Application of PRA in Risk-informed Risk Management

Jie Wu
Institute of Nuclear Energy Safety Technology,
Chinese Academy of Sciences

Abstract: This technical paper presents the concept of plant configuration risk management, the role of probabilistic risk assessment (PRA) in a risk-informed, performance-based integrated decision-making process during plant design, licensing and operation stages. It also provides an overview of PRA and its application commensurate technical adequacy, regulatory requirements for monitoring maintenance effectiveness and industry practice at operating nuclear power plants in the US.

Keywords: Configuration Risk Management, PRA Application, Maintenance Rule, MSPI, Equipment Reliability Monitoring Process.

1. INTRODUCTION

Risk is presented by undesirable consequences and the occurrence frequency of these consequences. Sometimes, risk is simply measured as the occurrence frequency of the undesirable consequences (as surrogate risk objectives/metrics). Presenting risk in a form of probability distribution requires much more detailed analysis. A summarized definition of risk can be described as a multiplication of frequency and consequence.

Questions associated with risk assessment generally include: What can go wrong? (a set of accident scenarios). How likely is it? (the probabilities of these scenarios). What are the consequences? (damage states). Prevent the accident occurrence and reduce the consequence is the principle of the risk management. The concept of risk management is application specific. It should be commensurate to deal with average risk and temporary risk increase associated with equipment out of service resulted from maintenance or other operational contingencies.

In a nuclear power plant, the commonly used risk metrics are Core Damage Frequency (CDF) and the Larger Early Release Frequency (LERF) resulted from the occurrence of an initiating event and failure of the expected mitigating system functions. The regulatory commission in nuclear industry also uses dose/consequence vs. frequency as acceptance criteria to ensure public safety. A postulated event with potential high dose release outside containment must have low occurrence frequency.

The license basis of a nuclear power plant specifies the upper limit of the cumulative CDF usually over 1 year time frame, i.e. the annual average risk. As far as accident probability is concerned, the annual average risk is managed through effective maintenance activities on risk significant equipment/components. Utilities may use Reliability Centred Maintenance (RCM) or streamlined RCM approach, establish Performance Indicator (PI) on plant, system and component level, predict future system reliability and compare with the previous system performance.

However, the temporary risk of a plant in a given configuration may exceed the average risk level due to equipment out of service, adverse weather conditions etc. The question here is how quick the inoperable equipment should be returned to service, or how long the plant can continue to operate with the increased temporary risk. Critical safety equipment down time or Allowed Outage Time (AOT) in a nuclear power plant is specified in standard Technical Specifications based on previous experience and deterministic approaches.

The concept of probabilistic approach for temporary risk management is to control the plant incremental risk within the acceptable level over the length of time associated with the temporary plant risk increase.

Overview of Probabilistic Risk Assessment

Probabilistic Risk Assessment, also referred as Probabilistic Safety Assessment (by IAEA definition), is an effective analysis approach that systematically analyses the accident sequence following a postulated initiating event, estimates the occurrence frequency, and identifies the associated dominant contributors to the defined end state of the accident sequence.

The PRA ultimately presents a set of scenarios, frequencies, and associated consequences, presented in such a way that forms a basis for design optimization, licensing support, determination of operational safety criteria and risk-informed decision making. Supporting decision-making in general requires quantification of uncertainty, and this is understood to be part of the PRA applications.

The first modern PRA, the Reactor Safety Study (WASH-1400), was completed in the mid of 1970s. Its stated purpose was to quantify the risks to the general public from commercial nuclear power plant operation. The PRA technology was introduced to China in the mid of 1980s. Chinese engineers were systematically trained at Gesellschaft für Reaktorsicherheit (GRS).

Key Tasks in Performing Probabilistic Risk Assessment:

- Systematic plant review (IE identification).
- Derivation of initiating event frequency.
- Plant response analysis (ET analysis).
- System reliability analysis (FT analysis).
- Reliability data collection and analysis.
- Accident sequence quantification.
- Uncertainty and sensitivity analysis.
- Results presentation and documentation.

2. THE ROLE OF PRA IN NPP DESIGN, LICENSING AND OPERATION

Application of PRA is now widely encouraged to play an important role in supporting the risk-informed integrated decision making process during NPP design, licensing application and during daily plant operation.

While still emphasizing the defense-in-depth principle in the risk-informed integrated decision-making process, the process looks the defense-in-depth principle in a more sophisticated way combining deterministic and probabilistic approaches. This can be briefly described by presenting the three aspects of the defense-in-depth and their linkage to PRA.

1). Defense-In-Depth in Design Aspect
General Design Criteria
Safety Design Guide

2). Defense-In-Depth in Process Aspect
Technical Specifications, Safe Operating Envelop,
Maintenance Rule, Impairment Manual, OP&P,
Risk-Informed Performance Indicator
and Equipment Reliability Monitoring Process.

3). Defense-In-Depth in Scenario Aspect

Emergency Operating Procedures
Severe Accident Management Guidelines
Emergency Planning

For example, in a traditional deterministic approach, single failure criterion is considered as an effective measure to achieve defense-in-depth, designers use single failure criterion on safety system design to enhance the system ability for accident mitigation. By combining deterministic and probabilistic approaches, the defense-in-depth is achieved in an integer fashion through a more balanced risk-informed integrated decision-making process, aiming on the reduction of CDF.

The role of PRA during plant design is mainly focused on how to use the risk insights obtained from PRA to optimize the plant design using risk-informed integrated decision-making as well as provide technical support to Severe Accident Mitigation Design Alternatives (SAMDAs). As the plant design evolves, level of detail of the PRA model will be increased accordingly. In the course of design certificate and licensing application, PRA will be used to demonstrate that the plant design meets the overall safety goals (in terms of CDF and LERF).

During plant operation, the role of PRA is further enhanced to provide necessary technical support in the risk-informed integrated decision-making process. The success key for a systematic application of PRA in this stage is to establish a risk-informed configuration risk management program at an operating plant to ensure safe and economical operation.

A well established risk-informed plant configuration risk management program ensures that potential risk is appropriately evaluated prior to the scheduled maintenance activities, and the risk associated with emergent event(s) is appropriately evaluated in a timely manner.

3. PRA TYPES AND APPLICATION COMMENSURATE TECHNICAL ADEQUACY

Being developed for more than two decades in methodologies and applications, PRA as a systematic analysis tool can be categorized in three development stages to suite different application needs.

The first stage is represented by Basic PRA model, in which the PRA model is basically used for design optimization and forms as part of the licensing basis support documentation.

The second development stage, represented by Living PRA model, emphasizes utility's needs to periodically update the PRA model to reflect the changes of plant safety characteristics such as design modification, system upgrade, change of operating procedures, aggregation of plant specific reliability data etc. The Living PRA model forms a basis for the risk-informed decision making by measuring the degree of risk increase based on permanent changes to the licensing basis. It is however difficult to use this model to trace the temporary risk changes during a plant operation.

The third PRA development stage, overwhelmed by the development of Risk Monitor Tools, symbolizes the beginning of systematic application of PRA to support the implementation of risk-informed and performance based regulation. This type of PRA model is called as Risk Monitor PRA model or sometimes simply referred as (dynamic) operational PRA model. It is a plant specific PRA model that reflects the actual plant configuration, explicitly defines running and standby trains, cross train connections, maintenance or other plant operational activities etc., and employs multiple build-in user friendly graphic interfaces via a risk monitor to quickly reflect the actual plant configuration of interest and significantly reduces the effort to operate a PRA model.

The Risk Monitor PRA model represents the trend of the future dynamic model development in PRA application. It is loaded into a risk monitor software to form a plant specific real-time analysis tool that can provide on-line technical support for risk-informed decision making under high stress adverse circumstances. Risk being monitoring by current risk monitor tools includes: CDF, LERF, Boiling Frequency and Spurious Trip Frequency. The future development trend of the tools will more likely cover monitoring capabilities for tracking economic risk, not only optimizing outage maintenance activities but also plant life and assert management strategies.

Based on the PRA development stages and their capabilities discussed above, PRAs can be categorized as the following three application commensurate types:

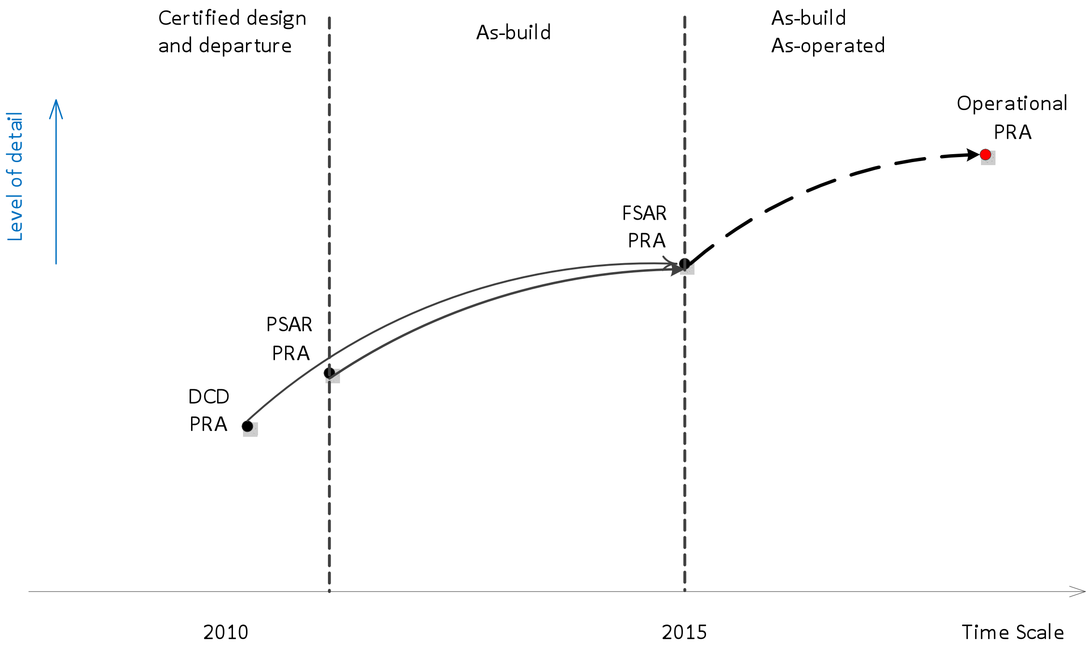
- Design Assist PRA
- Licensing Support PRA
- Plant Specific Operational PRA

Their characteristics and target application commensurate level of detail, measured against PRA capabilities specified in ASME PRA Standards, are summarized in the following table:

PRA Type and Characteristics Measured Against ASME PRA Standards

Application Stage	PRA Type	Characteristic	ASME PRA Stds
Design	Design Assist PRA	High Level	Category I
Design and Licensing	Licensing Support PRA	Level of detail up to a specific freeze date	Category II
Plant Operation	Living PRA	Reflect “as-build” and “as-operated”, not dynamic.	Category III
	Operational PRA	Reflect “as-build” and “as-operated”, dynamic, living, Risk Monitor compatible	Category III

General development stages of a PRA model is illustrated in the following diagram:



Where,

DCD PRA is used to support Design Control Document for Design Certification in the Combined Construction and Operating Licensing (COL) Approach;

PSAR PRA is used in the traditional licensing approach to support Preliminary Safety Analysis Report for Construction Permit, and to reflect site specific design features;

FSAR PRA is used to for both traditional licensing and COL approaches to support Final Safety Analysis Report for initial fuel loading, and to capture site specific and “As-build” features;

Operational PRA is a plant specific PRA reflecting both “As-build” and “As-operated” features, after the plant has been constructed and commissioned, to support risk-informed applications in the integrated decision-making process.

4. MANAGING PERMANENT RISK AND TEMPORARY RISK

Risk is generally presented by undesirable consequences and the occurrence frequency of these consequences. In the simple form, risk is a multiplication of frequency and consequence. In a nuclear power plant, the Core Damage Frequency (CDF) and Large Early Release Frequency (LERF), resulted from the occurrence of an initiating event and failure of the expected mitigating system functions, are the commonly used surrogate risk metrics.

Permanent risk is the risk level associated with the inherent plant features designed for accident mitigation, operational and maintenance practices that form the Licensing Basis (LB). Permanent risk is measured by the annual average CDF and LERF. Changes to licensing basis, such as back-fitting, modification of Technical Specifications will result in changes in permanent risk level of a nuclear power plant.

Though the license basis of a nuclear power plant specifies/documents the upper limit of the annual average risk, instantaneous risk of a plant at a given time point may well be above this upper limit. This is referred as the temporary (conditional) risk increase under a given plant configuration resulted from maintenance or other operational activities, random component failures, adverse weather or power grid conditions. Different concept is required to manage the temporary risk increase to ensure public safety.

Risks governed by Technical Specifications

The majority of the temporary risks should have been addressed in the traditional Technical Specifications through prescriptive completion time under a given Limiting Condition for Operation (LCO). Critical safety equipment down time or Allowed Outage Time (AOT) and Surveillance Testing Interval (STI) are specified in the Technical Specifications based on previous experience or deterministic approaches. The current trend is to risk-informing the traditional Technical Specifications.

Risks not governed by Technical Specifications

The traditional Technical Specifications do not govern the entire risk spectrum under various operating conditions of a nuclear power plant. Contingencies not addressed in the Technical Specifications include: multiple equipment/components out of service, likelihood of additional equipment/component failure, adverse weather or power grid conditions. These contingencies can eventually lead to the declaration of entering multiple LCOs that may not be well addressed in the Technical Specifications.

Technical Specifications

Technical Specifications govern normal plant operation. LCOs associated with equipment out of service and equipment Surveillance Requirements are specified in the Technical Specifications. They dictate what equipment must normally be in service, how long equipment can be out of service, and specifies compensatory actions within an allowed outage time (or completion time) and the surveillance test intervals to demonstrate equipment availability.

Risk-informed Technical Specifications take advantage of the risk insights derived from a plant specific PRA and consider them in an integrated decision making process to optimize the equipment Allowed Outage Time (AOT) and the Surveillance Test Interval (STI), maintain or improve safety while reducing unnecessary burden.

Since the mid-1980's, the NRC has been reviewing and granting improvements to Technical Specifications that are based, at least in part, on PRA insights. In its final policy statement on technical specification improvements of July 22, 1993, the Commission stated that it expects that licensees will utilize any plant specific PRA or risk survey in preparing their technical specification related submittals.

Maintenance Rule

NRC Maintenance Rule, 10 CFR 50.65 (a)(4), requires a licensee to assess and manage the increase in risk that may result from the proposed maintenance activities before entering the maintenance configuration and right after entering a non-voluntary configuration during all plant operation modes. It is one of the most influential regulatory rules in the risk-informed regulation and PRA applications.

The Maintenance Rule shares the fundamental principle of Technical Specifications to provide adequate assurance of the reliability and availability of equipment needed to prevent operational transients and mitigate accidents. It has significant implications for the evolution of Technical Specifications.

In addition to a balanced maintenance strategy between equipment unavailability and reliability, 10 CFR 50.65 (a)(1) requires a licensee to monitor the performance or condition of SSCs to assure their intended functions. As such, NRC has established a risk-informed performance monitoring process for safety significant mitigating systems of each operating NPP known as Mitigating System Performance Index.

MSPI Description

Mitigating System Performance Index (MSPI) is an improvement over the traditional Safety System Unavailability Performance Indicator (SSU PI). It is a risk-informed Performance Indicator (PI) in the Reactor Oversight Process (ROP), and relies heavily on the quality of a licensee's PRA and the reliability information.

MSPI is defined as the sum of changes in a simplified core damage frequency evaluation resulting from changes in unavailability (UAI) and unreliability (URI) relative to baseline values.

MSPI = UAI + URI

Where

UAI = the sum of all unavailability (UA) contributions on a train basis within a monitored system.
URI = the sum of all unreliability (UR) contributions on a component basis within that system.

The quantification of UAI and URI uses a plant specific PRA model and maintenance unavailability data based on three-year average maintenance and operating experience. MSPI took effect at the beginning of the second quarter of 2006 (or April 1, 2006). Licensees are required to report these two values for each of the monitored systems to NRC, and the summed MSPI value will be posted on NRC website.

Currently MSPI monitors the performance of the risk-significant functions of the following typical selected systems of an operating PWR plant:

- Emergency AC power system
- High pressure safety injection system
- Auxiliary feedwater system
  (Reactor core isolation cooling system in BWR)
- Residual heat removal system
- Cooling water support system (includes risk significant direct cooling functions provided by service water and component cooling water)

MSPI reflects the composite averaged performance of important components and trains within a monitored system over a 12 quarter (three-year) period, and is indexed to the change of core damage frequency resulting from changes in unavailability and unreliability of the monitored system.

Equipment Reliability Monitoring Process

The equipment reliability monitoring process combines RCM and PRA technique and further extents risk-informed PI to safety important equipment. It narrows down the safety important system to the equipment level through the application of risk-informed categorization of equipment and use PRA technique to establish, evaluate and optimize maintenance strategies. The expected reliability target of safety important equipment and the proposed maintenance strategies to achieve this target are clearly defined in the process. The effectiveness of the maintenance strategies is ultimately measured against the availability/reliability performance of the monitored equipment.

Major tasks (except reporting) in the equipment reliability monitoring process, methods and correlations to PRA are summarized in the following Table:

Risk-Informed Equipment Reliability Process, Methods and PRA Correlations

Reliability Process	**Method Summary**	**Correlation to PRA**
Identification and Rank Risk-Significant SSCs	Deterministic and Probabilistic	Strong Use PRA to identify and rank risk-significant SSCs
Specify Reliability Targets	Probabilistic	Strong Use PRA to set reliability targets for systems other than Safety Systems
Define Maintenance, Surveillance and Testing Programs	RCM, Maintenance Rule (Impairment Manual, OP&P and Heat Sink Manual)	Supportive Use PRA to optimize the maintenance strategy and surveillance test interval
Monitoring Performance and Condition	Measurable Parameter, PFU and risk-informed Performance Index	Strong Use PRA to predict future unavailability
Aging and Life Cycle Management	Trending Analysis and Long Term SSC Health	Supportive
Corrective Actions	Feedback and Improvement	Supportive

5. CONCEPT OF DEALING WITH TEMPORARY RISK

The concept of dealing with temporary risk increase is to control the plant incremental risk, the ICCDP, within the acceptable level over the length of the time associated with increased temporary plant risk.

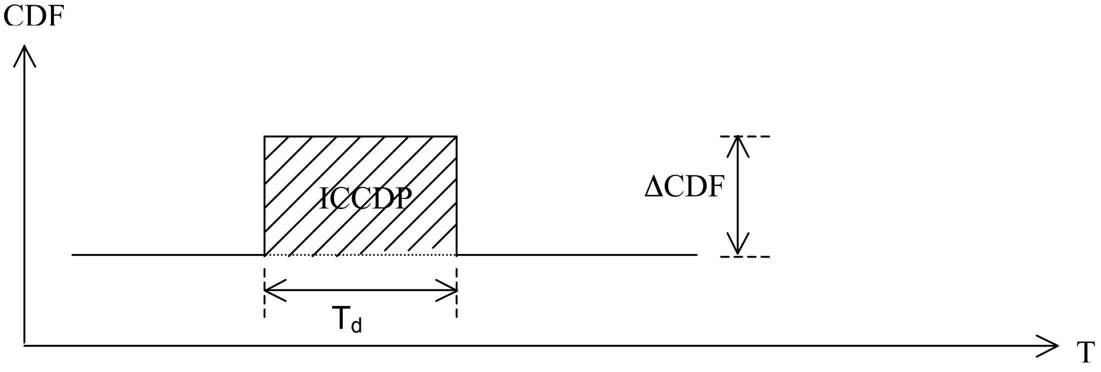


Figure1, Illustration of Quantitative Presentation of Temporary Risk

The temporary risk can be expressed by the following equation:

$ICCDP = \Delta CDF * T_d$

Where

ICCDP	= the incremental conditional core damage probability
ΔCDF	= the conditional risk increase under a given plant configuration
T_d	= the time duration of the specified plant configuration

To monitor the cumulative impact resulted from each temporary risk, a cumulative Risk Monitoring Program should be established. The total temporary risk increase over the observation time period, for example over 1 year, can be then measured as the 'sum of each individual ICCDP' (ΣICCDP) recorded over the 1 year time period, counting the actual completion time spent to restore the failed component(s).

The numerical values recommended for the parameters used for temporary risk control are presented as follows. They are subject to industry consensus and regulatory approval.

ICCDP:	$< 5 \times 10^{-7}$
ΣICCDP:	$< 10^{-6}$
ΔCDF:	$< 10^{-4}$

Actions related to temporary risk management are further discussed in next section.

6. NUMERICAL ACCEPTANCE GUIDELINES

Numerical acceptance guidelines for time-average plant risk, resulted from permanent changes to LB, are based on the Change of Plant Core Damage Frequency (ΔCDF) in three regions as specified in USNRC Regulatory Guide RG 1.174.

ΔCDF $< 10^{-6}$	The change request will be considered without a calculation of the total CDF.
$10^{-6} < \Delta$CDF $< 10^{-5}$	The change request will be considered only if the total CDF is less than 10-4 per reactor year.
$10^{-5} < \Delta$CDF	The change request would not normally be considered.

Numerical acceptance guidelines for actions related to temporary risk, resulted from maintenance or other operational activities, random component failures, adverse weather or power grid conditions are recommended as follows:

$10^{-4} < \Delta$CDF $< 5\ \text{x}10^{-4}$	Temporary measures should be in place when restoring failed component(s).
$5\ \text{x}10^{-4} < \Delta$CDF $< 10^{-3}$	This configuration should be avoided. When non-voluntary entering, more cautions should be excised.
$10^{-3} < \Delta$CDF	Current industry consensus consider this as a high risk region, the reactor should be shutdown.

7. DEALING WITH UNCERTAINTIES IN INTEGRATED DECISION-MAKING PROCESS

The purpose of the uncertainty analysis is to determine the degree of uncertainties associated with the calculated severe core damage frequency. The purpose of sensitivity analysis is to determine whether the results are strongly impacted by certain important elements of the PRA due to the existence of alternative modeling and analysis approaches.

Uncertainties in the PRA affect the soundness of the PRA insights and thus weaken the role of the PRA in the risk-informed integrated decision process. Different types and sources of uncertainties exist in the PRA model. They can be summarized as the following three main categories:

- Parameter Uncertainty.
- Model Uncertainty.
- Completeness Uncertainty.

Parameter uncertainty, stemming from having only a relatively small set of randomly generated data, appears in the component failure probabilities/rates, initiating event frequencies and human error probabilities. They are typically characterized by establishing probability distributions on the parameter values. The degree of uncertainty is generally represented by the "error factor" which determines the 95% upper confidence limit over the 50% value of an assumed log-normal distribution. Parameter uncertainty associated with individual basic event can be propagated to the distribution of the final PRA results such as CDF.

Model uncertainties arise when there are several alternative approaches to the analysis of certain elements of the PRA model. Different opinions on how the failure mechanism and plant response should be modeled and luck of industry's states of knowledge on certain phenomena are the main sources for model uncertainty. Examples would be approaches for Human Reliability Analysis (HRA), Common Cause Failure (CCF) modeling, and thermosyphoning on loss of electrical power to reactor coolant pumps. The impact of using alternative assumptions or models may be addressed by performing appropriate sensitivity studies or qualitative arguments.

Completeness uncertainty reflects the limitations in the PRA scope and is statistically not an uncertainty itself. However, unanalysed risk contribution introduce the uncertainty about where the true risk lies, and make it difficult to estimate the magnitude of the unanalysed risk portion. Examples are some external event PRA and the low power or shutdown state PRA. The issue of completeness in PRA scope can be addressed by supplementing additional analysis, or confirm that the out-of-scope contributors are not significant.

8. PATH FORWARD AND CURRENT ISSUES

The PRA technology was introduced to China in the mid of 1980s. Chinese engineers were systematically trained at Gesellschaft für Reaktorsicherheit (GRS). More than two decades have been passed before the usefulness of PRA was recognized by various organizations.

Currently, several design institutes and power plant utilities are actively using PRA for design optimization and supporting operational decision-making for enhanced safety and economic. The regulatory body, NNSA, is also actively working on risk-informed regulation and PRA application guide. In the recently issued regulatory codes and technical policy, NNSA emphasizes the use of PRA for severe accident sequence identification and increased use of PRA to support risk-informed integrated decision-making at operating plants.

However, due to inadequate technical resources, the establishment of comprehensive PRA application guidelines is still a long way to go. Experience from successful PRA application pilot projects are therefore of more important to accelerate this process.

Current issues for successful PRA application pilots are apparent in the following three aspects: (1) The role of PRA in the risk-informed integrated decision-making process; (2) Limitation of use of plant specific and high quality generic reliability database; (3) lack of harmonization in PRA model development at various stages and consistency in terms of level of detail.

References

[1] "Framework for Development of a Risk-Informed, Performance-Based Alternative to 10 CFR Part 50", NUREG-1860, July 2006.

[2] "Approaches to Risk-Inform and Performance-Base the Requirements for Nuclear Power Reactors", SECY-06-0007, January 2006.

[3] "Combined License Applications for Nuclear Power Plants (LWR Edition)", Part I, C.I.19, USNRC RG1.206, June 2007.

[4] "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sa-2009, February 2009.

[5] "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities", USNRC RG1.200, March 2009.