



Reliability Programs for Nuclear Power Plants

RD/GD-98

December 2011

DRAFT



Reliability Programs for Nuclear Power Plants

Regulatory Document RD/GD-98

© Minister of Public Works and Government Services Canada 2011

Catalogue number XXXXX

ISBN XXXXX

Published by the Canadian Nuclear Safety Commission

Extracts from this document may be reproduced for individual use without permission provided the source is fully acknowledged. However, reproduction in whole or in part for purposes of resale or redistribution requires prior written permission from the Canadian Nuclear Safety Commission.

Également publié en français sous le titre de : (Titre)

Document availability

This document can be viewed on the Canadian Nuclear Safety Commission Web site at nuclearsafety.gc.ca

To order a printed copy of the document in English or French, please contact:

Canadian Nuclear Safety Commission
280 Slater Street
P.O. Box 1046, Station B
Ottawa, Ontario K1P 5S9
CANADA

Tel.: 613-995-5894 or 1-800-668-5284 (in Canada only)

Facsimile: 613-995-5086

Email: info@cnsccsn.gc.ca

Web site: nuclearsafety.gc.ca

Publishing history:

November 2011 Version 2.0

Preface

Regulatory document RD/GD-98, *Reliability Programs for Nuclear Power Plants*, sets out the requirements and guidance of the Canadian Nuclear Safety Commission (CNSC) for the development and implementation of a reliability program for nuclear power plants in Canada.

RD/GD-98 captures the existing requirements previously found in S-98 (Revision 1), *Reliability Programs for Nuclear Power Plants*, and also replaces the latter document.

Key principles and elements used in developing this document and the associated regulatory document are consistent with national and international documents.

Nothing contained in this document is to be construed as relieving any licensee from pertinent requirements. It is the licensee's responsibility to identify and comply with the *Nuclear Safety and Control Act*, applicable regulations and licence conditions.

Table of Contents

1.	Introduction.....	1
1.1	Purpose	1
1.2	Scope.....	1
1.3	Relevant legislation.....	1
1.4	National and international documents	2
2.	Objective and requirements of reliability programs	3
2.1	Objective.....	3
2.2	Requirements	3
3.	Guidance for Reliability Programs	4
3.1	Using systematic methods to identify and rank systems important to safety	4
3.1.1	Identifying systems important to safety	4
3.1.2	Ranking identified structures, systems and components on the basis of relative importance to safety.....	5
3.1.3	Screening out structures, systems and components	6
3.2	Specifying reliability targets.....	6
3.3	Identifying and describing potential failure modes.....	7
3.4	Specifying minimum capabilities and performance levels	7
3.5	Maintenance program	7
3.6	Inspections, tests, modelling and monitoring.....	8
3.6.1	Providing for inspections and tests	8
3.6.2	Modelling.....	8
3.6.3	Monitoring performance and reliability.....	9
3.6.4	Performing reliability assessments	11
3.7	Implementing a reliability program	12
3.8	Recording and reporting results of reliability program activities	12
3.9	Documenting a reliability program.....	12
	Glossary	13
	References.....	16

Reliability Programs for Nuclear Power Plants

1. Introduction

1.1 Purpose

RD/GD-98, *Reliability Programs for Nuclear Power Plants*, sets out the requirements and guidance of the Canadian Nuclear Safety Commission (CNSC) for the development and implementation of a reliability program for a nuclear power plant (NPP) in Canada. The reliability program assures that the systems important to safety (SIS) shall meet their defined design, and performance criteria at acceptable levels of reliability throughout the lifetime of the facility.

1.2 Scope

This regulatory document describes the essential elements of a reliability program, including reliability assessment, modelling, evaluation and monitoring.

The document emphasizes reliability programs during the normal operation phase. However, the general approach applies to all phases of an NPP's lifecycle (design, construction, commissioning, start-up, operation and decommissioning).

To limit the risks of an NPP to a reasonable level, the plant must operate within some requisite bounds of overall safety. This overall safety can only be assured when the SIS at the NPP are both capable of adequately performing their purposes and available to do so. Thus, the SIS at NPPs must function at a certain level of reliability.

1.3 Relevant legislation

Relevant sections of the *Nuclear Safety and Control Act* (NSCA) and sections of its associated regulations to this guidance document include:

- Subsection 24(4) of the NSCA, which stipulates that “No licence may be issued, renewed, amended or replaced unless, in the opinion of the Commission, the applicant
 - (a) is qualified to carry on the activity that the licence will authorize the licensee to carry on; and
 - (b) will, in carrying on that activity, make adequate provision for the protection of the environment, the health and safety of persons and the maintenance of national security and measures required to implement international obligations to which Canada has agreed.”
- Subsection 24(5) of the NSCA, which provides that “a licence may contain any term or condition that the Commission considers necessary for the purposes of this Act.”

- Paragraphs 12(1)(a) to 12(1)(e) of the *General Nuclear Safety and Control Regulations*, which stipulate that “Every licensee shall
 - (a) ensure the presence of a sufficient number of qualified workers to carry on the licensed activity safely and in accordance with the NSCA, the regulations made under the act and the licence;
 - (b) train the workers to carry on the licensed activity in accordance with the NSCA, the regulations made under the NSCA and the licence;
 - (c) take all reasonable precautions to protect the environment and the health and safety of persons and to maintain security;
 - (d) provide the devices required by the NSCA, the regulations made under the NSCA and the licence and maintain them within the manufacturer’s specifications”;
 - (e) require that every person at the site of the licensed activity use equipment, devices, clothing and procedures in accordance with the NSCA, the regulations made under the NSCA and the licence”.
- Section 5 of the *Class I Nuclear Facilities Regulations*, which stipulates that “An application for a licence to construct a Class I nuclear facility shall contain the following information in addition to the information required by section 3:
 - (a) a description of the structures proposed to be built as part of the nuclear facility, including their design and their design characteristics;
 - (b) a description of the systems and equipment proposed to be installed at the nuclear facility, including their design and their design operating conditions;
 - (c) a preliminary safety analysis report demonstrating the adequacy of the design of the nuclear facility”.
- Subsection 6(d) of the *Class I Nuclear Facilities Regulations*, which stipulates that an application for a licence to operate a Class I nuclear facility shall contain, in addition to other information, “the proposed measures, policies, methods and procedures for operating and maintaining the nuclear facility”.
- Subsection 14(2) of the *Class I Nuclear Facilities Regulations*, which stipulates that “Every licensee who operates a Class I facility shall keep a record of
 - (a) operating and maintenance procedures; (...)
 - (c) the results of the inspection and maintenance programs referred to in the licence”.
- Subsection 14(4) of the *Class I Nuclear Facilities Regulations*, which requires every person who is required by subsection 14(2) of those regulations to keep records of “operating and maintenance procedures” and “the results of the inspection and maintenance programs referred to in the licence” to retain the required records “for 10 years after the expiry date of the licence to abandon issued in respect of the Class I nuclear facility.”

1.4 National and international documents

Key principles and elements used in developing this document are consistent with national and international documents, including the following:

- Institute of Electrical and Electronics Engineers, IEEE 933-1999, *Guide for the Definition of Reliability Program Plans for Nuclear Power Generating Stations*, September 1999
- Institute of Electrical and Electronics Engineers, IEEE *Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems*, 1987

- International Atomic Energy Agency, IAEA TECDOC-524, *Status, Experience and Future Prospects for the Development of Probabilistic Safety Criteria*, IAEA, Vienna, 1989

A complete list of Canadian and international reference documents is provided at the end of this document.

2. Objective and requirements of reliability programs

2.1 Objective

The reliability program shall ensure that all SIS at an NPP function reliably, in accordance with the relevant design and performance criteria, including any safety goals of the NPP and CNSC licence requirements.

2.2 Requirements

A reliability program for an NPP shall:

1. identify, using a systematic method, all SIS by:
 - a. identifying NPP structures, systems and components (SSCs) associated with the initiation, prevention, detection or mitigation of any failure sequence that could lead to damage of fuel, associated release of radionuclide or both
 - b. ranking the identified SSCs on the basis of their relative importance to safety
 - c. screening out SSCs that do not contribute significantly to plant safety (the remaining SSCs are the systems important to safety)
2. specify reliability targets for the SIS at the NPP
3. identify and describe the potential failure modes of the SIS at the NPP
4. specify the minimum capabilities and performance levels that the SIS must attain to achieve reliabilities that are consistent with NPP safety targets and regulatory requirements
5. provide information to the maintenance program to maintain the effectiveness of the SIS at the NPP
6. provide for inspections, tests, modelling, monitoring or other measures to effectively assess the reliability of the SIS at the NPP
7. include provisions to assure, verify and demonstrate that the program is implemented effectively
8. include provisions for recording and reporting the results of program activities, including the results of assessments, inspections, tests or monitoring of the reliability of the SIS at the NPP
9. clearly and comprehensively document the activities, attributes, elements, results and administration of the reliability program, including:
 - a. the activities that make up the program
 - b. procedures and schedules for conducting the program activities
 - c. the licensee's organization for managing and implementing the program, including the specific positions, roles and responsibilities of the persons involved
 - d. the methodology used to identify, rank and assign reliability targets to the SIS at the NPP
 - e. the list of SIS at the NPP

- f. the reliability targets for each of the SIS at the NPP
- g. potential failure modes of the SIS at the NPP
- h. methods used to determine the potential failure modes of the SIS at the NPP
- i. reliability assessments, inspections, monitoring, testing, verifications, and recording and reporting activities that the licensee will carry out to assure, verify, demonstrate or document that the reliability program is implemented correctly and effectively in accordance with regulatory requirements
- j. the results of the reliability assessments, inspections, monitoring, testing, verifications, and reporting activities that the licensee carried out as part of the reliability program

3. Guidance for Reliability Programs

An NPP's reliability program should possess the following elements to accomplish its objective of enhancing plant availability and safety:

- performance monitoring
- performance evaluation
- problem prioritization
- problem analysis and corrective action recommendation
- corrective action implementation and feedback

These elements are also shown in the equipment reliability process top-level diagram provided in INPO AP-913, *Equipment Reliability Process Description* (Revision 1), a document issued by the Institute of Nuclear Power Operations. The reliability of the SIS should be considered for different power levels and during start-up and shutdown of the reactor. The impact of the post-accident mission time should be considered for all aspects of the reliability program.

The effort and resources allocated to the reliability program for each of the SIS should be commensurate with the importance of the system to the safe operation of the NPP.

3.1 Using systematic methods to identify and rank systems important to safety

3.1.1 Identifying systems important to safety

NPP licensees should identify and document all SIS associated with the initiation, prevention, detection or mitigation of any failure sequence that could lead to damage of fuel, associated release of radionuclide, or both.

SIS should be identified using a systematic approach. The probabilistic safety assessment (PSA) is the most thorough and systematic method to do so, and includes the insights from a Level-2 PSA, shutdown PSA, and external events and hazards assessments. However, other principles and information – such as defence-in-depth, results of deterministic safety analysis, operating experience and expert judgment – should also be considered when identifying SIS.

The criteria for determining SIS are based on:

- safety function(s) to be performed
- consequence of failure
- probability that the SSCs will be called upon to perform the safety function
- the length of time between a postulated initiating event and the point when the SSCs will be called upon to operate, and the expected duration of that operation

The list of SIS may be revised in light of emerging operational data, system changes, new failure data, or when other new information is provided. The basis for revision must be fully documented.

3.1.2 Ranking identified structures, systems and components on the basis of relative importance to safety

Systems identified as important to safety should be ranked on the basis of their relative importance to safety and according to their contribution to the overall plant risk (risk of severe core damage and risk of associated radioactive releases).

This ranking should be performed using the results of a plant-specific PSA. However, in the absence of a PSA, engineering judgment may be used. The criteria used to rank the systems should be properly documented.

3.1.2.1 Using probabilistic safety assessment to rank systems important to safety

The following importance measures are used as criteria to assess the relative contribution of systems to plant risk:

- risk-increase ratio, also called risk achievement worth (RAW)
- Fussell-Vesely (FV) importance

The following points provide criteria and guidance for identifying SIS:

- Any system with $FV \geq 0.05$ (or component $FV \geq 0.005$) and $RAW \geq 2$ should be considered important to safety.
- If a system has $FV \geq 0.05$ (or component $FV \geq 0.005$) or $RAW \geq 2$, detailed justification should be provided if it is excluded from the list of systems important to safety
- Consideration should be given to those components identified as important to safety by the component screening criteria, and for which the associated system is screened out by the system-level screening criteria.
- Expert panels can be used to complement the PSA review group for consideration of the deterministic safety analysis and defence-in-depth principles. The rationale for the expert panel's decision to add or remove any system in the list of identified SIS should be fully documented.
- Insights from existing PSAs should be used to the extent practicable for the purpose of determining SIS, with consideration given to the quality, scope and limitations of the PSA. The gap between the existing PSA scope and quality, and the requirements in CNSC Regulatory Document S-294, *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*, should be compensated for by other means/considerations to be factored into the determination of the list of SIS.
- The list of SIS should be updated with consideration given to the PSA revisions, updates and improvements aimed at the requirements listed in S-294.
- The insights from Level-2 PSA (small and large release), the shutdown PSA, and external events and hazards assessment should be considered when identifying SIS.

3.1.2.2 Using other means to identify systems important to safety

If a plant does not have a PSA, then the identification of SIS starts by identifying all systems associated with the initiation, prevention, detection or mitigation of any failure sequence that could lead to fuel damage, associated release of radionuclide or both. The identification process

will be completed by reviewing the primary list of systems; this review is to identify only those systems that contribute significantly to plant safety, based on their importance to safety functions.

3.1.3 Screening out structures, systems and components

SSCs that do not contribute to plant safety may be screened out of the reliability program. If the licensee declares that specific SSCs are unimportant to safety, the rationale for this should be fully documented.

3.2 Specifying reliability targets

The objective of setting reliability targets for SIS is to establish a reference point against which to judge system performance. The reliability targets that the licensee assigns to SIS should be consistent with the NPP's safety goals and should consider industry-wide operating experience where practicable. Where no safety goals are in place, reliability targets should be based on good engineering judgment, accounting for dependencies between systems. A single system may be assigned multiple reliability targets, depending on different failure criteria.

The licensee should monitor the performance or condition of SIS against licensee-established targets, as a way to reasonably ensure that the SIS are capable of fulfilling their intended functions. When the performance or condition of any structure, system or component fails to meet established targets, appropriate corrective action should be taken.

Reliability targets may be developed during the initial phase of reliability programs. These targets are intended to be compared with actual plant performance, in order to identify deviations from expected performance.

The *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems* issued by the Institute of Electrical and Electronics Engineers gives the basis for establishing these numerical targets, which are based on the following:

- frequency of demand
- consequence of failure
- risk

The International Atomic Energy Agency's IAEA TECDOC-524, *Status, Experience and Future Prospects for the Development of Probabilistic Safety Criteria*, provides the principles for deriving numerical objectives.

The selection of reliability targets should maintain a balance between the prevention and mitigation of events. The following principles apply:

- Reliability targets for special safety systems should be set no lower than 0.999. This is consistent with established CNSC limits.
- For all other poised SIS, the target should be set at lower than 120% of the baseline performance of the system.

Reliability targets should be revised in light of emerging operational data, system changes or new failure data, or when other new information is provided. The basis for revision must be fully documented.

Appropriate corrective action should be taken whenever the performance or condition of a system important to safety does not meet established goals.

3.3 Identifying and describing potential failure modes

The potential failure modes of SIS should be identified, in order to determine necessary maintenance activities and ensure reliable system operation. Failure modes include failure to start on demand, and failure to run for a given mission time.

Failure modes can be identified from failure history or through the use of qualitative analytical methods, if the failure history is not available.

Any new identified failure mode should be incorporated into the reliability models.

3.4 Specifying minimum capabilities and performance levels

For each success criterion of a system important to safety, the minimum capabilities and performance levels should be defined. These capabilities and performance levels should be expressed in physical terms (e.g., pressure, flow, voltage, intensity).

A given system important to safety can present several failure modes (or success criteria), according to the sequence of events where it is needed. For each of these sequences, the success criteria for the system must be defined.

Failure criteria for a system important to safety should be stated in terms of the system **not** performing its function when required to do so. The failure criteria should be explicitly described or referenced in the reliability program document, and they should be consistent with the definition of system failure criteria used in other analyses and/or other documents that support the operating licence. SIS may have several different failure criteria, depending on the plant state, accident condition or consequences of the failure.

It is advocated to use the minimum allowable performance standards for the models required by this document (RD/GD-98), given that the conservative deterministic assumptions are in line with this document's scope and intent for defence-in-depth and design for reliability. It is also acceptable to use realistic assumptions from PSA models.

3.5 Maintenance program

The primary objective of a maintenance program is to maintain the plant equipment and systems in accordance with applicable regulations, codes and standards (including CNSC Regulatory Document S-210, *Maintenance Programs for Nuclear Power Plants*), vendor recommendations and previous experience, so that their performance meets reliability targets.

Preventive maintenance and consistent corrective maintenance may lead to improvements in failure trends. Reliability-centered maintenance is one technique that uses reliability principles to improve maintenance.

The modelling of the probability of failure of SIS includes information from the maintenance program. The maintenance program should also include all activities (such as surveillance) that are credited in the reliability models. As mentioned in section 3.3, the identification of the failure mode will determine maintenance activities.

Modification of the maintenance program could be recommended if the results of the reliability assessment show that the system is not meeting its target.

The reliability modelling of SIS provides information on how the maintenance program affects system reliability. This information is fed back into the maintenance program to improve its effectiveness.

3.6 Inspections, tests, modelling and monitoring

3.6.1 Providing for inspections and tests

Adequate testing programs for SIS should be in place as specified in S-210.

Where feasible, surveillance activities on redundant equipment should not be performed at the same time or using the same personnel. This is to avoid introducing a common-cause failure.

Sufficient testing before, during and after plant shutdowns should ensure that the assumptions of fault discovery intervals made in the reliability assessments remain valid at all times.

The frequencies, timing and substance of surveillance activities should be revised in light of emerging operational data, plant changes, failure data, or other new information – provided the reliability assessment is revised accordingly and that consistency with reliability targets is maintained.

If a test is missed, the following provisions apply:

1. A grace period is allowed. This is generally set at 25% of the test interval, with an upper limit of three months (or other time period, with the agreement of the CNSC).
2. The procedure used by the licensee to approve deferral of tests should be submitted to the CNSC for acceptance.
3. All tests that have been deferred, along with approval references, should be listed in the annual reliability report.
4. All records of approval of test deferrals should be available for inspection upon request.

3.6.2 Modelling

The model used to describe the system should accurately reflect the system's current configuration. The level of detail of the model should be such that dependencies are clearly identified, but also limited to equipment failure modes. (The failure mechanism could be of interest for specific purposes, but should not be included in the models required by this document).

The model could include human recovery actions (actions to mitigate system failure) if an equipment failure's impact on the failure of the entire system is developing slowly and the equipment failure can be fixed in the meantime.

The model should include, to the extent practicable:

- Every component and structure and their failure modes that could result in dependence between systems important to safety. Any new identified failure mode should be incorporated in the reliability models.

- Human errors (such as maintenance errors and non-detection of annunciate conditions) that could occur before the initiating event and that could contribute to failure of the system function.
- Maintenance or testing activities that impair component loops or channels while being performed.
- Failure data that represents the actual performance of the modelled components as accurately as possible. Site-specific failure data should be compared to the failure data used in the assessment. Where the information is insufficient, relevant generic failure data may be used to derive valid site-specific data. Generic failure data should preferably be extracted from other operating experience and should closely reflect the actual performance of the component.
- Estimation of human performance reliability that considers all conditions, shaping factors and other considerations specific to the plant, according to internationally established techniques for human reliability analysis.
- Consideration of the potential impact of uncertainties.
- An assessment of the importance, contribution and sensitivity of each component failure to the reliability of the entire system.
- On-demand failure, as well as any latent faults that are detectable through testing (for reliability models).
- A comparison to the reliability targets (for on-demand models only). The mission failure rate of relevant components should be tracked against mission testing programs.
- A support system (for SIS reliability models, and if the support system is exclusively devoted to the operation of systems important to safety).

3.6.3 Monitoring performance and reliability

Performance monitoring relies on gathering pertinent failure detection and in-plant reliability information. This includes both reliability monitoring (e.g., observation of failure frequency, outage rate, maintenance durations, outage times) and condition monitoring (e.g., observation of conditions related to failure, such as degraded performance, and/or changes in equipment parameters as measured by non-destructive tests, such as ultrasonic inspections, electrical continuity tests and acoustic vibration monitoring).

The reliability monitoring of SIS involves the review, recording, and trending of the reliability performance or condition of all SIS. This is to ensure they remain capable of meeting their functional specifications and will perform consistently with their specified reliability targets and reliability assessments. The licensee should establish a basis for excluding any specific components identified in the reliability assessments from reliability monitoring. This basis should be related to the limited likelihood or safety impact of component failure modes.

If a reliability problem is diagnosed, the reliability program should be capable of determining the cause of the problem and devising corrective actions to rectify it. The reliability program should have the means to monitor the efficacy of corrective actions, so it can ensure the proposed solution is adequate.

3.6.3.1 Monitoring the performance of systems

The reliability performance of all SIS should be monitored to assure that they remain capable of meeting their functional specifications and that they perform consistently with their specified targets. This monitoring process should include:

- Identification of incidents when SIS do not meet their defined specifications (including periods of scheduled out-of-service and occurrences of initiating events). An assessment should be made with regard to the severity of the condition and identification of the accident sequences affected. These incidents are reportable events, in accordance with CNSC Regulatory Document RD-99.1, *Reporting Requirements for Operating Nuclear Power Plants: Events*.
- Assessment of the consequences of unsafe component failures, in order to determine the impact on the reliability of the system.
- Consideration of the reliability of SIS during the planning of operational and maintenance activities. (The reliability monitoring of SIS should include an assessment of the impact of these activities on reliability performance and consistency with reliability targets. If a reduction in reliability cannot be avoided, the impact on any safety goals of the facility must be assessed.)

3.6.3.2 Monitoring the performance of components

The performance or condition of all components of SIS should be monitored. This monitoring of component reliability should include:

- Identification of components whose failure decreases the reliability of the system important to safety.
- Assessment and recording of every failure of a component that could affect the reliability of the whole system to which it belongs, as soon as practicable after the failure has been discovered.
- Analysis of component failures to determine if trends exist. If trends are found, their existence should be explained and their importance assessed in relation to the reliability targets.
- Analysis of component failures to determine if failures were due to non-random causes (such as being preventable by maintenance; aging or wear; or a design or installation problem). These failures represent safety problems of a different nature than what was previously reported and are therefore reportable events in accordance with CNSC Regulatory Document RD-99.1, *Reporting Requirements for Operating Nuclear Power Plants: Events*.
- Assessment of component failure(s) to ascertain if the cause of the failure(s) may be common to other components. Common-cause failures should be identified and recorded. The International Common-Cause Data Exchange protocol might be used to record the common-cause failure for site-specific failure data. To derive accurate site-specific failure data for SIS, the details of the failure history and in-service records for all relevant components should be recorded.

3.6.3.3 Monitoring human performance

Human actions that potentially could impact the reliability of SIS should be identified and monitored. The monitoring of human performance should include:

- recording of the occurrence of human errors
- a comparison of actual site-specific human performance with that used in the reliability assessment

3.6.4 Performing reliability assessments

Reliability assessments evaluate the predicted reliability of SIS, in order to demonstrate their ability to meet their specified reliability targets for all relevant plant states. The methods used to perform the assessment are at the discretion of the licensee. A system important to safety may require several different reliability assessments to account for different success criteria.

All modelled systems should be evaluated quantitatively, in order to derive their predicted reliabilities and to demonstrate they are consistent with their reliability targets. The assessments should reflect the actual operation, surveillance and maintenance activities of the systems as accurately as possible.

Reliability assessments should include:

- predicted reliability
- observed reliability
- specific reliability indices

3.6.4.1 Calculating predicted reliability

The future predicted reliability is assessed using current data, which should be compared to the values obtained for the current and previous years as well as to the target. The reliability assessments should be re-evaluated annually using the latest relevant failure data. Changes in the predicted probability from the value reported in the previous year should be explained.

3.6.4.2 Calculating observed reliability

Observed reliability is calculated using actual operating performance.

3.6.4.3 Reliability indices

Reliability indices are intended to capture trends in the SIS.

The following indices should be reported according to each system's specificity:

- the frequency of failure of active systems important to safety
- the probability of failure of poised systems important to safety

The licensee should perform a comparison between predicted reliability, reliability indices and reliability targets. Any differences should be explained.

The licensee should establish criteria for determining if an operational event, system change, or acquisition of new knowledge warrants immediate or near-term revision of system reliability models. As a minimum, system and procedural changes, emerging operational data, new system-related knowledge, and the latest failure data should be reassessed and documented

annually. The reliability assessment report should be updated to reflect changes to the model or new conclusions about the model results.

3.7 Implementing a reliability program

Following a CNSC staff inspection or request, a licensee should demonstrate effective implementation of its reliability program.

3.8 Recording and reporting results of reliability program activities

The CNSC should have access to the results of reliability programs at nuclear power plants. These results may be obtained at any time through periodic inspections of reliability programs and from reports prepared by licensees.

Results could be recorded in the form of operational logs, work orders, work plans, work permits, test results and calibration records. The review of this information is required to assure accurate, timely assessment and reporting of the reliability performance of SIS. This information is also reviewed in order to identify and help avoid reductions in the reliability of these systems.

Licensees have discretion as to how they structure their reports that describe reliability assessments of SIS. However, licensees should report the results of their reliability programs according to CNSC Regulatory Document RD-99.1, *Reporting Requirements for Operating Nuclear Power Plants*. Guidance on what is required in the annual report on the risk and reliability of the NPP, along with a sample template, can be found in CNSC Guidance Document GD-99.1, *Guide to the Reporting Requirements for Operating Nuclear Power Plants*.

The comparison between predicted reliability, reliability performance indices and reliability targets should be reported. Any differences should be explained.

3.9 Documenting a reliability program

This does not require specific guidance.

Glossary

common-cause failure

A concurrent failure of two or more structures, systems or components due to a single specific event or cause such as a natural phenomenon (earthquake, tornado, flood, etc.), design deficiency, manufacturing flaw, operation and maintenance error, human-induced destructive event, aging effect or other reason.

condition monitoring

Continuous or periodic inspections, measurements or trending of the performance or physical characteristics of SSCs, in order to indicate current or future performance and the potential for failure.

critical components

Equipment whose failure will result in complete system failure or functional failure.

degraded state

A state of equipment failure that is gradual, partial or both, and that effectively leads to a termination of the equipment's ability to perform its required function.

failure

The inability of a structure, system or component to function as per its design.

failure criterion

The measure point at which a system, structure or component is considered unable to meet its success criterion.

Fussell-Vesely (FV) importance

The FV parameter for a basic event is defined as the fractional decrease in the core damage frequency if the basic event in question can never occur; that is, the component is perfectly reliable with respect to that basic event – it is never failed or out of service.

importance measures

A quantitative analysis to determine the importance of variations in equipment reliability to system risk and/or reliability.

incipient failure

An imperfection in the state or condition of equipment that could result in a degraded or immediate failure if corrective action is not taken.

initiating event

An identified event that leads to anticipated operational occurrences or accident conditions.

maintenance

Organized activities, both administrative and technical, to keep structures, systems or components in good operating condition and to ensure they function according to their design.

nuclear power plant (NPP)

Any nuclear fission reactor installation that has been constructed to generate electricity on a commercial scale and that is a Class IA nuclear facility as defined under the *Class I Nuclear Facilities Regulations*.

observed reliability

A reliability measure that is calculated using actual operating performance.

performance evaluation

Analysis in terms of initial objectives and estimates and that is usually made on site, in order to provide information on operating experience and to identify required corrective actions.

performance monitoring

The determination of whether equipment is operating or is capable of operating within specific limits.

predicted reliability

The predicted probability that a system will meet its success criterion when required to do so. This is calculated using current reliability data.

reliability

The ability of a system, structure or component to perform, in accordance with its defined specifications, its required function under given conditions for a defined time period or upon demand.

reliability-centered maintenance

A series of orderly steps for identifying system and subsystem functions, functional failures, and dominant failure modes, prioritizing them, and selecting applicable and effective preventive maintenance tasks to address the classified failure modes.

reliability monitoring

Direct monitoring of reliability parameters of a plan, system, or equipment (for example, failure frequency, downtime due to the maintenance activities, or outage rate).

reliability targets

The reliability goals to be achieved by the plant systems. These targets are intended to be compared with actual plant performance, in order to identify deviations from expected performance.

risk

The chance of injury or loss, defined as a measure of the probability and severity of an adverse effect (consequences) to health, property, the environment or other things of value; mathematically, it is the probability of occurrence (likelihood) of an event multiplied by its magnitude (severity).

risk-increase ratio (risk achievement worth [RAW])

The factor by which core damage frequency increases when the basic event has occurred with certainty.

safety goals

A nuclear power plant's probabilistic goals that can be expressed in terms of frequency of severe core damage or frequency of release of radionuclides. Safety goals are set to meet safety objectives, in order to protect reactor facility staff, the public and the environment by establishing and maintaining effective defences against the release of the radiological hazards.

safety systems

Systems to ensure the safe shutdown of a reactor or residual heat removal from the reactor core, or to limit the consequences of anticipated operational occurrences and design basis accidents.

structures, systems and components (SSC)

A general term encompassing all elements (except human factors) of a facility or activity that contribute to protection and safety. Structures are passive elements such as buildings, vessels or shielding. Systems comprise several components that are assembled in order to perform specific (active) functions.

Components are discrete elements of a system such as wires, transistors, integrated circuits, motors, relays, solenoids, pipes, fittings, pumps, tanks, and valves.

systems important to safety (SIS)

Structures, systems and components of a nuclear power plant associated with the initiation, prevention, detection or mitigation of any failure sequence and that have the most significant impact in reducing the possibility of damage to fuel, associated release of radionuclide or both.

success criterion

A criterion for a structure, system or components that designates the minimum functional capability and performance levels required for effectiveness.

References

1. Canadian Nuclear Safety Commission, S-98/Rev. 1, *Reliability Programs for Nuclear Power Plants*.
2. Institute of Electrical and Electronics Engineers, IEEE 933-1999, *Guide for the Definition of Reliability Program Plans for Nuclear Power Generating Stations*, September 1999.
3. Institute of Nuclear Power Operations, INPO AP-913, *Equipment Reliability Process Description AP-913*, Revision 1, November 2001.
4. Institute of Electrical and Electronics Engineers, *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems*, 1987.
5. International Atomic Energy Agency, IAEA TECDOC-524, *Status, Experience and Future Prospects for the Development of Probabilistic Safety Criteria*, IAEA, Vienna, 1989.
6. Canadian Nuclear Safety Commission, R-7, *Requirements for Containment Systems for CANDU Nuclear Power Plants*, February 1991.
7. Canadian Nuclear Safety Commission, R-8, *Requirements for Shutdown Systems for CANDU Nuclear Power Plants*, February 1991.
8. Canadian Nuclear Safety Commission, R-9, *Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants*, November 2008.
9. Canadian Nuclear Safety Commission, RD-337, *Design of New Nuclear Power Plants*, November 2008.
10. Canadian Nuclear Safety Commission, S-210, *Maintenance Programs for Nuclear Power Plants*, July 2007.
11. Canadian Nuclear Safety Commission, RD-99.1, *Reporting Requirements for Operating Nuclear Power Plants: Events*, publication anticipated fall 2011.
12. Canadian Nuclear Safety Commission, GD-99.1, *Guide to the Reporting Requirements for Operating Nuclear Power Plants: Events*, publication anticipated fall 2011.
13. Canadian Nuclear Safety Commission, RD-99.2, *Reporting Requirements for Operating Nuclear Power Plants: Compliance Monitoring*, publication anticipated fall 2011.
14. Canadian Nuclear Safety Commission, GD-99.2, *Guide to the Reporting Requirements for Operating Nuclear Power Plants: Compliance Monitoring*, publication anticipated fall 2011.