Describe the Facility response analysis and modelling.

6. Description of the low power and shutdown operation PRA
    a) Identify and describe the non-full-power modes of Operation addressed in the risk evaluation.
    b) If the evaluation of some modes is incorporated into (or bounded by) the evaluations of other modes, describe the methods used to conduct the grouping and bounding analyses.
    c) Describe the methodology used to develop the low-power and shutdown PRA models.
    d) List the initiating events (internal and external) that are addressed in the PRA.
    e) List the success criteria used to delineate Accident sequences, discuss how they were determined, and identify any T-H and severe Accident codes used.
    f) Summarize the Accident sequences modelled in the PRA.
    g) List the Facility systems and associated functions that are included in the PRA model.
    h) Identify the source of all numerical data (initiating event frequencies, component failure rates, equipment unavailabilities due to test or Maintenance, human error probabilities, common-cause failure parameters, etc.), especially for numerical data that is based on expert judgement or expert elicitation.
    i) Identify the PRA software platform used to construct the model.
    j) State the truncation frequency used to solve the PRA model.

Regulatory Submittal Documentation

Article (55)

A summary report on the PRA scope, quality and application shall be provided with the application to construct and operate the NPP. The summary report shall describe:

1. How the PRA conforms with nationally or internationally recognised quality standards. This should include a discussion of the technical adequacy of the PRA and the results of any relevant PRA Peer Reviews.
2. The scope and level of modelling detail in the PRA, including a description of SSCs, human actions, internal and external events, site specific factors, modes of Operations and key assumptions.
3. Key results from the PRA, including:
    a) Results from the Level 1 PRA (internal and external events)

- The total mean Core Damage Frequency and uncertainty distribution.

- The Safety Significant[1] core damage sequences, and their mean core-damage frequencies.

- The Safety Significant initiating events, and their percent contributions to the total Core Damage Frequency.

- The Safety Significant functions, SSCs, and Operator actions, and provide their Risk Achievement Worths, Fussell-Vesely Importance Measures or any other measures used to determine risk significance.

- The results and insights from sensitivity and uncertainty analyses.

b) Results from the Level 2 PRA (internal and external events)

- The total mean large release frequency and total mean conditional Containment failure probability and their uncertainty distributions.

- For functional event sequences involving Containment failure or bypass with a mean frequency $\geq 10^{-7}$/yr, provide the time declaration of Site Area Emergency until Containment failure or bypass.

- The Safety Significant large release sequences and categories and provide their mean release frequencies.

- Explain how the fission product source terms were developed, and identify any computer codes.

- The Safety Significant initiating events, and their percent contributions to the total large release frequency.

- The Safety Significant functions, SSCs, and Operator actions, and their Risk Achievement Worths and Fussell-Vesely Importance Measures (or any other measures used to determine risk significance).

- The results and insights from sensitivity and uncertainty analyses.

---

[1] The determination of Safety significance is a function of how the PRA is being, or is intended to be, used. When a PRA is being used to support an application, the Safety significance of an accident sequence or contributor is measured with respect to whether its consideration has an impact on the decision being made. For the base PRA model, Safety significance can be measured with respect to the contribution to the total CDF or LRF, or it can be measured with respect to the contribution to the CDF or LRF for a specific hazard group or operational mode / configuration, depending on the context. For the purposes of this guide, the following should be used.
Safety Significant accident sequence: A Safety Significant sequence is one of the set of sequences, defined at the functional or systemic level that, when ranked, compose 95% of the CDF or the LRF, or that individually contribute more than ~1% to the CDF or LRF.
Safety Significant Basic Event / contributor: The Basic Events (e.g., equipment unavailabilities, human failure events) that have a Fussell-Vesely importance greater than 0.005 or a risk-achievement worth greater than 2 (20 for common cause Basic Events.).
Safety Significant SSCs: Use the results from application of the guidance in Article (39).

c) Results from the low power and shutdown operations PRA

- The total mean Core Damage Frequency and large release frequency and their uncertainty distribution.

- For each Facility state, describe the Safety Significant core-damage, large release, and offsite consequence (optional) sequences, and provide their mean values.

- For each Facility state, identify the Safety Significant initiating events, including both internal and external events, and provide their percent contributions to the total Core Damage Frequency and the large release frequency.

- For each Facility state, identify the Safety Significant functions, SSCs, and Operator actions, and provide their Risk Achievement Worths, Fussell-Vesely Importance Measures or any other measures used to determine risk significance.

- Discuss the results and insights including those from importance, sensitivity, and uncertainty analyses.

4. If a CoO PRA was used, changes made to the CoO PRA to reflect State unique conditions (e.g., site) or other proposed Design or operational changes and their impact on the CoO PRA results.

5. How the PRA results have been, or will be used to:

a) Support Design in the following areas:

- Assess the Safety Significance of new information, Safety issues and Design changes to an existing Facility Design, if the application is based upon a previously approved Facility Design;

- complement the selection of Safety Significant SSCs;

- complement the identification of SSC EQ needs and methods, based upon their Safety Significance and service conditions;

- establish performance goals for Safety Significant SSCs that are to be monitored over the life of the Facility; and

- demonstrate how Facility risk compares with the Authority's probabilistic Safety targets, including confirmation that no single, SSCs, or human actions contributes disproportionately to risk.

b) Support Construction in the following areas:

- Prioritise Construction Inspection and testing activities; and

- assess the Safety Significance of Construction errors.

c) Support Operation in the following areas:

- Ensure that Emergency and Accident Management procedures address the most Safety Significant event sequences and Operator actions;

- ensure that the Operator training programme addresses the most Safety Significant event sequences and Operator actions;

- ensure that the technical specifications address the most Safety Significant event sequences and plant configurations, and consider risk implications in setting allowable outage times and surveillance intervals;

- inform the configuration control programme regarding the Safety Significance of plant configurations;

- ensure that aging management focuses on the most Safety Significant SSCs;

- ensure that Maintenance, surveillance, in-service Inspection and in-service testing programmes focus on the most Safety Significant SSCs; and

- evaluate the Safety Significance of operating events, plant modifications, Inspection findings, and new Safety issues.

d) Support the Physical Protection programme in the following areas:

- Assess the impact of Physical Protection measures / changes on Safety and

- assess the impact of Design or operational changes and Maintenance outages on Physical Protection.

6. At the time of each PRA update, a summary report on the update should be provided to the Authority describing what was updated, the results of the update (e.g., changes in CDF, LRF, key insights) and how the updated information is being used.

Source Information

Article (56)

USNRC Regulatory Guide 1.200 (Ref 8) as well as USNRC RGs 1.175, 1.177, 1.178, 1.182, and 1.201 (References 12, 7, 13, 11, and 5, respectively) provide the basis for much of this document.

References

Article (57)

1. FANR Regulation, FANR-REG-05, “Regulation for the Application of a PRA at Nuclear Facilities”

2. FANR Regulation, FANR-REG-01, “Regulation for Management Systems for Nuclear Facilities”

3. IAEA – International Nuclear Safety Group (INSAG): “A Framework for Integrated Risk-Informed Decision-making Process” (in publication)

4. FANR Regulation, FANR-REG-03, “Regulation for the Design of Nuclear Power Plants”

5. U.S. Nuclear Regulatory Commission Regulatory Guide 1.201, Guidelines for Categorizing Structures, Systems and Components in Nuclear Power Plants According to Their Safety Significant, Rev 1, May 2006

6. FANR Regulatory Guide, FANR-RG-004, "Evaluation Criteria for Probabilistic Safety Targets and Design Requirements"

7. U.S. Nuclear Regulatory Commission Regulatory Guide 1.177, “An Approach for Plant Specific, Risk-Informed Decisionmaking: Technical Specifications,” August 1998

8. U.S. Nuclear Regulatory Commission Regulatory Guide 1.200, An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities, Rev 2, March 2009

9. IAEA Safety Standards Series No. SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants Specific Safety Guide

10. IAEA Safety Standards Series No. SSG-4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants Specific Safety Guide

11. U.S. Nuclear Regulatory Commission Regulatory Guide 1.182, “Assessment and Managing Risk Before Maintenance Activities at Nuclear Power Plants,” May 2000

12. U.S. Nuclear Regulatory Commission Regulatory Guide 1.175, “An Approach for Plant Specific, Risk-Informed Decision-Making: In-Service Testing,” August 1998

13. U.S. Nuclear Regulatory Commission Regulatory Guide 1.178, “An Approach for Plant Specific Risk-Informed Decision-Making for In-Service Inspection of Piping,” September 2003

14. U.S. Nuclear Regulatory Commission Regulatory Guide 1.205, “Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants,” December 2009

15. Nuclear Energy Institute, NEI-06-09

16. Nuclear Energy Institute, NEI-04-10