18th International Conference on Structural Mechanics in Reactor Technology (SMiRT 18)
Beijing, China, August 7-12, 2005
SMiRT18-M01-2

SEISMIC SAFETY DESIGN AND RISK ASSESSMENT

Takaaki Konno
Secretariat of Nuclear Safety Commission
3-1-1 Kasumigaseki, Chiyoda-ku, Tokyo 100-8970, Japan
Phone: +81-3-3581-9841, Fax: +81-3-3581-9836
E-mail: takaaki.konno@cao.go.jp

ABSTRACT

The adequacy and sufficiency of NPP seismic safety design are confirmed by the defense-in-depth safety performance and the risk profile. Seismic safety design and risk assessment are now inseparable for safety assurance of nuclear facilities. Applying the defense-in-depth principle to NPP seismic safety is a difficult issue with respect to the current seismic design philosophy in Japan. The defense-in-depth seismic safety of NPP requires not only resisting seismic events but also assuring safety when safety measures do not function as designed in the seismic events. The current deterministic design practice is not appropriate for the defense-in-depth principle when earthquake shaking demand increases because of new knowledge. Probabilistic risk assessment allows application of the defense-in-depth principle to NPP seismic safety design in these cases. The probability of failure, the maximum conditional probability of failure and the ground motion at the condition derived with the relationship between the realistic seismic load and seismic capacity are the three important indexes for safety design. Performing the safety performance analyses considering maximum conditional probability of failure and the risk assessment complying the probability of failure is essential to satisfy the necessary and sufficiently conditions for the defense-in-depth safety requirements of NPPs.

Keywords: Nuclear Power Plant, Seismic, Safety, Risk, Defense in depth, Deterministic, Probabilistic,

1. INTRODUCTION

The seismic safety of reactor facilities required to assure the reactor safety and radiation protection to the public health and safety should be assessed using the “defense-in-depth” principle. This principle requires not only resisting seismic events but also assuring safety when safety measures do not function as designed. The defense-in-depth principle states that a safety strategy should acknowledge redundancy or diversity of accident prevention and accident mitigation within the operational system to ensure that no single human or equipment failure would lead to harm to the public, and even combinations of failures that are only remotely possible would lead to little or no harm. This idea of multiple levels of protection is the central feature of defense-in-depth principle. Applying the defense-in-depth principle to the seismic safety is considered a difficult issue with respect to the current deterministic seismic design philosophy in Japan as increasing earthquake shaking demand can overcome the multiple levels of protection.

The current deterministic design practice confirms structural integrity for the design basis earthquake ground motion only. This deterministic approach is not appropriate given the defense-in-depth principle. Seismic safety should consider the probability of ground motions in excess of design basis earthquakes, with appropriate accounting for the inherent uncertainties in the characteristics of postulated earthquake events and in ground motion predictions. For such low probability, large amplitude earthquake events, defense-in-depth seismic safety

must consider multiple and common failures of the diverse safety-related structures, systems and components (SSCs) that is installed including various redundancies. In that case, a deterministic approach reduces the design effectiveness of redundancies. Seismic events have potential to fail the multibarrier system, but also have the probability to preserve safety functions in certain conditions. If only the preservation rate of safety functions assures that the multibarrier system is not jeopardized and is capable of functioning as designed, power operation is allowed. Performance-based design therefore is strongly recommended to properly accommodate the redundancies within multibarrier system for large seismic events.

Seismic engineering technology in Japan has a long history of development, with improvements coming from earthquake experience. Recent earthquake experiences noticed the necessity of more discussions on the seismic safety issues considered for NPPs. An example is the need for safety assurance for earthquake events larger than the design earthquake. There is possibility of near field earthquake larger than M6.5 by underlying blind faults. The 1995 Kobe earthquake showed us the devastating power of a near fault earthquake by the diverse severe damages of the modern seismic structures. The damaging power of the near fault earthquake may not be adequately estimated by the inversion of ground motion records at far fields. Near fault earthquake records recently accumulating by highly densely arrayed earthquake observations are noticed us the strong motions of earthquakes have a high dependency of the fault rupture process and the deep structure. The dependency provide diversity and uncertainty of the ground motions as the characteristics of natural phenomenon such as strong ground motions excess acceleration as over 1g in a near fault region, locally amplified shakings affecting the integrity of structures, or large aftershock occurrence following closely the main shock. A study of the damaging power of near fault earthquakes considering the variability and uncertainty is a new important factor in the seismic engineering.

The current Examination Guide for Seismic Design (Seismic Guide) by the Nuclear Safety Commission (NSC) in Japan has qualitative conservatism and less accountability of safety assurance of defense-in-depth for seismic events. It should be evolved introducing recently advanced seismic safety engineering technology based on the probabilistic approach as the Examination Guide for Seismic Safety Design. It should be a risk-informed and performance-based design guide.

The understanding of diversity and uncertainty of seismic shaking and structure damage occurrences as learned in recent earthquake experiences is important to conduct properly seismic safety engineering. Recent advanced technology can handle the diversity and uncertainty quantitatively based on the probability of seismic hazards and the damage rates of safety-related SSCs. The seismic safety design philosophy complying defense-in-depth principle was discussed based on the deterministic and probabilistic methodology.

2. DEFENSE-IN-DEPTH SEISMIC SAFETY

2.1 Safety Accountability

Seismic safety is a goal for NPPs. Seismic design generally aims to build structural integrity to assure the safety for large earthquake events. On the other hand, seismic safety of NPPs is required not only resist seismic events even though it beyond the design basis earthquake ground motions but also assure the safety when the safety measure is not worked properly in the seismic events as designed based on the defense-in-depth principle. Safety functions of diverse safety-related structures, systems and components (SSCs) installed in NPPs that have the safety functions of redundancy or diversity of accident prevention and accident mitigation within the operational system are derived comply with the defense-in-depth principle. The idea of multiple levels of protection is the central feature of defense-in-depth principle.

The current Seismic Guide classified the seismic grades of reactor facilities in accordance with the importance of the safety functions into four classes from high important to low important facilities as called seismic grades As, A, B, and C from the point of the magnitudes of radiation release impacts to public health and environments. The corresponding design basis earthquake ground motions are categorized into four classes from extreme to small earthquake magnitudes considering probability of occurrence frequencies, that are, extreme design earthquake (S2), maximum design earthquake (S1), 1.5 times a non-nuclear facilities design earthquake as the S_B, and non-nuclear facilities design earthquake as the S_C so that the integrity of safety-related SSCs required should be maintained, respectively. Each seismic grade facilities are designed to maintain the structural and functional integrities for corresponding earthquakes. Each seismic grade facilities should not be damaged to loss the safety functions by the failure of lower class facilities. The maximum design earthquake S1 is determined based on past earthquakes, earthquakes due to active faults with high activity whose recurrence interval is shorter than 10,000 years. The extreme design earthquake S2 is determined based on the both of seismo-tectonic structures and active faults of high to less activity faults whose recurrence interval is shorter than 50,000 years considering the

seismological possibilities of excess the S1 event occurrence based on the characteristics of past earthquakes, active faults and possible blind faults. Current seismic design employed deterministically the seismic source of magnitude M6.5, and hypocenter distance X=10 km, the distance is a site specific matter, to represent the unknown blind faults assuming that could take place at any inland location in Japan. This seismic design requirement is intended to consider sufficient range of earthquakes to assure reactor safety for any potential earthquake shaking. These deterministic considerations require explanation of the adequacy and sufficiency of the safety assurance of reactor safety and radiation protection for the probabilistic occurrence events of seismic hazards to enhance the public acceptance. As long as the integrity of the safety functions installed by the defense-in-depth concept is maintained appropriately, the safety requirement is assured as intended. Although seismic events have a potential to failure multibarrier system, but also have the probability to preserve safety functions in certain conditions. The seismic safety performance analyses should be performed based on the damage rates of the safety functions of safety-related SSCs to assure the reactor safety and radiation protection for the beyond design basis earthquake ground motions. The consideration of safety beyond design basis earthquake ground motions was proposed to be enhanced accountability (Konno, 2001) [1]. Furthermore, severe accident managements should be prepared complying with defense-in-depth concept.

A probabilistic approach to seismic safety assessment is important from the point of view of "How safe is safe enough." Such an approach takes into account the ground motions from the full range of earthquake magnitudes, allowing explanation of the relationship between the reactor safety performance and the structural integrity of safety-related SSCs considering the uncertainties within the seismic hazard and the safety performance system. In order to enhance the safety accountability, NSC is implementing to define a safety goal common for all nuclear facilities. Safety regulations are studying to be the performance-based and risk informed regulations complying with the safety goal.

2.2 Safety Requirement

2.2.1 Reactor safety and radiation protection

The safety requirement for reactor safety and radiation protection is established by defense-in-depth concept applied to the three basic functions: 1) controlling the power, 2) cooling the fuel and confining the radioactive material and 3) that radioactive materials do not reach people or the environment. The requirements for reactor safety and radiation protection are defined clearly for the internal events depend on the plant safe states that are, in normal operation state and in abnormal plant states, respectively. These requirements are confirmed the satisfaction by the safety performance analyses for internal events in a safety design. The requirement should also be confirmed for the seismic events. The current Seismic Guide require that nuclear power facility shall maintain its structural integrity against any postulated seismic force likely to occur at the site that no earthquake leads to a major accident. The safety performance of reactor safety and radiation protection is difficult to evaluate directly by the structural integrity. The safety performance is confirmed by the satisfactory of safety function performance. The performance of safety function is endorsed by the satisfactory of structural integrity. The sufficiency of the structural integrity to assure the safety performance for seismic cannot therefore be estimated without the safety performance analyses of safety functions of the SSCs. The seismic safety performance of the reactor safety and radiation protection should be evaluated based on the safety performance analyses of the safety functions consisting success path to the safety conditions required for the design basis events that are selected adequately to represent the design conditions of safety-related SSCs considering the combination of potential human and mechanical failures with the multiple failures of SSCs by seismic.

In general, earthquake occurrence frequency is higher for small seismic events. The safety conditions that should be assured are: normal operation during high frequency occurrence earthquakes; transient incident of moderate frequency occurrence earthquakes; accidental incident of low frequency occurrence earthquakes. As shown in the Figure 1, generally speaking, plant safety conditions might be induced into from slightly abnormal conditions to highly abnormal conditions along with the intensity of earthquake events increased. Furthermore, assuming the combination with a low occurrence frequency/large accident event by random failure, the safety conditions can be induced to severe condition even in a small earthquake. How much the severe earthquake events should be considered and also how much the severe internal events should be considered for combination therefore is dominate the plant safety conditions to be designed. The event combinations are considered by the probability of occurrence frequency. Large earthquake events are depend on the magnitude of earthquake sources. Identification of most significant earthquake source that limit the excess seismic events at a site is important for seismic safety design.

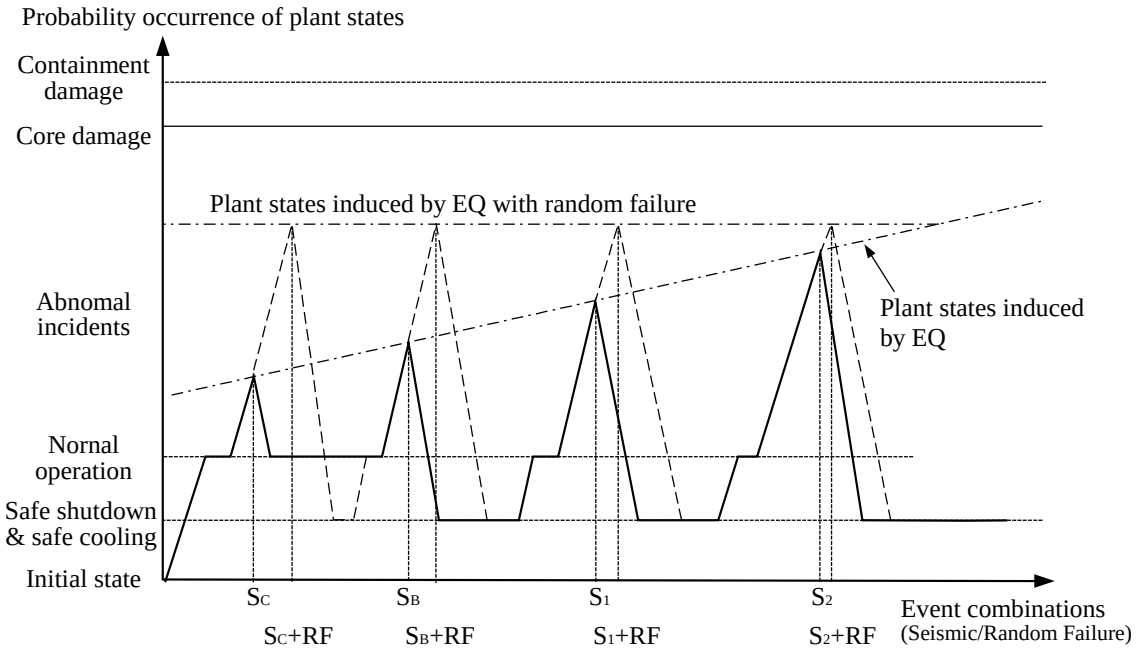


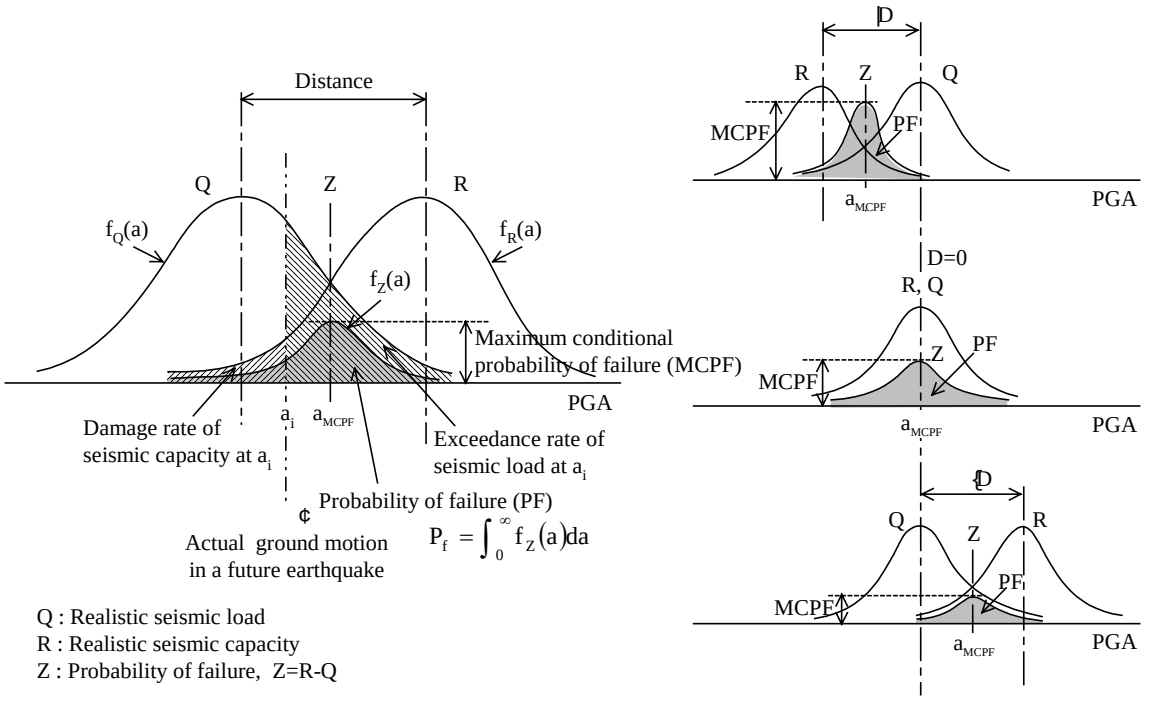
Fig. 1 Plant safety levels related with earthquake events. The safety level is higher when the plant states closer to the normal operation. Identification of most severe seismic source that limits the excess seismic event at a site is important to establish the defense-in-depth safety for seismic.

2.2.2 Structural integrity

The structural integrity rate by a seismic event is a key factor to analyze the functional integrity rate of safety-related SSCs and to endorse the safety performance analysis. In order to analyze the structural and functional integrity rates, both of the realistic seismic capacity of structures and the realistic seismic loads of seismic events are required to be clarified. In the estimation of the realistic seismic capacity of structures, consideration of the differences between design conditions and real conditions is important. In the structures damaged at the 1995 Kobe earthquake, various types of damage were observed. These damages might largely be caused by the differences between the actual and the design input ground motions. The determination of design conditions considering the differences with the realistic one was realized more difficult than intended to assure the ultimate seismic capacity without informing the diversity and uncertainty of the seismic hazards and structures. The performance-based design to estimate the seismic capacity with the probability in the realistic conditions is necessary to be developed. The analysis of nonlinear 3-D response by 3-D inputs is desirable to understand the capacity of structural and functional integrities of safety-related SSCs more realistic basis to be useful for the safety performance evaluations into the ultimate condition.

The seismic capacity of structures is derived by the dynamic interaction among the structures, the site conditions and the input ground motions. Considering the diversity and uncertainty of earthquake ground motions and structures, the realistic seismic load and seismic capacity of a plant can generally be represented by lognormal density functions as shown in the Figure 2. The median value of the seismic load is designated by the earthquake source as a site specific condition. When the most significant earthquake source can be identified, the seismic capacity can therefore be designed as a plant specific to control the failure rate that can be limited by the distance of median values between the seismic load and the seismic capacity, and the standard deviations. Damage rate of seismic capacity, exceedance rate of seismic load and a conditional probability of failure to actual ground motion in a future earthquake can be evaluated using realistic seismic load and seismic capacity if the actual ground motion can be identified. Actual ground motion in a future earthquake can be anticipated in the range of realistic seismic load cannot be exactly predicted but the most severe ground motion level is designated at the maximum conditional probability of failure. The distance of median values between the seismic load and the seismic capacity should therefore be selected to satisfy the safety requirements of reactor safety and radiation protection by the safety performance considering the maximum conditional probability of failure. The probabilistic failure of the seismic capacity to the realistic seismic load is evaluated by the integration of a conditional probability of failure

that multiply the damage rate of the seismic capacity and the exceedance rate of the seismic load in the full range of realistic seismic load for risk assessment basis. The probability of failure (PF), the maximum conditional probability of failure (MCPF) and the ground motion at the MCPF derived with the relationship between realistic seismic load and seismic capacity are the three important indexes for safety design. The probability of failure is used to evaluate the risk. The safety performance with the state of the maximum conditional failure of the SSCs consisting success path should be evaluated to confirm the safety assurance for the seismic event. The ground motion at the maximum conditional failure is used to evaluate the structural integrity and to endorse the safety performance.



(a) Probabitity of failure by realistic seismic load and capacity

(b) Probability of failure changing by the distance between realistic seismic load and capacity

Fig. 2 Three indexes derived by the realistic seismic load and capacity. The probability of failure (PF), the maximum conditional probability of failure (MCPF) and the ground motion at the MCPF derived by the relationship between realistic seismic load and seismic capacity are the three important indexes for safety design. The probability of failure derived by the distance of realistic seismic load and seismic capacity is used to evaluate the risk. The safety performance with the state of the maximum conditional failure of the SSCs consisting success path should be evaluated to confirm the safety assurance for the seismic event. The ground motion at the maximum conditional failure is used to evaluate the structural integrity and to endorse the safety performance.

3. SEISMIC SAFET DESIGN AND RISK ASSESSMENT

3.1 Objectives of Safety Design and Risk Assessment

The adequacy and sufficiency of the seismic safety design of nuclear power plants should be confirmed by the defense-in-depth seismic safety performance and the risk profile. Seismic safety design and the risk assessment are now inseparable for safety assurance of nuclear facilities. Considering recent earthquake experiences, seismic safety should consider the probability of ground motions in excess of design basis earthquakes, with appropriate accounting for the inherent uncertainties in the characteristics of postulated earthquake events and in ground motion predictions. The occurrence of earthquake ground motions at a site is generally predicted in the range from high to low occurrence probability by a seismic hazard curve. This is done either for the aggregate hazard or for a scenario earthquake hazard. For such low probability, large amplitude earthquake events, defense-in-depth seismic safety must consider common failure of the diverse safety-related structures, systems and components (SSCs) that include various redundancies. That approach reduces the design effectiveness of redundancies in the prevention and mitigation systems installed. Performance-based design therefore is strongly recommended to properly accommodate the redundancies for large seismic events.

Generally, seismic safety design is conducted based on the philosophy of conservative and uses a deterministic basis method. Seismic safety design is oriented to establish the success conditions satisfying the safety requirements for design basis events. On the other hand, seismic risk assessment is conducted using probabilistic methods based on the philosophy of realistic. That is, seismic risk assessment is oriented to estimate the probability of failure conditions in satisfying the safety requirements. Success rates cannot accumulate for the safety estimation but failure rates should be accumulated for the risk estimation that reduces the success rates consequently. The overall seismic risk is derived by integration of the multiple of the occurrence probability of failure conditions and the seismic event exceedance occurrence frequency. The design basis events are sufficient to select severe conditions only to confirm the success conditions. The risk basis events should be selected to cover every possible event in order to evaluate the risk. The dual approach of safety design and risk assessment is important in order to provide quantitative understanding of the deterministic conservatism and to select design basis events adequately for safety design. Of importance is to not miss the potential side effects of safety conditions and failure conditions. The seismic safety design and the risk assessment are conducted by iteration to have an agreement between the safety and the risk. As shown in the Figure 3, design basis events activate the seismic safety design and risk basis events that are supposed considering every possible events than design basis events, activate the risk assessment. The seismic safety design is conducted until the safety performance considering the maximum conditional probability of failure derived by the distance between the seismic load and the seismic capacity is confirmed to satisfy the safety requirements of reactor safety and radiation protection for the severe conditions. The risk assessment is conducted until the risk profile derived by the relationship between the seismic load and the seismic capacity is accessible considering every possible event. The distance of the median values between the realistic seismic load and seismic capacity should therefore be selected to satisfy the safety requirements by the safety performance considering the maximum conditional probability of failure and the risk profile by conducting the iteration between seismic safety design and risk assessment. Performing the both approach is essential to satisfy the necessary and sufficiently conditions for the safety requirements of NPPs from the both points of safety performance and the risk profile.

Unnecessary conservatism in the classification of seismic grades of structural integrity in the current Examination Guide for Seismic Design can be reduced by the safety performance analyses considering the maximum conditional probability of failure using event tree and fault tree systems of the safety-related SSCs. At the same time the safety requirement should be changed from structural integrity to functional integrity. The classification of seismic grade of individual safety-related SSCs might be reduced when considering redundancy and functional integrity. The current Examination Guide for Seismic Design should evolve into an Examination Guide for Seismic Safety Design that is risk-informed and performance-based. The seismic safety design philosophy should use a probabilistic approach to properly address the defense-in-depth principle.

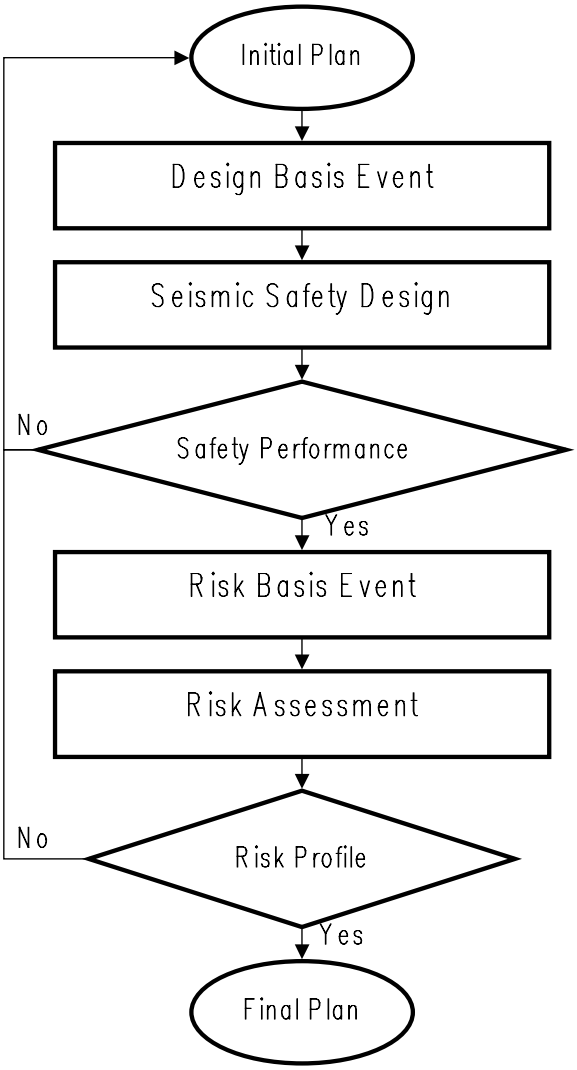


Fig. 3 Iteration between seismic safety design and risk assessment. The seismic safety design is conducted until the safety performance is confirmed to satisfy the safety requirements. The risk assessment is conducted until the risk profile is accessible.

3.2 Design Basis Event and Safety Performance

The seismic safety design to assure the reactor safety and radiation protection for the seismic hazard at a site should include the safety performance analyses in accordance with the multiple levels of plant conditions derived by design basis events. Design basis events should be selected adequately to confirm the safety establishments in the case of combination failure occurrence events that are combinations of potential human and mechanical failures with probabilistic seismic structural failures. They should consider the dynamic interactions among technology, human and environment in seismic events concerning the plant states for the normal operation during high frequency occurrence events, for the transient incident in moderate frequency occurrence events, and for the accidental incident in the low frequency occurrence events. Safety science concerning the interaction among human, technology, and environment has long been important vehicle to drive properly the nuclear safety. Technology construct hardware systems, human programs soft ware systems, and environment provides activity grounds. Initiating events to cause abnormal plant conditions such as potential human errors, random mechanical failures and seismic failures are generated by the dynamic interaction among the deviation occurrence frequency of hardware systems, software systems and variable situations of environment, as shown in the Figure 4. Random

failures usually might be sleeping and will be activated when a seismic event occurred. The safety reliability analysis system represented by event tree and fault tree is analyzed the probability of success or failure along with the sequential events following the initiating events.

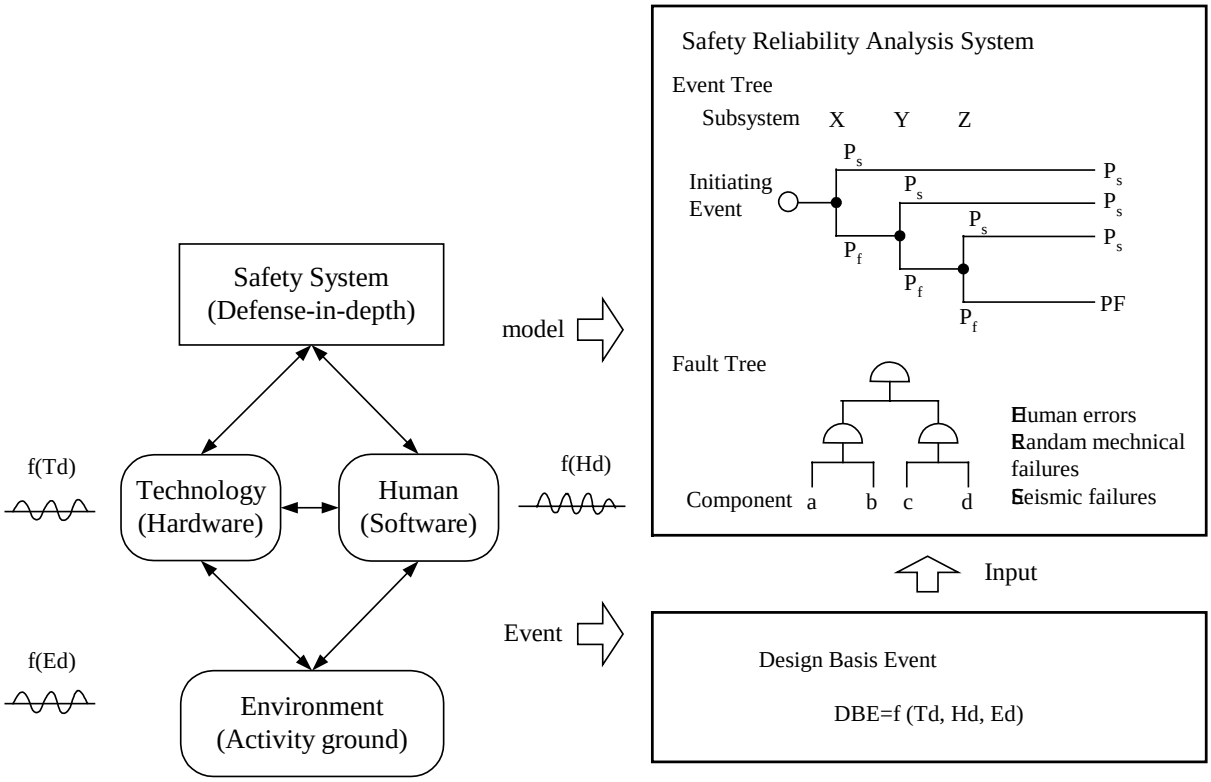


Fig. 4 Driving factors of safety system. Technology construct hardware systems, human programs soft ware systems, and environment provides activity grounds. The safety reliability analysis system represented by event tree and fault tree is analyzed the probability of success or failure along with the sequential events following the initiating events such as potential human errors, random mechanical failures and seismic failures that are generated by the dynamic interaction among the deviation occurrence frequency of hardware system, software system and variable situations of environment.

To find the success path to lead plant safety conditions, the trace of the sequence route counting failure rates on the event tree with the branch by fault tree composed by the safety-related SSCs are performed following the initial event by the design basis events. The safety performance analyses for the selected success paths are performed based on the probabilistic failure of safety functions to confirm the safety establishment for the plant damage states. Previous results of seismic probabilistic safety assessment (seismic PSA) for Japanese NPPs showed that the risk profile derived was not proportional with the seismic intensity. The reactor core damage frequency by seismic events has the curve with several peaks along the intensity of earthquake ground motions because of the safety functional seismic capacity of the safety systems to cope with the initial events are different depend on the event significance as shown in the Figure 5. This suggest the seismic safety establishment considering the combination of potential human and mechanical failures with probabilistic seismic structural failures can not so simply defined as intended by the deterministic seismic classifications of the safety functions of SSCs in the current Seismic Guide. The seismic classification is rather preferable to be defined as a plant specific based on the risk profile. Design basis events for safety design should be selected to confirm the safety performance at the risk peak events.

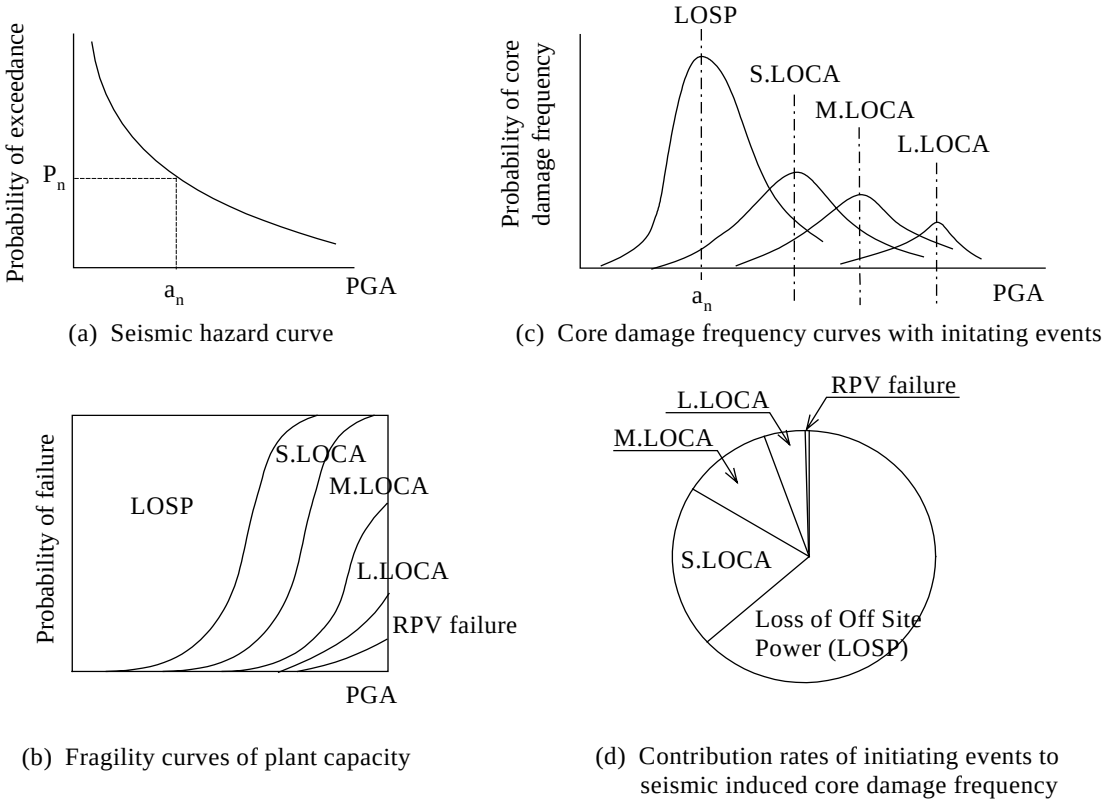


Fig. 5 Risk profile by seismic PSA. The risk profile derived was not proportional with seismic intensity that have several high peaks of risk contributions because of the safety functional seismic capacity of the safety systems are different to cope with the each initial event.

3.3 Seismic Hazard and Design Basis Earthquake Ground Motion

There are generally many earthquake sources that can generate influential ground motions at a site. The influences of seismic hazards for nuclear facilities at a site are difficult to represent by design basis earthquake ground motions. Earthquake ground motions are generated with substantial diversity and uncertainty inherited by the complex effects of the source, path, and site conditions, that is, it can be said the same ground motion will not again, and the influence of seismic hazard is dominated by the dynamic response for the ground motions among the various frequency of structures, systems and components. There is difficulty to decide what ground motion is the most severe to structures based on the limited experiences of damaging earthquakes in the modern complex structures, as the large earthquakes are rarely occurrence events. The design basis seismic force can be determined to safety side but the design basis earthquake ground motions could not be determined to safety side. The design basis seismic force is determined after the dynamic response analyses using ground motions. While, the influences of the design basis earthquake ground motions are varied by the complex structures of diverse frequency and multiple degrees of freedom. The design basis earthquake ground motions should therefore be determined based on the realistic basis seismic hazards to clarify the probabilistic occurrence frequency of the ground motions at a site. The diversity and the uncertainty of seismic events by surrounding seismic sources can be evaluated realistic basis using probabilistic seismic hazard analysis, then the influence of the ground motions from a large number of possible earthquakes become considerable, and their frequencies of occurrence are key parameters characterizing earthquake ground motions as seismic hazard curves. A probabilistic approach to characterizing the ground motions that a given site will experience in the future is very compatible with the current trends in earthquake engineering and the development of performance design. The site specific hazard curves, from which the requested sets of Uniform Hazard Spectrum may be obtained, should also accommodate uncertainty in the site specific dynamic material properties as well as local and regional seismicity and attenuation characteristics. The adequacy of design basis earthquake ground motions to assure the seismic safety of the complex facilities of NPPs does not suitably explained only by the envelopment response spectrum or a uniform hazard spectrum of seismic sources

because of the diverse frequency contents and multiple degrees of freedom of the complex safety-related SSCs on NPPs. One of the objectives in developing seismic design spectra is to achieve approximate uniformity of seismic risk for structures, systems, and components designed to those spectra, across a range of seismic environments, annual probabilities, and structural frequencies.

The deterministic decisions above mentioned such as M6.5 for blind fault or active faults recurrence interval shorter than 50,000 years for S2 earthquake could be explained the adequacy to quantify the design conservatives studying the realistic feature of seismic hazards by performing a site specific probabilistic seismic hazard analysis and de-aggregation of the probabilistic seismic hazard in terms of earthquake magnitudes and distances.

The risk assessment using probabilistic seismic hazard is important to evaluate the risk profile for all potential earthquake events and to select adequate design basis events for seismic safety design. The risk contribution rates of seismic hazards are not proportional with the seismic intensities shown by the previous seismic PSA. The reason is that even if the influence of the structural and functional integrities of the safety-related SSCs is proportional, the influence of the combination with random failures is not proportional along with seismic intensities. Looking the risk profile obtained by seismic PSA, the design basis ground motions should be determined based on the most influential seismic source to conduct seismic safety performance analyses at the risk peak seismic events for the safety-related SSCs composing the success path to lead reactor safety conditions. Risk-informed design basis earthquake ground motion determination methodology was proposed (Konno, 2003) [2]. In the determination of design basis ground motions, site investigation is important to identify and characterize the source for the scenario earthquake as the risk peak seismic event based on regional and site geological and geophysical data, historical and instrumental seismicity data, the regional stress field, and geological evidence of prehistoric earthquakes. Large numbers of earthquake ground motions can be predicted considering possible variability among the source, path, and site parameters even for a single seismic source. As shown in the Figure 6, a seismic hazard curve is obtained by the contribution of many sources and the contribution rate of the sources to the annual exceedance of earthquake occurrence frequency is different by each source. The seismic safety assurance of NPPs is required for all seismic events by the sources. Seismic safety design using all predicted ground motions is practically impossible. The identification of most significant source influencing at a site is important to determine the design basis earthquake ground motions. The ground motions selected from the most influential seismic source in the risk profile are important to confirm the seismic integrity of the safety-related SSCs by the dynamic response analyses to assure the safety performance evaluated. The probabilistic seismic hazard represents the effects of whole seismic events by the aggregate hazard. The most influential seismic source can be selected by the de-aggregation analysis of the probabilistic seismic hazard in terms of earthquake magnitudes and distances.

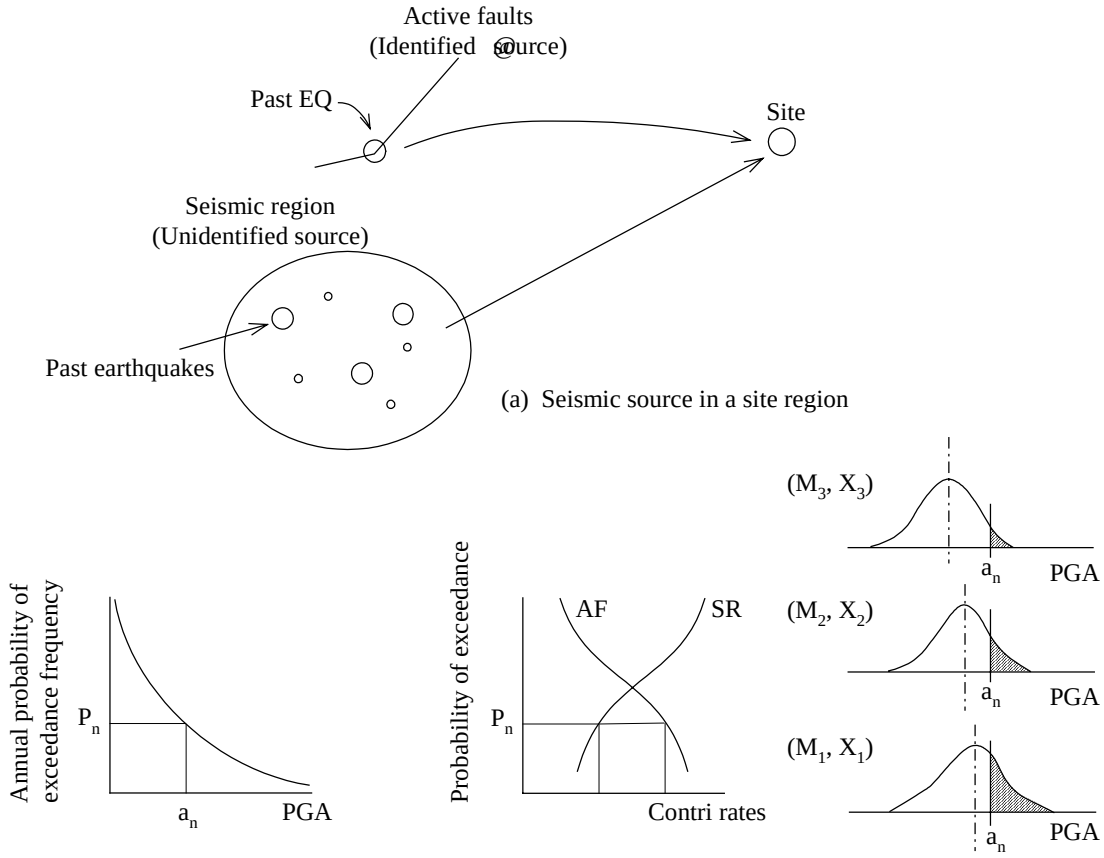


Fig. 6 Source contributions to seismic hazard at a site. The each source contribution rates to the ground motions at a site are changed according with the probability of exceedance frequency changing. The identification of most significant source is important to determine the design basis ground motion.

Evaluation of an individual seismic event is important as experienced the disasters by the near-fault earthquake ground motions of the 1995 Kobe Earthquake. The estimation of the effects of earthquakes to structures is difficult only from the response spectra of earthquake ground motions. The seismic impacts to structures should be evaluated by time domain dynamic response analyses. The ground motions from an individual seismic event can be estimated by adequate scenario earthquake hazard. It has been recommended that modern method should be employed to predict design earthquake ground motions for a scenario earthquake hazard considering the effects of fault asperity, rupture process and directivity of the wave propagation.

One approach to account more realistically for these effects in ground motion prediction models is to include them in empirical models by using a large number of predictive parameters related to source, path and site conditions. An empirical method for evaluating response spectra and time-dependent features of horizontal and vertical earthquake ground motions on free rock surfaces was proposed (Noda, et al., 2002) [3]. Another approach is to use seismologically-based ground motion models that take account of the specific source, path and site conditions. If numerical simulation methods are used to estimate the ground motions, then the spatial distribution of slip on the fault and the time function of slip on the fault also need to be characterized. Irikura proposed a recipe for prediction of scenario earthquake strong ground motion caused by active fault by means of numerical analysis (Irikura, 2000) [4]. Strong ground motions in the near-source area are controlled by heterogeneous source processes. Source characterization includes source effects such as those due to asperity, rupture process, rupture directivity or the orientation of fault, and the effects of deep structure such as sedimentary basins, basin edges, and buried folds and faults therefore is one of key issue for more precise strong ground motion prediction. The new, high-quality data recorded in the near-source region of recent large earthquakes are useful to evaluate

source characterization such as spatial variations of slip, slip velocity, or rupture velocity for accomplish precise strong motion prediction by modern earthquake ground motion evaluation technology.

3.4 Risk Assessment Grade

Risk assessment is performed to answer the questions from the point of verification, validation and certification on the evaluation depth in high hazard systems such as nuclear installations (Rasmussen, et al., 1994) [5].

- Verification is an assessment of the degree to which the results meet the requirements of the design specification. Verification is supposed to answer the questions: Is the design right? Does the product meet the design intentions?
- Validation is an assessment of the degree to which the design achieves the original system objectives. Validation is thus supposed to answer the questions: Does the product meet the needs of the end user? Is it the right design?
- Certification is a particular type of validation with a focus on the constraints around the original system objectives. This explicit focus is particularly important when advice systems are introduced, which are based on heuristic rules, as in expert systems. While it is practically possible to validate the systems within the design basis, it is very difficult to certify that the response of heuristic rules to unpredicted situations outside the design basis will not have unacceptable side effects. Thus, certification of software and hardware will very become a major concern for regulatory bodies.

In the recent review of the evaluation problem in high hazard systems such as nuclear power plant, Tanabe emphasized the need to explicitly evaluate the potential side effects of system functions during abnormal operational conditions (Tanabe, 1991) [6]. That is, in the validation of system objectives, explicit considerations are necessary for certification. The effectiveness of hardware systems can be evaluated in a design phase but the thorough evaluation of the effectiveness of software systems need to be performed in operation phase. To evaluate the safety management, a performance-based approach is necessary for regulatory body to define the effectiveness and efficiency.

3.5 Risk Assessment Phase

Seismic probabilistic risk assessment (“Seismic PRA”) of NPPs should be conducted following a three-phase procedure to fit the Japanese regulatory system, according to the progress of plant design and operation conditions. In the first phase, the seismic risk assessment scenario is confirmed depending on the seismic design specification in a safety design assessment report submitted for siting license to verify the safety establishment by the scenario. In the second phase, the seismic PRA is performed with the detailed design and construction data before the operating permit to validate the safety scenario. In the third phase, the seismic PRA is certified by reassessment based on the plant walk-down inspection due to the plant operation. The assessment philosophy for the seismic safety of NPPs in Japan was proposed (Konno, 2001) [7].

The assessment in a site licensing phase is intended to confirm the sufficiency and the feasibility of the safety achievement in the reactor operations as the basic design intended. In the assessment, the design basis events are confirmed whether it is selected adequately or not considering the dynamic interaction among technology, human and environment. In the safety review of the basic design, the following should be considered as preventive measures: Consideration of the possibilities, if any, of deviating from these conditions when these are put to use; Required implementation of specific safety designs against not only wrongful operation but also intentional error while taking into consideration the potential event. Returning to the original concept of “Defense-in-depth” fail safe, fool proof, and preventive measures for intentional error should be taken at the facilities.

The assessment in the plant construction phase is intended to confirm the safety assurance that was specified in the site license. For the assessment of the seismic safety assurance, seismic PRA in the plant construction phase is performed based on the detailed design and construction data before the operation approval. Characteristic analyses of the seismic design system, construction system, and inspection system before operation should be performed to answer the question from the point of the validation in the construction phase. The characteristic analyses of production method and the procedure will be performed based on the actual procedure. The assessment results are utilized to the safe operation standard manual as the issues to be concerned.

In the plant operation phase, the technical ability and the safety operation management that were confirmed to have adequate safety assurance in the siting license phase should be certified by periodic inspection and safety assessment in subsequent regulation. The performance of the seismic PRA based on plant walk-down inspection concerning to the reactor safety function are maintained properly to act surely in the earthquake, the deterioration of the low level safety function does not injured the high level safety function due to plant operations is essential for the safety assessment of the seismic safety assurance in the plant operation phase. For the seismic safety in the operating phase, the performance of operator support systems under seismic condition is important. Operator should be provided with operational guides related to prioritized systems and components based on safety shutdown path for preventing core damage, considering that some of them may be inoperable due to seismic motion. Inspection systems to check safety activities of facilities by regulations should have resident inspectors, periodic safety reviews, systems for qualification of shift supervisors, qualification of engineers for nuclear fuel material handling, guidance for performing probabilistic risk assessment studies and preparing severe accident management measures, and other features.

3.6 Development Activity

Development activities of a seismic PSA methodology are ongoing within JAERI, NUPEC, electric power utilities, and other organizations in Japan. This methodology will be utilized in a risk-informed safety management not only concerning prevention of severe accident but also concerning shutdown management, on-line maintenance, in-service inspection, and in-service testing.

A case study of seismic PSA and seismic margin analysis (SMA) for a Japanese standard BWR was performed as an objective to establish seismic PSA methodologies for Japanese plant (Sakagami, et al., 2000) [8]. In the study, an emphasis was made on the following points: first, to study a procedure of integrating expert opinions in the seismic hazard evaluation; second, to develop fragility database for domestic plant components; third, to study dominant contributors to core damage frequency. The seismic PSA results showed that dominant contributors were common cause random failure and seismic failure of several components and that random failure had a large portion of contribution to core damage frequency (CDF). On the other hand, the SMA results showed that dominant contributors were seismic failure of several components. The dominant contributing seismic acceleration region was around (0.6-2.5) times S2 in seismic PSA, while the SMA results gave a plant capacity of High Confidence Low Probability of Failure (HCLPF) value about 2.5 times S2, which was larger than the contributing acceleration region in seismic PSA. Dominant accident sequences obtained were almost the same in seismic PSA and SMA.

Recognizing the potential importance of operator support system under seismic conditions, the Japan Atomic Energy Research Institute (JAERI) has started a feasibility study to develop a concept of an Operator Support System under Seismic Conditions (OSSC) as one of seismic risk management strategies. A conceptual design of operator support system under seismic conditions was proposed utilizing the results and findings from seismic PSA (Oikawa, et al., 2000) [9]. If a large earthquake occurs near a nuclear power plant, it may cause abnormal situations to the NPP such as occurrence of multiple initiating events and failures of mitigation systems. Many difficulties may arise in diagnosis of the plant status and actions operators and technical support staff of the NPP due to highly stressful conditions. In the case of the 1995 Hyogo-ken Nanbu earthquake, many thermal power plants, substations, and transmission and distribution facilities near the epicenter suffered various types of damages from the earthquake. As many alarms and annunciators sounded in unison at that time, it was difficult for operators to move to approach the panels or consoles to confirm and stop them [10]. Considering that the stress may be induced to the operators by earthquake and some of the engineered safety systems actuate automatically in short term, it is important to provide operators with guides for confirmation of the systems to be started automatically and manipulation which operators ought to perform in a short term. On the other hand, for the middle and long terms, it is important to provide operators with guides for assisting diagnosis of the plant status and for responding to multiple failures in the plant. The primary aim for assist function provided to the operators should be changed depending on the level of severity of earthquake motion at the plant.

The evaluation of fragility is important factor in the seismic PSA. Seismic performance of the structures, equipment and components is required to prove that the ultimate strengths are sufficient not to cause sever reactor accident due to the earthquake events. Seismic capacity data for component fragility evaluations based

on the structure failure models were obtained for many component categories of Japanese standard plants; for examples, pressure vessel and its support, primary loop recirculation system, reactor core internal structures, control rod drive hydraulic unit, tanks, gas insulation switchgear, and so on (Nishihata, et al., 2000) [11]. The capacity data of passive components were evaluated on the basis of the safety factor method using the results of seismic design analyses. For the active components and the electrical equipment whose failure modes are functional, they were evaluated on the basis of data from shaking table tests performed in Japan and from engineering judgment. The capacity data of active components and electrical equipment were determined by both capacities due to structural failure and functional failure mode. The value of capacity for major components in Japanese LWR plants generally proved to be relatively high.

The Nuclear Information Center of Central Research Institute of Electric Power Industry (CRIEPI) serves utilities by providing safety- and reliability- related information on operation and maintenance of the nuclear power plants, and by evaluating the plant performance and incident trends. As a result of these evaluations, a nuclear component reliability data system has been developed for estimating failure rate of major components for use in PSA. Internet-Web client at the utilities can access this data system. The users can select component, plant system and time period, and then compute the failure rate by the data system. Data of component failure are then continuously being collected from utilities and transferred into the data system for the estimation of component reliability within Japan. A set of domestic component reliability data on 49 Japanese LWRs from April 1, 1982 to March 31, 1997 was reported (Kirimoto, et al., 2000) [12].

4. CONCLUSION

Viewing seismic safety engineering technology advancement and seismic safety issues from recent earthquake experiences, a philosophy and a methodology of seismic safety design and risk assessment was discussed based on the deterministic and probabilistic approaches. Safety designs should establish defense-in-depth. Risk assessments confirm the sufficiency and the feasibility of the safety achievement. The adequacy and sufficiency of the seismic safety design of nuclear power plants should be confirmed by the risk assessment. Seismic safety design and the risk assessment are now inseparable for safety assurance of nuclear facilities. The combined approach of safety design and risk assessment is important for selecting design basis events adequately for safety design. This approach must be risk informed and must not miss the potential side effects in the safety and failure conditions. Performing the combined approach is essential to satisfy the necessary and sufficiently conditions for the safety requirements of NPPs.

Following are important points to establish the methodology for performance-based seismic safety design on nuclear facilities assuring defense-in-depth safety:

- Consideration of diversity and uncertainty of seismic events and structure failures;
- Determination of design basis events for seismic safety design considering dynamic interaction among technology, human and environment based on a risk assessment;
- Determination of design basis earthquake ground motions on the most significant source based on the probabilistic seismic hazard;
- Evaluation of the structural and functional failure rates of safety-related SSCs for risk-significant seismic events;
- Confirmation of safety performance for reactor safety and radiation protection based on the failure rates of the safety-related SSCs; and
- Iteration between the safety design and the risk assessment to converge on the safety requirements.

DISCLAIMER

The views expressed in this paper are those of author and should not be construed to reflect the official Japanese NSC position.

REFERENCES

1. Konno, T., (2001) “Present and Future Seismic Safety Guideline for NPPs in Japan” SMiRT-16, Washington,

DC, USA
2. Konno, T., (2003) “A Developing Risk-informed Design Basis Earthquake Ground Motion Methodology “ SMiRT-17, Plague, Czech Republic
3. Noda, S., Yashiro, K., Takahashi, K., Takemura, M., Ohno, S., Tohdo, M., Watanabe, T., (2002) “Response Spectra For Design Purpose Of Stiff Structures On Rock Sites,” OECD/NEA Workshop on The Relations between Seismological Data and Seismic Engineering Analyses, Istanbul, Turkey
4. Irikura, K., (2000) “Prediction of Strong Motion From Future Earthquakes Caused by Active Faults-Case of the Osaka Basin,” 12WCEE, Auckland, NZ
5. Rasmussen, J., Pejtersen, A.M., Goodstein, L.P., (1994) “Cognitive Systems Engineering,” Jhon Wiley & Sons, Inc.
6. Tanabe, F., (1991) “Issues in Man-Machine System Evaluation,” SMiRT 11th Post-Conference Seminar on Probabilistic Safety Assessment Methodology
7. Konno, T., (2001) “Reassessment Philosophy for the Seismic Safety of NPPs in Japan” QECD/NEA Workshop on Seismic Re-evaluation EC JRC/ISPRA, ITALY
8. Sakagami, M. and Hirano, M., (2000) “Comparison of Trial Seismic PSA and Seismic Margin Analysis for a BWR” PSAM5, Osaka, JPN
9. Oikawa, T., Muramatsu, K., Kasahara, T., Kawamata, K. and Morota, H., (2000) “Conceptual Design of Operator Support System under Seismic Conditions” PSAM5, Osaka, JPN
10. Kansai Electric Power Company, Restoration Record in the Southern Hyogo prefecture earthquake, (in Japanese)
11. Nishihata, M., Shibuya, A. Sakagami, M. and Mizumachi, W., (2000) “Evaluation of Component Fragility for Seismic PSA on Japanese LWRs,” PSAM5, Osaka, JPN
12. Kirimoto, Y., Emukai, F. and Sasaki, A., (2000) “Component Reliability Data from 1982 to 1997 on 49 Japanese LWRs Accumulated in the Nuclear Component Reliability Data System” PSAM5, Osaka, JPN

