

Probabilistic Safety Assessment (PSA)

December 2007

**Incorporated administration agency
Japan Nuclear Energy Safety Organization
JNES**

Preface

"Probabilistic Safety Assessment, PSA"

We have experienced big accidents of large-scale and complex systems typified by huge plants, transportation systems, etc., which were created by human beings with state-of-the-art technology and knowledge. And, many researches have been conducted, reflecting the bitter experiences and aiming at making them safer systems, and many improvements have been accomplished. The PSA is an assessment method aimed at ensuring safety by analyzing factors to cause a big accident and its probability and taking measures in advance. A nuclear power plant is a typical huge plant where its safe operation is ensured with many systems and components as well as personnel who manage its safe operation. Nuclear power plants are designed using the PSA as one of their safety assessment methods. For helping you better understand the PSA after the example of an event somewhat familiar to you, a study using the PSA method on "Whether the RMS Titanic accident occurred due to many unfortunate events in succession or as an accident waiting to happen", presented at the 1st research introduction meeting in FY 1999 held by the Ship Research Institute, Incorporated administration agency: National Maritime Research Institute is introduced here: More details are available at the Website (*1), though it is unfortunately only in Japanese.

The analysis of the RMS Titanic accident with an event tree methodology (*2) that is one of PSA assessment methods shows as follows. "The probability of the wreck at sea that is similar to the RMS Titanic accident is 2.05×10^{-2} times / voyage, which means that an accident similar to the RMS Titanic accident will happen with a large probability as much as approximately once every 49 voyages. So, a sea trip in early 20th century was riskier than we can image. That is, high-speed navigation was conducted at night without benefits of weather forecast and radar, and furthermore, search and rescue organization in case of an accident was very poor. The number of life boats was far fewer than the number of passengers aboard the Titanic, there was no distress beacon generator like the emergency position indicator radio beacon (EPIRB), and the system receiving wireless signals was not prepared. The RMS Titanic case can be said as an unavoidable accident under the circumstances of those days." Furthermore, the study introduction continues as follows.

"This accident was taken as a lesson learned leading to various safety measures including navigation methods, which has prevented the occurrence of an accident similar to the RMS Titanic case and has ensured safe voyage. For example, it is considered that the threat of icebergs must have been newly recognized due to the accident. Actually, the USCG (*3) has provided important data and information on icebergs for the safety of navigation, etc."

"Various safety measures have been taken and voyages have become safer these days

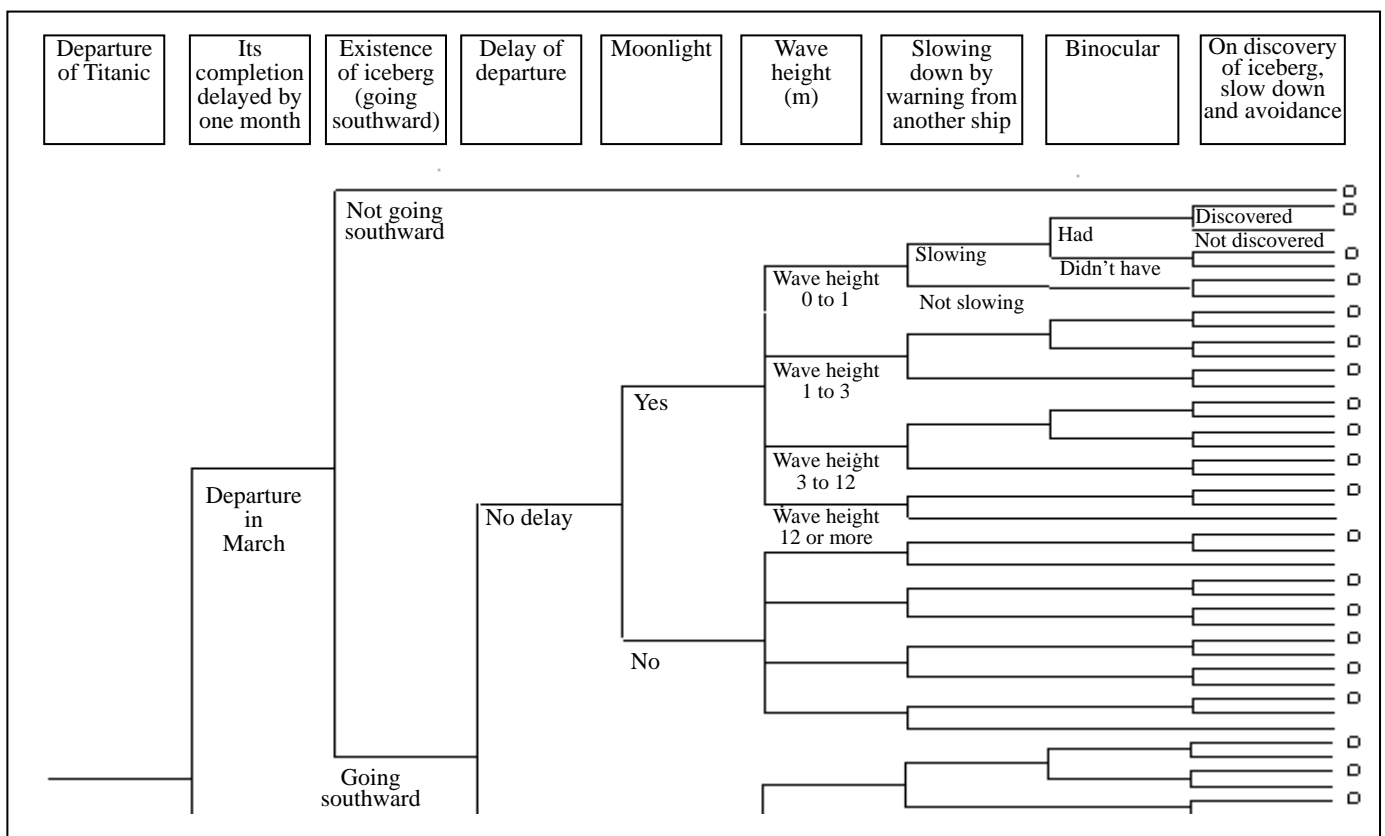
compared with back then. The actual accident-occurrence probabilities in 1978 to 1995 support this fact." Finally, the study concludes as follows. "The PSA quantitative assessment method using event tree analysis shows some examples from which the useful information for the accident analysis / accident investigation can be obtained. It is desirable to further discussions on ensuring safety also in the maritime field based on such a quantitative assessment."

Thus, the PSA is used aiming at enhancing the safety of large-scale and complex systems, such as huge plants, transportation systems by numerically identifying the weaknesses of the systems and taking the specific measures.

(*1): <http://www.nmri.go.jp/sed/psa/titanic/>

(*2): A part of event tree for the RMS Titanic accident

The causes for the RMS Titanic accident were analyzed, and taking the measures that could eliminate the causes one by one, an accident of this kind is to be prevented.



(*3): United States Coast Guard, U.S. Department of Homeland Security

Table of Contents

1. Introduction
 2. History of Development of PSA Technologies
 3. Summary of PSA Technologies
 4. PSA Technology Utilization
 5. Summary of Level 1 PSA
 6. Summary of Level 2 PSA
 7. Summary of Level 3 PSA
 8. Summary of Seismic PSA
 9. Issues in the Near Future
 10. Summary
- References

1. Introduction

Due to the progress in probabilistic safety assessment ([PSA](#)) technology, many countries, mainly Western ones, have recently carried out an attempt to perform effectively and efficiently the safety management of reactor facilities, utilizing the risk information obtained from the PSA.

The U.S. nuclear power plants have attained high availability factor, and the maintenance management utilizing the risk information and the development of rational safety regulation responding to it can be cited as one of the reasons.

At present, energetic activities have been promoted also in Japan towards utilization of risk information, and the PSA technology is its underlying one.

2. History of Development of PSA Technology

The PSA technology for reactor facilities has been developed in U.S. since 1960s, and the reactor safety study disclosed in October 1975 almost established its conceptual framework.

Since the [Three Mile Island \(TMI\) accident](#) that occurred in March 1979, the safety of the light water reactors has been improved remarkably following the progress of studies on the [severe accident](#) (an event that is far more significant than any events postulated at design and results in the significant core damage). As events similar to the Three Mile Island accident have been addressed in reactor safety studies, the PSA technology have been focused and since then, the PSA has come to be frequently used as a comprehensive assessment means for the safety of nuclear power plants not only in U.S. but also in many countries.

Countries that operate and/or construct nuclear power plants have PSA implementing programs specific to individual plants. In some countries, the PSA has become substantially a requirement for licensing, and utilization of [risk](#) information obtained from the PSA has become almost indispensable for plant safety management.

On the other hand, the industrial society that experienced a drastic increase in plant operation cost, such as an increase in the number of plant personnel, plant modification cost, loss due to reactor outages during modification, following the enhanced regulation after the Three Mile Island accident, considered that regulatory requirements with low contribution to safety should be relaxed, and resources should be allocated with an emphasis on more essential risk reduction activities, and proposed to the NRC to introduce the quantitatively-risk-based regulation in 1992.

The NRC considered the total policy on utilization of the PSA in regulatory activities, announced in August 1994 a proposal of policy statement for utilization of the PSA for nuclear regulation and a proposal to systematically implement the PSA, and started toward an introduction of a quantitative risk into the regulation.

The NRC stated in the final policy statement in August 1995 "that a framework to apply PSA to nuclear regulatory activities should be established in such a way that PSA can be applied in a consistent and foresighted manner to promote regulatory stability and efficiency."

Moreover, the NRC has promoted studies on specific issues, such as review of in-service-test frequency, introduction of quality assurance according to the importance of systems and components to the overall risk, review of in-service-inspection items, as a pilot application study on the risk-informed regulation, and based on these experiences, has developed rules and guidelines related to the regulation that encourage utilization of the risk information and established a framework for serious utilization of risk information.

These guidelines do not replace the existing guidelines, but are added as options. Namely, applicants can choose a method that conforms to either guideline, in changing the equipment subject to test and its frequency, for an example.

At the same time, European countries, who experienced the [Chernobyl accident](#), have fostered the safety culture through the IAEA and OECD/NEA and come to take measures such as plant modifications and establishment of emergency operation procedures, sharing the latest PSA technology and risk information for prevention and mitigation of a severe accident.

Many initial purposes of the PSA were to understand relative design weaknesses and improvement of operation manuals, but in these days, it has come to be applied to support operation activities, such as maintenance and tests, inspection and quality assurance. Furthermore, it is being applied to online real-time risk assessment during operation and aging management activities.

3. Summary of PSA Technology

Since nuclear reactor facilities contain a large amount of radioactive material, a large potential of risk is involved. Therefore, in the deterministic safety assessment method, measures for safety protection, such as "measures to prevent an anomaly such as a failure or a trouble", "measures to prevent escalation of an anomaly and its development to an accident", and "measures to prevent an abnormal release of radioactive materials" are taken in parallel based on the defense-in-depth concept. And also, assuming design basis events, the behaviors of a nuclear reactor facility and its impact on a surrounding environment are assessed to confirm the adequacy of those safety protection measures.

As for the design basis events, small number of representative sequences that could lead to the severest consequence to the public are selected taking into consideration the potential progressiveness of many anomalies and accidents, and are assessed based on conservative assumptions (for example, assumption of a single failure in the most effective accident mitigation system and no operator action to be expected for a short time period after the occurrence of the event).

On the other hand, the probabilistic safety assessment using PSA is to quantitatively analyze and evaluate the frequency of initiating events, such as an anomaly and a failure, the failure probability of safety functions that prevent escalation of the event that has occurred and mitigate the consequence, and the progress and effects of the event, covering all theoretically conceivable accident sequences, and then evaluate the overall safety based on the initiating event probability and extent of the consequences, or the product of both (risk).

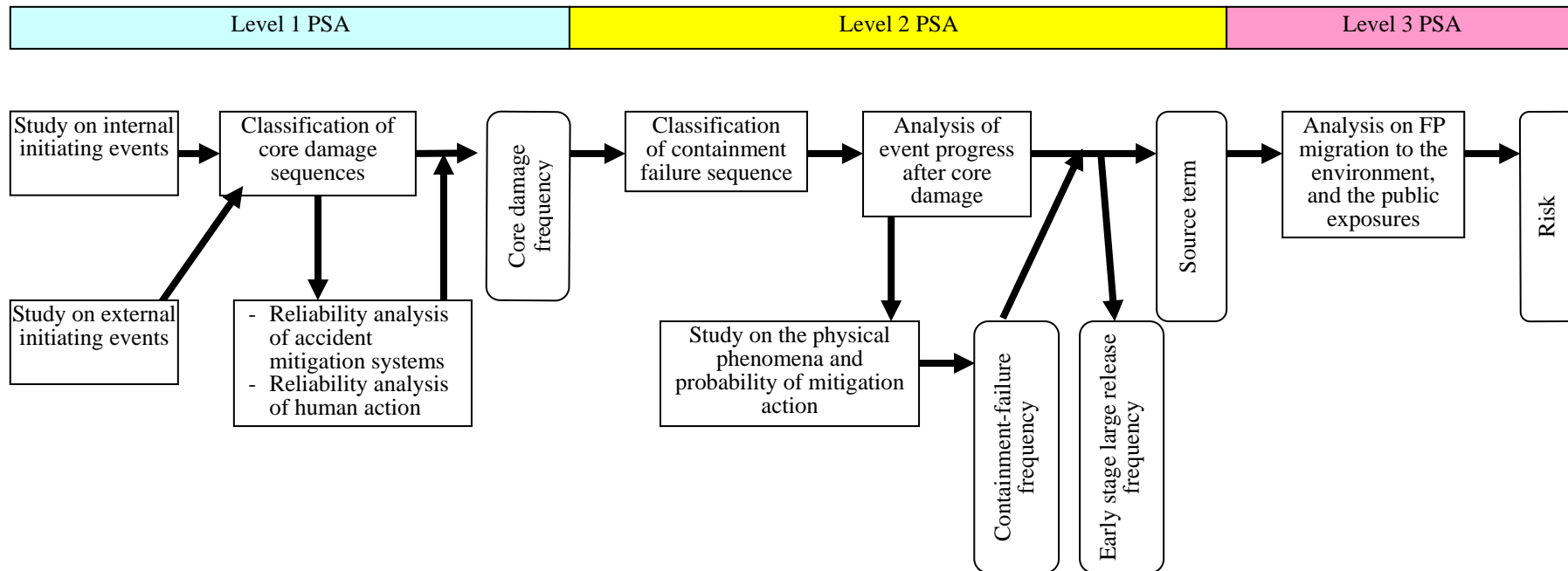
The PSA is especially effective in comprehensive assessment of various measures to prevent a severe accident of which probability is very small but its progress is extensive and wide-ranging, and mitigate its consequences.

Comparisons between features of the deterministic safety assessment and the probabilistic safety assessment using PSA are given in Table 1.

The PSA is divided into three steps as shown in Figure 1. The scope of the level 1 PSA is to analyze the reliability of systems and components that consist of the nuclear reactor facility and then assess the frequency of a core damage, that of the level 2 PSA is to assess the frequency of an accident that releases a large amount of radioactive material outside of the facility and source terms (type of radioactive materials, chemical forms, amount of the release, onset and duration of the release, etc.), and the level 3 PSA is to assess the public risk.

Table 1: Comparison between [Deterministic Safety Assessment](#) and Probabilistic Safety Assessment of Nuclear Reactor Facilities

	Deterministic safety assessment	Probabilistic safety assessment
Events to be covered	Small number of representative events considered to be the severest among conceivable events	All accidents considered to be significant
Frequency	Simply assumed to occur (no discussion of its frequency)	Since the frequency has a probability distribution, it is assessed with a median value, or a mean value and uncertainty width.
Method of an accident analysis	In accordance with the scenario defined by the Regulatory Guide for Reviewing Safety Assessment of Light Water Nuclear Power Reactor Facilities etc., it is analyzed based on conservative assumptions (for example, a single failure is assumed for the most effective accident-mitigation system).	Taking into account progresses of various conceivable accidents, all significant accidents (accident sequences) are analyzed under the realistic assumptions (multiple failures of mitigation systems are to be assumed.)
Risk assessment	NA or qualitative analysis	Quantitative analysis
Treatment of uncertainties	Discussion on uncertainties is avoided by following "the conservative methods for accident analysis."	Quantitative analysis including the propagation of uncertainties (in order to make a realistic assessment, the uncertainty will become large in addressing the areas with poor knowledge).
Interpretation of assessment results	Individual interpretation for each accident.	Comprehensive interpretation based on all accident sequences.
Examples of application	Appended documents 10 of the Application for Reactor Establishment License	U.S. Nuclear Regulatory Commission: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400



[Major information to be obtained]

- Frequency of initiating events
- Non-reliability of the system, equipment and human action
- Core damage frequency (CDF)
- Containment failure frequency (CFF)
- Large early-stage release frequency (LERF)
- Source terms (type of radioactive materials, chemical form, amount of release, etc.)

- Risks (health effect on individual and group for a member of the public etc.)
- Risk importance of systems or equipment
- Uncertainty width and its contributing factors of analytical results
- Dominant core-damage sequence
- Relative vulnerable points of systems
- Core damage frequency variation due to a change in design, operation management, etc.

Figure 1 Scope of probabilistic safety assessment and information to be obtained

4. PSA Technology Utilization

(1) Cases of PSA utilization in Japan

The concept of risks has been used partially in design and assessment of nuclear power plants, but the PSA technology has remarkable features and advantages in its capability to assess the overall plant risk clearly, quantitatively and systematically.

The PSA makes clear risk characteristics of a nuclear power plant: that is, what kind of scenario would increase risk, which system would play an important role and where weaknesses exist in the scenario. Thus, this will lead to the information on what kind of measures is effective in reducing the plant risk.

(a) Case 1 of PSA Utilization: Accident management

There is a case that the PSA was used in addressing an issue called [accident management \(AM\)](#). Electric utilities carried out the PSA for all of the domestic plants, and understood the plant features from a viewpoint of risk, so to speak, risk profile of each plant by around 1994. Following the results, effective measures for reducing risks (called AM measures) were planned and implemented. Establishment of these measures was completely over in 2002, and it was confirmed that the actual reactor safety improved substantially by the PSA carried out again (Figure 2).

(b) Case 2 of PSA Utilization: Risk management during plant operation and shutdown

As a PSA utilization for operation management, a study on more scientific and rational review of management rules for operation and maintenance, which were established based on the experience or deterministic concept in the past, based on quantitative risks obtained by the PSA has also being promoted. For example, when deciding processes and/or schedule of a periodical inspection, it is possible to reduce the high risk involved using the results of PSA conducted in advance. That is, when it is found that there is a time period with very high risk, the processes and/or schedule of the periodical inspection can be adjusted a little so as to eliminate such a time period (Figure 3.) Furthermore, the adequacy of changes in processes and/or schedule can be confirmed with the risk assessment. That is, reasonable and safety-ensured management of daily activities during the plant periodic inspection also becomes possible by preparing an appropriate arrangement and organization for a relatively high-risk time period due to the change.

(c) Case 3 of PSA Utilization: Importance assessment of an event that occurred

The importance assessment of an event is another example of PSA utilization in operation management. This is intended to quantitatively assess the effects of an event that occurred at a power plant on risk (importance) using PSA, and to use the results for a study on rational measures. There was a case that indicated the importance to safety of

the [ECCS](#) strainer plugging using the PSA in studying the issue. Such an effort is helpful for enhancement of licensees' operation-and-maintenance management (Figure 4).

(d) Case 4 of PSA Utilization: Evaluation of scram frequency

As a safety indicator and plant shutdown risk indicator, an assessment method of the frequency of events that do not result in core damage, but lead to reactor shutdown has been put in practical use. Since this method models components of normal systems that are not covered in the level 1 PSA for assessment of core damage frequency, and it is possible to assess the importance of the equipment other than those of safety systems, it is expected that this method leads to expansion of the PSA scope and its application from now on.

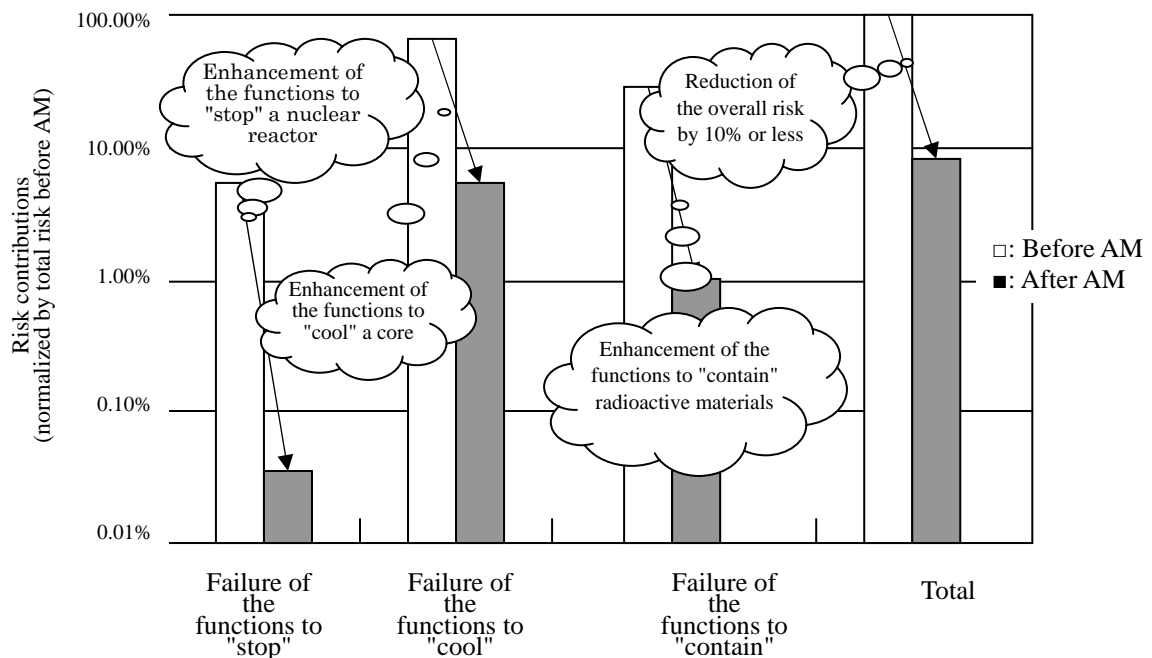


Figure 2 Example of PSA results and AM effectiveness

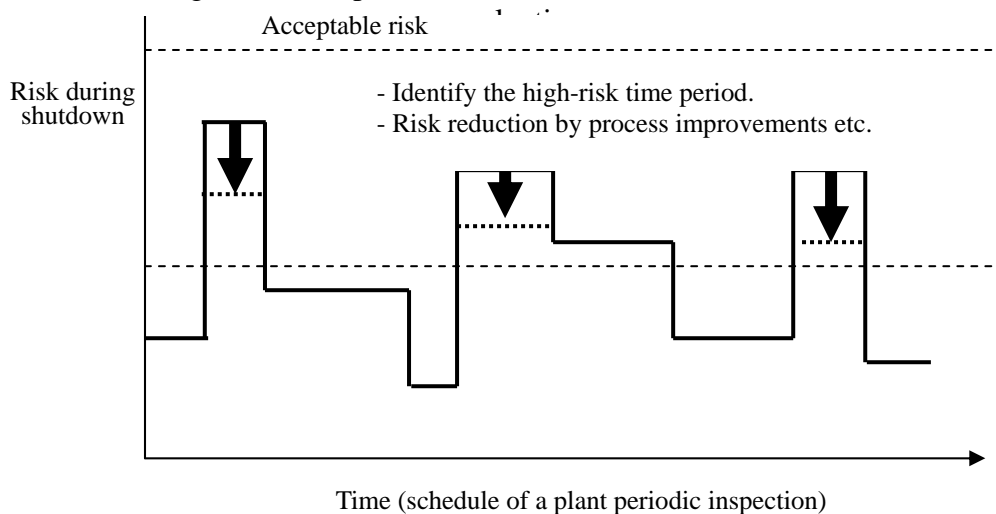


Figure 3 Image of schedule control using the risk information

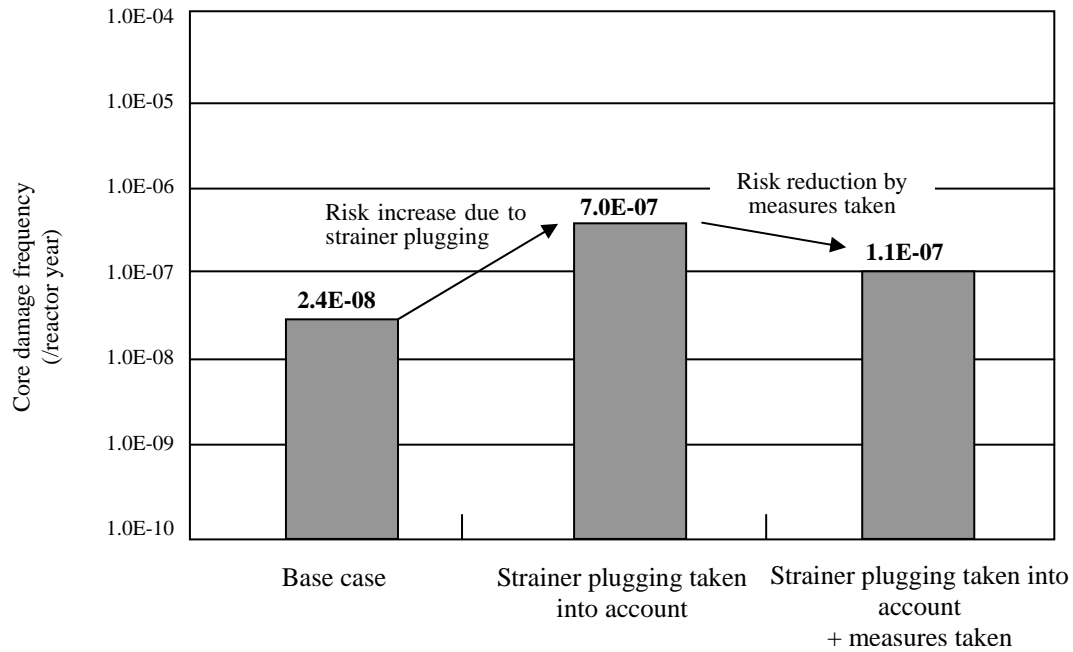


Figure 4 Example of impact assessment of ECCS strainer plugging event

(2) Cases of PSA utilization in U.S.

Five regulatory guidelines for risk utilization issued by the Nuclear Regulatory Commission in 1998 played a large role in the progress of the risk-information utilization in U.S.

Among these, the guideline to be called a comprehensive guidance, Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis" describes the change process of the plant's license basis and five principles (meeting the current regulations, consistency with the defense-in-depth philosophy, maintaining sufficient safety margins, maintaining the risk increase small, and monitoring the impact).

The "maintaining the risk increase small" means to determine the acceptability of proposed changes according to increments of core damage frequency increase (Δ CDF) due to a certain change with the current core damage frequency (CDF) as the criteria taken as a horizontal axis (Figure 5.)

Other risk indicators that are used in the four remaining individual guidelines are the risk importance and cumulative risk.

Using risk importance, the relative importance of the activity concerned is changed using the quantitative importance indicator assessed for each component: i.e., the activities important to safety should be adequately addressed, and those less important to safety should be correspondingly treated, aiming at proper allocation of various resources.

And, cumulative risk is used for setting a time limit to continue a certain plant condition, such as standby status of components. Some cases are presented in the following.

(a) Revision of technical specifications

The technical specifications of Browns Ferry-2 / 3 (BWR) specified that the allowable outage time (AOT) of emergency diesel generators be seven days. That time was not long enough for inspections of mechanical systems and electrical systems to be simultaneously performed. Therefore, an application to extend this AOT to 14 days was submitted.

The NRC approval was obtained with conditions to take compensatory administrative measures not to simultaneously perform risk-increasing maintenance and not to conduct a online maintenance of the emergency diesel generators under adverse weather conditions since the incremental conditional core damage probability (ICCDP) was less than the reference value (5×10^{-7}) of the Regulatory Guide 1.177.

(b) Risk-Informed In-Service inspection

Surry-1 (WH-PWR) submitted an application to review the in-service inspections using risk information. Modeling failure frequency and its effects of 515 piping segments, their safety significance was estimated and 108 segments were classified as safety significance high and the rests as safety significance low, and a change in the number of the sections to be inspected and their inspection methods were studied.

Compared with the inspection program of ASME Section XI, this change could lead to reduction of the risk of core damage frequency, etc. and radiation exposure, and so the NRC approved the change.

(3) Risk-importance categorization (10 CFR 50.69)

In 2004, the NRC announced a new rule (10 CFR 50.69) that broadly relates to many regulatory requirements, introducing the risk-informed regulation to the conventional regulation based on classification of safety systems and normal systems. This rule categorizes structures, systems, and components (SSCs) of nuclear power plants according to their risk importance (Figure 6), and regulates them according to their Risk-Informed Safety Class.

For instance, Risk-Informed Safety Class (RISC)-1 SSCs are safety-related that perform safety significant functions, which are strictly regulated as previously, but the RISC-3 SSCs are safety-related that perform low safety significant functions, which are a little less strictly regulated (for example, inservice testing is exempted.) On the other hand, the RISC-2 SSCs are non-safety-related that perform safety significant functions, which are to be strictly regulated as in the past (performance monitoring.)

(4) Requirements for ECCS performance (Revision of 10 CFR 50)

The requirements for combustible-gas control were revised so that inerting should be maintained in inerted containment, but the flammability control system is not required.

Furthermore, a proposal for rule amendment on ECCS requirements was released. The proposal for rule amendment defines the large break LOCA as a pipe rupture equivalent to rupture frequency 10^{-5} / year, and a larger rupture exceeding this is defined as a LOCA exceeding the design base, and the requirements for the case are that the criteria of cladding maximum temperature is not to be applied, the credit of offsite power to be permitted, and a single failure criteria not to be applied.

(5) Technical specifications on risk-management

In accordance with the performance-based maintenance rule issued in 1996, a risk monitor was introduced. The South Texas Project has applied to the NRC a pilot program as one of the risk-management technical specifications.

The specific contents are to implement the risk management with compensatory

measures, as necessary, when the increments of core damage probability (ICDP) exceed 10^{-6} and to shift to an operation mode to reduce risk when the ICDP exceeds 10^{-5} .

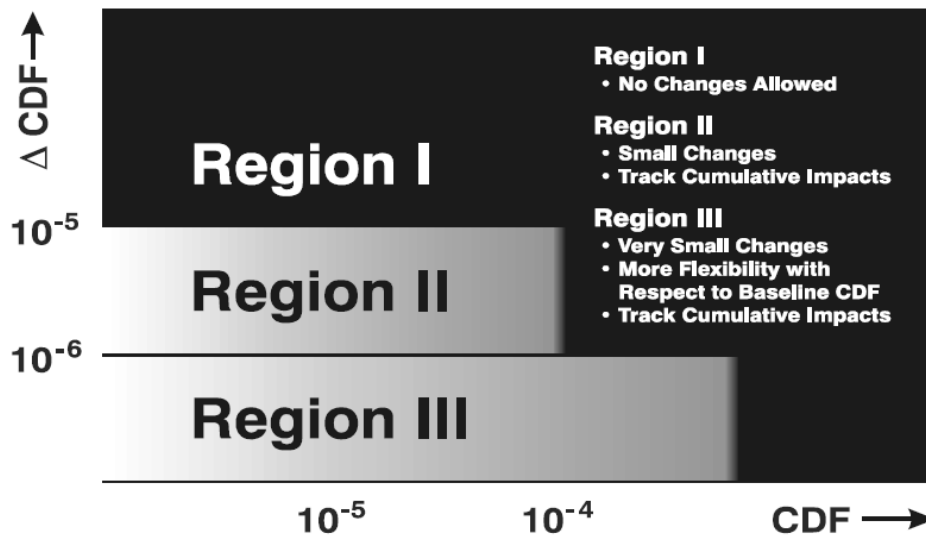


Figure 5 Acceptance Guidelines for Core Damage Frequency (CDF) of the NRC

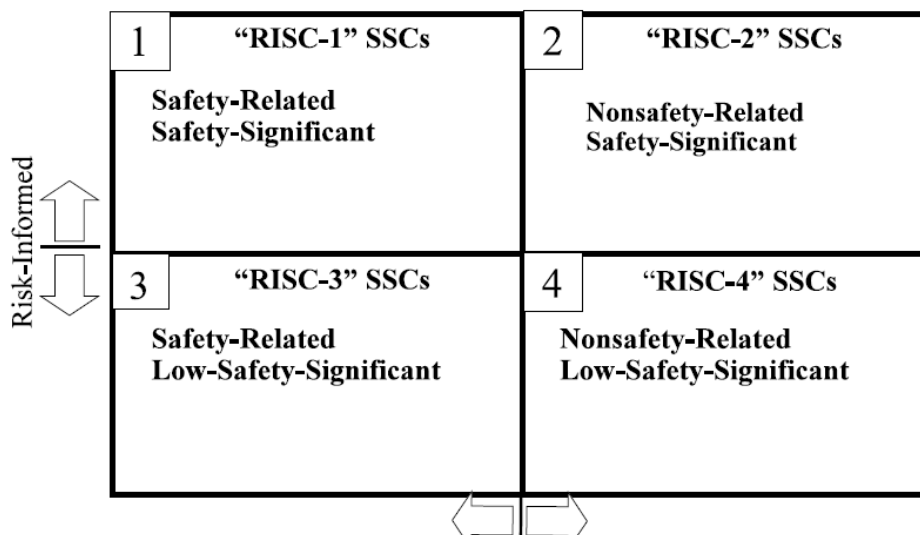


Figure 6 Categorization of risk importance

§50.69 RISC Categories

5. Summary of Level 1 PSA

(1) Framework of the level 1 PSA

The PSA is categorized according to the scope of its analysis, events to be covered, operating conditions, etc., but the level 1 PSA to address the internal events during power operation is discussed in the following.

In order to assess the core damage frequency and its consequences, firstly, it is necessary to identify the potential scenarios for core damage accident. Since a light water reactor is a very complex system, in order to identify and classify the scenarios, a systematic methodology is required.

[WASH-1400](#), which is the world's first report addressing the PSA, defines core damage accident scenarios as a combination of initiating events and a success or a failure of mitigation systems and operational actions to prevent the initiating events from progressing to core damage (called "accident sequence"), and uses a method to express the results classified based on this concept as an event tree (ET).

Here, an initiating event is an event that prevents normal operating conditions, which could lead to core damage and containment damage.

The ET starts from an initiating event and branches by a success or a failure of safety equipment or an operational action, and each path will show the accident sequence. The final state which is core damage or safe shutdown is determined to each accident sequence.

The accident sequence frequency leading to core damage (a core damage accident sequence) is calculated as the product of an initiating event frequency and branch probability (probability of a success or a failure) of the ET.

Moreover, the scenario that leads to a failure of the mitigation equipment etc. is analyzed to a level of a component failure or a human error, and the above-mentioned branch probability is assessed using statistical data on component failure rates and human error probabilities that are estimated with human-reliability analysis (HRA.)

This framework is shown in Figure 7.

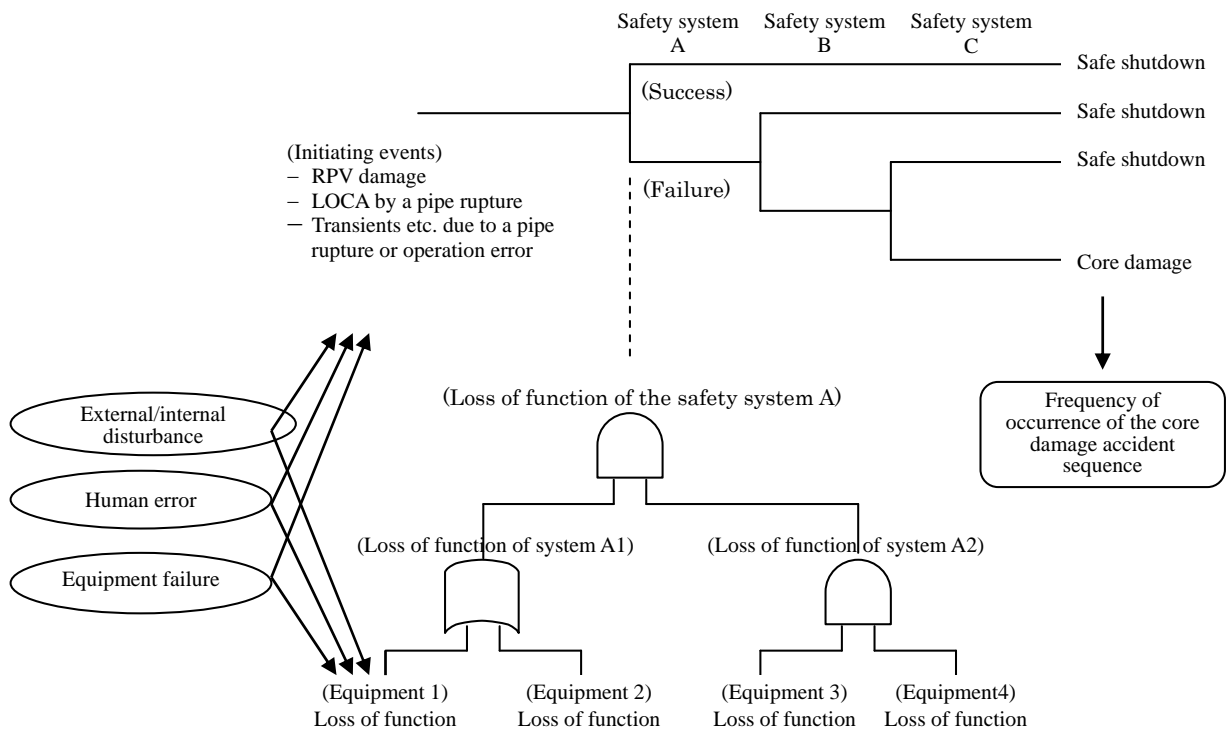


Figure 7 Level 1 PSA Framework

(2) Workflow for level 1 PSA

Figure 8 shows workflow for level 1 PSA in line with the above-mentioned framework.

The objective of each work is as follows.

- (a) In studying plant configuration and characteristics, information on plant design and operation procedures required for the PSA are obtained and organized.
- (b) In identifying initiating events and assessing their frequencies, potential initiating events are sorted out based on the design information and operation experience information and their frequencies are assessed based on operating experience database etc.
- (c) In establishing success criteria, the equipment and operator actions required to lead each initiating event to a safe shutdown state are identified including the number of systems of the equipment etc. for each initiating event. Conditions required to achieve such safety functions are called "success criteria."
- (d) The analysis of accident sequences is to predict the progress of an accident with an initiating event as a start point, according to the information on success criteria and operation procedures, and to develop an ET with branch points of a success and a failure in equipment or operator actions that affect the accident progress. The conditions at the branch points of ET are called heading.

(e) The system reliability analysis is to analyze the events that could cause a failure of the equipment etc. used as the branch point of the ET, and to assess the failure probability (non-reliability) as a system using parameters, such as an equipment failure rate, which are obtained from operating experience database etc.

(f) The development of the database is to accumulate the data on failure, trouble, scram event, etc. obtained from operating experiences as database and to derive parameters used by PSA based on the database, such as initiating events frequencies and equipment failure rates.

(g) The human-reliability analysis is to identify human errors to be taken into consideration by analyzing operation and maintenance activities related to safety functions, and to assess their probabilities.

(h) The quantification of accident sequences is to assess the frequency of occurrence of each core damage accident sequence and the core damage frequency (CDF) as their sum by inputting the frequencies of initiating events and the results of system reliability analysis or HRA etc. as the branch probabilities of ET.

(i) The uncertainty analysis and sensitivity analysis is to study the factors and magnitude of uncertainties accompanying the model and data used for the PSA, and based on the results, to assess quantitatively the uncertainties accompanying the information on CDFs, frequencies of occurrence of accident sequences and contributors etc. obtained as the PSA results and to analyze their dominant factors.

(j) The documentation is to compile procedures, models, data, results of assessment, etc. used by the PSA in a report etc. in order to use them for review, application, updating, quality assurance etc. of the PSA.

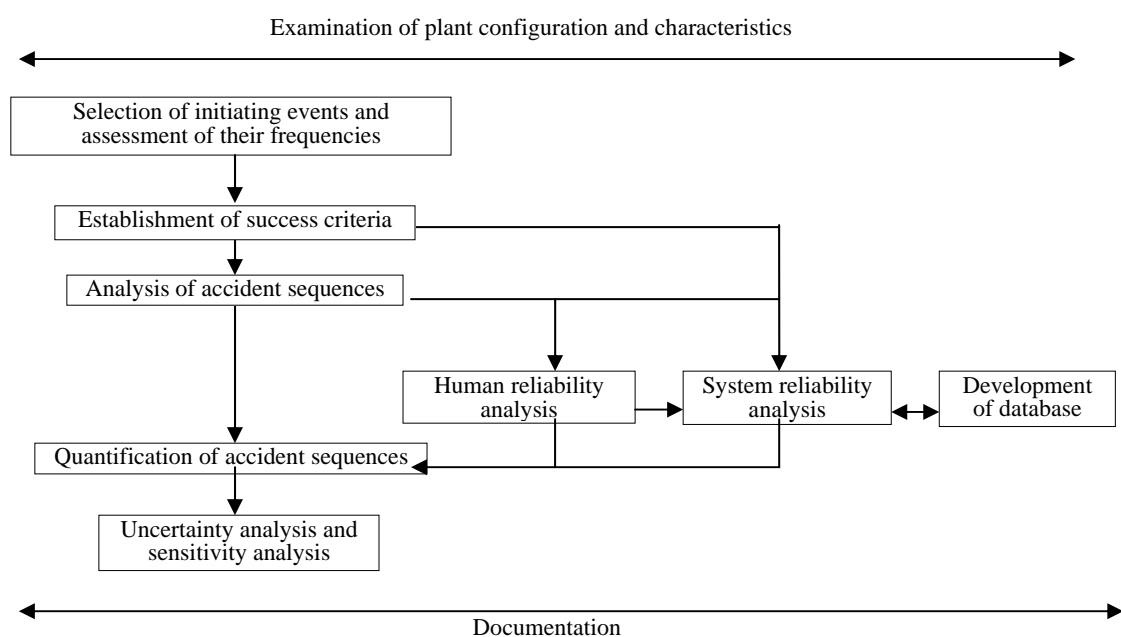


Figure 8 Workflow of level 1 PSA

6. Summary of Level 2 PSA

The level 2 PSA assesses the types, frequencies and [source terms](#) of accident sequences that release a large amount of radioactive material to the environment.

An accident that releases a large amount of radioactive material to the environment resulting in a large effect on the environment is a severe accident far beyond the design assumption, such as an occurrence of core damage and a loss of containment integrity. The level 2 PSA addresses such a severe accident.

In order to understand the contents of the level 2 PSA, it is important to get to know the progress of a severe accident and behavior of radioactive materials. The summary is shown in the following.

(1) Progress of a severe accident

This section describes a summary of severe accident progress by presenting an example of severe conditions that water injection into a core after occurrence of an accident, such as a loss of coolant accident (LOCA), by the emergency core cooling systems etc. fails completely.

(a) Accident progress within a reactor cooling system

After the occurrence of an accident, if all actuations of safety systems and accident mitigation operation actions fail completely, the cooling water in a core is lost and the core would be damaged.

Then, if further core cooling fails, some fuels melt due to heat of metal and water (steam) reaction in addition to decay heat. The molten fuel mixed with reactor core structures starts to move down to the lower part of a reactor pressure vessel.

If the molten fuel accumulates in the lower portion of the reactor pressure vessel, a part of the reactor pressure vessel is damaged due to the heat transfer from the hot molten material, and the molten material moves to the cavity of the containment.

A part of non-condensable gas such as hydrogen, generated from steam inside the reactor cooling system and the metal-water reaction, is released to the containment from rupture openings or valves.

The containment is gradually pressurized with these steam and non-condensable gas.

(b) Accident progress inside the containment

If the reactor pressure vessel is damaged and the molten material moves to the containment, the interaction of the molten material with the concrete of containment

generates steam and non-condensable gas, and they accumulate in the containment.

In case that the functions of engineered safety features such as container spray, are lost and all accident mitigation operation actions after the core damage also fail, the containment atmosphere is further pressurized with these steam and non-condensable gas.

(c) Severe accident phenomena with respect to the containment integrity

If the molten material contacts the cooling water that remains in the lower part of the reactor pressure vessel after the core damage, it may cause a steam explosion, which destroys the reactor core structures, lifts the reactor vessel head, and these structures collide with the containment wall (steam explosion inside a reactor pressure vessel).

When the reactor pressure vessel is damaged in a condition that pressure of the reactor cooling system is high, the fragmented molten material and gas blow off into the containment at high speed, and the temperature and pressure of the containment atmosphere rise in a short time (direct heating of the containment atmosphere).

If the fragmented molten material that blew off into the containment contacts the remaining water in the cavity, the steam explosion or rapid steam generation will generate a load to the containment (steam explosion inside the containment).

Moreover, the containment wall could be damaged when a part of the blew-off molten material contacts the containment wall (direct contact of the molten material with the containment wall).

If the blew-off molten material reacts with the concrete of the containment, a large volume of the non-condensable gas and steam are produced to increase the pressure load to the containment (over-pressurization rupture).

If the temperature of containment atmosphere rises, integrities of the hatches, upper head seals and/or electrical-cable penetrations of the containment could be lost (over-temperature rupture).

Moreover, combustible gas accumulated in the containment atmosphere, such as hydrogen and carbon monoxide will ignite and produce a large load to the containment (hydrogen combustion).

The level 2 PSA analyzes all of the severe accident phenomena that affect such a containment integrity described above.

(2) Behavior of radioactive materials

(a) Behavior of radioactive materials during a severe accident

If a core is significantly damaged, high-volatile radioactive materials, such as noble gas, iodine, cesium etc., are released from fuel to the reactor cooling system and become aerosols.

A part of aerosols containing such radioactive materials are released into the containment atmosphere through pipe-rupture openings or valve openings. A part of aerosols, through behaviors such as gravity settling, heat migration, diffusiophoresis, and inertial-impingement, deposits on the surface of structures, piping etc.

When the reactor pressure vessel is damaged and the molten material blows off into the containment, the radioactive materials are released from the molten material following the reaction of molten material and concrete.

The aerosols containing these radioactive materials rapidly flocculate into large-diameter particles, and deposit on the surface of structures.

The reduction effect of the suspended radioactive materials due to deposition is very large.

(b) Removal of radioactive materials with the engineered safety features

The containment spray system and the emergency filter system are effective in reducing a release of radioactive materials into the environment. Moreover, the suppression pool of a BWR serves as water filter, and is very effective for removal of radioactive materials. The pressurizer relief tank, etc. of a PWR has the same effect.

(3) Procedures of level 2 PSA

(a) Summary of Procedures

Firstly, for accident sequences leading to core damage, combining a success or a failure of the accident mitigation actions inside a containment system with the occurrence of severe accident phenomena etc., a containment event tree is established to classify the accident sequences that release a large amount of radioactive material to the environment.

Secondly, for the accident sequence concerned, the accident progress is analyzed and the probabilities of a success or a failure at the branch points of the containment event tree are calculated.

Multiplying the probabilities by the frequencies of occurrence of the accident sequences leading to core damage, the frequencies of occurrence of the accident sequences classified in the containment event tree are obtained.

Moreover, source terms are analyzed for the accident sequences classified in the containment event tree. Following these procedures, the combinations of frequencies of

occurrence and source terms of the accident sequences that release a large amount of radioactive material to the environment are obtained.

(b) Plant damaged conditions

Although there are various conditions that release a large amount of radioactive material during a core damage accident, many analytical studies and experimental studies have been carried out, and it is known that the types of the accidents can be classified into some groups.

The types that release a large amount of radioactive material to the environment during a core damage accident can be classified by a combination of the initiating events and a success and a failure in the accident mitigation actions by the time the accident leads to core damage (called core damage accident sequences), and a combination of a success and a failure in the accident mitigation actions after core damage (called plant damaged conditions).

The first step of level 2 PSA is to classify all of the core damage accident sequences obtained at the level 1 PSA into plant-damaged conditions. In the case of a light water reactor, it can be classified into approximately 10 to 20 plant-damaged conditions.

(c) Containment event tree

In order to identify the accident sequences that lead to a containment failure during a core damage accident, for each plant damaged condition, a tree diagram with branches with or without a loss of containment integrity due to the physicochemical phenomena, such as hydrogen combustion, etc. in addition to the initiating events and a success or a failure in the accident mitigation actions until and after the core damage is made (called a containment event tree).

The endpoints of the containment event tree show the final state of the containment, such as sound, over-pressurization failure, over-temperature failure, failure due to direct heating of the containment atmosphere, etc.

In this way, the core damage accident sequences can be classified into the accident sequences that result in containment failures.

(d) Accident progression analysis

Following the accident sequences of the containment event tree, the time frames etc. of core damage, reactor vessel failure, and containment failure are analyzed, and the time margins for mitigating actions to mitigate the accident progression are analyzed.

The containment loads accompanying the phenomena of releasing a large amount of energy in a short time, which are threats to the containment integrity, such as steam explosion, direct heating of the containment atmosphere, hydrogen detonation etc. are

analyzed.

(5) Source term analysis

In addition to the accident progression analysis, a release of radioactive materials from fuel, deposit behavior in the reactor cooling system, release behavior from the molten material inside the containment system, deposit behavior inside the containment system and their removal by the engineered safety features are analyzed to obtain the source terms.

Since the radioactive material is an exothermic body, it is important to combine the behavior of radioactive materials and thermal hydraulics.

(6) Probabilistic approach

The probability distribution of success or failure in the accident mitigating actions is calculated from the time margins of the accident mitigation operation obtained by the results of the accident progression analysis, and the probability distribution of a containment failure is calculated from the comparison of the results of the containment load analysis accompanying the physicochemical phenomena of a severe accident with containment tolerance.

The conditional probability of occurrence of the accident sequence classified according to the probability of the branch point of the containment event tree is calculated, and the frequency of occurrence of an accident sequence is calculated from the conditional probability multiplied by the frequency of occurrence of a plant damaged condition.

This calculation should be performed for all plant-damaged conditions. In this way, the types, frequencies of occurrence, and source terms of the accident sequences that release a large amount of radioactive material to the environment are determined.

(4) Examples of level 2 PSA

In 2004, the Nuclear and Industrial Safety Agency reviewed the reports of probabilistic safety assessment performed by the electric utilities for existing 52 nuclear power plants.

The core damage frequencies and containment failure frequencies of existing 52 units in Japan assessed by the electric utilities are summarized in Figure 9. The horizontal axis shows the core damage frequency (CDF) of each nuclear reactor facility, and the vertical axis shows the containment failure frequency (CFF) corresponding to the CDF. The figure shows that the core damage frequency of the nuclear reactor facilities in Japan is less than 10^{-6} / reactor year, and the containment failure frequency is less than 10^{-7} / reactor year. These numbers are smaller compared with the PSA results in western countries.

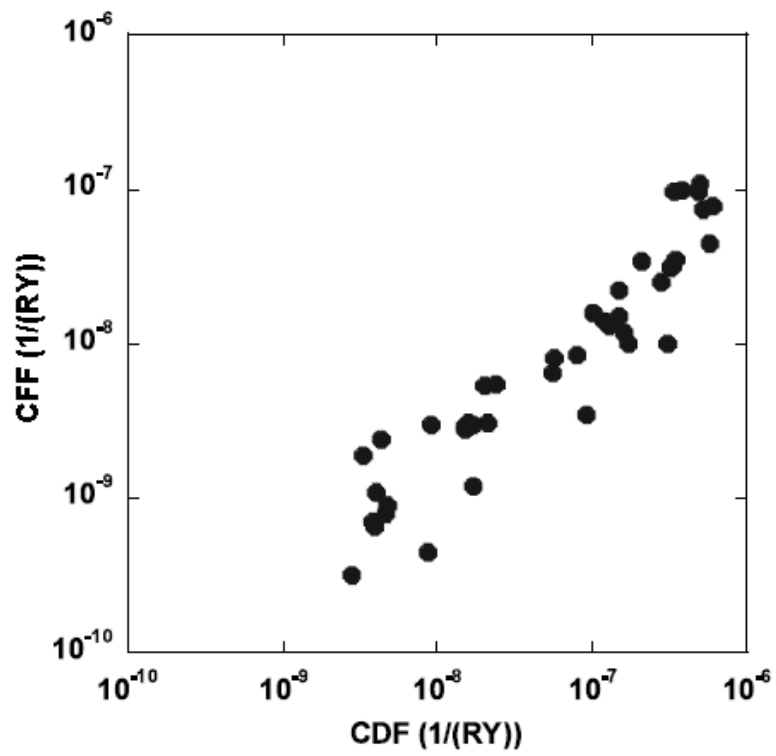


Figure 9 Core damage frequencies and containment failure frequencies of existing nuclear power plants (52) in Japan

7. Summary of Level 3 PSA

The level 3 PSA analyzes the migration behavior of the released radioactive materials in the environment using the source terms during an accident obtained by the level 2 PSA as the input, and assesses the effects on the human health and the economical consequences.

The atmosphere is very important as a release path of radioactive materials to the environment during a reactor accident. The effects of radioactive materials released to the atmosphere are assessed by the following procedures.

- (1) Establishment of source terms
- (2) Meteorological sampling
- (3) Evaluation of atmospheric diffusion and deposition
- (4) Dose assessment
- (5) Analysis of radiation-dose reduction by protective measures
- (6) Evaluation of health effects

- (1) Establishment of source terms

The information on the release sources provided from the level 2 PSA is called the source terms during an accident. As the source terms, the amount of released radionuclide, time from occurrence of an accident until the start of the release to the environment, duration of the release, thermal energy of the released materials due to the accident phenomena, release position (height), and time margin to recognize the release to the environment before its start are established.

The level 3 PSA normally addresses 60 or so nuclides to be assessed out of the nuclides accumulated in a reactor from a viewpoint of their inventories, half lives, and biological hazards. The information concerning the physicochemical forms of released nuclides is important particularly for calculation of the deposition within respiratory organs accompanying the deposition and inhalation in the environment. For nuclides other than noble gas, a distribution of particle sizes is important information for deposition behavior as they are normally released into the environment as particles.

- (2) Meteorological sampling

The space-time distribution of released materials is significantly influenced by meteorological conditions during the release. In addition to a calculation of the effects for all possible meteorological conditions at the subject site at the time of an accident, the level 3 PSA should estimate the appearance probability of the meteorological

conditions.

However, since it is theoretically impossible to calculate them for all meteorological conditions that could appear, it is necessary to choose some typical ones.

(3) Evaluation of atmospheric diffusion and deposition

The first step to assess the effects of an accident is to analyze the transportation, diffusion, and deposition on the ground surface of the radioactive nuclides released to the atmosphere and to calculate space-time distribution of the airborne concentration and surface-deposition concentration of each nuclide.

The Gauss plume model has been used so far for an assessment of the atmospheric diffusion. This is a model that the released substance called a plume are transported down the wind and forms the Gaussian distribution in the horizontal and vertical directions at right angles to the wind direction due to atmospheric turbulence. In addition to this model, the effects on the diffusion due to buildings near the release point, rise of the released substance by its buoyancy, collision to the substances on the ground surface, deposition by the collision with raindrop in the rain, etc. are taken into consideration.

(4) Dose assessment

The following six paths are mainly taken into consideration as the exposure paths to persons by the radioactive materials transported to the environment during an accident:

- (1) External exposure from the radioactive materials in the plume,
- (2) Internal exposure due to direct inhalation of the plume,
- (3) External exposure from the substances deposited on the skin or clothing,
- (4) External exposure from the ground surface deposits,
- (5) Internal exposure due to inhalation following the re-suspension of the ground surface deposits, and
- (6) Internal exposure due to ingestion of the contaminated foods.

According to the analysis on the Chernobyl accident, etc. to date, external exposure from the plume containing noble gas etc., internal exposure by inhalation of iodine and tellurium, and external exposure from the ground surface deposits serve as the major exposure paths for the early exposure during a reactor accident.

Moreover, external exposure from the ground surface deposits of ^{137}Cs and internal exposure by ingestion of contaminated foods serve as the major exposure paths of the

long-term exposure as experienced in the Chernobyl accident.

(5) Analysis for radiation-dose reduction with protective measures

Many protective measures are taken in order to reduce the exposure dose to the public during an accident, and for actual estimation of the exposure of residents in the vicinity, it is necessary to take into consideration the effects of the radiation-dose reduction due to protective measures.

The protective measures taken into account by the level 3 PSA is classified roughly into an early stage countermeasures and long-term countermeasures depending upon the time of their application.

The early stage countermeasures, such as sheltering, evacuation, preventive taking of stable iodine tablets, which are applied before or immediately after a release of radioactive materials to the environment, reduce the health effects at an early stage by controlling the external exposure by the plume and the ground surface deposits and internal exposure by inhalation.

The long-term countermeasures, such as relocation, decontamination, and ingestion restriction, reduce the late health effects by controlling the external exposure from the ground surface deposits and the internal exposure by ingestion of contaminated foods.

(6) Evaluation of health effects

The harmful effects to the health due to radiation exposure are classified into the somatic effects that appear to the exposed individuals and the genetic effects that appear to descendants.

Furthermore, the somatic effects are divided into the early effects that appear in a short period of time after the exposure, and the late effects that appear after a long period of time after the exposure. The level 3 PSA calculates these as the health effects.

(7) Expression of risks

The results of level 3 PSA, such as health effects, calculated in the above-mentioned assessment procedures are normally shown for each concentric-circle-like assessment sectors divided by distances and directions from the release point.

(8) Application situation of the level 3 PSA in Japan

In Japan, the Special Committee for Safety Goals of the Nuclear Safety Commission proposed the safety goal in 2003 that an indicator of individual risk in the vicinity of a nuclear facility is used as an extent of risk reduction required by the safety regulatory activities to licenses' activities to use nuclear energy (10^{-6} / year / site for both of average acute death risk and average cancer death risk).

8. Summary of Seismic PSA

(1) Procedures of seismic PSA

Figure 10 shows the procedures of seismic PSA.

1) Collection and analysis of plant information

First of all, information on design, construction, and inspection, etc. of the plant to be assessed and similar plants are collected and analyzed.

2) Implementation of a plant walk-down

A scope for assessment should be established, a team consisting of specialists on the scope should be formed, and the contents to be focused on identified.

- Compare the design specifications with the actual plant situations in the plant concerned, and check matters hard to obtain from the desk information. Particularly check the foundations of the equipment concerned.
- Check plant-specific features, such as mutual interference of the functions between equipment, mutual interference between systems, and subordinacy between systems, etc.
- For the functionally related equipment, check the secondary effects, such as collision with other equipment due to deformation, breakaway, and movement, etc. of the equipment.
- For modeling the systems to assess accident sequences, check the accessibility to the equipment of which functional restoration by a repair work at a site can be expected.

3) Preliminary analysis and establishment of accident scenarios

Using the plant related information and walk down information, the preliminary accident scenarios should be extensively analyzed, selected without a oversight, and screened.

Major points of concern for selection of the preliminary accident scenario are shown below.

- The accident scenarios should be determined depending on whether they could lead directly or indirectly to core damage. As an example for indirect scenario, there are indirect effects, such as damages to the auxiliary equipment, etc. due to a collapse of a nearby slope or a drop of an indoor crane.
- The way of studying an accident scenario should be changed depending on a type of

earthquake ground motion, main shock or aftershock.

- It should be considered whether the building and equipment, etc. are in newly constructed states or aged conditions after in-service for a long period of time. In the case of the latter, the aging effects should be taken into account particularly based on the periodical inspection and preventive maintenance history.

4) Identification of accident scenarios and analysis of the initiating events

In order to efficiently perform an assessment of core damage frequency, the initiating events should be analyzed after identifying the accident scenarios based on the results of accident scenario analysis and their establishment.

5) Development of a building and equipment list

Moreover, according to the identified accident scenario and initiating events, the buildings and equipment that are involved in accident sequences and fragility assessments to be described later should be identified, and their list should be developed.

6) Seismic hazard assessment

First of all, the locations, levels and frequencies of occurrence of earthquakes that could occur around the subject site should be established using a database on similar geological formation, active faults, and earthquakes that occurred in the past (modeling of an epicenter.)

Secondly, the intensity and frequencies of occurrence of the earthquake ground motion caused by these earthquakes should be calculated using a distance decay formula for earthquake ground motion or a fault model (modeling of propagation of the earthquake ground motion).

The above-mentioned modeling of epicenters and propagation of the earthquake ground motion include some uncertainties. The factors are roughly divided into accidental uncertainties specific to physical phenomena and uncertainties due to lack of knowledge and information, and the combination of the latter factors should be shown logically in a logic tree (development of a logic tree).

Moreover, for each branch tree consisting of the logic tree, a seismic-hazard curve reflecting accidental uncertainty factors should be calculated and statistically processed according to the magnitude of earthquake ground motion, and the width of uncertainties should be shown (assessment of seismic hazard.)

Furthermore, taking into consideration phase characteristic and wave shape characteristics of earthquake ground motions, the earthquake ground motion for fragility assessment should be obtained (assessment of earthquake ground motion for fragility

assessment.)

7) Fragility assessment of building and equipment

First of all, the building and equipment subject to the fragility assessment are selected from the building and equipment list. Hereinafter, the building and equipment is a general term for reactor building, control building, intake pit, outdoor civil engineering structures like a sea water piping duct, slopes around the facility, passive components like tanks and batteries, active component like pumps and electric panels, and piping, and equipment include approximately 50 ones that are categorized according to the type etc.

Damaged area and damage mode of the selected buildings and equipment are established using a database (establishment of the subjects and damage modes for assessment).

Then, the fragility of the buildings and equipment are assessed using these damaged areas and modes, selecting assessment methods according to the required accuracies and applications of the assessment (selection of assessment method.)

Furthermore, using the assessment results of the realistic load bearing and the realistic response of individual building and equipment mentioned above, the conditional damage probability; i.e., the fragility when the realistic response exceeds the realistic load bearing for each earthquake ground motion intensity should be obtained (fragility assessment).

8) Assessment of accident sequences

First, using the analysis results of the accident scenarios and the initiating events, and the building and equipment list developed, initiating events that trigger a core damage accident should be established (decision of initiating events.)

Second, reactivity control functions, core cooling functions, containment heat removal functions, etc. that are required to prevent core damage after the occurrence of an earthquake should be selected for each initiating event, and a success criteria that is a combination of systems required to ensure these functions should be established. Based on these, an event tree should be developed modeling successes and failures of the equipment and actions for achieving safety functions (modeling of accident sequences.)

In addition, in modeling systems for the plant mitigation systems in the event tree, the human errors during an earthquake, etc. should be taken into consideration in development of the fault tree (system modeling). Then, using these event and fault trees, and the results of the building and equipment fragility assessment and seismic hazard assessment, the accident sequences should be quantitatively assessed for the core damage frequencies including the uncertainties (quantitative assessment of accident

sequences).

In addition, in order to proceed to an assessment of the loss-of-function frequency of the containment at an earthquake, scenarios of accident progression, which lead to a loss of function of the containment, should be analyzed (analysis of a loss-of-function scenario of the containment).

9) Development of a written report

A written report should be developed so that the following requirements are satisfied

- Required information should be able to be obtained when it is utilized in decisionmaking etc.
- Specialists other than the assessors can understand the complete picture of the assessment and easily review the validity of the assessment contents and results.

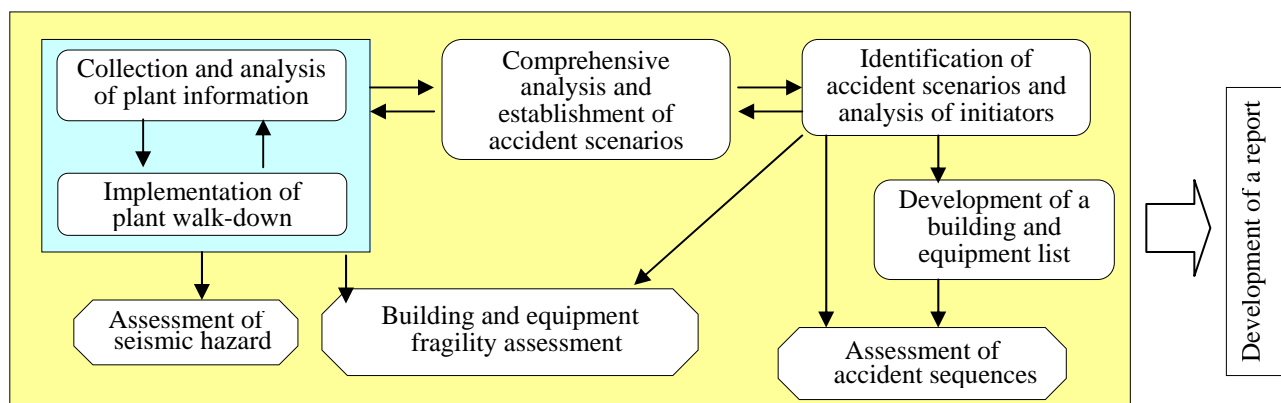


Figure 10 Procedures of seismic PSA

(2) Application of the seismic PSA

(1) Utilization to the Regulatory Guide for Reviewing Seismic Design of Nuclear Power Reactor Facilities (U.S.)

In 1997, U.S. introduced the probabilistic seismic hazard assessment method in addition to the conventional deterministic method for establishing a size and location of the design basis earthquake in the siting and seismic guideline. The introduction was made because the deterministic method only was judged not to be adequate to meet the public's concern on this issue since the data on active faults and the earthquakes that occurred in the past were not sufficient in the east of the Rocky Mountain Range.

(2) Utilization for seismic improvements of nuclear power plants in U.S.

In 1990, the results of external-event PSA including significant seismic events for Peach Bottom (BWR) and Surry (PWR) were made public in U.S. Successively, assessments on external events for all U.S. plants were performed, and various seismic improvements in anchoring of equipment, relay of controllers etc. were made.

(3) Prospect of utilization for the Regulatory Guide for Reviewing Seismic Design of Nuclear Power Reactor Facilities (Japan)

A revision of the Regulatory Guide for Reviewing Seismic Design of Nuclear Power Reactor Facilities by the Nuclear Safety Commission started in July 2001, and through the general invitation for the public comments in May to June 2006, a new seismic guideline was established in September. This proposal of the revised guideline requires that the factors of uncertainties and the degree of their magnitudes in establishing the reference earthquake ground motion S_s be sufficiently considered, and the probability of exceeding response spectra of the established S_s be described in the application document for a use at the safety review as the reference information. Furthermore, it requires that efforts to make the "remaining risk" due to an earthquake ground motion exceeding S_s as small as rationally possible be made since possibility of an earthquake ground motion with intensity exceeding S_s cannot be denied. In order to satisfy these requirements, seismic PSA methods is likely to be applied.

(4) Utilization for seismic improvements of nuclear power plants in Japan

Japan Atomic Energy Agency assessed loss of offsite power events at a virtual nuclear power plant. The core damage frequencies were assessed for the important safety-related equipment identified by the seismic PSA in two cases with and without the equipment modified to quake absorbing structures, and the results show that the modifications could reduce the frequencies by approximately 70 to 80%. Moreover, assessing the total cost of expected loss during plant lifetime for both cases, it is shown that the cost effectiveness of the modifications is high.

9. Issues in the near future

(1) Utilization of risk information

The PSA of nuclear power plants is a method to model the activities in a comprehensive manner for ensuring safety in the areas of design, construction, inspection, operation, prevention of an accident / failure and disaster, and standards and guidelines, and to quantitatively assess the risk of nuclear power plants.

Moreover, when the design and/or operation management of a nuclear power plant are changed, it can quantitatively assess their effects on risk.

Furthermore, the PSA can assess quantitatively what kind of accident scenario mainly contributes to risk and what kind of preventive measure is effective in reducing accidents. For instance, the PSA can quantitatively identify the dominant sequence to core damage frequency and effective mitigation measures to reduce core damage frequency. Furthermore, it can assess how and to what extent the reliability of each system and equipment and a success or a failure of each operational action affect risk of a nuclear power plant.

By using such risk information, the validity of ensuring safety based on the conventional deterministic methods can be verified quantitatively using a unified scale in terms of risk.

However, in making use of risk information for safety regulation, there are issues to clarify the methods to keep consistency with the current regulatory philosophy for ensuring safety, such as maintaining the defense in depth and ensuring safety margin in addition to issues concerning the risk information, such as ensuring the quality of PSA methods and data.

(2) Development of PSA method

In Japan, before a use of the PSA for the assessment of effectiveness of the safety assessment and accident management (AM) of the periodic safety review in 1992, the development of PSA methods had been promoted. Therefore, the development and application of PSA methods in Japan is considered to be on the same level as those in U.S., but the modeling for the human reliability analysis is not necessarily adequate, and the modeling for the PSA methods in consideration of the aging effects and organizational factors has not been established yet.

It is desired to promote a study aiming at upgrading human reliability assessment methods and establishment of the PSA methods for aging or organizational factors from now on. Moreover, establishment and standardization of assessment methods for risk due to external events other than seismic events such as tidal-wave events, and due to fire events inside a nuclear power plant are required.

(3) Development of PSA data

In the PSA for the periodic safety review or AM development, the database that is comparatively old even in U.S., such as the "LER failure rate" of U.S. NRC, "IEEE Std. 500", etc. has been used in Japan. On the other hand, the data of equipment failure rate developed in Japan have been partially used only for sensitivity analysis.

Concerning the development of the data on equipment failure rate in Japan, since the early 1980s, Japanese licensees have voluntarily collected the information on accidents and incidents subject to the laws and/or generic letters and the information on troubles not subject to them, and developed the database on equipment failure rate for the major equipment to be used for PSA based on the information. Moreover, in October 2003, the Nuclear Information Archives "NUCIA" opened in the Central Research Institute of Electric Power Industry, and it is to collect and make public events related to safety but not subject to reporting to NISA as the maintenance quality information.

In order to promote the utilization of the Japanese database of equipment failure rate developed by licensees and the "NUCIA" information, it is desirable that fair and neutral academic societies and industrial associations, etc. review the information. Furthermore, aiming at PSA quality improvement, the plant-specific data should be collected, accumulated and disclosed by licensees.

Moreover, concerning the data of human error rate, the method and data of the handbook (NUREG/CR-1278) developed by U.S. NRC have been used as it is, and Japan-original data have not been developed. As the data on human error rate is closely related to assessment model of human errors, cases in Japan should be collected for development of the database together with a development of the assessment method.

(4) Ensuring PSA Quality

Since 1992, the PSA has been applied to the safety assessment of the periodic safety review and the effectiveness assessment of the accident management in Japan.

Introduction of the risk-informed safety regulation requires the PSA quality to be fully ensured. Moreover, it is necessary to improve the PSA quality as the risk information plays a larger role in judgment at the safety regulation.

In the near future, it is necessary to study on a measure of the PSA quality and to establish a reliable and transparent mechanism to verify the PSA quality. Therefore, it is required to prepare a guideline that provides basic requirements for the PSA quality (validity of the scope, depth of model and technical adequacy of PSA). Moreover, it is necessary to identify expectations to academic societies and industrial associations that standards of private sectors to specify specific requirements to verify conformance to the basic requirements are developed under a fair and neutral procedure including public review, and a mechanism to perform the technical review of the standards of private

sectors.

10. Summary

The PSA is an excellent technology with many advantages for both regulatory side and licensees, which can be effectively used in wide areas from design to maintenance management of nuclear power plants.

At the present time, PSA-applied areas and applications are still limited, but it is expected to use the PSA more positively in the near future as an excellent tool to more reasonably achieve higher safety by increasing actual applications and efforts for PSA.

References

1. "An Introduction to Probabilistic Safety Assessment (PSA) for Light Water Reactors", Journal of Nuclear Science and Technology, Atomic Energy Society of Japan, Vol. 48, No. 3, No. 4, No. 6, No. 8, No. 9, No. 10 (2006)
2. "PROBABILISTIC SAFETY ASSESSMENT (PSA)", Long-term Training Course On Safety Regulation and Safety Analysis / Inspection 2005, from September 7 to November 11, 2005, JNES
3. "LEVEL 2 PSA METHODOLOGY", Long-term Training Course on Safety Regulation and Safety Analysis / Inspection 2005, September 7 to November 11, 2005, JNES
4. USNRC, Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH 1400, (1975).
5. An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, Regulatory Guide 1.174, rev. 1, USNRC, (2002).
6. Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to their Safety Significance, Regulatory Guide 1.201(for trial use), USNRC, (2006).
7. USNRC, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG 1150, (1991).
8. "New Regulatory Guide for Reviewing Seismic Design of Nuclear Power Reactor Facilities", JNES, July (2007)
9. Study on Areas to Apply the Risk Information and their Effects on Safety Regulation, JNES/SAE05—119, June 2006