EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Development of a Shutdown Qualitative Risk Assessment Standard

1016231

Development of a Shutdown Qualitative Risk Assessment Standard

1016231

Technical Update, December 2007

EPRI Project Manager

D. Hance

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

ERIN Engineering and Research Inc.

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

CITATIONS

This document was prepared by

ERIN Engineering and Research, Inc.
1210 Ward Avenue, Suite 100
West Chester, PA 19380

Principal Investigator
L. Shanley

This document describes research sponsored by the Electric Power Research Institute (EPRI).

This publication is a corporate document that should be cited in the literature in the following manner:

Development of a Shutdown Qualitative Risk Assessment Standard. EPRI, Palo Alto, CA: 2007. 1016231.

PRODUCT DESCRIPTION

This report documents development of a shutdown qualitative risk assessment (QLRA) standard. This standard has been developed in support of Working Group ANS-58.22 of the Standards Committee of the American Nuclear Society (ANS) in conjunction with ongoing efforts to develop a standard for low power and shutdown (LPSD) probabilistic risk assessments (PRAs). This Technical Update will provide a starting point for review and comment by the ANS Working Group and other interested parties on the proposed qualitative risk assessment standard.

Results and Findings

The report provides an overview of a proposed shutdown QLRA that embodies cumulative industry experience with QLRA methods. Also described are the technical elements of QLRA that are included in the proposed standard: safety functions (SF), end states (ES), plant operational states (POS), higher risk evolutions (HREs), and systems analysis (SY). To provide for consistent application of QLRA, the proposed Shutdown QLRA Standard has adopted several concepts shared by the American Society of Mechanical Engineers (ASME) PRA Standard and draft ANS LPSD PRA Standard. The applications of these concepts to QLRA, and exceptions to them, are discussed.

Challenges and Objectives

The goal of the proposed shutdown QLRA standard is to encompass all of the major elements of QLRA that are currently used in the nuclear industry. Using the high level requirements (HLRs), supporting requirements (SRs), capability indices, and peer review requirements, the objective is to provide a framework for QLRA quality that applies the ASME PRA Standard methodology to the distinctive characteristics of QLRA.

Applications, Values, and Use

Qualitative risk assessment is a proven method for configuration risk assessment and management in the nuclear industry. This report has been prepared to encourage discussion among stakeholders in the risk-informed standards and configuration risk management communities regarding the role of QLRA methods in LPSD configuration risk management. The proposed standard is an effort to codify requirements for consistent risk-informed methods and also capture improvements in a format consistent with the ASME PRA standard and the draft ANS LPSD PRA Standard, currently under development.

EPRI Perspective

The nuclear industry has many years of experience using configuration risk management (CRM) programs to support work planning, scheduling, and configuration control during LPSD conditions. The qualitative method has enhanced nuclear safety and provided a cost-effective framework for risk management. The proposed shutdown QLRA standard provided in this report represents a step forward in the development of LPSD configuration risk management by providing a structured process to achieve greater consistency within the industry and to recognize state-of-the-art practices.

Approach

The proposed standard retains the familiar elements of NUMARC 91-06—which provided the foundation for the methodology in the early 1990s—such as decay heat removal, inventory control, reactivity control, containment closure, and power availability. It also includes advances in the technology, such as improved rigor in the definition of plant operating states, and the potential for linking qualitative end states to quantitative evaluations.

Keywords

Low power and shutdown
Probabilistic risk assessment
Defense in depth
Standards

ACKNOWLEDGMENTS

Contributions to this report were made by Leo Shanley, of ERIN Engineering and Research, Steve Hess, of EPRI, Bryan Carroll, of Duke Energy, and Doug Hance, of EPRI.

CONTENTS

1
OVERVIEW

The nuclear industry has many years of operating experience using qualitative risk assessment (QLRA) methods based on defense-in-depth (DID) principles for configuration risk management (CRM). NUMARC 91-06 provided the foundation for the methodology in the early 1990s. The techniques have improved over the years such that the safety features typically monitored in the industry exceed the five key safety functions presented in NUMARC 91-06. In addition, recent research has documented successful QLRA methods and how to develop them in *Qualitative Risk Assessment Methods for Shutdown Risk Management, EPRI, Palo Alto, CA: 2006. 1013501*

A proposed Shutdown QLRA Standard is provided in Appendix A, which embodies cumulative industry experience with QLRA methods. The QLRA scope covered by this Standard is primarily concerned with evaluating Safety Function DID with respect to challenges normally considered as "internal events," excluding internal flooding, during shutdown conditions.

This standard also includes advancements in QLRA methods less widely used, considered to be higher quality practices in a graded format using the ASME Ra-Sc-2007 PRA standard Capability Category model as a template. In lieu of using the ASME PRA Standard Capability Category definitions, this standard uses QLRA-specific definitions, called Capability Indices. In doing this, the proposed standard provides a two-fold path for the future of qualitative risk assessment.

- First, it provides guidance for the advancement and improvement of existing QLRA methods through the Capability Indices and peer review process. The graded quality template for QLRA, supplemented by a peer review process will provide a better basis for comparison from one QLRA method to another and it will enable nuclear operating companies to more objectively assess QLRA method quality. In so doing, the process set forth in this standard will provide confidence in the continuing role of QLRA methods in protecting the health and safety of the public and complying with 10CFR50.65(a)(4).
- Second, it provides for benchmarking of qualitative methods against quantitative methods. The requirements that implement these portions of the standard are represented by Capability Index 3 elements that will recognize the efforts of nuclear operators who seek to link their QLRA methods to quantitative evaluations. This will provide an additional level of confidence in the results provided by QLRA methods.

2
SHUTDOWN QLRA TECHNICAL ELEMENTS

This section provides a description of the technical elements of QLRA that are included in the proposed standard. These elements are Safety Functions (SF), End States (ES), Plant Operational States (POS), Higher Risk Evolutions (HREs), and Systems Analysis (SY).

Safety Functions

As described in NUMARC 91-06, the key safety functions typically included in a QLRA are as follows:

- *DECAY HEAT REMOVAL CAPABILITY: The ability to maintain reactor coolant system (RCS) temperature and pressure, and spent fuel pool (SFP) temperature below specified limits following a shutdown.*
- *INVENTORY CONTROL: Measures established to ensure that irradiated fuel remains covered with coolant to maintain heat transfer and shielding requirements.*
- *REACTIVITY CONTROL: Measures established to preclude inadvertent dilutions, criticalities, power excursions or losses of shutdown margin, and to predict and monitor core behavior.*
- *CONTAINMENT CLOSURE: The action to secure primary (PWR) or secondary (BWR) containment and its associated structures, systems, and components as a FUNCTIONAL barrier to fission product release under existing plant conditions.*
- *ELECTRICAL POWER AVAILABILITY: Measures established to maintain power availability in support of maintaining other safety functions. [NOTE: Definition not explicitly provided in NUMARC 91-06]*

End States

The metric for reporting QLRA DID for a safety function is an end state representing the extent of DID capability for a safety function. Typically the extent of DID is represented by a color, a numeric integer value (where the value represents the number of available trains or methods available to support the safety function), or other qualitative measures of DID status. Table 2-1 shows an example of these metrics.

Table 2-1 Example Risk Metrics

COLOR	METRIC	STATUS OF SAFETY FUNCTION
GREEN	ACCEPTABLE	Very high or maximum level of DID. Lowest risk level. Configurations with this DID do not require additional actions to manage risk (i.e. normal work controls are sufficient).
YELLOW	REDUCED	Adequate DID. Slightly elevated risk level, but still relatively low risk. Configurations with this DID may take actions to minimize the duration of exposure and/or implement compensatory actions to reduce risk.
ORANGE	MINIMAL	Reduced DID. Elevated risk, but tolerable for short durations. Configurations with this DID require detailed planning for the configuration including compensatory actions to minimize exposure time, and contingency planning to restore and/or protect alternate means of supporting the safety function. Typically represents the case where a single failure will result in loss of DID for the safety function.
RED	UNACCEPTABLE	Unacceptable DID characterized by the inability to support the safety function. Risk is unacceptably high and not tolerable for any duration. Typically represents a state that will not be planned for or entered voluntarily.

Plant Operational States (POS)

The draft ANS LPSD PRA Standard discusses the importance of "plant operational states" (POS). The need for POS comes directly from differences between LPSD and full power.

Full-power operations can be considered as a relatively static set of conditions, controlled within a narrow band of physical parameters (i.e., temperature, pressure, and decay heat), with operating and maintenance alignments limited by Technical Specifications, in contrast to the range of low power and shutdown conditions. During full-power operations, the basic plant configuration, defined as the mitigating systems fulfilling the critical safety functions (reactivity control, decay heat removal, injection capability) and the barriers to release (the reactor coolant system pressure boundary and containment) remain relatively unchanged. The primary focus of the plant during power operations is to maximize the time at full power producing electricity and to minimize the impact of test and maintenance activities.

During low-power and shutdown operations, the focus shifts to test and maintenance activities, temporarily forgoing the capability to produce electricity in order to refuel and/or to ensure equipment is maintained to assure reliable operation. Low-power and shutdown operations present a relatively dynamic situation when compared to full-power operations, consisting of a number of distinct and significantly different sets of plant configurations. These varying plant configurations are required in order to accomplish the refueling, maintenance, and testing activities associated with an outage.

For example, in order to move fuel assemblies during a refueling outage, the reactor vessel head must be removed, which in turn requires the reactor coolant system to be depressurized with temperature below 200°F, and decay heat removal provided by the residual heat removal system.

A refueling outage typically provides the widest range of low-power and shutdown configurations and activities of the historical outages types. The distinctions in plant configuration generally can be categorized into the following general plant states. These distinctions apply to both pressurized water reactor (PWR) and boiling water reactor (BWR) types.

- Full Power - Nominal full power includes small reductions in power that may be required for on-line testing and maintenance.
- Low Power - Power levels at which major secondary components are out of service as a plant shuts down or starts up. This is typically a transition mode to/from hot/cold shutdown. Designated as Startup in a BWR when transitioning from cold shutdown to power operations.
- Hot shutdown - zero power, non-critical state where temperature and pressures are still relatively high. This is typically a transition mode to cold shutdown or refueling. The plant uses steaming as the primary means of decay heat removal.
- Cold shutdown – plant state where the primary temperature and pressures are relatively low. The plant uses the residual heat removal system for decay heat removal. The reactor coolant system pressure boundary remains generally intact.
- Refueling – in this plant state, the primary system is depressurized with low temperature. The plant uses the residual heat removal system for decay heat removal. The reactor coolant system is opened for fuel movement.

Within these different plant states, there are also key differences in plant operation relating to the plant's ability to prevent or mitigate a core damage event that would lead to a release of radionuclides. These differences are related to decay heat removal mechanisms, system and component success criteria, and barriers to release.

The use of plant operating states (POS) is the modeling technique used to account for the impact of the LPSD plant states on the risk assessment. Full power operations can be considered as one plant operating state, and this state could be evaluated with one set of specific operating and maintenance alignments. During an outage, the plant transitions through a number of low-power and shutdown plant operating states, each with many operating and maintenance alignments.

Within each of the LPSD plant operating states, the plant differences described above are reflected as differences in the safety function requirements and capabilities (and hence the DID models), resulting in important differences in risk end state results. In some POS (e.g., PWR midloop operation) the risk represented by the Decay Heat Removal safety function will be much higher than while in other POS (e.g., PWR reactor cavity flooded) with the same equipment available. These differences are due primarily to the reactor coolant system (RCS) configuration, decay heat removal mechanisms available, and time to respond to a challenge.
Thus, the concept of a POS is an information management technique to handle the numbers of different states the plant can be in during an outage.

Higher Risk Evolutions

Higher Risk Evolutions (HREs) are defined in NUMARC 91-06 as "outage activities, plant configurations or conditions during shutdown where the plant is more susceptible to an event causing the loss of a key safety function." HREs consist of: (1) activities or events with the potential to directly challenge the success state of a safety function, (2) activities or events with the potential to cause an unplanned loss of one or more systems supporting the safety function.

An HRE presents a challenge to the success of one or more safety functions. If an activity, event or configuration increases the likelihood of challenging a Safety Function, then it can be considered an HRE. In a QLRA, an HRE is manifested as a degradation of DID. Examples of HREs include switchyard maintenance and activities with the potential to drain the RCS or reactor vessel.

System Analysis

System Analysis for a QLRA differs from that associated with a PRA. Specifically, system models developed for QLRAs are primarily concerned with SSC unavailability/availability, as opposed to failure modes and probabilities. However, many of the steps needed for a PRA System Analysis are the same, including gaining an understanding of system operation, system success criteria, and support system impacts. The purpose of the systems analysis is to identify the success criteria and the causes of unavailability for each plant system represented in the safety function DID analysis.

In summary, the basic elements of a QLRA are the key safety functions to be monitored and the supporting logic, higher risk evolutions that impact the safety functions, the end states that provide qualitative measures of risk and management guidance for particular configurations, and the plant operational states that provide boundary conditions for each configuration.

3
SHUTDOWN QLRA COMPARISON TO PRA STANDARDS

To provide for consistent application of QLRA, the proposed Shutdown QLRA Standard has adopted several concepts shared by the ASME PRA Standard and draft ANS LPSD PRA Standard. The applications of these concepts to QLRA, and exceptions to them, are noted below.

High Level Requirements – The Shutdown QLRA standard includes the following HLRs: End States (ES), Plant Operational States (POS), Safety Functions (SF), Higher Risk Evolutions (HRE), and Systems Analysis (SY)

Supporting Requirements - The SRs for each of the QLRA Elements are presented in Section 4 of the standard as action statements, using the Capability Indices described in Section 1.5 of the standard. For each Capability Index, the SRs define the minimum requirements necessary to meet that Capability Index.

Capability Indices - Similar to the Capability Categories in the ASME PRA Standard, this standard provides for three Capability Indices. These indices manifest themselves through the presence of (potentially) three different Supporting Requirements (SRs) for each technical issue covered, written to address the three different capability levels. Note that when an action statement in a Supporting Requirement spans multiple Capability Indices, it applies equally to each Capability Index. When necessary, the differentiation between Indices is made in other associated Supporting Requirements.

As used in the ASME PRA Standard and the draft ANS LPSD Standard, the Capability Categories are a metric of the PRA's capability to be used in a wide variety of applications. In the case of the proposed shutdown QLRA standard, the application is limited to configuration risk management in support of 10CFR50.65(a)(4). Accordingly, the standard has been written to assess QLRA capabilities for each Supporting Requirement using the Capability Indices, rather than by specifying a "capability level" or grade for the overall QLRA.

In addition, the application of the QLRA standard has been intentionally limited to shutdown conditions. This is not a technical limitation of the technology, but rather an attempt to codify current standard practice in the industry and to complement current efforts to implement risk-managed technical specifications (RMTS). Virtually all nuclear operators in the United States use QLRA methods for cold shutdown and refueling conditions. The applicability of RMTS includes operating modes 1 and 2 for both PWRs and BWRs, as described in NEI 06-09, Risk-Informed Technical Specifications Initiative 4b Risk-Managed Technical Specifications (RMTS) Guidelines. Accordingly, the Shutdown QLRA standard applies to cold shutdown, refueling, hot shutdown, hot standby (PWR) and equivalent modes for BWRs.

Peer Review – A peer review process, modeled after the ASME PRA Standard, has been codified in the proposed Shutdown QLRA Standard. The peer review team is comprised of at least two members for a period of 3 days. Since the scope of a QLRA is typically less than a PRA, the number of reviewers and duration are less. This is consistent with the reduced scope peer review specified in the ASME PRA Standard for revisions to a PRA. The peer review process in the shutdown QLRA standard encompasses all of the SR elements for each of the HLRs, End States (ES), Plant Operational States (POS), Safety Functions (SF), Higher Risk Evolutions (HRE), and Systems Analysis (SY)

4
SUMMARY

The proposed shutdown QLRA standard provided in Appendix A encompasses all of the major elements of QLRA that are currently used in the nuclear industry and includes improved practices as well. The proposed standard retains the familiar elements of NUMARC 91-06, such as decay heat removal, inventory control, reactivity control, containment closure, and power availability. It also includes advances in the technology, such as improved rigor in the definition of plant operating states, and the potential for linking qualitative end states to quantitative evaluations.

The HLRs, SRs, Capability Indices, and Peer Review requirements provide a framework for QLRA quality that applies the ASME PRA Standard methodology to the distinctive characteristics of QLRA. The SRs and Capability Indices are written with rigor and an appropriate level of detail. The standard is applicable to plant shutdown conditions, and QLRA methods contain a fewer number of HLRs than PRAs do. Accordingly, the peer review requirements, while less extensive than that for a PRA, provide sufficient depth to ensure a detailed review.

The proposed standard captures the technical elements of quality QLRA methods and a rigorous process derived from the ASME PRA standard. This provides for continuing confidence in QLRA methods to protect the health and safety of the public and a path for improvement. This report has been prepared to encourage discussion among stakeholders in the risk-informed standards and configuration risk management communities regarding the role of qualitative risk assessment (QLRA) methods in LPSD configuration risk management.

5
REFERENCES

ASME Ra-Sc-2007, Addenda To ASME Ra-S-2002, “Standard For Probabilistic Risk Assessment For Nuclear Power Plant Applications,” Addenda C

American Nuclear Society Low Power and Shutdown PRA Standard Draft 7a, September 2005

Nuclear Management and Resources Council, NUMARC 91-06, "NUMARC Guidelines for Industry Actions to Assess Shutdown Management,” Nuclear Management and Resources Council, December 1991.

Qualitative Risk Assessment Methods for Shutdown Risk Management, EPRI, Palo Alto, CA: 2006. 1013501

NEI 06-09 (Revision 0) – A, Risk-Informed Technical Specifications Initiative 4b, Risk-Managed Technical Specifications (RMTS) Guidelines, November 2006

A
SHUTDOWN QUALITATIVE RISK ASSESSMENT STANDARD

SECTION 1

INTRODUCTION

1.1 Scope

This Standard sets forth requirements for Qualitative Risk Assessments (QLRAs) using Defense-In-Depth (DID) principles to support risk assessment and management for low-power and shutdown (LPSD) operations of commercial light water nuclear power plants within the limitations of the plant Technical Specifications. This Standard is applicable to the cold shutdown, refueling, hot shutdown, and hot standby modes of operation (modes 5 and 6 for PWRs and modes 3, 4 and 5 for BWRs, based on the mode definitions for improved Technical Specifications). The use of QLRA is recognized by NUMARC 93-01 [1] as a method to assess and manage the risk of maintenance activities, as required by 10CFR50.65(a)(4) (the "Maintenance Rule"). Since the development of NUMARC 91-06 [2], it has been the primary method used within the industry for risk assessments and Configuration Risk Management (CRM) during shutdown and refueling conditions.

The QLRA scope covered by this Standard is primarily concerned with evaluating Safety Function DID with respect to challenges normally considered as "internal events," excluding internal flooding. This is not to say that Safety Function DID for "external events" (including internal fires) cannot be evaluated using the requirements set forth herein, but that is not the primary emphasis of this standard.
This Standard also includes advancements in QLRA methods less widely used, that represent higher quality and "best" practices in a graded format using the ASME Ra-Sc-2007 PRA Capability Category model as a template. In lieu of using the ASME PRA Standard Capability Category definitions, this standard uses QLRA-specific definitions, called Capability Indices. In doing this, the Standard provides a two-fold path for the future of qualitative risk assessment.

- First, it provides guidance for the advancement and improvement of existing QLRA methods through the Capability Indices and peer review process. The graded quality template for QLRA, supplemented by a peer review process will provide a better basis for comparison from one QLRA method to another and it will enable nuclear operating companies to more objectively assess QLRA method quality. In so doing, the process set forth in this standard will provide confidence in the continuing role of QLRA methods in protecting the health and safety of the public and complying with 10CFR50.65(a)(4).
- Second, it provides for benchmarking of qualitative methods against quantitative methods. The requirements that implement these portions of the standard are represented by Capability Index 3 elements that will recognize the efforts of nuclear operators who seek to link their QLRA methods to quantitative results. This will provide an additional level of confidence in the QLRA methods.

1.2 Relationship to PRA Standards

This Standard is intended to augment and compliment the ANS LPSD PRA Standard [3]. Since the qualitative method is the primary method employed to manage shutdown risk at U.S. nuclear power plants, this Standard is intended to ensure consistent and accurate risk-informed decisions are reached. This Standard follows a similar convention and nomenclature as ASME Internal Events PRA Standard [4] and the ANS LPSD PRA Standard [3]. Where applicable, the same HLR and SR are used (e.g., in the SY section).

1.3 Special Considerations

The technical basis for QLRA methods has developed since the implementation of NUMARC 91-06 [2]. LPSD QLRA methodology has several special considerations that are included throughout the technical requirements. Attachment 1 to this Standard provides an approach to analyze plant operational states. A summary of the current technical basis for QLRA is provided in Attachment 2 to this Standard based on EPRI TR-1013501 [5]. Four of these special considerations for QLRA are described below.

1.3.1 Risk Definition and Risk Assessment Techniques - The definition of risk in the context of QLRA can be characterized as a surrogate measure of the traditional risk definition of frequency multiplied by consequence. Although characteristically there are corollaries to the traditional risk definitions, the measures represent different perspectives of safety. For example, a typical QLRA measures key safety function DID as defined and described in NUMARC 91-06 [2]. Increased DID for a key safety function correlates to reduced risk, while reduced DID of key safety functions represents increased risk. In this regard, the measures are the antithesis of each other.

Traditional quantitative risk assessments address the initiating event likelihood (frequency), capabilities of systems and operator performance to mitigate the event and the consequence for failure of the mitigation measure (e.g. boiling, core damage and large early release end state consequences). QLRA applies similar risk considerations. For QLRA, changes in initiating event frequencies are represented by higher risk evolutions (HREs) or those activities with the potential to reduce capability or challenge key safety function DID. Additionally, initiating event frequencies may change as the Plant Operating State (POS) changes, based on the plant conditions, such as reactor coolant system (RCS) inventory. Availability of systems to support key safety functions are addressed similar to the mitigation systems, when applied in tools that consider dependencies and integrated logic assessments. Operator actions are implicitly considered in the availability of systems/components that are not automatically initiated (e.g., feed and bleed cooling in a PWR, standby liquid control injection in a BWR). The end states of QLRA are consequences ranging from degraded to lost safety functions. For some end states, loss of a key safety function can be associated with a traditional PRA end state. For example, a sustained loss of the decay heat removal safety function will result in a core damage end state, and when combined with the loss of containment integrity can be correlated to radionuclide release.

The risk definition in a QLRA complements the quantitative risk definition of frequency of event multiplied by consequence of event:

Table A1.3.1-1 Quantitative Versus Qualitative Risk Assessments

RISK METHOD	*FREQUENCY OF EVENT*	*CONSEQUENCE OF EVENT*
Quantitative	*Likelihood of initiating event and probability that event mitigation capabilities fail*	*Typically core damage or large early release*
Qualitative	*DID assessment considering potential for initiating events (including higher risk evolutions) and relative reliability and availability of safety function mitigation capabilities*	*Loss of safety function, which in some cases can be correlated to core damage or large early release.*

One benefit of the DID approach is that the information can be presented in a format understandable to typical plant operators, engineers and managers. Plant staff can better understand that an activity can challenge a safety function and functional availability of equipment/capabilities rather than numerical frequencies of occurrence and probabilities of failure. For example, Emergency Operating Procedures (EOP) and Functional Recovery Guidelines focus on recovery of safety functions. Similarly, the status of a safety function provides for more focus and understanding of the challenge to nuclear risk and appropriate risk management actions, as opposed to core damage or large early release frequencies.

Furthermore, the approach provides an accurate and repeatable process to categorize the relative risk of plant configurations so that management can implement appropriate risk management actions, thus ensuring that adequate levels of nuclear safety are maintained.

1.3.2 Defense In Depth - The DID concept has served as a standard in the design and operation of nuclear power facilities since early in the genesis of commercial nuclear power. The inherent considerations of redundancy and diversity of safety systems are readily apparent in the design of operating commercial facilities. The concept of DID provided the safety margin and risk management capabilities successfully in those early years, in the absence of technologies and capabilities to perform current state of the art risk modeling and simulation.

Defense-in-depth is measured by number, redundancy and diversity of systems, structures and components (SSCs) which are needed to mitigate challenges to the respective safety function(s). The DID concept addresses the goal of maintaining multiple barriers to radionuclide release. This includes maintaining key safety functions from both an operational context (in operating procedures) and in evaluation of mitigation capabilities. Multiple frontline and support systems operate to satisfy the safety function requirements.

DID for shutdown can be seen as providing SSCs to ensure backup of key safety functions using redundant, alternate and diverse systems. The key safety functions identified for shutdown in NUMARC 91-06 include:

- *DECAY HEAT REMOVAL CAPABILITY: The ability to maintain reactor coolant system (RCS) temperature and pressure, and spent fuel pool (SFP) temperature below specified limits following a shutdown.*
- *INVENTORY CONTROL: Measures established to ensure that irradiated fuel remains covered with coolant to maintain heat transfer and shielding requirements.*
- *REACTIVITY CONTROL: Measures established to preclude inadvertent dilutions, criticalities, power excursions or losses of shutdown margin, and to predict and monitor core behavior.*

- *CONTAINMENT CLOSURE: The action to secure primary (PWR) or secondary (BWR) containment and its associated structures, systems, and components as a FUNCTIONAL barrier to fission product release under existing plant conditions.*
- *ELECTRICAL POWER AVAILABILITY: Measures established to maintain power availability in support of maintaining other safety functions. [NOTE: Definition not explicitly provided in NUMARC 91-06]* [2]

1.3.3 Defense In Depth Metrics - The metric for reporting QLRA DID for a safety function is an end state representing the extent of DID capability for a safety function. Typically the extent of DID is represented by a color, a numeric integer value (where the value represents the number of available trains or methods available to support the safety function), or other qualitative measures of DID status. Table 1.3.3-1 represents an example of these metrics.

Table A1.3.3-1 Example Risk Metrics

COLOR	METRIC	STATUS OF SAFETY FUNCTION
GREEN	ACCEPTABLE	Very high or maximum level of DID. Lowest risk level. Configurations with this DID do not require additional actions to manage risk (i.e. normal work controls are sufficient).
YELLOW	REDUCED	Adequate DID. Slightly elevated risk level, but still relatively low risk. Configurations with this DID may take actions to minimize the duration of exposure and/or implement compensatory actions to reduce risk.
ORANGE	MINIMAL	Reduced DID. Elevated risk, but tolerable for short durations. Configurations with this DID require detailed planning for the configuration including compensatory actions to minimize exposure time, and contingency planning to restore and/or protect alternate means of supporting the safety function. Typically represents the case where a single failure will result in loss of DID for the safety function.
RED	UNACCEPTABLE	Unacceptable DID characterized by the inability to support the safety function. Risk is unacceptably high and not tolerable for any duration. Typically represents a state that will not be planned for or entered voluntarily.

1.3.4 Plant Operational States (POS) - The draft ANS LPSD PRA Standard [3] discusses the importance of "plant operational states" (POS). The need for POS comes directly from differences between LPSD and full power.

Differences in Plant Operations from Full Power to LPSD - Full-power operations can be considered as a relatively static set of conditions, controlled within a narrow band of physical parameters (i.e., temperature, pressure, and decay heat), with operating and maintenance alignments limited by Technical Specifications in contrast to the range of low power and shutdown conditions. The basic plant configuration, defined as the mitigating systems fulfilling the critical safety functions (reactivity control, decay heat removal, injection capability) and the barriers to release (the reactor coolant system pressure boundary and containment) remain relatively unchanged. The primary focus of the plant during power operations is to maximize the time at full power producing electricity and to minimize the impact of test and maintenance activities.

During low-power and shutdown operations, the focus shifts to test and maintenance activities, temporarily forgoing the capability to produce electricity in order to refuel and/or to ensure equipment is maintained to assure reliable operation. Low-power and shutdown operations present a relatively dynamic situation when compared to full-power operations, consisting of a number of distinct and significantly different sets of plant configurations. These varying plant configurations are required in order to accomplish the refueling, maintenance, and testing activities associated with an outage.

For example, in order to move fuel assemblies during a refueling outage, the reactor vessel head must be removed, which in turn requires the reactor coolant system to be depressurized with temperature below 200°F, with decay heat removal provided by the residual heat removal system.

A refueling outage typically provides the widest range of low-power and shutdown configurations and activities of the historical outages types. The distinctions in plant configuration generally can be categorized into the following general plant states. These distinctions apply to both pressurized water reactor (PWR) and boiling water reactor (BWR) types.

- Full Power - Nominal full power includes small reductions in power that may be required for on-line testing and maintenance.
- Low Power - Power levels at which major secondary components are out of service as a plant shuts down or starts up. This is typically a transition mode to/from hot/cold shutdown. Designated as Startup in a BWR when transitioning from cold shutdown to power operations.
- Hot shutdown - zero power, non-critical state where temperature and pressures are still relatively high. This is typically a transition mode to cold shutdown or refueling. The plant uses steaming as the primary means of decay heat removal.
- Cold shutdown – plant state where the primary temperature and pressures are relatively low. The plant uses the residual heat removal system for decay heat removal. The reactor coolant system pressure boundary remains generally intact.
- Refueling – in this plant state, the primary system is depressurized with low temperature. The plant uses the residual heat removal system for decay heat removal. The reactor coolant system is opened for fuel movement.

Within these different plant states, there are also key differences in plant operation relating to the plant's ability to prevent or mitigate a core damage event that would lead to a release of radionuclides. These differences are related to decay heat removal mechanisms, system and component success criteria, and barriers to release.

The Need for Plant Operating States (POS) - The use of plant operating states (POSs) is the modeling technique used to account for the impact of the LPSD plant states on the risk assessment. Full power operations can be considered as one plant operating state, and this state could be evaluated with one set of specific operating and maintenance alignments. During an outage, the plant may transition through a number of low-power and shutdown plant operating states, each with many operating and maintenance alignments.

Within each of the LPSD plant operating states, the plant differences described above are reflected as differences in the safety function requirements and capabilities (and hence the DID models), resulting in important differences in risk end state results. In some POSs (e.g., PWR midloop operation) the risk represented by, for example, the Heat Removal Safety Function DID will be much higher than while in other POSs (e.g., PWR reactor cavity flooded) with the same equipment available. These differences are due primarily to the reactor coolant system (RCS) configuration, decay heat removal mechanisms available, and time to respond to a challenge.

Thus, the concept of a POS is an information management technique to handle the numbers of different states the plant can be in during an outage. Section 2 presents definitions associated with the concept of

POS that are specific to this Standard and Section 4.5 provides the requirements for POSs. Additional information is provided in the ANS LPSD PRA Standard (e.g., Appendix A of that document), although there are some differences in POS evaluation for PRAs as compared to QLRAs.

1.4 Applicability

This Standard applies to QLRAs used to support configuration risk assessments as required by 10CFR50.65(a)(4) while in a shutdown condition. This Standard is applicable to the cold shutdown, refueling, hot shutdown, and hot standby modes of operation (modes 5 and 6 for PWRs and modes 3, 4 and 5 for BWRs, based on the mode definitions for improved Technical Specifications).
Section 3 addresses the risk assessment process.

1.5 Qualitative Capability Indices

Similar to the PRA Standards, which include Capability Categories, this Standard provides for three Capability Indices. These indices manifest themselves through the presence of (potentially) three different Supporting Requirements (SRs) for each technical issue covered, written to address the three different capability levels. Note that when an action statement in a Supporting Requirement spans multiple Capability Indices, it applies equally to each Capability Index. When necessary, the differentiation between Indices is made in other associated Supporting Requirements. A QLRA's capabilities are evaluated for each Supporting Requirement, rather than by specifying a "capability level" for the whole QLRA. Table 1.5-1 provides the bases for the QLRA Capability Indices.

1.6 Requirements for QLRA Elements

1.6.1 QLRA Elements - *The requirements for this Standard are organized by five elements that comprise an LPSD QLRA.. They and their abbreviations are as follows:*

(a) End States (ES)

(b) Plant Operational States (POS)

(c) Safety Functions (SF)

(d) Higher Risk Evolutions (HRE)

(e) Systems Analysis (SY)

The Plant Operational States element is similar to and based on the ANS LPSD Standard, and the System Analysis element is based on the ASME standard, modified to account for qualitative modeling. The other elements are unique to this QLRA Standard.

1.6.2 High Level Requirements - A set of Objectives and High Level Requirements (HLRs) are provided for each QLRA Element in Section 4. All QLRAs using this Standard shall satisfy each of these HLRs. The HLRs set forth the minimum requirements for meeting this Standard in general terms and present the top level logic for the derivation of the more detailed Supporting Requirements (SRs) for each of the QLRA Capability Indices. The HLRs reflect not only the diversity of approaches but also the need to accommodate future technological innovations. Hence, they are general in nature.

1.6.3 Supporting Requirements - The SRs for each of the QLRA Elements are presented in Section 4 as action statements, using the Capability Indices described in Section 1.5. For each Capability Index, the SRs define the minimum requirements necessary to meet that Capability Index.

The SRs specify what to do rather than how to do it, and, in that sense, specific methods for satisfying the requirements are not prescribed. Nevertheless, certain established methods were contemplated during the development of these requirements. Alternative methods and approaches to the requirements of this Standard may be used if they provide results that are equivalent or superior to the methods usually used and they meet the HLRs and SRs presented or referenced in this Standard. The use of any particular method for meeting an SR shall be documented and shall be subject to review by the peer review process described in Section 5.

Table A1.5-1 Bases for QLRA Capability Indices

Attributes of QLRA	I	II	III
1. Scope and level of detail: The degree to which the scope and level of detail of plant design, operation, and maintenance are modeled.	Resolution and specificity sufficient to identify the contributors to loss of key safety functions. Modeling is at the system and/or train level.	Resolution and specificity sufficient to identify the significant contributors to degradation and loss of key safety functions. Modeling is at the train and super-component level. [Note (2)]	Resolution and specificity sufficient to determine the relative importance of the significant contributors to degradation and loss of key safety functions. Modeling is at the super-component and component level. [Note (2)]
2. Plant Specificity	Use of generic information, analyses or evaluations that account for unique design features of the plant.	Use of plant-specific information, analyses or evaluations for determining SSC, HRE and POS impact on key safety functions.	Use of plant-specific information, analyses or evaluations, including quantitative risk or reliability calculations, for determining SSC, HRE and POS impact on key safety functions.
3. Logical Structure [Note (1)]	Departures from the logical structure of the qualitative method will have moderate impact on the conclusions and risk insights as supported by good practices [Note (3)].	Departures from the logical structure of the qualitative method will have small impact on the conclusions and risk insights as supported by good practices [Note (3)].	Departures from logical structure of the qualitative method will have negligible impact on the conclusions and risk insights as supported by good practices [Note (3)].

NOTES:
(1) The logical structure of a qualitative method includes any logic method used to represent interactions, e.g., a dependency matrix, logic trees, fault trees, safety system functional assessment trees, etc. Departures from the logical structure are assessments of conditions outside the logical model used, e.g., assessment of switchyard maintenance, or augmented cooling water sources not modeled. Such assessments may result in compensatory measures.
(2) The definition for Capability Indices II and III is not meant to imply that the scope and level of detail includes identification of every component, but only those needed for the function of the system being modeled.
(3) Differentiation from moderate, to small, to negligible is determined by the extent to which the impact on the conclusions and risk insights could affect a decision under consideration. This differentiation recognizes that the qualitative risk assessment would generally not be the sole input to a decision. A moderate impact implies that the impact is of sufficient size that it is likely that a decision could be affected; a small impact implies that it is unlikely that a decision could be affected, and a negligible impact implies that a decision would not be affected.

1.7 QLRA Configuration Control

QLRA configuration control SHALL be accomplished according to the requirements found in Section 5 pf this Standard. The objective of the QLRA Configuration Control Program is to ensure that the QLRA reflects the as-built, as-operated facility to a degree sufficient for the application in which the QLRA is used.

1.8 Peer Review Requirements

In order to conform to this Standard, a LPSD QLRA SHALL be peer-reviewed to evaluate the capability of each of its elements to support the intended applications. Section 5 provides the requirements for the peer review, which are based to some extent on the ASME standard (ASME-2005). General peer review requirements are supplemented by specific requirements applicable to LPSD QLRAs.

SECTION 2
ACRONYMS AND DEFINITIONS

The list of acronyms and definitions from ASME-2005 is adopted for this Standard by reference. The following *additional* acronyms and definitions are provided to ensure understanding of terms as they are used in this Standard.

2.1 Acronyms

ANS: American Nuclear Society
ASME: American Society of Mechanical Engineers
CRM: Configuration Risk Management
DHR: Decay Heat Removal
DID: Defense in Depth
HRA: Human Reliability Analysis
HRE: Higher Risk Evolution
LPSD: Low Power and Shutdown
OOS: Out of Service
P&ID: Piping & Instrument Diagram
POS: Plant Operational (or Operating) State
QLRA: Qualitative Risk Assessment
PRA: Probabilistic Risk Assessment (used interchangeably with probabilistic safety assessment, PSA)
RHR: Residual Heat Removal
SAR: Safety Analysis Report

2.2 Definitions

The definitions provided herein, especially those regarding plant modes, are provided for general reference and to provide a context within this Standard. In the implementation of this standard, applications should be governed by plant-specific definitions, such as the definitions provided by plant Technical Specifications.

activity: a personnel interaction with the plant, such as to conduct maintenance, to re-align the plant operating configuration, or to change plant operating parameters (e.g. power level).
cold shutdown: a set of POSs during which the reactor is subcritical with the primary system depressurized at (relatively) low temperature (<200ºF) and the reactor vessel intact (head on), with heat removal via RHR shutdown cooling. Cold shutdown is defined by Technical Specifications (Mode 5 for PWRs, Mode 4 for BWRs) for the condition with the primary temperature below 200ºF with the reactor vessel head tensioned.

defense in depth: the concept of maintaining multiple barriers to radionuclide release, accomplished through redundancy and diversity of safety systems, providing the appropriate safety margin needed to mitigate challenges to pre-defined safety functions.

full power: a POS during which the reactor power is at or near its normal designed value. In this POS, the primary system configuration (power level, pressure, temperature, boundaries, etc) is maintained essentially constant.

higher risk evolution: *"outage activities, plant configurations or conditions during shutdown where the plant is more susceptible to an event causing the loss of a key safety function"* [2].

hot shutdown: a set of POSs during which the reactor is subcritical with the primary system pressurized at elevated temperature. Hot shutdown is defined by Technical Specifications (Mode 4 for PWRs, Mode 3 for BWRs) for the condition with the primary temperature above 200ºF with the reactor vessel intact.

hot standby: a POS (or set of POSs) during which the reactor is subcritical with the primary system at or near normal operating temperature and pressure. Hot standby is defined by Technical Specifications (Mode 3 for PWRs, not used for BWRs) for the condition with the primary temperature above 350ºF with the reactor vessel intact.

Hot midloop: a POS (or set of POSs) in a PWR during which the water level in the reactor vessel is drained below the top of the hot leg, which occurs early in an outage when decay heat levels are relatively high. This evolution occurs to support primary system maintenance, such as steam generator tube inspection. This is also termed “early midloop” and typically occurs within the first week after shutdown. This is contrasted with “cold” or “late” midloop.

LPSD evolution: a series of connected or related activities, such as a reduction in power to a low level, or plant shutdown, followed by the return to full-power plant conditions. LPSD evolutions are modeled as a series of POSs. Outage types are a general type of a shutdown evolution, and a refueling outage is a specific example. Reducing power to 30% in order to conduct maintenance or an operational activity is another example of a low-power evolution. LPSD evolutions are characterized by a transition down to the POS where the activity is conducted, followed by a transition back to full power.

low power: a POS (or set of POSs) during which the reactor is at reduced power, below full-power conditions. In this POS, the power level may be changed as the reactor is shutting down or starting up. The power level that distinguishes full power and low power is the power level below which major plant evolutions are required to reduce or increase power (e.g., taking manual control of feedwater level).
mode: status of plant operation, as defined by plant technical specifications.
outage: the entire set of POSs with the plant subcritical. This term is used interchangeably with the term "shutdown."

outage types: term used to describe the general cause of the plant being at zero power. Different outage types result from maintenance and refueling requirements that necessitate different LPSD evolutions and resulting POSs. For example, a “refueling” outage type leads to cold shutdown with some or all of the fuel elements transferred out of the reactor pressure vessel; whereas a “maintenance” outage conducted at cold shutdown to repair steam piping would be a different outage type. Generally outage types are: hot shutdown (or hot standby), cold shutdown (secondary non-drained), cold shutdown (secondary drained), and refueling. Outage types can be further divided into planned refueling or maintenance outages and unplanned (forced) maintenance outages.

POS: plant operational (or operating) state. Each POS is a standard configuration of the plant during which the plant conditions are relatively constant, are modeled as constant, and are distinct from other configurations in ways that impact risk - e.g., core power level, primary water level, primary temperature, primary vent status, containment status, and decay heat removal mechanisms. A POS can be a steady state or represent a transition between steady state POSs. For example, full power and cold shutdown while on residual heat removal cooling may be two steady state POSs. In this example there may be one or two transition POSs to cover the range of temperatures and pressures the plant goes through in shutting down to cold shutdown. For example, a hot standby POS that covers a temperature range of 350°F to 200°F may be modeled as one POS with a temperature of 350°F. Note, the impacts of unavailability of individual systems or components due to test or maintenance are included as part of the quantification process rather than in the definition of the POS.

refueling: this term has two generally accepted meanings in the LPSD PRA context: (a) an outage type that occurs on a periodic basis, during which a portion of the spent nuclear fuel is replaced with new (unburned) fuel; and (b) a set of POSs during which the reactor vessel head is removed. The second definition is also a plant mode defined by Technical Specifications (Mode 6 for PWRs, Mode 5 for BWRs) for the condition during which the reactor vessel head is removed to allow fuel assemblies to be removed. In this Standard, the phrase “refueling outage” is used when the first meaning is implied.

shutdown: this term has two generally accepted meanings in the LPSD PRA context: (a) a POS during which the reactor power level is being decreased from full power to low power (as in “a normal plant shutdown is the first step in a refueling outage”) , and (b) the collection of POSs during which the reactor is subcritical . In this Standard, the phrase “plant shutdown” is used when the first meaning is implied. In general in this Standard, the second meaning is used (e.g., LPSD).

startup: this term has two generally accepted meanings in the LPSD PRA context: (a) a POS during which the reactor power level is increased from low power to full power following a plant outage, and (b) a plant mode defined by Technical Specifications (Mode 2) during which the power level is less than 5% with the reactor critical for PWRs or the position of the Mode Selector Switch for BWRs.

transition: a set of POSs during which the plant configuration is changing between normal, full-power heat removal and shutdown heat removal via RHR. For a refueling outage, transition states would include low power (shutdown, startup) and hot standby/shutdown.

SECTION 3
QUALITATIVE RISK ASSESSMENT EVALUATION PROCESS

3.1 Scope and Purpose

The scope and level of detail of this Standard are adequate to assess the quality of Qualitative Risk Assessment Methods used for Low Power and Shutdown conditions. QLRAs are used to assess and manage the risk of individual configurations during an outage, i.e., support the evaluations required by 10CFR65(a)(4) within the limitations of the plant Technical Specifications. The quality of a QLRA depends upon its capabilities as compared to this Standard. This section provides a general discussion of how to evaluate the QLRA and supplementary analyses or requirements that can be used.

It is recognized that some utilities have developed shutdown risk monitors that include both a QLRA component and a PRA component. This Standard shall be used to assess the quality of the QLRA component if it is used to implement 10CFR50.65(a)(4). Utilities that have a shutdown PRA can assess the quality of the PRA using ANSI/ANS 58.22-2007, "Low Power and Shutdown PRA Methodology". Note: Evaluation results are always subordinate to Technical Specification requirements .

3.2 Determination and Description of Capability Indices

Section 4 of this Standard sets forth SRs for three Capability Indices whose attributes are described in Subsection 1.5. The QLRA is evaluated against each SR to determine which Capability Index is met by the QLRA method. The following provides a description of each Capability Index:

- *Capability Index I:* Basic risk assessment of configurations. Provides the ability to perform an adequate risk assessment in support of the maintenance rule (a)(4) requirements,. Capability Index I requirements depend heavily on other inputs such as work week reviews, work practice precedents, or engineering judgment. Provides the capability to determine the safety function viability and identify important SSCs; however this Capability Index only provides limited capability to distinguish risk levels or rank SSCs by risk impact. It is expected that most current QLRAs will meet at least Capability Index I for most Supporting Requirements.
- *Capability Index II:* Graded risk assessment of configurations. Provides the ability to perform a risk assessment in support of the maintenance rule (a)(4) requirements, using a robust methodology. Provides capability to determine the level of safety function availability and/or degradation and the capability to identify SSCs important to the safety functions, with some ability to qualitatively rank SSCs by risk impact. It is expected that some current QLRAs will meet Capability Index II for a majority of the Supporting Requirements, and most should be able to be enhanced to Capability Index II with minimal to moderate effort. NOTE :The use of external inputs, such as work week reviews, work practice precedents, or engineering judgment are limited to those that are justified and documented.. Examples of this would include: 1) documented limitations of the QLRA method for specific configurations and compensatory measures to address them, 2) supplementary analyses used to support the risk assessment, and 3) procedures that provide for documented and reviewed evaluations of the QLRA of specific configurations.
- *Capability Index III:* Risk assessment of configurations which can be correlated to quantified risk values. Provides capability to determine the level of safety function availability or degradation, and correlate to quantified risk. Capability to identify SSCs important to the safety functions, with the ability to rank SSCs by risk impact. Few current QLRAs are expected to meet Capability Index III for a substantial number of Supporting Requirements.

3.3 Assessment of QLRA for Necessary Scope, Results, and Models

Determine if the QLRA provides the results needed to adequately assess the plant risk [for a given POS]. If some aspects of the QLRA are insufficient to assess the risk, then upgrade them according to the SRs of Section 4 for its corresponding Capability Index, generate supplementary analyses, or apply bounding deterministic criteria.

3.4 Comparison of QLRA Model to Standard

Determine if each part of the QLRA satisfies the SRs at the appropriate Capability Index. If the QLRA does not satisfy a SR for the appropriate Capability Index, then determine whether or not the difference is important. An example of an acceptable difference is when the difference is not applicable or does not affect the risk assessment.

If the difference is not important, then the QLRA is acceptable. If the difference is important, then either upgrade the QLRA to address the corresponding SRs stated in Section 4, generate supplementary analyses (see Subsection 3.5), or apply bounding deterministic criteria.

3.5 Use of Supplementary Analyses/Requirements

In the event that the scope of either the QLRA insufficient, supplementary analyses or requirements may be used. These supplementary analyses may involve deterministic methods such as bounding or screening analyses, and determinations made by an expert panel. They shall be documented.

SECTION 4
RISK ASSESSMENT TECHNICAL REQUIREMENTS

4.1 Purpose

The purpose of this section is to provide requirements by which adequate QLRA capability can be identified when a QLRA is used for LPSD risk assessment. The specific focus of this section is the set of the unique and specific requirements by which an adequate LPSD QLRA can be identified.
One methodology for developing a QLRA capable of performing risk assessments is provided in EPRI TR-1013501 [5]. This document describes the details and bases for establishing POS, end states and safety function success criteria in a QLRA. It is recognized that other methodologies have been used to develop the QLRA methods currently in use in the industry.

4.2 Process Check

Consistent with the ASME PRA Standard, the process of reviewing analyses and/or calculations used directly by the LPSD QLRA or used to support the LPSD QLRA shall be reviewed by knowledgeable individuals who did not perform those analyses or calculations. Documentation of this review may take the form of hand-written comments, signatures or initials on the analyses/calculations, formal sign-offs, or other equivalent methods. Review may also include demonstration, or acceptance testing, of the QLRA method.

4.3 Use of Expert Judgment

To the extent applicable in a QLRA, the requirements for the use of expert judgment outside the QLRA analysis team are the same as those described in Section 4.3 of the ASME PRA Standard [4], and are incorporated by reference.

4.4 End State Metrics

The end states of QLRA typically relate the status of a Safety Function (SF), and range from fully functional, to degraded, to complete loss of safety function capability. Consequences are a function of factors such as DID level, plant operating state, time after shutdown and duration of the degraded or SF loss condition. In some cases, loss of a key safety function can be associated with a quantitative PRA type of consequence (e.g., loss of decay heat removal safety function may result in a core damage end state).

The following list identifies potential consequences associated with the loss of each safety function:

- Loss of Decay Heat Removal
  - Core boiling
  - Core uncovery
  - Core damage
  - Fission product release

- Loss of Inventory Control
  - Core uncovery
  - Core damage
  - Fission product release

- Loss of Reactivity Control
  - Inadvertent criticality
  - Core boiling
  - Core damage

  - Fission product release

- Loss of Containment (closure)
  - Fission product release

- Loss of Power Availability
  - Loss of one or more safety functions (above)

For a given plant operating state (POS), the metric for reporting QLRA DID for a safety function is an end state representing the extent of DID capability for the safety function. Typically the extent of DID is represented by a color, a numeric value, or other qualitative measures which represent the relative DID status.

When choosing the end state metrics, sufficient levels should be selected such that SF degradation challenges can be effectively differentiated. One of the levels should be chosen to represent a SF condition that is deemed unacceptable (e.g., RED). The levels should include the ability to reflect the increased likelihood of a loss of the SF (i.e., Higher Risk Evolutions). Thus, a minimum of three levels of DID measures would be expected. Industry experience and common risk management practices suggest four levels of DID: unacceptable, minimal, reduced and adequate provide sufficient discrimination to represent levels of risk and permit appropriate levels of management attention to properly allocate resources and effectively manage risk. More than four levels provides better granularity, but may be too fine to realistically and accurately measure different levels of DID and to provide different levels of management attention (i.e., could lead to inconsistencies).

The purpose of this technical element is to define the end state metrics for use in a QLRA model, including the method for assigning plant configurations to an end state.

Objectives: The objective of the end state analysis is to define the means by which safety function capability is communicated and what combination of SSCs and Higher Risk Evolutions (HREs) are associated with each Safety Function and POS. The end states must have the following characteristics.

(a) End states must distinguish between Safety Function capabilities (e.g., acceptable versus unacceptable DID).

(b) End state definitions must be consistently applied to all Safety Functions

(c) Actions must be associated with end state results.

(d) End state definitions and bases must be documented.

TABLE A4.4-1 HIGH LEVEL REQUIREMENTS FOR END STATE METRICS (HLR-ES)

Designator	Requirement
HLR-ES-A	End state metrics shall be designed to represent the level of capability (e.g., Defense In Depth) for a safety function. A sufficient number of end state results should be defined such that safety function degradation challenges can be effectively differentiated. End states shall be consistently applied to all safety functions evaluated.
HLR-ES-B	For each POS and safety function, define the impact of available equipment, HRE status and intrinsic POS risk on each end state.
HLR-ES-C	Actions shall be associated with each end state result.
HLR-ES-D	The end state metrics shall be documented in a manner that facilitates application of the model, updates to the model, and peer review.

TABLE A4.4-2 Supporting Requirements for End State Metrics - High Level Requirement A

End state metrics shall be designed to represent the level of capability (e.g., Defense In Depth) for a safety function. A sufficient number of end state results should be defined such that safety function degradation challenges can be effectively differentiated. End states shall be consistently applied to all safety functions evaluated. (HLR-ES-A)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
ES-A1	DEFINE End State Metrics in a way that represents the capability of a safety function. *Comments*: Typically, end state metrics are defined to show the level of DID for a safety function.		
ES-A2	DEFINE end states so as to follow a recognizable progression from better to worse. *Comments*: Typically, end state metrics are defined as colors, numbers or some other qualitative descriptor.		
ES-A3	DEFINE end states in a manner that is consistent between safety functions (i.e., the end state means the same thing from one safety function to the next).		
ES-A4	ENSURE end state results reflect changes in the safety function capability.	ENSURE end state results are self-consistent *within* a safety function. *Comments*: This means that configurations with similar relative risk levels should be assigned the same end state result (e.g., color), while configurations with relatively higher or lower risk levels are assigned the proper end state metric compared to each other (within a safety function). However, it is not necessary that the absolute	End state results shall REPRESENT or BE CORRELATED with risk, based on a calculated value.

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
		risk associated with an end state in one safety function be consistent with the absolute risk associated with the same end state in a different safety function. *For example*: Decay Heat Removal Safety Function in a PWR with a 4-color system – 2 trains of DHR available with the cavity flooded should be evaluated as having relatively less risk than 2 trains of DHR available at mid-loop.	
ES-A5	DEFINE a minimum of two end state categories to differentiate between acceptable and unacceptable configurations.	DEFINE at least three end state categories. *Comments*: For example, unacceptable, minimal, adequate. It is preferred that 4 end states be defined (e.g., unacceptable, minimal, adequate, full DID). Note that more than 4 end state categories provides better granularity, but may require extensive benchmarking. Rare exceptions for individual safety function end states may be taken with justification. For example, a transition from green to red would normally not be considered Capability Index II. However, a documented justification that includes compensating factors, such as applicability to limited POSs, long operator action times or alternate means of mitigation can be considered as valid exceptions. However, in all cases where an exception is taken, both the exception and its basis shall be documented.	DEFINE at least three end state categories which are correlated to some risk value. *Comments:* It is preferred that 4 end states be defined.

TABLE A4.4-3 Supporting Requirements for End State Metrics - High Level Requirement B

For each POS and safety function, define the impact of available equipment, HRE status and intrinsic POS risk on each end state. (HLR-ES-B)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
ES-B1	For each POS, DEFINE the minimum set of equipment (i.e., success criteria) needed for a safety function to be supported.		
ES-B2	For each POS and safety function, DEFINE the type and number of SSCs needed for each end state result. *Comments*: This may be done using rules (e.g., N, N+1) and/or by specifying exact combinations of SSCs and/or POS. For example, in a BWR with the RPV level is high, fewer ECCS trains are required to be available to maintain adequate DID.		CORRELATE the POS and number of available SSCs with a risk value, in order to assign and end state result.
ES-B3	No requirements for Capability Index I.	CONSIDER AND REPRESENT the POS impact alone on the end state result. *Example:* Midloop in PWR may be evaluated with a higher risk endstate than loops filled, even with the same SSCs available.	CORRELATE the POS with a risk value.
ES-B4	CONSIDER the impact of HREs on the end state result.	EVALUATE the types of HREs and DETERMINE whether HREs should be binned, based on their impact to the Safety Function. If warranted, GROUP HREs based on their impact and INCORPORATE appropriately in the evaluation of end state results.	Evaluate the impact of each specific HRE on the end state result.
ES-B5	CONSIDER time-dependent effects. At a minimum, decay heat levels based on decay heat curves or analyses must be identified and included in the method	CONSIDER time-dependent effects. Decay heat levels are identified and included in the method. CONSIDER integrated effects in the method. Example: Multiple orange results for Key Safety Functions are considered for equivalency to a red condition, by evaluation or definition.	CONSIDER time-dependent effects. Decay heat levels are identified and included in the method. Cumulative and integrated effects are also included in the method. Examples: Water level is monitored as an input. Time-to-boil is calculated based on system parameters. Multiple orange results for Key Safety Functions are considered for equivalency to a red condition, by evaluation or definition.

TABLE A4.4-4 Supporting Requirements for End State Metrics - High Level Requirement C

Actions should be associated with each end state result. (HLR-ES-C)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
ES-C1	ASSOCIATE general risk management actions or statements with each end state. Example: Green – No action required Yellow – Heightened Risk Awareness Orange – Outage Manager Approval Required Red – Not allowed.	ASSOCIATE specific management action levels for each end state. *Example:* Green – Normal configuration management controls. No actions required Yellow – Contingency actions required and Outage Manager approval Orange – Contingency actions required and approved by Outage Manager. General Manager – Plant Operations approval required for entry into any Orange condition. Red – Prohibited	

TABLE A4.4-5 Supporting Requirements for End State Metrics - High Level Requirement D

The end state metrics shall be documented in a manner that facilitates application of the model, updates to the model, and peer review. (HLR-ES-D)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
ES-D1	End State Definitions DOCUMENT end state definitions. DOCUMENT the process and criteria used to define the end state metrics. DOCUMENT the defining characteristics of each end state.		
ES-D2	NA	End State Results Self-consistent. DOCUMENT the process used to validate self-consistency.	End State Results Represent Risk DOCUMENT how the end state results are correlated to risk.
ES-D3	End State Results Based on POS, SSCs and HREs DOCUMENT the basis for the minimum equipment required for each safety function and POS. DOCUMENT the rules used and/or combination of SSCs needed for each end state result. DOCUMENT how POS risk is accounted for in end state results. DOCUMENT how and why HREs affect the end state result.		Risk impact of POS, SSCs and HREs correlated to risk In addition to the Capability Index I/II requirements, DOCUMENT how the combination of POS, SSC and HREs are correlated to risk.
ES-D4	Actions Associated With End States DOCUMENT required actions associated with each end state and basis thereof.		

4.5 Plant Operating States (POS)

Objectives: The objective of the POS analysis is to define multiple sets of unique reactor and plant conditions that cover the entire spectrum of low-power and non-power operation that provide constant boundary conditions within each POS for evaluation of key safety functions. The POS analysis must have the following characteristics.

(a) Each low-power and shutdown state required to be considered for the specific application is identified and characterized as to all important conditions affecting the delineation and evaluation of the key safety functions.

(b) Low-power and shutdown states that are subsumed into each other must be shown to be represented by the characteristics of the subsuming group.

(c) Low-power and shutdown states are divided into POSs based on the unique impact on plant response to safety function challenges. A POS may represent a static or transitional plant configuration.

(d) Decay heat levels are characterized. The relationship between decay heat level, reactor level and pressure, and the systems capable of satisfying safety functions must be well defined. This can be done at the POS level, but may also be done at the system level.

(e) The POS development and grouping are documented.

TABLE A4.5-1 HIGH LEVEL REQUIREMENTS FOR PLANT OPERATIONAL STATE ANALYSIS (HLR-POS)

Designator	Requirement
HLR-POS-A	Using a structured, systematic process, the POS analysis shall identify and characterize a set of plant states during low-power and shutdown operations that are representative of all the plant states to be evaluated using the QLRA.
HLR-POS-B	The POS analysis shall justify any grouping of POSs to facilitate the practicality and efficiency of the qualitative assessment. POSs with less limiting characteristics may be grouped with a state with more limiting characteristics.
HLR-POS-C	If desired, the POS definitions may include the representative decay heat levels associated with each POS. At a minimum, decay heat levels must be factored into determining the capability of systems to meet certain safety functions (e.g., see supporting requirements SF-C2 and SF-C3).
HLR-POS-D	The POS analysis shall be documented in a manner that facilitates application of the model, updates to the model, and peer review.

TABLE A4.5-2 Supporting Requirements for Plant Operational State Analysis - High Level Requirement A

Using a structured, systematic process, the POS analysis shall identify and characterize a set of plant states during low-power and shutdown operations that are representative of all the plant states to be evaluated using the QLRA. (HLR-POS-A)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
POS-A1	INCLUDE the following plant operating modes in the definition of the Plant Operating States (POS): • Refueling • Cold Shutdown Note: For plants using Improved Technical Specifications, this applies to modes 5 and 6 for PWRs and modes 4 and 5 for BWRs.		INCLUDE the following plant operating modes in the definition of the Plant Operating States (POS): • Refueling • Cold Shutdown • Hot Shutdown • Hot Standby (PWR) Note: For plants using Improved Technical Specifications, this applies to modes 3, 4, 5, and 6 for PWRs and modes 3, 4, and 5 for BWRs.
POS-A2	IDENTIFY a representative set of LPSD evolutions (low-power and shutdown evolutions or outage types include refueling outage, drained-down maintenance outage, non-drained maintenance outage, hot shutdown) to be modeled. *Comment:* The LPSD evolutions to be analyzed depend on the application and outage(s) to be modeled. The qualitative methods employed, end state metrics, and inputs correlate with both the outage type and the POS.		

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
POS-A3	For each LPSD evolution, REVIEW plant specific documentation (such as Technical Specifications, normal shutdown, refueling and startup procedures) and records (such as recent outage plans and records, maintenance plans and records, operations data, trip history and control room logbooks) for the following: • Reactor Coolant System Technical Specification mode of operation. • Reactor Coolant System configurations, such as vented or not vented; presence of vessel internals (which in some plants changes the decay heat removal mechanism from natural circulation basin cooling to forced circulation on the RHR system); and decay heat removal mechanisms, such as steaming or residual heat removal. • Reactor Coolant System parameters, e.g. power level or decay heat level, temperatures, pressures, and water level • Activities changing RCS configuration and parameters used to define the POS, e.g., draindown, filling and venting, dilution, and/or cooldown. • Fuel and Control Rod Status (e.g., fuel movement to/from fuel pool, fuel shuffling) • Containment Requirements (e.g., integrity required) *Comment:* During shutdown, decay heat level is determined by the time after shutdown. For QLRAs, system alignments, component maintenance unavailabilities, and containment status are typically variables within a POS, as opposed to being used to define the POS		
POS-A4	DEFINE the characteristics of each Plant Operational State in terms of unique combinations of: • Reactor Coolant System Technical Specification mode of operation. • Reactor Coolant System configurations, such as vented or not vented; and decay heat removal mechanisms, such as steaming or residual heat removal. • Reactor Coolant System parameters, e.g. power level or decay heat level, temperatures, pressures, water levels. • Activities changing RCS configuration and parameters used to define the POS, e.g., draindown, filling and venting, dilution, and/or cooldown. • Fuel and Control Rod Status • Containment Requirements and/or Status The POS defined should encompass the LPSD evolutions of interest. Consideration should be given to both static and transitional plant configurations (e.g., changing modes) when defining POSs. *Comment*: During shutdown, decay heat level can be determined by the time after shutdown. For QLRAs, system alignments, component maintenance unavailabilities, and containment status are typically variables within a POS as opposed to being used to define the POS.		

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
POS-A5	REVIEW plans for future planned LPSD evolutions (e.g. the next outage) to ensure the selections made in POS-A3 remain valid and appropriate. As a minimum, consider the following: • Plant Operational States that were not previously encountered; for example, if a PWR did not previously have a hot midloop POS in its history, but will have this state in the next outage. • Earlier entry into a POS, resulting in substantially higher decay heat; or later entry into a POS, resulting in substantially lower decay heat. (See also POS-B5 and POS-C4)		
POS-A6	In characterizing the POSs based on relevant and capable SSCs: ASSESS the ability of each system to protect each key safety function for each POS, : considering changes in alignment, availability of systems, and status of containment. *Comment*: The characterization process is iterative with the development of subsequent QLRA tasks such that the initial POS characterization may change.		
POS-A7	No requirements for interviews.	INTERVIEW appropriate plant personnel (e.g., operations, maintenance, engineering, safety analysis, and outage planning) to determine if potential Plant Operational States have been overlooked. Information from interviews conducted at similar plants may be used but is not a substitute for plant-specific information.	

TABLE A4.5-3 Supporting Requirements for Plant Operational State Analysis - High Level Requirement B

The POS analysis shall justify any grouping of POSs to facilitate the practicality and efficiency of the qualitative assessment. POSs with less limiting characteristics may be grouped with a state with more limiting characteristics. The POS analysis shall also justify defining unique POSs. (HLR-POS-B)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
POS-B1	If desired, COMBINE Plant Operational States into groups to facilitate efficient QLRA model development and assessment. The grouping process and definition of final POS conditions shall ensure that the most severe or constraining characteristics (with respect to Safety Function success criteria) of any group are chosen for the combined group. *Comments*: Grouping is recommended as opposed to screening of plant states. POSs can be combined based on similar parameters e.g. temperature, pressure, decay heat, and decay heat removal mechanisms such as residual heat removal cooling as described in SR POS-B2.		
POS-B2	GROUP Plant Operational States in accordance with BOTH criteria: (a) POSs can be considered similar in terms of plant response, success criteria, timing, and the effect on the functionality and performance of operators and relevant mitigating systems; (b) POSs subsumed into a group are bounded by the worst case impacts within the “new” group provided that this does not mask the key contributors. *Comments*: (1) Care should be taken when combining POSs into larger groups. For example, if the success criteria for one safety function (e.g., Electric Power Availability) does not change over several POS, but the success criteria for another Safety Function (e.g., Decay Heat Removal) does change substantially, it would not be prudent to group the POS based on the requirements of the first safety function. (2) For LPSD conditions, the “worst case” of all POS characteristics must be chosen. For some characteristics, this may be the entry conditions and for some, it may be the exit conditions of the POS. For example, a PWR “draindown and midloop” state would have the decay heat level associated with the start of the draindown; a water level associated with the drained-down end state; even though it is not possible to have both conditions at the same time. If this grouping scheme produced an unreasonable result, then it would be necessary to subdivide the POS into smaller states.		
POS-B3	Define unique POSs with different plant response impacts (i.e., those with different success criteria) or those that could have more severe radionuclide release potential . This may include distinction between (PWR) refueling pool connected (or not) to flooded reactor vessel; (BWR) reactor pressure vessel upper internals installed or removed or a containment leak test in progress.		
POS-B4	N/A: See Higher Risk Evolutions.		
POS-B5	REVIEW plans for future planned LPSD evolutions (e.g. the next outage) to ensure the grouping remains valid. *Comment*: Shorter outages often means POSs are entered sooner with higher decay heat levels. The higher decay heat may affect the success criteria of a system or component. (See also POS-C4)		

TABLE A4.5-4 Supporting Requirements for Plant Operational State Analysis - High Level Requirement C

If desired, the POS definitions may include the representative decay heat levels associated with each POS. At a minimum, decay heat levels must be factored into determining the capability of systems to meet certain safety functions (e.g., see supporting requirements SF-C2 and SF-C3). (HLR-POS-C)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
POS-C1	N/A		
POS-C2	Within the LPSD evolutions evaluated for HLR-POS-A and HLR-POS-B, DETERMINE the time frames after shutdown for each Plant Operational State based on a review of applicable plant specific records (such as outage plans, maintenance records, logbooks). The purpose of this step is to determine the approximate decay heat level for each POS, if decay heat level is to be used to define POS.		
POS-C3	N/A		
POS-C4	REVIEW future plans or upcoming outage schedules to ensure the determinations of decay heat levels for each POS remain valid. *Comment*: Shorter outages often means POSs are entered sooner with higher decay heat levels. The higher decay heat may affect the system success criteria or ability to maintain a key safety function.		
POS-C5a	If using decay heat levels as a defining POS characteristic, DETERMINE the decay heat level associated with each POS using historical records supplemented by generic calculations or decay heat curves.	If using decay heat levels as a defining POS characteristic, DETERMINE the decay heat level associated with each POS using plant specific decay heat curves and/or analysis.	
POS-C5b	If decay heat level is not used to define the POS, then it must be used in the system or safety function analysis to DETERMINE the capability of a system or component to support the safety function. In this case, DETERMINE the decay heat level associated with a given time after shutdown by generic calculations or decay heat curves.	If decay heat level is not used to define the POS, then it must be used in the system or safety function analysis to DETERMINE the capability of a system or component to support the safety function. In this case, DETERMINE the decay heat level associated with each POS using plant specific decay heat curves and/or analysis.	

TABLE A4.5-5 Supporting Requirements for Plant Operational State Analysis - High Level Requirement D

The POS analysis shall be documented in a manner that facilitates application of the model, updates to the model, and peer review. (HLR-POS-D)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
POS-D1	Identification and Characterization of LPSD evolutions and Plant Operational States DOCUMENT LPSD evolutions definitions. DOCUMENT the process and criteria used to identify Plant Operational States. DOCUMENT the defining characteristics of each Plant Operational State.		
POS-D2	Grouping of Plant Operational States DOCUMENT the process and criteria used to group Plant Operational States. DOCUMENT the definition of each Plant Operational State group.		
POS-D3	Decay Heat for Each Plant Operational State DOCUMENT the decay heat levels associated with each POS, if applicable.		
POS-D4	Key Assumptions DOCUMENT the key assumptions with regard to POS identification, grouping, and quantification.		
POS-D5	Interfaces with other PRA tasks DOCUMENT specific interfaces with other tasks for traceability, e.g., procedural controls, and qualitative risk tools, and to facilitate configuration control when interfacing tasks are updated. *Comment*: The POS element is the organizing structure for the LPSD qualitative method.		

4.6 Key Safety Functions

One of the principle tenets of QLRA is that a set of Safety Functions can be identified that encompass the elements that represent risk of a given configuration. For the purposes of managing nuclear safety risk during shutdown, NUMARC 91-06 applies the concept of defense-in-depth (DID) of key safety functions. The key safety functions identified for shutdown in NUMARC 91-06 include:

- *DECAY HEAT REMOVAL CAPABILITY: The ability to maintain reactor coolant system (RCS) temperature and pressure, and spent fuel pool (SFP) temperature below specified limits following a shutdown.*
- *INVENTORY CONTROL: Measures established to ensure that irradiated fuel remains covered with coolant to maintain heat transfer and shielding requirements.*
- *REACTIVITY CONTROL: Measures established to preclude inadvertent dilutions, criticalities, power excursions or losses of shutdown margin, and to predict and monitor core behavior.*
- *CONTAINMENT CLOSURE: The action to secure primary (PWR) or secondary (BWR) containment and its associated structures, systems, and components as a FUNCTIONAL barrier to fission product release under existing plant conditions.*
- *ELECTRICAL POWER AVAILABILITY: Measures established to maintain power availability in support of maintaining other safety functions. [NOTE: Definition not explicitly provided in NUMARC*

91-06] [2]

Due to the various dependencies of frontline systems on key support systems, it is important to consider treating support systems as a Safety Function. This enables a broader picture of defense in depth, since support systems may impact more than one frontline system, and failure of a support system could result in the simultaneous failure of multiple frontline systems to meet their success criteria. Significant degradation of a support system could result in a high risk condition, but may not be reflected as such in the "primary" safety functions (e.g., Inventory Control).

The purpose of this technical element is to define the Key Safety Functions to consider in a QLRA model, including consideration for success criteria and systems capable of supporting the Safety Function.

Objectives: The objective of the Safety Function analysis is to define the safety functions that will be evaluated in the QLRA, determine the success criteria for the Safety Functions, and the SSCs capable of supporting the Safety Functions.

TABLE A4.6-1 HIGH LEVEL REQUIREMENTS FOR SAFETY FUNCTIONS (HLR-SF)

Designator	Requirement
HLR-SF-A	The Safety Functions evaluated by the QLRA shall at a minimum include the Key Safety Functions from Section 1.3.2 and repeated in Section 4.6. Additional Safety Functions may be evaluated.
HLR-SF-B	Safety Function success criteria shall be defined for each POS.
HLR-SF-C	Systems capable of supporting the Safety Function shall be defined.
HLR-SF-D	The Safety Function analysis shall be documented in a manner that facilitates application of the model, updates to the model, and peer review.

TABLE A4.6-2 Supporting Requirements for Safety Functions - High Level Requirement A

The Safety Functions evaluated by the QLRA shall at a minimum include NUMARC 91-06 Key Safety Functions. Additional Safety Functions may be evaluated. (HLR-SF-A)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
SF-A1	INCLUDE the following Key Safety Functions in the QLRA: ▪ Decay Heat Removal ▪ Inventory Control ▪ Reactivity Control ▪ Containment Closure ▪ Electric Power Availability	INCLUDE the five Key Safety Functions in the QLRA. Additionally, CONSIDER support system status explicitly. *For example*, cooling water systems should be considered explicitly in front-line safety function assessments, or considered as a separate safety function. An additional example is the support functions for Emergency Diesel Generators (e.g., air start system, room cooling) may also need to be evaluated to show degradation.	

TABLE A4.6-3 Supporting Requirements Safety Functions - High Level Requirement B

Safety Function success criteria shall be defined for each POS. (HLR-SF-B)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
SF-B1	For each POS, define the parametric requirements for safety function success and/or the minimum set of equipment needed for a safety function to be supported. *[Same as ES-B1]*		

TABLE A4.6-4 Supporting Requirements for End State Metrics - High Level Requirement C

Systems capable of supporting the Safety Function shall be defined. (HLR-SF-C)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
SF-C1	For each POS, define which SSCs or combination of SSCs, beyond the minimum set required [SF-B1], can be used to satisfy the safety function.		
SF-C1a	For Decay Heat Removal, SPECIFY the front-line cooling sources capable of satisfying the safety function. ACCOUNT for the effects of HREs.	For Decay Heat Removal, SPECIFY the primary cooling sources capable of satisfying the safety function. ACCOUNT for the effects of HREs. Also, INCLUDE alternate cooling sources and dependencies, such as alternate decay heat removal systems, fuel pool cooling assist, and removal of intra-unit fuel pool cross-tie gates.	
SF-C1b	For Inventory Control, SPECIFY the front-line injection sources capable of satisfying the safety function. ACCOUNT for the inventory control needs of the vessel and the spent fuel pool. ACCOUNT for the effects of initial inventory levels and HREs.	For Inventory Control, SPECIFY the front-line injection sources capable of satisfying the safety function. ACCOUNT for the inventory control needs of the vessel and the spent fuel pool. ACCOUNT for the effects of initial inventory levels and HREs. Also, INCLUDE other realistic coolant sources, such as fire water, alternate service water or component cooling water.	
SF-C1c	For Reactivity Control, SPECIFY the status of control rods (i.e., all rods inserted or the core offloaded is acceptable) and Boron Concentration (e.g., greater than shutdown concentration). ACCOUNT for the effects of HREs. Note that boron injection performs a mitigative function only.		
SF-C1d	For Containment Closure, PWR: SPECIFY the status of containment integrity and the front-line systems capable of satisfying the safety function. CONSIDER the time required to establish containment closure if the containment integrity is not established. ACCOUNT for the effects of HREs. BWR: SPECIFY the status of primary and secondary containment and frontline systems capable of satisfying the safety function.	For Containment Closure, PWR: SPECIFY the status of containment integrity and the front line systems capable of satisfying the safety function. CONSIDER the time required to establish containment closure if the containment integrity is not established. ACCOUNT for the effects of HREs. In addition, IDENTIFY plant-specific alternate systems and configurations (e.g., containment boundaries or penetration configurations) that maintain Containment Closure. BWR: SPECIFY the status of primary and secondary containment and frontline systems capable of satisfying the safety function. CONSIDER the time required to establish secondary containment integrity if not established. ACCOUNT for the effects of HREs. IDENTIFY any plant-specific alternate secondary containment conditions.	

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
	ACCOUNT for the effects of HREs.		
SF-C1e	For Electrical Power Availability, SPECIFY the front-line electric power sources.	For Electrical Power Availability, SPECIFY the front-line electric power sources. INCLUDE AC, Instrument AC and DC systems. Explicitly INCLUDE supporting equipment (e.g., EDGs, battery chargers) and their support systems as necessary to properly evaluate the DID for all systems (See SF-A1)	
SF-C1f	No requirements for Capability Index I	SPECIFY the additional support systems (e.g., cooling water, HVAC) that should be explicitly considered for DID. Explicitly INCLUDE these systems in the front-line safety function evaluations, or as separate "Safety Functions." ACCOUNT for the effects of HREs.	
SF-C2	ENSURE that frontline and alternate sources used to satisfy safety functions are justifiable, based on plant procedures, and if needed, documented engineering evaluations.		
SF-C3	ENSURE time is available to align and initiate normal and alternate systems to meet the Safety Function success criteria. CALCULATE time available based on generic decay heat curves and actual inventory. DETERMINE time needed by operators based on operator interviews.	ENSURE time is available to align and initiate normal and alternate systems to meet the Safety Function success criteria. CALCULATE time available based on plant-specific decay heat curves and actual inventory. DETERMINE time needed by operators based on operator interviews and table-top talk-throughs.	ENSURE time is available to align and initiate normal and alternate systems to meet the Safety Function success criteria. CALCULATE time available based on outage-specific decay heat curves and actual inventory. DETERMINE time needed by operators based on operator interviews and simulator exercises or walk-throughs.
SF-C4	No requirements for Capability Index I	CONSIDER the inherent reliability and capability of systems used to satisfy the Safety Function. FACTOR this into the DID determinations performed for a given system and the end state result assigned. *Example:* Non-essential Service Water may be capable of cooling Safety Related front-line systems, but is not as reliable (e.g., not DG backed, poor performance) as Essential Service Water. In this case, two trains of Non-essential Service Water may be considered to provide the same DID level as one train of Essential Service Water.	CONSIDER the inherent reliability and capability of systems used to satisfy the Safety Function. FACTOR this into the DID determinations performed for a given system and the end state result assigned using correlation to a calculated value.

TABLE A4.6-5 Supporting Requirements for Safety Functions - High Level Requirement D

The Safety Function analysis shall be documented in a manner that facilitates application of the model, updates to the model, and peer review. (HLR-SF-D)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
SF-D1	DOCUMENT the Safety Functions to be evaluated in the QLRA.		
SF-D2	DOCUMENT the minimum required SSCs for the Safety Function and the basis for the minimums.		
SF-D3	DOCUMENT the SSCs considered for the Safety Function and the bases for their selection. DOCUMENT the time available and time required (and their bases) for aligning and starting front-line or alternate systems credited in the QLRA. DOCUMENT any weighting that is applied to systems based on their inherent reliability, and the basis thereof.		

4.7 Higher Risk Evolutions (HREs)

The purpose of this technical element is to define Higher Risk Evolutions (HRE) and how to factor their occurrence into the QLRA. Higher Risk Evolutions (HREs) are defined in NUMARC 91-06 as *"outage activities, plant configurations or conditions during shutdown where the plant is more susceptible to an event causing the loss of a key safety function."* [2] HREs consist of: (1) activities or events with the potential to directly challenge the success state of a safety function, (2) activities or events with the potential to cause an unplanned loss of one or more systems supporting the safety function.

An HRE presents a challenge to the success of one or more safety functions. If an activity, event or configuration increases the likelihood of challenging a Safety Function, then it can be considered an HRE. In a QLRA, an HRE is manifested as a degradation of DID. Some specific examples of HREs are:

- Switchyard Maintenance – Depending on the evolution, switchyard maintenance can be considered an HRE for the Electric Power Availability Safety Function. During switchyard maintenance, there is an increased likelihood that offsite power could be lost to the site, affecting the defense in depth of the safety function.
- Operations with the Potential to Drain the Reactor Vessel (OPDRV) or Reactor Cavity (OPDRC) – Activities designated as OPDRVs or OPDRCs represent challenges to the Inventory Control Safety Function, since they increase the likelihood for the loss of inventory control.
- Mid-loop for PWRs – This is an example of a POS that is inherently an HRE for the Decay Heat Removal Safety Function. During midloop operations, industry experience has shown that it is more likely to have a loss of DHR event, thus challenging the Decay Heat Removal Safety Function. [6]
- Tornado Warning – This condition could be considered as an HRE for the Electric Power Availability Safety Function, due to the potential for a Loss of Offsite Power (LOOP) event.

By their definition, HREs should be regarded as subjective activities or conditions, i.e., 'higher' can be interpreted different ways, resulting in varying degrees of risk. As such, engineering judgment must be applied when considering the likelihood and consequences of HREs, and how they are factored into the DID analysis. For example:

- A plant that plans a freeze seal on a large pipe. The evolution and resultant configuration should be

evaluated if it is high risk and whether it should be designated an HRE.

- The operation of a new system for the first time in an outage may be considered an HRE, if the improper operation of the system could result in a challenge to one or more Safety Functions.

Depending on the severity of the HRE, it is common practice to equate an HRE to one or two levels of DID.

Objectives: The objective of the HRE analysis is to determine the activities and events that should be considered as HREs, and define how they will be evaluated in the QLRA.

TABLE A4.7-1 HIGH LEVEL REQUIREMENTS FOR SAFETY FUNCTIONS (HLR-HRE)

Designator	Requirement
HLR-HRE-A	Criteria shall be established for designating an activity or event as an HRE.
HLR-HRE-B	The impact of HREs shall be factored into the Safety Function analysis in the QLRA.
HLR-HRE-C	The HRE analysis shall be documented in a manner that facilitates application of the model, updates to the model, and peer review.

TABLE A4.7-2 Supporting Requirements for Higher Risk Evolutions - High Level Requirement A

Criteria shall be established for designating an activity or event as an HRE. (HLR-HRE-A)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
HRE-A1	For each modeled Safety Function, ESTABLISH the criteria for designating an activity, event, or configuration as an HRE.		
HRE-A2	REVIEW plant history and industry events to determine potential activities to consider for HREs.		
HRE-A3	EVALUATE each activity to determine whether it should be considered as an HRE.		
HRE-A4	Environmental conditions may be REPRESENTED as an HRE. CONSIDER environmental conditions that may make more than one SSC unavailable. [See SY-B8]		

TABLE A4.7-3 Supporting Requirements for Higher Risk Evolutions - High Level Requirement B

The impact of HREs shall be factored into the Safety Function analysis in the QLRA. (HLR-HRE-B)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
HRE-B1	For each Safety Function evaluated in the QLRA, INCORPORATE the occurrence of an HRE into the assessment.		
HRE-B2	DEFINE AND IMPLEMENT rules or guidance for how the Safety Function capability is affected by the presence of an HRE. *Comments* – An example would be that an HRE will degrade the end state result by one level.	For each combination of SSC availability, DETERMINE the impact on the end state result given the occurrence of an HRE and IMPLEMENT in the Safety Function evaluation. *Comments* – As compared to Capability Index I, this requires each combination of POS, SSC availability, and HRE to be evaluated to determine the end state result, as opposed to applying a general rule for HRE impact.	For each combination of SSC availability, DETERMINE the impact on the end state result given the occurrence of an HRE by correlating the configuration to a calculated risk value and IMPLEMENT in the Safety Function evaluation. *Comments* - A PRA quantification of the end state is not required; however, a calculation of the system level impact of out of service equipment plus the higher risk evolution supporting the key safety function would be the minimum required to meet this Capability Index. Assumptions and limitations on such an analysis shall be documented.
HRE-B3	IDENTIFY POS which may be considered implicitly as HREs and INCLUDE the impact in the Safety Function evaluation.	REVIEW each POS and DETERMINE whether the POS should be considered as an HRE for one or more Safety Functions. INCLUDE the impact in the Safety Function evaluation.	

TABLE A4.7-4 Supporting Requirements for Higher Risk Evolutions - High Level Requirement C

The HRE analysis shall be documented in a manner that facilitates application of the model, updates to the model, and peer review. (HLR-HRE-C)

	CAPABILITY INDEX I	CAPABILITY INDEX II	CAPABILITY INDEX III
HRE-C1	*HRE Definition* DOCUMENT the types of events or activities that are considered as HREs. DOCUMENT the performance of historic and industry events reviews.		
HRE-C2	*HRE Affect on Safety Function* DOCUMENT the rules and/or guidance used to affect the Safety Function end state result during the occurrence of an HRE. DOCUMENT the identification, review and impact of POS on the Safety Function evaluation.		

4.8 Systems Analysis (SY)

System Analysis for a QLRA differs from that associated with a PRA. Specifically, system models developed for QLRAs are primarily concerned with SSC unavailability/availability, as opposed to failure modes and probabilities. However, many of the steps needed for a PRA System Analysis are the same, including gaining an understanding of system operation, system success criteria, and support system impacts.

Objective: The objective of the systems analysis element is to identify the causes of unavailability for each plant system represented in the safety function DID analysis in such a way that:

(a) System-level success criteria and assumptions provide the basis for the system logic models as reflected in the model. A reasonably complete set of SSC unavailability modes for each system is represented. [In this context, "unavailability mode" refers to the operational modes that equipment can be taken out of service, e.g., valves can be taken out of service in the open or closed position.]

(b) Success criteria for systems is properly accounted for, based on POS and Safety Function.

(c) Different initial system alignments are evaluated to the extent needed based on POS.

(d) Intersystem dependencies and intra-system dependencies that could influence system unavailability or the system's impact on safety function DID are identified and accounted for.

Table A4.8-1 High Level Requirements for Systems Analysis (SY)

Designator	Requirement
HLR-SY-A	The systems analysis shall provide a reasonably complete treatment of the causes and modes of system unavailability represented in the logical structure of the qualitative method.
HLR-SY-B	The systems analysis shall provide a reasonably complete treatment of intersystem and intrasystem dependencies, as well as dependencies on Plant Operational States.
HLR-SY-C	The systems analysis shall be documented consistent with the applicable supporting requirements.

Table A4.8-2 Supporting Requirements for HLR-SY-A

The systems analysis shall provide a reasonably complete treatment of the causes and modes of system unavailability represented in the logical structure of the qualitative method. (HLR-SY-A)

Index No.	Capability Index I	Capability Index II	Capability Index III
SY-A1	DEVELOP system models for those systems needed to provide or support the key safety functions.		
SY-A2	COLLECT pertinent information to ensure that the systems analysis appropriately reflects the as-built and as-operated systems. Examples of such information include system P&IDs, one-line diagrams, instrumentation and control drawings, spatial layout drawings, system operating procedures, abnormal operating procedures, emergency procedures, success criteria calculations, the final or updated SAR, Technical Specifications, training information, system descriptions, design documents, actual system operating experience, outage-specific planning guides, temporary system alignments, and interviews with system engineers and operators.		
SY-A3	REVIEW plant information sources to define or establish *(a)* system components and boundaries *(b)* dependencies on other systems *(c)* instrumentation and control requirements (Note that many components which		

	receive automatic actuation at power, do not rely on automatic actuation while shutdown) *(d)* testing and maintenance requirements and practices *(e)* operating limitations such as those imposed by Technical Specifications or administrative requirements *(f)* component operability and design limits *(g)* procedures for the operation of the system during normal and accident conditions *(h)* system configuration during normal and accident conditions *(i)* temporary alignments or equipment used during outages (e.g., temporary EDG, spoolpiece alignments)	
SY-A4	CONFIRM that the system models correctly reflect the as-built, as-operated plant through discussions with system engineers and plant operations staff.	PERFORM plant walkdowns and interviews with system engineers, plant operators and outage management personnel to confirm that the systems models correctly reflect the as-built, as-operated plant.
SY-A5	INCLUDE the effects of normal, alternate and temporary system alignments, to the extent needed to determine system availability to support the safety function(s).	
SY-A6	In defining the system model boundary (see SY-A3), INCLUDE within the boundary the SSCs required for system operation, and the SSCs providing the interfaces with support systems required for actuation and operation of the system components, as necessary to adequately represent the plant configuration.	
SY-A7	DEVELOP train or system-level models that have sufficient level of detail to capture the major dependencies needed for the qualitative method to adequately evaluate the impact of support system unavailabilities.	DEVELOP detailed component-level system models, with system – level modeling or super-events used only with justification.
SY-A8	ESTABLISH the boundaries of the components required for system operation. Ensure that the impact of subcomponents (e.g., a valve limit switch that is associated with a permissive signal for another component) that are shared by another component or affect another component are CONSIDERED in the QLRA in order to account for the dependent failure mechanism. *Comments:* It is not necessary to explicitly model the subcomponents as long as the impact of the subcomponent unavailability is accounted for in implementation of the model (e.g., via schedule translation).	ESTABLISH the boundaries of the components required for system operation. MODEL as separate inputs to the model, those subcomponents (e.g., a valve limit switch that is associated with a permissive signal for another component) that are shared by another component or affect another component, in order to account for the dependent failure mechanism.
SY-A9	DELETED (ASME 2005)	
SY-A10	N/A	
SY-A11	INCORPORATE the effect of variable success criteria (e.g., success criteria that change as a function of POS) into the system modeling. Example causes of variable system success criteria are: *(a) different safety functions.* Different success criteria are required for some systems to support different success criteria (e.g., flow through the RHR HX is not	

	required for Inventory Control [it can be bypassed], but is required for Heat Removal); *(b) dependence on other components.* Success criteria for some systems are also dependent on the success of another component in the system (e.g., operation of additional pumps in some cooling water systems is required if non-critical loads are not isolated or if seasons change); *(c) time dependence.* Success criteria for some systems are time-dependent (e.g., two pumps are required to provide the needed flow early in an outage when decay heat is high, but only one is required for mitigation later in the outage); *(d) sharing of a system between units.* Success criteria may be affected when both units are challenged by the same initiating event (e.g., LOOP).
SY-A12	INCLUDE in the system model the unavailability of the equipment and components that would affect system functionality (as required to maintain the key safety functions). This equipment includes both active components (e.g., pumps, valves, and air compressors) and passive components (e.g., piping, heat exchangers, and tanks) required for system operation.
SY-A12a	INCLUDE WITH CAUTION component unavailability that would be beneficial to system operation. For example, a valve that is unavailable in the open position and is required to be open to perform a given system function is acceptable to include. However, if the same valve is required to be closed for a different function, that function must be considered unavailable.
SY-A12b	INCLUDE those unavailabilties that can cause flow diversion pathways that result in failure of systems or components required to support one or more key safety functions.
SY-A13	When identifying unavailability in SY-A12 INCLUDE consideration of all out of service configurations of the SSC, consistent with the level of detail of the qualitative method and sufficient to maintain the key safety functions. ”Out of service configuration” refers to the state of the equipment when it is taken out of service, e.g., valves can be taken out of service in the open or closed position. Note that some of these may be redundant and only one mode may be required for a particular qualitative risk assessment method. For example: *(a)* active component unavailable to start *(b)* active component unavailable to continue to run *(c)* closed component unavailable to open *(d)* closed component unavailable to remain closed *(e)* open component unavailable to close *(f)* open component unavailable to remain open *(g)* plugging of an active or passive component *(h)* active or passive component unable to maintain pressure boundary *(i)* internal leakage or rupture of a component *(j) unavailability of* signal to operate a component (e.g., instrumentation, controls) *(k)* other unavailabilies of a component that would prevent it from performing its required function
SY-A14	N/A
SY-A15	N/A
SY-A16	N/A
SY-A17	N/A
SY-A18	INCLUDE unavailability in systems models at a level consistent with how the systems are typically taken out of service for maintenance Examples of out-of-service unavailability to be modeled: *(a)* train outages; *(b)* a functional equipment group (FEG) removed from service; *(c)* a relief valve taken out of service.

SY-A18a	INCLUDE the capability of representing the simultaneous unavailability of redundant equipment.		
SY-A19	IDENTIFY system conditions that cause a loss of desired system function, e.g., Plant Operational State, excessive heat loads, excessive electrical loads, excessive humidity, etc.		
SY-A20	DO NOT TAKE CREDIT for system or components when the potential exists for rated or design capabilities to be exceeded.	TAKE CREDIT for system or component functionality only if an analysis exists to demonstrate that rated or design capabilities are not exceeded.	TAKE CREDIT for system or component functionality, including credit for beyond design or rated capabilities, if supported by an appropriate combination of *(a)* test or operational data *(b)* engineering analysis *(c)* expert judgment
SY-A21	DEVELOP system model nomenclature in a consistent manner to allow model manipulation and to represent the same designator when component unavailability is used in multiple systems or trains.		
SY-A22	DO NOT MODEL or CONSIDER recovery of unavailable equipment, unless the probability of recovery is justified through an adequate analysis or examination of data.		
SY-A23	Mapping of equipment unavailability from the plant schedule or actual plant status to the correct model element (basic event, supercomponent, train, system) is critical for the proper evaluation of qualitative model. DEFINE the process and controls used to accomplish this, including boundaries, assumptions, grouping, etc.		

Table A4.8-3 Supporting Requirements for HLR-SY-B

The systems analysis shall provide a reasonably complete treatment of intersystem and intrasystem dependencies, as well as dependencies on Plant Operational States. (HLR-SY-B)

Index No.	Capability Index I	Capability Index II	Capability Index III
SY-B1	N/A		
SY-B2	N/A		
SY-B3	N/A		
SY-B4	N/A		
SY-B5	ACCOUNT for the modeled system's dependency on support systems or interfacing systems in the logical structure of the qualitative method using simplified logic trees, rules, or administrative controls, such as procedures, or guidance documents	ACCOUNT explicitly for the modeled system's dependency on support systems or interfacing systems in the modeling process using a detailed logic model and/or detailed rules.	
SY-B6	PERFORM reviews to determine the need for support systems that are plant-specific and reflect the variability in the conditions required to support the key safety functions. NOTE: Support system requirements may change based on the POS.		
SY-B7	BASE support system modeling on conservative success criteria. *Comment:* Use of conservative success criteria means that requirements for support	BASE support system modeling on realistic plant-specific success criteria for important systems. Conservative success criteria may be used for less important systems or	BASE support system modeling on realistic plant-specific success criteria and timing. *Comment:* Use of realistic success criteria means that requirements

	system dependencies may be based on design basis or tech spec requirements.	where realistic success criteria is not available. *Comment:* Use of conservative success criteria means that requirements for support system dependencies may be based on design basis or tech spec requirements.	for support system dependencies should be based on evaluations similar to those used in the PRA, as opposed to, for example, design basis or tech spec requirements.
SY-B8	Spatial and environmental hazards may impact multiple systems or redundant components in the same system. ACCOUNT for known spatial and environmental conditions that make equipment unavailable. This could be considered in the unavailability determination or as a HRE. [See HRE-A4]		
SY-B9	DELETED		
SY-B10	When modeling a system, INCLUDE appropriate interfaces with the support systems required for successful operation of the system to support the key safety functions Examples include: *(a)* component motive power *(b)* cooling of components *(c)* actuation logic (Note that many systems may not have automatic actuation logic available during shutdown POSs.) *(d)* support systems required for control of components *(e)* any other identified support function (e.g., heat tracing) necessary to support the key safety functions.		
SY-B11	IDENTIFY those systems that are required for initiation and actuation of a system. ACCOUNT for them unless a justification is provided (e.g., the initiation and actuation system can be argued to be highly reliable and is only used for that system, so that there are no intersystem dependencies arising from failure of the system). *Note: Many systems are actuated manually (i.e., not automatically) during shutdown conditions.*	ACCOUNT for those systems that are required for initiation and are required for initiation and actuation of a system. *Note: Many systems are actuated manually (i.e., not automatically) during shutdown conditions.*	
SY-B12	MODEL air, power, and cooling support systems as required to support key safety functions.		
SY-B13	DO NOT USE proceduralized recovery actions as the sole basis for eliminating a support system from the model.		
SY-B14	Some systems include SSCs that are common to multiple systems. INCLUDE components if their failure affects more than one system (e.g., a common suction pipe feeding two separate systems) that supports the key safety functions.		
SY-B15	N/A		
SY-B16	ENSURE that systems that require operator actions are only credited where procedures exist and adequate time is available to align and operate the equipment.		

Table A4.8-4 Supporting Requirements for HLR-SY-C

The systems analysis shall be documented consistent with the applicable supporting requirements (HLR-SY-C).

Index No.	Capability Index I	Capability Index II	Capability Index III
SY-C1	DOCUMENT the systems analysis in a manner that facilitates application of the model, upgrades to the model, and peer review.		
SY-C2	DOCUMENT the system functions and boundary, the associated success criteria, the modeled components and their unavailability states, and a description of modeled dependencies including support systems, including the inputs, methods, and results. For example, this documentation typically includes: *(a)* system function and operation under normal and emergency operations *(b)* system model boundary *(c)* system schematic illustrating all equipment and components necessary for system operation *(d)* information and calculations to support equipment availability considerations and assumptions *(e)* actual maintenance and outage history or processes indicating how the equipment is taken out of service *(f)* system success criteria and relationship to safety function success *(g)* reference to system-related test and maintenance procedures *(h)* system dependencies and shared component interface *(i)* component spatial information (if applicable) *(j)* assumptions or simplifications made in development of the system models *(k)* the components and unavailability states included in the model and justification for any exclusion of components and unavailability *(l)* a description of the mapping process (SY-A23) *(m)* records of resolution of logic loops (if used) *(n)* the sources of the above information (e.g., completed checklist from walkdowns, notes from discussions with plant personnel) *(o)* the nomenclature used in the system models.		
SY-C3	DOCUMENT the key assumptions associated with the systems analysis.		

SECTION 5
CONFIGURATION CONTROL

5.1 Purpose

This Section provides requirements for configuration control of a QLRA to be used with this Standard to support risk-informed decisions for nuclear power plants.

5.2 Configuration Control Program

A QLRA Configuration Control Program shall be in place. It shall contain the following key elements:

(a) a process for monitoring QLRA inputs and collecting new information

(b) a process that maintains and upgrades the QLRA to be consistent with the as-built, as operated plant

(c) a process that ensures that the cumulative impact of pending changes is considered when applying the QLRA

(d) a process that evaluates the impact of changes on previously implemented risk-informed decisions that have used the QLRA, if applicable

(e) a process that maintains configuration control of computer codes, if any, used to support QLRA calculations

(f) documentation of the Program

5.3 Monitoring QLRA Inputs and Collecting New Information

The QLRA Configuration Control Program shall include a process to monitor changes in the design, operation, maintenance, and industry-wide operational history that could affect the QLRA. These changes shall include inputs that impact operating procedures, design configuration, outage processes, higher risk evolutions, and SSC unavailability. The program should include monitoring of changes to the QLRA technology and industry experience that could change the results of the QLRA model.

5.4 QLRA Maintenance and Upgrades

The QLRA shall be maintained and upgraded, such that its representation of the as-built, as-operated plant is sufficient to support the applications for which it is being used.
Changes in QLRA inputs or discovery of new information identified pursuant to Section 5.3 shall be evaluated to determine whether such information warrants QLRA maintenance or QLRA upgrade. The following describe the difference between maintenance and upgrades with respect to a QLRA [note that they are essentially the same as the definitions provided in the ASME PRA Standard [4]:

- *Maintenance:* the update of the QLRA models to reflect plant changes such as modifications, procedure changes, or outage processes.
- *Upgrade:* the incorporation into a QLRA model of a new methodology or significant changes in scope or capability. This could include items such as a new end state methodology or the addition of new safety functions.

Changes that would impact risk-informed decisions should be prioritized to ensure that the most significant changes are incorporated as soon as practical. Changes to a QLRA due to QLRA maintenance shall meet the requirements of Section 4. Upgrades of a QLRA shall satisfy the peer review requirements specified in Section 6, but limited to aspects of the QLRA that have been upgraded.

5.5 Pending Changes

This Standard recognizes that immediately following a plant change, or upon identification of a subject for model improvement, a QLRA may not represent the plant until the change is incorporated. Therefore, the QLRA configuration control process shall consider the cumulative
impact of pending changes. These changes should be addressed in a fashion similar to the approach used in Section 3 to address elements that are determined to be inadequate.

5.6 Use of Computer Codes

The computer codes used to support and to perform QLRA analyses, if any, shall be controlled to ensure consistent, reproducible results.

5.7 Documentation

Documentation of the Configuration Control Program and of the performance of the above elements shall be adequate to demonstrate that the QLRA is being maintained consistently with the as-built, as-operated plant.

The documentation typically includes:

(a) a description of the process used to monitor QLRA inputs and collect new information

(b) evidence that the aforementioned process is active

(c) descriptions of proposed changes

(d) description of changes in a QLRA due to each QLRA upgrade or QLRA maintenance

(e) record of the performance and results of the appropriate QLRA reviews

(f) record of the process and results used to address the cumulative impact of pending changes

(g) record of the process and results used to evaluate changes on previously implemented risk-informed decisions pursuant to Section 5.6, if applicable

(h) a description of the process used to maintain software configuration control

SECTION 6
PEER REVIEW

6.1 Purpose

This section summarizes the requirements for peer review of a LPSD QLRA covered by this Standard. QLRAs used for applications applying this Standard shall be peer reviewed.
The peer review shall assess the QLRA to the extent necessary to determine if the methodology and its implementation meet the requirements of this Standard. The peer review need not assess all aspects of the QLRA against all Section 4 requirements; however, enough aspects of the QLRA shall be reviewed for the reviewers to achieve consensus on the adequacy of methodologies and their implementation for each QLRA Element.

6.1.1 Frequency

Only a single complete peer review is necessary to establish the quality of a QLRA against this Standard. In addition, Section 5 of this Standard requires peer review for upgrades of a QLRA. When peer reviews are conducted on QLRA upgrades, the latest review shall be considered the review of record. The scope of an additional peer review may be confined to changes to the QLRA that have occurred since the previous review.

6.1.2 Methodology

The review shall be performed using a written methodology that assesses the requirements of Section 4 and addresses the requirements of Section 6.

The peer review methodology shall consist of the following elements:

(a) a process for selection of the peer review team

(b) training in the peer review process

(c) an approach to be used by the peer review team for assessing if the QLRA meets the supporting requirements of Section 4 of this Standard

(d) a process by which differing professional opinions are to be addressed and resolved

(e) an approach for reviewing the QLRA configuration control

(f) a method for documenting the results of the review

NEI-00-02 [7] provides an example of an acceptable review methodology for PRAs; this can be used as a guideline, although all aspects of PRA peer reviews do not apply for a QLRA.

6.2 Peer Review Team Composition and Personnel Qualifications

6.2.1 Collective Team

The peer review team shall consist of personnel whose collective qualifications include:

(a) the ability to assess all the QLRA Elements of Section 4 and the interfaces between those elements

(b) the collective knowledge of the plant NSSS design, containment design, and plant operation

6.2.2 General

6.2.2.1

The peer review team members individually shall:

(a) be knowledgeable of the requirements in this Standard for their area of review

(b) be experienced in performing the activities related to the QLRA Elements for which the reviewer is assigned

6.2.2.2

When a peer review is being performed on a QLRA upgrade, reviewers shall have knowledge and experience appropriate for the specific QLRA Elements being reviewed. However, the other requirements of this Section shall also apply.

The peer review team members shall:

(a) not be allowed to review their own work or work for which they have contributed

(b) not be allowed to review a QLRA for which they have a conflict of interest, such as a financial or career path incentive or disincentive that may influence the outcome of the peer review

6.2.3 Specific

The peer reviewer shall also be knowledgeable (by direct experience) of the specific methodology, code, tool, or approach that was used in the QLRA Element assigned for review. Understanding and competence in the assigned area shall be demonstrated by the range of the individual's experience in the number of different, independent activities performed in the assigned area, as well as the different levels of complexity of these activities. One member of the peer review team (the technical integrator) shall be familiar with all the QLRA Elements identified in this Standard and shall have demonstrated the capability to integrate these QLRA Elements.

The peer review team shall have a team leader to lead the team in the performance of the review. The team leader need not be the technical integrator. The peer review should be conducted by a team with a minimum of two members, and shall be performed over a minimum period of three days. If the review is focused on a particular QLRA Element, such as a review of an upgrade of a QLRA Element, then the peer review should be conducted by a team with a minimum of two members, performed over a time necessary to address the specific QLRA Element. Exceptions to the requirements of this paragraph may be taken based on the availability of appropriate personnel to develop a team. All such exceptions shall be documented in accordance with Section 6.6 of this Standard.

6.3 Review of PRA Elements to Confirm the Methodology

The peer review team shall use the requirements of this subsection for the QLRA Elements being reviewed to determine if the methodology and the implementation of the methodology for each QLRA Element meet the requirements of this Standard. Some subsections in 6.3 contain specific suggestions for the review team to consider during the review. Additional material for those Elements may be reviewed depending on the results obtained. These suggestions are not intended to be a minimum or comprehensive list of requirements. The judgment of the reviewer shall be used to determine the specific scope and depth of the review in each QLRA Element.

The results of the overall QLRA, including models and assumptions, and the results of each QLRA Element shall be reviewed to determine their reasonableness given the design and operation of the plant (e.g., investigation of cutset or sequence combinations for reasonableness). The HLRs and the composite of the SRs of Section 4 shall be used by the peer review team to assess the completeness of

a QLRA Element.

6.3.1 End States (ES)

A review shall be performed on end state definitions and criteria. The portion of the end state analysis selected for review typically includes:

(a) End state definitions, including the number selected and the meaning of each end state

(b) Relative risk associated with end-states consistent within a safety function (the degree to which this is done defines the Capability Index)

(c) Minimum set of equipment required for a safety function, and the rules used to determine the impact on the end state based on SSC unavailability, HREs and POS risk.

(d) Actions assigned to each end state are appropriate.

6.3.2 Plant Operational States (POS)

A review shall be performed of the POS analysis. The portion of the POS analysis selected for review typically includes:

(a) Definition of POSs that are representative of the outage conditions expected and have consistent success criteria throughout a POS
(b) Grouping of multiple POSs into one POS.
(c) Treatment of decay heat levels (either at the POS or system function level)

6.3.3 Safety Functions (SF)

A review shall be performed of the safety functions included in the QLRA.. The portion of the safety function analysis selected for review typically includes:

(a) The scope of safety functions considered, including support system safety functions, if appropriate for the Capability Index
(b) Equipment is defined for each safety function, including the minimum set, and bases for including the systems are provided

6.3.4 Higher Risk Evolutions (HRE)

A review shall be performed for HREs. The portion of the HRE evaluation selected for review typically includes:

(a) Definition of HREs, including examples
(b) Impact of HREs on end state results

6.3.5 Systems Analysis (SY)

A review shall be performed on the system analysis. The portion of the system analysis selected for review typically includes:

(a) Dominant systems contributing to the success of the safety functions
(b) Level of detail in system models
(c) Incorporation of support system dependencies
(d) Inclusion of unavailability of SSCs, based on plant practices

6.4 PRA Configuration Control

The peer review team shall review the process, including implementation, for upgrading the QLRA against the configuration control requirements of this Standard.

6.6 Documentation

6.6.1 Peer Review Team Documentation

The peer review team's documentation shall demonstrate that the review process appropriately implemented the review requirements. Specifically, the peer review documentation shall include the following:

(a) identification of the version of the QLRA reviewed
(b) the names of the peer review team members
(c) a brief resume on each team member describing the individual's employer, education, and QLRA and QLRA Element experience and expertise
(d) the elements of the QLRA reviewed by each team member
(e) a discussion of the extent to which each QLRA Element was reviewed
(f) results of the review identifying any differences between the requirements in Sections 4 and 5 of this Standard and the methodology implemented, defined to a sufficient level of detail that will allow the resolution of the differences
(g) identification and significance of exceptions and deficiencies with respect to SRs
(h) at the request of any peer reviewer, differences or dissenting views among peer reviewers
(i) recommended alternatives for resolution of any differences

6.6.2 Resolution of Peer Review Team Comments

Resolution of Peer Review Team comments shall be documented. Exceptions to the alternatives recommended by the Peer Review Team shall be justified.

SECTION 7
REFERENCES

[1] NUMARC 93-01, “Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants,” Nuclear Energy Institute, Revision 3, July 2000.

[2] NUMARC 91-06, "NUMARC Guidelines for Industry Actions to Assess Shutdown Management,” Nuclear Management and Resources Council, December 1991.

[3] ANSI/ANS-58.22-2007, Low Power and Shutdown PRA methodology, American Nuclear Society, DRAFT #7f, July 2007.

[4] ASME Ra-Sc-2007, Addenda to ASME RA-S-2002 Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME.

[5] Qualitative Risk Assessment Methods for Shutdown Risk Assessment, EPRI, Palo Alto, CA: 2006, 1013501

[6] An Analysis of Loss of Decay Heat Removal Trends (1989-2000): Outage Risk Assessment and Management (ORAM) Technology, EPRI, Palo Alto, CA: 2001. 13003113

[7] NEI 00-02, Probabilistic Risk Assessment (PRA) Peer Review Process Guidance, Nuclear Energy Institute, Revision A3.

[8] NUREG/CR-6144, “Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1,” USNRC, October 1995.

[9] IAEA-TECDOC-1144, “Probabilistic Safety Assessments of Nuclear Power Plants for Low Power and Shutdown Modes,” International Atomic Energy Agency, 1999

ATTACHMENT 1 (NON-MANDATORY) PLANT OPERATIONAL STATE ANALYSIS METHODOLOGY

1.0 Objective

The objective of this task is to categorize the many possible plant states encountered during during an outage into discrete sets of boundary conditions affecting the shutdown QLRA. These discrete plant states are termed *plant operational states* (POSs).

The process of analyzing the plant operational states includes the following steps:

(1) Determine the plant outage types to be evaluated by the model, e.g., refueling, forced outage.

(2) Define plant operational states (POSs), and the associated characteristics within a POS, for the expected outage types, and

(3) Determine the scope of POS to be modeled in the QLRA.

This is a task that is specific to the LPSD PRA and QLRA, since the full-power PRA typically models only a single plant state. This section describes the general process used to develop the POSs for the shutdown analysis, including the methods and general inputs and outputs.

2.0 POS Methods

Generic guidance for non-power system models is provided in the Surry Low Power and Shutdown Events study sponsored by the USNRC (NUREG/CR-6144, [8]. This concurs with international guidance documented in IAEA-TECDOC-1144; [9]. Although these references are for PRAs, some of the general principles discussed can be applied to POS methods for QLRAs.

In general, the types of outages that the plant typically encounters are identified first, and then the plant operational states that the plant goes through in conducting each of the outage types are identified and characterized. The general method for plant outage type definition and selection of the shutdown plant operational states is described below in Sections A.2.1 and A.2.2.

2.1 Outage Type Definition

Historically for pressurized water reactors (PWR), there are typically four general types of outages as follows.

- Refueling outage (some or all of the fuel assemblies transferred to the Spent Fuel Pool)
- Cold shutdown drained maintenance outage
- Cold shutdown (non-drained) maintenance outage
- Hot standby maintenance outage

The Refueling outage type is generally selected as representative of all the plant operational states because it has the widest variety of plant conditions of any outage type. POSs represent the distinct plant configurations within the plant outage type that affect the QLRA.

2.2 Plant Operational State Selection

Plant operational states (POSs) represent the distinct plant configurations within the plant outage type that affect the QLRA safety function *success criteria.* They are mainly differentiated by the Reactor States

(mode, level, RCS integrity, fuel location), containment status, and possibly the decay heat levels. POSs consist of steady-state portions and transition states from one set of plant conditions to another.
Three steps are taken in defining plant operational states for QLRAs. First, the *safety functions* being evaluated in QLRA are defined (see Section 4.6). Second, a *procedure review* of the shutdown and start-up procedures is conducted to determine the impact of the start-up and shutdown on the safety systems used to fulfill the critical safety functions. Finally, the *impact of varying outage types* is evaluated. Each of these areas is further described below followed by a discussion on the treatment of *variables within a POS*.

3.0 Safety Functions. The safety functions for the QLRA are defined in accordance with the SF requirements presented in Section 4.6. Typical safety functions are:

- Decay Heat Removal
- Inventory Control
- Reactivity Control
- Containment Closure
- Electric Power Availability

4.0 Procedure Review. Plant operating procedures for shutdown and startup operations are reviewed. The actions described in the various steps in the procedures are examined to determine if any changes in the plant could result in changes in any of the following [Note: These items are selected since they should be considered in determining the plant-specific systems used to fulfill the critical safety functions listed above]:

- Reactivity
- Thermal-hydraulic conditions of the RCS (temperature, pressure, level)
- Capability of systems for decay heat removal and inventory control
- Status of containment penetrations (air locks, ventilation ducts, pipes)

General guidelines used to differentiate the procedure steps during POS definition are as follows.

- Changes in plant configurations that change the numerator of the safety function success criteria (e.g. *M* out of N pumps), or cause whole systems to be unavailable or ineffective, are generally the boundary lines in defining the POSs. [Note: Changes in the denominator of the safety function success criteria (e.g. M out of *N* pumps) do not constitute new POSs. Instead, these effects are incorporated as the maintenance configuration evaluated by the QLRA].
- Major changes affecting the actuation of safety systems such as whether manual or automatic actuation is available, and the time required for action, may also considered as boundaries in defining POSs.
- A change in the boundary conditions for any of the critical safety functions results in the definition of a new POS. For example, when reactor decay heat removal shifts from secondary heat removal to the residual heat removal system, a new POS is defined.
- Specific POSs may be defined for states with the potential for specific conditions or accidents, e.g., fuel handling accidents during core unloading or containment overpressure testing which affects automatic safety injection actuation systems.
- Transitions (from one steady-state POS to another) which are initiated or completed by manual operation, and which have the potential for a loss of safety function, may also be defined as a distinct POS or may be grouped with a similar POS. For example, draindown to midloop in a PWR can be a unique POS or grouped with the midloop POS.

In this step, both identification and grouping are inherently occurring as the procedural steps are mapped

into a smaller number of plant states. In theory, each step in the procedure could be mapped to a unique plant state. However, grouping into a smaller set of POSs is typically conducted based on the safety function success criteria.

5.0 Impacts of Varying Outage Types. The parameters defining the POSs allow the same POSs to be used in characterizing the different Outage Types. The Refueling Outage type typically defines the set of POSs included in the Shutdown QLRA model. Other outage types typically use a subset of the Refueling Outage POSs.

6.0 Variables Within a POS. Decay heat level, plant configuration, and equipment out of service for test or maintenance may vary *within* a POS. As previously discussed, SSCs that are unavailable or out of service are generally evaluated by the QLRA. The treatment of decay heat and plant configuration in the QLRA model is described below.

Decay Heat should be treated as an independent variable based on time after shutdown. Typically, the decay heat level will define the available time to align and/or actuate systems, and determine the viability of certain methods of decay heat removal and/or inventory control. Thus, the decay heat level can be used to define the success criteria for a safety function, and thus can be a factor in discrimination between POS. Alternately, decay heat can be used in the model logic to allow or disallow systems to support safety functions. Additionally, time to boil or time to core damage (inversely related to decay heat level) may be considered as equivalent to one or more levels of defense in depth.
Generally, if a POS does not contain decay heat level, the model will be more flexible, since any POS can be reached at any time after shutdown. This allows the shutdown QLRA model to be simpler by not requiring multiple POSs for the same RCS configuration, plant mode, etc.

Plant Configurations, except for the RCS, fuel and containment status, are generally independent of POS. The alignment of which pumps are running, which are in standby, and which are out of service for test or maintenance are typically variables that are used as an input to the QLRA evaluation, but are not typically used for selection of the shutdown POSs. This is because there are so many variations possible that modeling each as a unique plant state could make the model too large to be practical. This modeling also accommodates temporary systems that may be brought in for a specific outage.

7.0 Discrimination in Transient and Steady-State Plant Operational States. Discrimination between transient and steady-state conditions should be considered in defining POSs. A POS is considered a transition state when thermal power, temperature, and/or pressure of the reactor coolant system or the system related conditions for heat transfer change during the POS. The transition state can be modeled as a separate POS; it may also be subsumed into a steady-state POS, if the steady-state POS is bounding. Care must be taken and justification is necessary when combining transition and steady-state configurations into a single POS.

ATTACHMENT 2
TECHNICAL BASIS FOR QLRA METHODOLOGY

Information in this section was adapted from EPRI TR-1013501 [5].

This provides the basis for using QLRAs to effectively assess and manage configuration risk during shutdown operations. A QLRA developed using this Standard and the applicable portions of the methodology provided in EPRI TR-1013501 [5] is capable of providing a measure of risk (for the purposes of ensuring effective risk management) based on the following:

- Safety functions can be used to represent risk, since the loss of a safety function (and conversely, the success) can be shown to have an impact on one or more undesirable end states traditionally used for risk assessment (e.g., CDF, LERF).
- Increased capability of the safety function is analogous to decreased risk. If it is less likely for the safety function to be lost, the risk is lower. Conversely, decreased capability represents an increase in risk.
- A minimum acceptable level of safety function capability (i.e., DID) is determined. This defines the success criteria for the safety function.
- The likelihood of safety function success can increase or decrease from the minimum acceptable level, based on:
  - The number of SSCs capable of fulfilling the safety function.
  - The relative reliability, redundancy and diversity of the SSCs credited.
  - The presence or absence of Higher Risk Evolutions, which represent challenges to the safety function (i.e., initiating events).
  - The inherent risk associated with certain POS.
- The impact of available equipment, HREs and POS risk on safety function success likelihood can be compared on a relative basis.

The ingredients for QLRA applied for shutdown risk assessment include:

- Complete definition of each key safety function.
- Requirements and risk associated with minimal DID for each safety function.
- Systems, trains and components capable of satisfying each key safety function.
- Risk implications of Higher Risk Evolutions.
- Risk implications of Plant Operating States and Plant Configurations.
- Measure of Risk Condition.

Complete Definition of Safety Functions

- NUMARC 91-06 addresses key safety functions necessary to maintain frontline defense in depth.
- NUMARC 91-06 recommendation to include a Support System “safety function” provides the means to assess the risk of dependencies on a support system that can affect multiple frontline systems and key safety functions.

Requirements and Risk Associated with Minimal DID for Safety Function

- The minimum requirements for success of the Safety Function are defined for each POS. Below the minimum, risk is unacceptable; at or above the minimum, risk is acceptable with some gradation in acceptability and in the level of required compensatory risk management actions.
- The minimum requirements can be defined based on design basis, quantitative or bounding assessments.
- Minimal DID End States are scrutinized to assess the adequacy of operating in the minimal DID posture.
- Compensatory risk management actions are emphasized in this state.

Systems, Trains and Components Capable of Satisfying Safety Function

- Only systems capable of satisfying the safety function for the plant condition (DID level) evaluated that provide a measurable reduction in risk are credited
- Qualitative reliability of DID levels considers:
  - Necessary equipment is functional and available.
  - Complexity of aligning equipment (access, environment, tools).
  - Operator procedures, training and familiarity with equipment alignment.
  - Time necessary to align equipment is compared to the time available before undesirable end state (e.g., CDF, RCS boiling) occurs.
  - Duration alignment is effective.
  - Independence of equipment required from critical dependencies (power, cooling water) from other DID levels credited for the safety function
- DID levels with common critical dependencies (power, cooling water) are not credited as redundant capability due to the constraint of the common system potential to fail both trains

Risk Implications of Higher Risk Evolutions (HRE)

- HREs represent an increase in the likelihood of a challenge to a safety function; thus for the purposes of QLRA, they can be viewed as analogous to an initiating event.
- Activities with the potential to result in loss of an operating or standby DID level are presumed to result in the loss of the capability from a safety function assessment. (conservative)
- Typically this is applied by reducing the DID level by one grade (e.g., green to yellow) to highlight the need for risk management actions. However, the relative risk associated with the HRE should be compared to a DID level to determine the impact on DID (i.e., an HRE could reduce DID level by two if it is significant enough).
- Compensatory measures promote actions to protect equipment, recover equipment if the event occurs and/or restore DID level unaffected by the HRE to increase DID.

Risk Implications of Plant Operating State and Plant Configuration

- The minimal capability for the each safety function is defined for each POS.
- SSCs not capable of supporting their intended safety functions based on the POS are not credited.
  - Attributes of the POS that reduce the available time for operator actions are considered in determining the viability of applying DID levels.
- The inherent risk associated with the POS is factored into the evaluation of the Safety Function DID.
  - For example, risk is relatively lower with the reactor cavity flooded, because a large volume of water is available, increasing the time to boil and reducing the impact of leaks and draindowns.
  - The relative impact of the POS must be assessed and compared with the impact of a DID level.

Measure of Risk Condition

- The grades of DID are designed to promote awareness of degraded safety function conditions and promote risk management actions.
- Nominally, at least three levels of DID measures: unacceptable, minimal and acceptable are required to provide sufficient discrimination and allow appropriate management controls.
  - Recommended practices suggest four levels of defense in depth: unacceptable, minimal, reduced and acceptable.
- Risk ranking results must be validated to ensure that the relative risks assigned for the various POS/HRE/SSC combinations within a Safety Function are self-consistent. This means that configurations with similar relative risk levels should be assigned the same end state metric (e.g., color), while configurations with relatively higher or lower risk levels are assigned the proper end state metric compared to each other.
  - The risk associated with different DID levels between safety functions may also be compared. This will provide a better risk classification for the configuration. However, it is not necessary for the purpose of developing and implementing risk management actions. The possible benefits that could be obtained by doing this need to be balanced with the additional effort required.

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute (EPRI)

The Electric Power Research Institute (EPRI), with major locations in Palo Alto, California; Charlotte, North Carolina; and Knoxville, Tennessee, was established in 1973 as an independent, nonprofit center for public interest energy and environmental research. EPRI brings together members, participants, the Institute's scientists and engineers, and other leading experts to work collaboratively on solutions to the challenges of electric power. These solutions span nearly every area of electricity generation, delivery, and use, including health, safety, and environment. EPRI's members represent over 90% of the electricity generated in the United States. International participation represents nearly 15% of EPRI's total research, development, and demonstration program.

Together…Shaping the Future of Electricity

Printed on recycled paper in the United States of America

1016231

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com