Risk-Informed Defense-In-Depth Seismic Design of Nuclear Power Plants

Tadakuni Hakata[1)]

1) TH Consulting, Japan

ABSTRACT

"Defense in Depth" is the basic philosophy for nuclear safety. Earthquakes are stochastic events and seismic probabilistic safety assessment (PSA) methodology has been much progressed. The strategy should be used for seismic safety. This paper investigates a risk-informed approach to attain optimum allocation of defense-in-depth measures to ensure adequate seismic safety of nuclear power plants. The safety-related structures, systems and components (SSC) are first grouped into categories by the characteristics of accident sequences, and ranges of required capacity of the SCC are determined in terms of High Confidence Low Failure Probability (HCLFP) according to the categories. Seismic PSA were conducted for a typical PWR plants to refine the strategy and to assure the adequacy, aiming at safety goals and appropriate risk balance among accident sequences.
This approach will provide a guide to an effective seismic design of nuclear power plants.

INTRODUCTION

"Defense in Depth" philosophy requires that nuclear facilities shall be provided with multiple defenses in depth to assure safety of nuclear facilities so that any single failure of SSC does not cause severe consequences. The risk-informed defense-in-depth approach and the procedures however do not seem to have been sufficiently developed for seismic design of nuclear power plants. .

Risk-Informed Defense-In-Depth Measures for Seismic Safety

Defense-in-depth measures for nuclear power plants (NPP) consist of the following steps as show in Fifure 1.:

Level 1: Prevent occurrence of abnormal events
Level 2: Prevent propagation of abnormal events to accidents
Level 3: Mitigate consequence of accidents
Level 4: Severe accident management (AM)
Level 5: Off-site emergency response

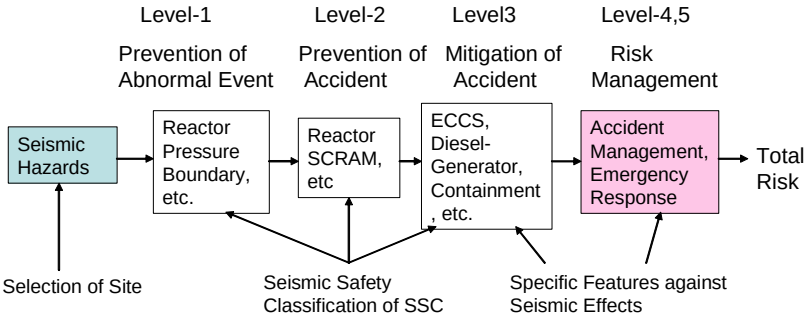

Fig. 1 Defense-in-Depth Measures for Seismic Safety

Risk of Nuclear Power Plants at Earthquakes

The overall risk of nuclear power plants is expressed by two elements as:

$$\text{Risk} = \Sigma \text{ (Seismic hazards) x (Plant level seismic fragility)} \quad (1)$$

Seismic hazards are frequency of occurrence of earthquakes versus acceleration of the ground motion. Plant level seismic fragility is the probability of the plant to fail to withstand seismic load and to result in severe accidental conditions, such as core damage or containment failure, etc. The risk is estimated by seismic PSA methods. Figure 2 shows the typical relationship of the elements of Eq. 1.

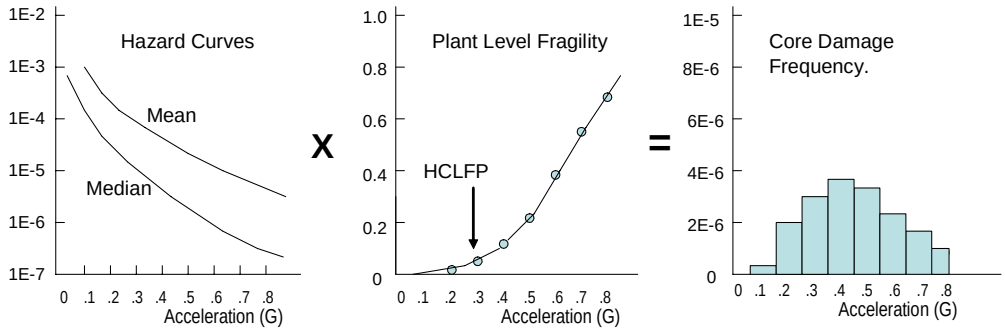

Figure 2 Seismic Probabilistic Safety

Seismic design is usually based on design basis earthquake ground motion (DBE), which is defined from historical earthquakes and seismological and seismic engineering examination of the site characteristics. DBE is also determined from seismic hazard curves and a reference cumulative frequency, such as 10^{-5}/ry (Median) [1] or 10^{-4}/ry (Mean).

Fragility of safety-related structures, systems and components (SSC) is represented by the median and standard deviations of randomness and uncertainty with Log-normal distribution function. The fragility of SSC can be also represented by HCLFP (refer to Appendix A)[2], which is defined at 95% confidence 5% failure probability. Mean failure probability of SSC (50% confidence) is about 1%. If all safety-related SSC of a reactor plant are designed to have HCLFP at DBE, the plant level HCLFP may be around at DBE.

RISK-INFORMED SEISMIC DESIGN

Risk-Informed assignment of HCLFP for initiating events and mitigating systems is investigated by engineering analysis and seismic PSA method [3] for a typical PWR plant of similar design as Surry plant [4]. The design basis earthquake is assumed at 0.20G (referring to mean cumulative frequency of 10^{-4}/ry and LLML hazard curve), although the safety shutdown earthquake of the Surry is 0.15G. This study and conclusion is not for Surry plant.
Three cases are examined to obtain adequate allocation of Defense-In-Depth elements.

Case 1: HCLFP of all safety-related SSC at DBE

We assume that HCLFP of all essential safety-related SSC are at DBE of 0.2 G, including initiating events which are initiated by failure of seismically qualified SSC (excluding Loss of Station Power and Transients) and safety-related mitigating systems. The mean failure probability of the safety-related SSC is then about 1% at DBE, and the plant mean core damage frequency (CDF) at DBE may be:

$$\text{CDF at DBE} < (10^{-4}/\text{ry}) \times (0.01) = 10^{-6}/\text{ry /sequence} \quad (2)$$

This case is a provisional starting point, since general deterministic limit of acceptable safety per sequence is 10^{-6} /yr.

Seismic PSA was conducted with the above assumptions.

Results of Case 1

Figure 3 shows the fractions of CDF of accident sequences. The seismic risk of this case is dominated by reactor vessel rupture (RVR) and Building failures, contributing 75% to the total CDF of 4.1x 10^{-5}. This is because the two sequences do not have effective mitigating systems.
The plant level HCLFP is 0.22G which is nearly DBE.
This case meets safety goal of 10^{-4}, but not 10^{-5} and risk Balance is not good. This case is not acceptable.

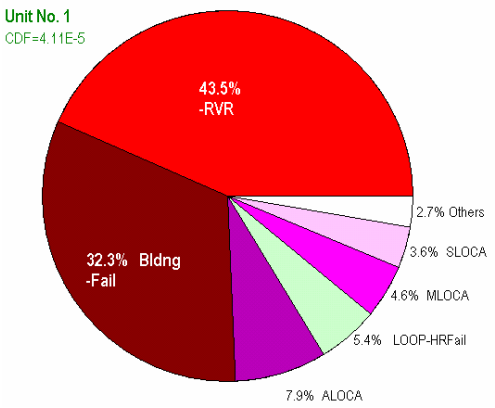

Fig. 3. Results of Case 1 SPSA

Increase HCLFP acceleration of risk dominant SSC

Eq. 1 is rewritten as:

$$\text{Risk} = \Sigma\,(\text{Seismic Hazards}) \times (\text{Accident sequences})$$
$$= \Sigma\,(\text{Seismic Hazards}) \times (\text{Initiating Events}) \times (\text{Mitigating Systems})$$
$$= \Sigma\,(\text{Frequency of Initiating Events}) \times (\text{Fragility of Mitigating Systems}) \quad (3)$$

Eq. 3 indicates that we should consider combination of frequency of occurrences of initiating events and fragility of mitigation systems so as to meet safety targets and to achieve appropriate risk balance.

For the purposes, accident sequences are grouped into categories taking consideration of the specific characteristics of the initiating events and mitigating systems. Required ranges of HCLFP for prevention of initiating events (Defense-In-Depth level 1) and required seismic capacities of mitigating systems (Defense-In-Depth level 2, 3), which are taken credit for safety, are determined for each category.

The categorization and their provisional requirements are defined as:

1) Category 1: Occurrence of the initiating events, which have no effective mitigating systems or failures of which may fail the required mitigating systems by common cause, should be extremely unlikely. The initiators of SSC should have sufficiently high HCLFP seismic acceleration or median of the fragility.
2) Category 2: Occurrence of loss of coolant type initiating events (LOCA, SGTR and RCP seal LOCA) should be very unlikely, since those events may challenge containment integrity. Those initiating events must have high HCLFP acceleration and high median of fragility. The mitigating systems should be seismically qualified.
3) Category 3: Loss of Station Power (LOSP) and Transients, which are possible to occur at earthquakes lower than DBE, should have highly reliable and seismically qualified mitigating systems. Active systems should be provided with redundancy or diversity and passive equipments should have high HCLFP or median of fragility.
4) Category for Buildings whose failure could fail multiple safety-related systems should be designed with Sufficiently high HCLFP acceleration or fragility. Examples are building failures at the building interface which may cause multiple ruptures of pipes and cables. Failure of enclosure buildings may also cause damages of multiple safety systems inside.

Table 1 shows sample categorization and the requirements on HCLFP acceleration. They are determined based on engineering judgment, because scenario-based important analysis methods are currently not available.

Table 1. Categories and Desirable HCLFP Acceleration Level of Safety-related SSC for Prevention of Core Damage

Cat.	Characteristics of Accident Sequence		Targets of HCLFP of SSC		
	Initiating Events (Examples)	Mitigating System Reliability	Initiating Events Requirement	**HCLFP**	Mitigating Systems PGA of **HCLFP**
1	Severe Accident Initiators Reactor Vessel Rupture, Multiple LOCA with ECCS un-enabled	No effective mitigating system available .	Extremely unlikely	**1.5 ~ 2.5 DBE**	none
	Failure of Structure such as Intake channel	If diverse ultimate heat sink is not provided	Very unlikely	**1.5 ~ 2 DBE**	Diverse ultimate heat sink might be desirable
2	Large LOCA	Reliable mitigating system required	Very unlikely	**1.5 ~ 2 DBE**	**DBE**
	Medium / Small LOCA SGTR RCP seal LOCA	A single failure must not negate mitigation	Not Likely	**1 ~ 1.5 DBE**	**DBE** / channel Single passive Comp. **1.2 ~ 1.5 DBE**
3	LOSP and Transient	Reliable Scram to prevent ATWS	(Likely)		Redundant System **DBE/** channel
		Reliable diverse heat removal system required			**DBE/** channel Single passive comp. **1.2 ~ 1.5 x DBE**
4.	Building Failure causing multiple system failures			**1.5 ~ 2 x DBE**	
5		Essential Supporting Sys such as Batteries, DG			**DBE/** channel
6	Other safety-related items		Reliable as practical		

Case 2: Increased HCLFP Acceleration for Risk-significant Initiating Events

HCLFP accelerations of LOCA-related Initiating Events and Buildings are set at higher value as shown in Table 1. Results of Case 2 SPSA: The results of Case 2 SPSA are shown in Figure 4. CDF is reduced to 1.26 x 10^{-5} /ry (by about 70%) and the risks are more balanced. The plant level HCLFP is 0.35G. This case is almost acceptable except that all of the safety-related mitigating systems have the same HCLFP at DBE, regardless of the risk-importance.

Case 3 : Desirable Allocation of HCLFP or Fragility of Initiating Events and Mitigating Systems

HCLFP accelerations or fragility of risk dominant safety-related mitigating systems SSC is increased in addition to Case 2 as in TABLE 1 (see also Table 2) General data of fragility are used for non-dominant mitigating systems. Results of Case 3 : The results of seismic PSA for case 3 is shown in Fig.5. The total CDF is 6.9 x 10^{-6} / ry (reduced by 45% from Case 2). Plant level HCLFP is 0.41 G This case is acceptable.

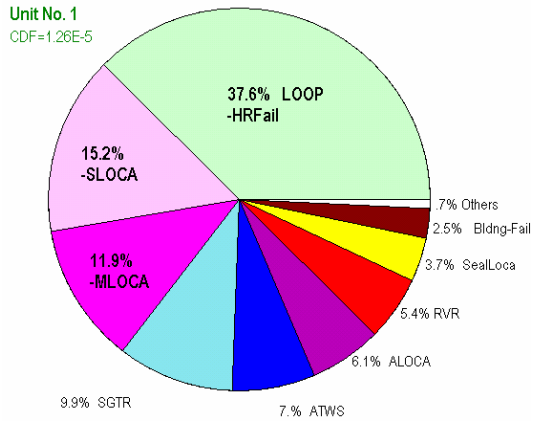

Fig. 4 Results of Case 2

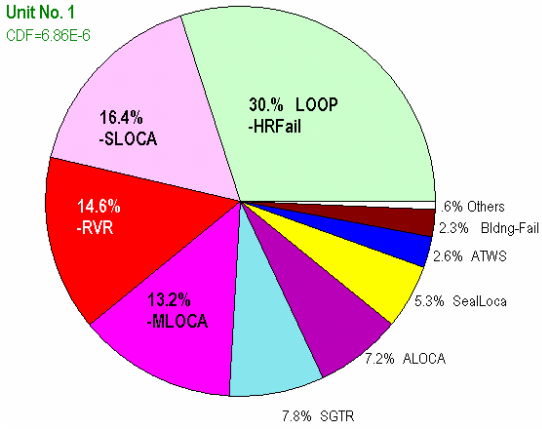

Fig. 5 Results of Case 3

SUMMARY OF RESULTYS AND DISCUSSIONS

Table 2 summarizes conditions and results for cases 1, 2 and 3. Figure 6 depicts the total CDF and CDF of the most dominant initiating event for three cases.

Table 2. HCLFP and Medians of Fragility of safety-Related SSCc and SPSA results of three case studies

		case 1			case 2			case 3				Typical
		HCLFP	Median	*M / D*(1)	F_{DBE}(2)	HCLFP	Median				*M / D*	Median(3)
Initiating Events	RVR	0.2	(1.3G)	*6.5*	2.5	0.5G	(3.2G)	←			*16*	4.27G
	ALOCA	0.2	(1.3G)	*6.5*	2	0.4	(2.6G)	←			*13*	1.83G
	MLOCA	0.2	(0.82G)	*4.1*	1.5	0.3	(1.2G)	←			*6*	1.50G
	SLOCA	0.2	(0.86G)	*4.3*	1.25	0.25	(1.1G)	←			*5.5*	0.96G
	SGTR	0.2	(0.86G)	*4.3*	1	0.2	(0.86G)	←			*4.3*	
	LOOP	Generic				(0.06)	(0.25G)	←			*1.25*	0.25G
	Transients	Generic					(0.075G)	←			*0.37*	
								F_{DBE}	HCLFP	Median		
Mitigating System	DG	0.2	(1.1G)	*5.5*	←			1	0.2G	1.1G	*5.5*	1*G*
	SCRAM Train	0.2	(2.6G)	*13*	←			1.2	0.25	3.2G	*16*	
	RWST	0.2	(0.76G)	*3.8*	←			1.2	0.25	0.95G	*4.7*	
	CST	0.2	(0.76G)	*3.8*	←			1.2	0.25	0.95	*4.7*	
	CCWS HX	0.2	(0.72G)	*3.6*	←			1	0.2	0.72G	*3.6*	
	Building	0.2	(0.5G)	*2.5*	2	0.4G	(1.0G)	←			*5*	1.5-1.8G
	Other SSC	0.2			←			Generic				
CDF		4.1 E-5			1.26 E-5			6.96E-6				
Plant Level HCLFP		0.22 G			0.35G			0.41G				

Note(1): *M/D* is Median/DBE, (DBE=Design Basis Earthquake)
Note(2): F_{DBE} =Multiplier of DBE. HCLFP is at F_{DBE} * DBE.
Note(3): Typical Data are from a Typical SPSA[4]

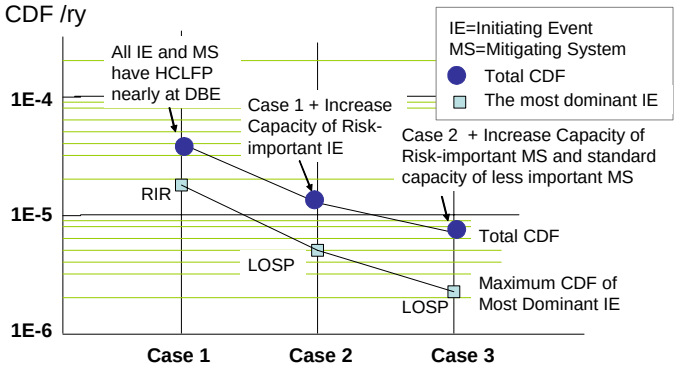

Fig.6 CDF of Case 1,2,and 3

Following summarize the findings obtained from this study:

1) Case 1 shows that median of the fragility of initiating events with the same HCLFP acceleration are different for different SSC, depending on their uncertainties --- the larger the uncertainty is, the higher the median of fragility (for HCLFP at DBE) is.
2) Case 3 shows the ratios of *M/D* (=Median of Fragility/ DBE) must be much larger than 1 for risk-dominant SCC's. Especially Reactor Vessel Rupture, Buildings and SCRAM train, etc. should have medians of fragility higher than DBE by 10 times or more, that are needed safety margins.

3) Case 3 indicates that HCLFP or fragility of mitigating systems should be determined by considering risk-importance.

Mean Failure Probability of Various SSC's vs. HCLFP

Figure 7 shows the variation of mean failure probabilities (50% confidence) of various SSC at DBE (0.2 G). For instance, failure probability of a SSC with HCLFP acceleration of 0.1G is about 0.2 at DBE (0.2G). The mean failure probability of SSC with HCLFP of 0.2 G is 0.01 (1 %) at DBE (0.2G).

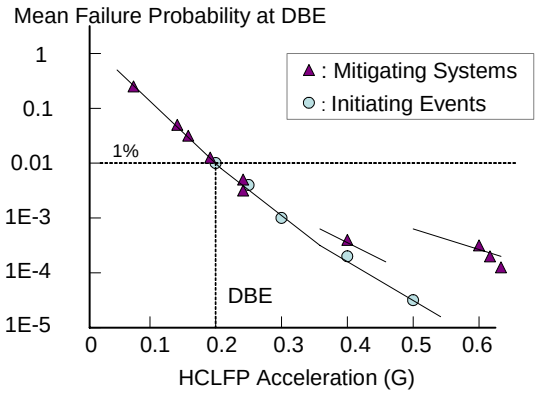

Figure 7 Mean Failure Probability at DBE vs. HCLFP

Other Consideration.

Containment Failure

This study was performed for prevention of core damage. The general target of containment failure probability conditional on core damage is 0.1, which is generally difficult to attain for seismic events because of the common effects.

Optimum seismic design for containment integrity and heat removal during severe earthquakes remains as a next task.

Severe Accident Management

Accident management (AM) may be classified as follows:

Table 3. Severe Accident Management for Earthquakes

Types of AM	Effective Range
a) Non-Seismically qualified AM (Non-safety-classified source of water, CV vent, etc.)	less than DBE
b) Ties of safety-related systems between units (DG, RWST, CST, Ultimate Heat Sink, etc.)	within DBE
c) Additional equipment or devices with seismic capacity larger than DBE (Additional shared emergency power of highly seismically qualified capacity, etc.)	beyond-DBE

Type a) and b) AM is effective for relatively high risk plants, not for low risk plants.

Type b) is effective to improve site integrated risks in a multi-unit site as well as individual plants as shown in Figure 8 [5].

Type c) is effective for all ranges including Beyond-DBE.

AM should be planned strategically, taking into consideration characteristics of AM measures in relation with the effective range of accelerations.

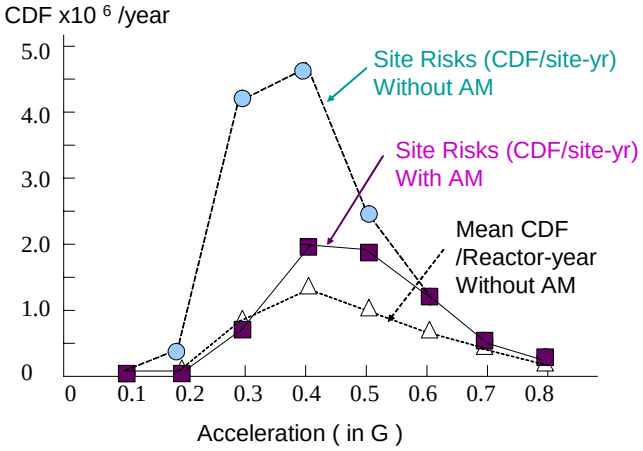

Figure 8. Effects of Ties of DG, RWST and CST For 5-unit site

CONCLUSION

Risk-informed defense-in-depth approach for seismic safety design of nuclear power plants was studied. . Accident sequences are first grouped into categories from the characteristics of the accident sequences. HCLFP or fragility of the safety-related structures and equipments are then determined accordingly so as to have risk balance. Seismic PSAs were then conducted parametrically for a typical PWR plant. The results meet the general safety goals for CDF with appropriate risk balance among accident sequences.

It may be concluded that such a risk-informed defense-in-depth approach can offer guidance to reasonable and effective seismic design of nuclear power plants and enhance seismic safety of operating plants against earthquakes effectively.

REFERENCE

1. NRC, “Identification and Characterization of Seismic Sources and Determination of Safe Shutdown Earthquake Ground Motion”, RG-1.165, March 1997
2. NRC,” Perspectives Gained From the Individual Plant Examination of External Events (IPEEE) Program”, NUREG-1742
3. Tadakuni Hakata, “Seismic PSA Method for Multiple Nuclear Power Plants in a Site”, Reliability Engineering and System Safety, 92/7 PP.883-894 (July 2007)
4. M.P. Bohn,et al. Analysis of Core Damage Frequency: Surry Power Station, Unit 1 External Events, NUREG/CR-4550/ SAND86 -2084 Vol3, Rev.1 Part 3, December 1990
5. Tadakuni Hakata, “Seismic PSA Methodology for Multi-Unit Site”, OECD NEA Specialist Meeting on the Seismic PSA of Nuclear Facilities, Jeju Island Korea, 6-8 November 2006

APPENDIX A Definition of HCLFP

The peak gland acceleration (PGA) at High Confidence Low Failure Probability (HCLFP) is obtained by setting failure probability P_f at 0.05 in the following equation:

$$P_f = \Phi\left[\frac{Ln(Mr(pga)/Mf) + \sqrt{\beta_{R-U}^2 + \beta_{C-U}^2}\,\eta_{95}}{\sqrt{\beta_{R-r}^2 + \beta_{C-r}^2}}\right] = 0.05 \qquad \text{(A-1)}$$

where,

Φ is the standard normal cumulative distribution function

$Mr(pga)$ is the median of the component response and Mf is the median of the component fragility

β_{R-r}, β_{C-r} are the random logarithmic standard deviations of the response and fragility, respectively.

β_{R-U} , β_{C-U} are for systematic uncertainty. η_{95} is for 95% confidence: $\eta_{95} = \Phi^{-1}[0.95]$

For the point estimate the following equation is applied to obtain failure probability.

$$P_{f-PE} = \Phi\left[\frac{Ln(Mr(pga)/Mf)}{\sqrt{\beta_R^2 + \beta_C^2}}\right] \qquad \text{(A-2)}$$

where β_R is the composite standard deviation of response = $\sqrt{\beta_{R-r}^2 + \beta_{R-U}^2}$ and , $\beta_C = \sqrt{\beta_{C-r}^2 + \beta_{C-U}^2}$