Deterministic and Probabilistic Effects of External Event in Safety Assessment

Takaaki KONNO

Secretariat of Nuclear Safety Commission

ABSTRACT

Safety assurance implicitly assumes a certain risk. The risk results from the cumulative contribution of many kinds of events. The safety design of nuclear facilities is expected to minimize the overall risk considering the deterministic and probabilistic effects from internal and/or external events. Conventional safety assessment for external events is based on a conditional risk insight, considering the severe hazard that will cause large deterministic effects on safety systems. When low probability effects are considered, the safety margins calculated by the conventional assessment are not clear, and it is not certain that the risks remain acceptably low. Assessment considering low probability effects should be performed for external events in order to strengthen the reliability of the risk constraint. These aspects of low probability effects in nuclear facilities are not yet fully integrated in a total risk management for external events. A rational safety design for external events is therefore required to comply with the risk constraint based on the probabilistic safety assessment. The cumulative probabilistic hazard is needed to evaluate the risk constraint and the risk significant effect of the hazardous events. A de-aggregation of the cumulative probabilistic hazard is necessary to develop design basis events that are risk dominant events for use in a deterministic safety design. The determination of design basis events based on the de-aggregation from the cumulative probabilistic hazard must not compromise the risk constraint. Aspects of the deterministic and probabilistic effects of external events are categorized by the indexes of damage rate and the probability of failure, respectively. This paper discusses a new methodology for enhancing the reliability of safety assurance by safety and risk assessments that comply with damage rate and probability of failure.

INTRODUCTION

Nuclear facilities install multiple safety systems in order to assure the defense-in-depth safety for unexpected failure occurrences during internal and/or external events. Internal events are potential hazards inherently in the safety systems. Examples are: malfunctions, mishandlings, errors in maintenance activities, aging, and other situations that are inevitable in a large complex facility. External events are natural events such as earthquakes, floods, landslides, or man-made external events such as aircraft crashes, explosions, etc. The effects of these events results from interaction between the characteristics of affecting events and responding facilities. The effects should be clarified in order to ensure the safety for such events. Effects of the internal and/or external events can be graded from the low safety significance to the high safety significance depend on severity. Conventional safety designs to evaluate the capacity of the safety installations to overcome the effects of such events are based on the deterministic design basis events. However, the predicted intensity of the safety significance events is uncertain because of the spatial and temporal variability of future events. The performance capacity of safety installations also has uncertainty influenced by the variability both of the constructional and the operational conditions. The effects of the past events are known deterministically. Effects of future events can only be predicted probabilistically assuming past events experiences and present knowledge. The characteristics of future events will depend on the many uncertain factors when the prediction is conducted based on past experience. In order to clarify effects of future events, uncertainties for both the future event characteristics and the safety performance capacity should be considered. To perform this rational safety design, the defense-in-depth should be established in accordance with the characteristics of external future events. The actual safety margin is generally uncertain because of the influence of environmental conditions in the construction, operation, and maintenance. The logical safety of defense-in-depth must explicitly consider such uncertainty factors.

For the internal events, safety is established based on the experiences of the past events for the safety systems, accumulated during nearly 40 years operations. The efficiency of defense-in-depth has been demonstrated for the internal events by maintained safety at occurrences of incidents or accidents in operation. Defense-in-depth safety is not yet established for the external events. There are few experiences of external events on the defense-in-depth safety systems in nuclear facilities. Past external events experiences like earthquake events show us that the aspect of the events were varied diversely and also the effect were varied diversely even in the non-nuclear/conventional facilities which do not have complex safety systems of defense-in-depth. It is therefore deduced that defense-in-depth safety systems of nuclear facilities will response more diversely to external events than the response to internal events because of the extensive nature of effects by external events. The extensive nature of effects from external events can negate the efficiency of the diversity and redundancy of the safety systems that are useful for internal events. Conventional deterministic safety design for external events is therefore criticized when uncertainty is considered. The safety accountability considering the uncertainty should be enhanced to comply with such criticism. A safety design methodology that is compatible with both the deterministic effects and the probabilistic effects of the safety significance events could be enhance the safety accountability. Effects of safety significance events could be categorized in the deterministic domain or the probabilistic domain considering the damage rate and the failure probability of events for the safety assurance. The methodology of safety assurance by defense-in-depth based on the safety and risk assessments is important for external events. The logical safety of defense-in-depth for external events that assures risk insignificance is established by performing both deterministic and probabilistic safety design and risk assessments. For the seismic events, a methodology of risk-informed design basis earthquake ground motion was proposed (Konno, 2003) [1], and a methodology of seismic safety design and risk assessment was proposed (Konno, 2005) [2]. The categorization of the effects of external events into the deterministic and/or probabilistic is helpful to understand the importance of the safety design and risk assessment.

EFFECTS OF EXTERNAL EVENTS

In the safety assessment of the nuclear facilities, initial internal design events are selected deterministically based on effects causing incidents or accidents to confirm the safety performance. In the external event, the effects have to be analyzed based on the structural interaction between the affecting external events and responding facilities. The characteristics of both of the external events and the facilities will depend on the many uncertainty factors when assessment is conducted for future occurrences. Effects are mainly dominated by the relationship between the intensity of external events and the performance capacity of safety installations. As the intensity of external events becomes larger than the capacity of the safety installations, the deviation from the safety conditions becomes larger and induces incidents or accidents.

What is the point of categorizing the effect of external events to deterministic or probabilistic effects? Past external events are examples of the deterministic effects regardless the severity because of the effects appeared were actual results with a conditional effect in each probability of occurrence in the relationship of events and facilities. That is, a deterministic effect is a conditional effect. But the characteristics of future events will vary depending on the many uncertainty factors in the prediction.

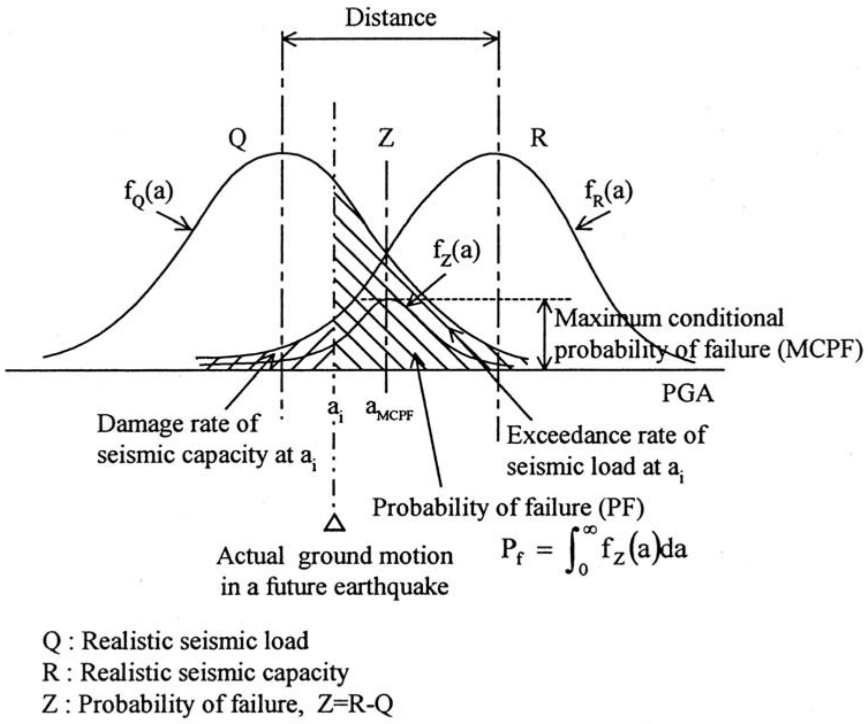
Distance
Q
Z
R
$f_Q(a)$
$f_R(a)$
$f_Z(a)$
Maximum conditional probability of failure (MCPF)
PGA
a_i
a_{MCPF}
Damage rate of seismic capacity at a_i
Exceedance rate of seismic load at a_i
Probability of failure (PF)
$P_f = \int_0^\infty f_Z(a)da$
Actual ground motion in a future earthquake
Q : Realistic seismic load
R : Realistic seismic capacity
Z : Probability of failure, Z=R-Q

Figure 1 Relationship of seismic event and seismic capacity

Figure 1 shows the probability distribution functions of an affecting seismic event and the capacity of a responding facility, representing the variability depending on the many factors of uncertainty. The relationship is a common feature in the natural events. Both the intensity of an affecting event and the performance capacity of a responding facility are generally represented by lognormal probability density functions. The occurrence probability of incidents or accidents therefore can be derived regardless the magnitudes of the intensity of external events or the capacity of the facilities. In the estimation of the effects derived by the relationships, the values of median and standard deviation of the events and facilities respectively are important metrics. The influence rate of the events can be evaluated by controlling the distance of each median value as related with the standard deviation between the affecting events and responding facilities. Considering the variability, two types of effects can be derived from such relationships of events and facilities. The one is a conditional failure probability that is derived as a probable actual case in the occurrence variability and the other one is the failure probability derived as non-conditional in a set of occurrence density functions of event and facility by the integration of the conditional failure probability. Looking from positive side, the conditional failure probability can be seen as a damage rate. The occurrence of the damage influences directly the safety performance. How safety performance is degraded depends on the damage rate. The acceptable damage rate will be defined by confirming the safety performance can be maintained with the damage rate. If the safety performance is sufficient to maintain safety with the damage rate then the damage rate is acceptable. The safety performance is required to maintain safety for the maximum damage rate in the conditional failure probability. The maximum damage rate is the deterministic effect in the relationships of events and facilities and is the most safety-significant parameter for the safety design.

Looking from the negative side, the failure probability shows the necessary probability of failure to maintain safety even though the maximum damage rate is acceptable. This means that safety assured by the safety performance still needs to confirm risk insignificance for the design events. The probability of failure derived as the sum of the conditional failure probability is the probabilistic effect in the relationships of events and facilities to be used for the risk assessment.

The categorization of external event effects is that the deterministic effect is the positive side of effect such as the damage rate as the safety significant condition to be used for the safety assessment while the probabilistic effect is the negative side of the effect such that the probability of failure is the risk significant condition to be used for the risk assessment.

SAFETY AND RISK ASSESSMENTS

It is important to recognize the difference between safety and risk assessments. There is no absolute safety, but the probability of success or failure defines rational safety assurance. Both the estimated capacity and the predicted intensity could vary in the future in accordance with the probability of occurrences, respectively. Consider that variability in the capacity of safety installations can not always cover the intensity of safety obstructions. There is a probability of failures even if a rational safety level is designed.

In order to estimate the insignificance of such probability cases, the risk evaluation methodology was developed. Risk is represented quantitatively by multiplying the event occurrence frequency, safety failure probability and the consequence of the outcome. When a hazardous event would be induced an incident/accident the safety functions of the facilities responds in order to ease the progress of going through the success path for plant safety conditions. These routes are confirmed by the event trees and fault trees composed using the safety installations. Safety for such events is maintained when the progress of the incident/accident is controlled through a success path with the necessary safety performance. If the progress of the incident/accident goes to the failure path, then safety is not maintained. Whether the progress of the incident/accident come to success or failure to maintain safety is estimated in the basis of probability and depends on the relationship of the safety capacity and event intensity. Nuclear facilities are designed such that incidents/accidents go through the positive safety path with high confidence, but not with a zero probability of failure. As the event occurrence frequency become high the probability of failure also increases even if the failure probability by the individual event is low.

Therefore it is important to perform not only safety assessment but also risk assessment in order to have not undue risk from nuclear facilities to the public. The relationship between safety and the risk can be seen. The safety assessment confirms safety performance for the most safety significant event based on the maximum damage rates. The most safety significant event can be determined by the combination of the probability density functions both of the intensity of events and the capacity of safety installations. The risk assessment intends to confirm the risk insignificance as evaluated by the cumulative failure probability distribution functions based on the occurrence frequency of all events and the consequences. Safety is assured for the each safety significant event to confirm safety performance. Risk is evaluated based on the failure probabilities accumulating with every event occurrence frequencies. The safety level for the each event can not control the risk level because of the risk is provided by the effects of cumulative events.

The combination of safety and risk levels should be the high safety level and low risk level but it is possible to appear any types such as, both of the safety and risk levels are high, the safety level is high and risk level is low, the safety level is low and risk level is high, and both of the safety and risk levels are low. When the safety level is very high it might be acceptable the risk level is high. While even the risk level is very low it might be not acceptable if the safety level is low. Acceptable safety level will be decided by the combination with the risk level as shown in the Figure 2.

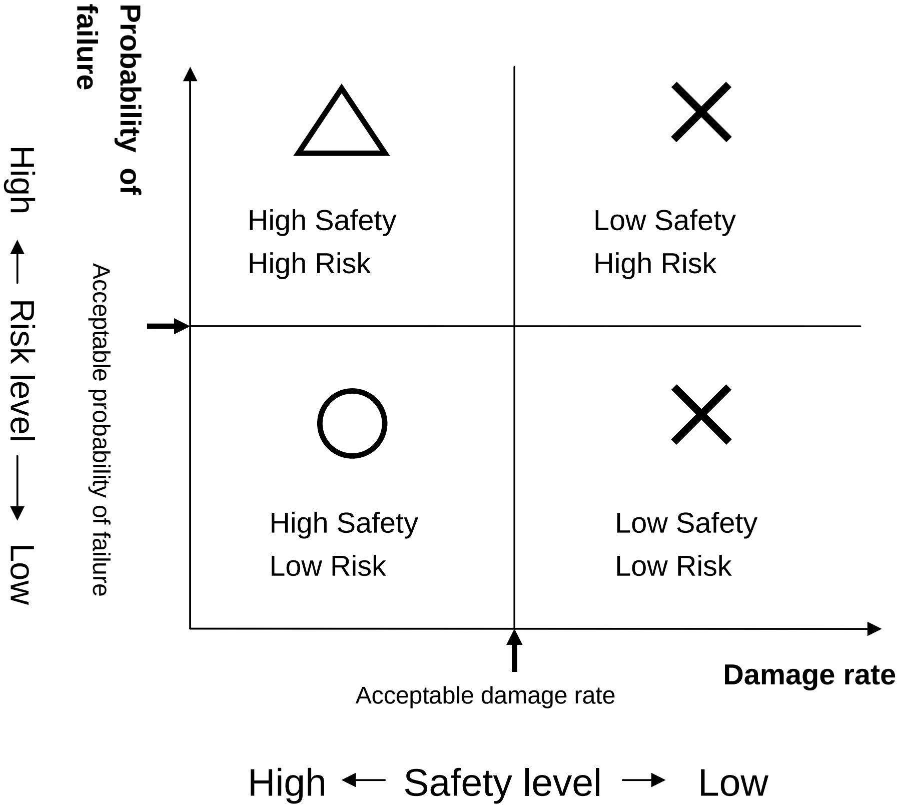

Figure 2 Relationship of safety and risk levels

Rational safety design is therefore not enough without formal risk assessment. The safety performance analysis is also important in the safety design. Safety performance should be confirmed during the damage rate derived by the most safety significant event, while risk assessment should be performed with the cumulative failure probability derived from the contribution of every event occurrence frequencies.

To assure the practical safety for external events, the logical safety of defense-in-depth should be established in the safety design considering the uncertainty of the future external events. The practical safety is generally influenced by the interaction among the variable conditions of construction, operations, and environments. The logical safety of defense-in-depth is needs to also consider such uncertainty factors. There are few experiences of external events on the defense-in-depth safety systems for nuclear facilities. The experiences of past external events like earthquake events shows the aspect of the events varied diversely and the effect appearances varied diversely even in the non-nuclear conventional facilities without complex safety systems of defense-in-depth. It is deduced that defense-in-depth safety systems of nuclear facilities will respond with more complexity in the external events than the response in the internal events because of the more extensive effects in external events. The common cause of failures in external events can reduce or eliminate the efficiency of safety systems.

The methodology of safety assurance by both safety and risk assessments is important for establishment of defense-in-depth safety for external events. The risk is calculated by the contribution of all kinds of affecting events but the technology and knowledge has not matured yet to estimate the risk of every kind of event on the basis of total risk management. The risk estimated by all events such as earthquakes, floods, etc., will be used as the risk constraint in risk management.

CNCLUSION

The safety assurance of nuclear facilities in Japan currently endorses deterministic the safety design. Safety confirmed by such safety design is based on the conditional success probability of maintaining safety conditions. However, the safety based on this conditional success probability can not prove risk insignificance because of the quantity of the failure probability is derived by the total of every event’s contributions even though each event only contributes a low probability of failure. The probability of failure is not zero even though the probability of success to safety is very high. The risk based on the failure probability therefore must be constrained by the insignificance level in order to enhance the reliability of the safety assurance. Effects of external events can be categorized to the positive/deterministic effect and the negative/probabilistic effect. The conditional success probability stands on the positive side and can be represented by the damage rate that is used to confirm the safety performance. The failure probability stands on the negative side to assess the risk significance. The failure probability is derived from the total contributions of many events even though each event has only a low probability of failure. The defense-in-depth safety logic for nuclear facilities should consider both of the positive and negative effects of external events. The safety significant conditions can be determined deterministically but the significance of failure conditions can not determine deterministically. The maximum damage rate derived from the safety significant conditions should be confirmed to be acceptable by the safety performance analysis with the damage rate. The failure probability derived from the all events should confirm the risk insignificance. Performing both the safety assessment for the deterministic effects and the risk assessments for the probabilistic effects are important aspects to enhance the safety assurance reliability and to more precisely comply with the inherent success and failure probabilities in the affecting external events and responding facilities.

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., (2003) "A Developing Risk-informed Design Basis Earthquake Ground Motion Methodology " SMiRT-17, Plague, Czech Republic

2. Konno, T., (2005) "SEISMIC SAFETY DESIGN AND RISK ASSESSMENT " SMiRT-18, Beijing, China