Proceedings of the International Symposium on Engineering Lessons Learned from
the 2011 Great East Japan Earthquake, March 1-4, 2012, Tokyo, Japan

ROBUSTNESS AND RESILIENCE AS EXTENTIONS OF RISK CONCEPT AFTER FUKUSHIMA EVENT

Tsuyoshi TAKADA

Professor, Graduate School of Engineering, The University of Tokyo,
Tokyo, Japan, takada@load.arch.t.u-tokyo.ac.jp

ABSTRACT: The concept of risk against inevitable uncertain future events has been emphasized, but not intensively been implemented to ensure the safety of Japanese nuclear power plants for many years. The most important lesson from the Fukushima Daiichi nuclear power plant accident on March 11, 2011 probably be the need of the risk concept and further extension of the concept to the one in space as well as the one in time. In the present paper, these features, which will be refereed to as “robustness” and “resilience ”, respectively, will be demonstrated along with the brief report of the Fukushima accident, and their concept will be clarified for NPP safety.

Key Words: risk, robustness, resilience, risk management, earthquake disaster, tsunami.

INTRODUCTION

The 2011 Great East Japan Earthquake has brought a tremendous disaster to Japan, Earthquake, Tsunami, and the Fukushima NPP accident, all of which have resulted in large and long-lasting consequence to the modern society. People have often called the disaster "beyond expectation", which sometimes sounds "reconciliation" or "Act of God", "limit of science" as if human beings could not do anything but give up. From engineering point of view, however, it is very important that the safety of the NPP should be secured against such a severe condition. The risk concept has been recognized as essential concept for almost all engineering systems so far. The risk in the engineering discipline is defined as the combination of the probability and the consequence of events, and the risk concept has been effectively utilized in various aspects in conjunction with uncertainty. The author recognizes the effectiveness of the risk concept, further claims further need of extension of the risk concept in light of the Fukushima daiichi NPP accident. In the present paper, it is demonstrated that the disaster due to the 2011 Great East Japan Earthquake will be very briefly reported, then the risk concept related to the safety of NPP will be stated, and finally the need of further extensions of the risk will be stressed.

DISASTER DUE TO TSUNAMI AND LARGE SHAKING

Earthquake

The gigantic 2011 Great East Japan Earthquake occurred with an earthquake magnitude 9.0, which is the super mega earthquake from the Japanese observation history, and its earthquake source region in the plate boundary ranges 500 km in North-South length and 200km width in East-West direction. The spatial distribution of JMA intensity at the Tohoku region is plotted in Fig.1, and the regions with JMA intensity 5 greater to intensity 6 greater are quite wide coastal area. In a Tokyo Metropolitan area, the wide area was shaken with JMA intensity 5 greater and the long duration time of shaking, say, 2 minutes was observed. More than one hundred thousand commuters were unable to get home. Furthermore, So may aftershocks including earthquake magnitude 7.0 followed. Figure 2 shows the epicenters of the aftershocks in two months after March 11, and most of aftershock earthquakes with more than magnitude 7.0 occurred much closer to the land, which might have produced larger ground motions to some areas than that from the main shock did.

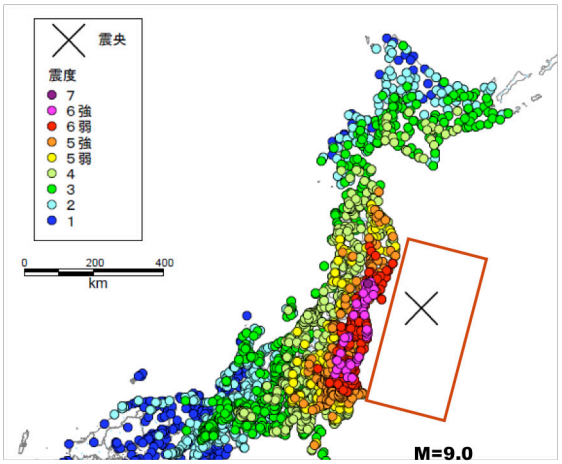

Figure 1 JMA intensity (ADEP, 2011)

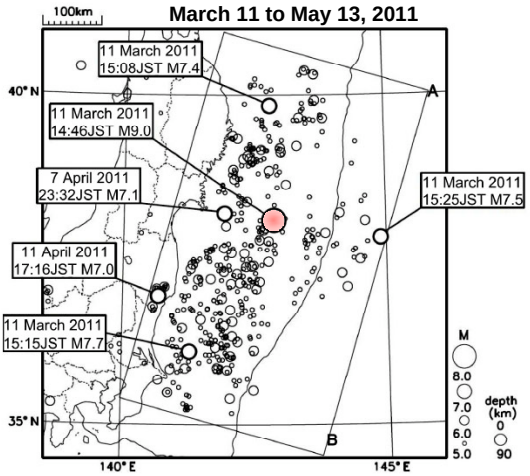

Figure 2 Location of aftershocks (ERI, 2011)

Tsunami

The huge tsunami hit the very wide area, 500 km long the Tohoku coast, and tsunami wave height observed varied from 6 to 40 meters, dependent upon topography of coast, configuration of bay areas. It resulted in around 16,000 people dead and 3,400 people missing, and 2, 350 thousand houses flashed away. The number of casualties, region by region, seems to be highly dependent on the location of the region and their emergency evacuation plan against tsunami, rather than presence of tidal embankments constructed.

The spatial distribution of tsunami height compiled by a special investigation group is shown in Fig. 3. A region with no dots in the figure is close to the Fukushima NPP where tsunami height data were not collected because of radioactive controlled area. This figure clearly shows that very wide area were affected by tsunami and the tsunami height close to 40 meters were observed, which are found much larger than the height of embankment in some of regions.

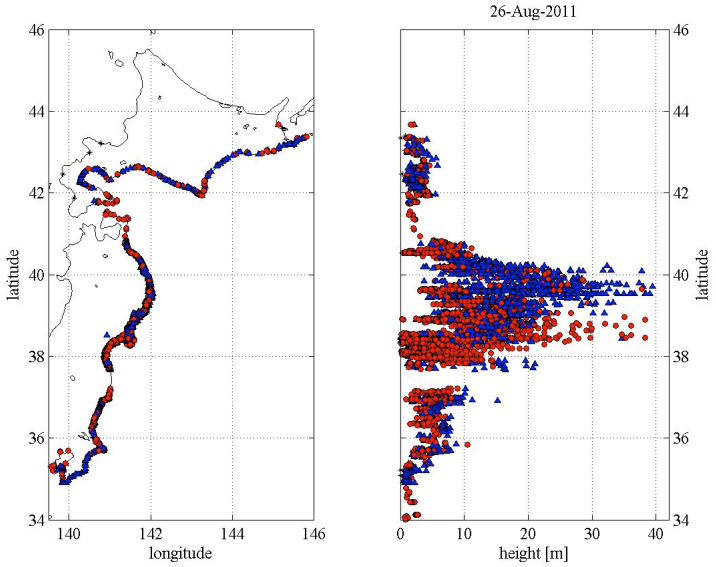

Figure 3 Spatial distribution of wave height (ERI et al., 2011)

Indeed, the total economic loss due to this disaster including earthquake and tsunami has been estimated 16 to 5 trillion Japanese yen, which is the biggest loss in the past. Despite the tremendous efforts of recovery operation in all regions in the last ten months, still the recovery process seems very slow because of wide regions affected and the Fukushima accident.

Accident of Fukushima Daiichi NPP

A nuclear accident have occurred at the Fukushima Daiichi Nuclear Power Plant as the result of the giant earthquake and tsunami of the Great East Japan Earthquake. It is a typical multiple hazard disaster to the plant, where there were large ground shaking and the following tsunami wave, both of which affected the plant. While the details of the accident still remain to be fully determined, the accident is outlined below from the viewpoint of the three rules for ensuring safety of nuclear power plants during nuclear plant emergencies, i.e. “Stop”, “Cool down”, and ”Confine” (Takada, 2011).

As the result of the ground shaking during the Great East Japan Earthquake that occurred on March 11, 2011, control rods were firmly inserted into the cores of reactors No. 1, 2, and 3 of the Fukushima Daiichi Nuclear Power Plant, which were operating at the time of the earthquake, as part of the automatic shutdown procedure, and thus the first rule of "Stop the reactor" was accomplished. However, as a result of the earthquake, off-site electric power was rendered impossible, and thus the plant's emergency diesel generators were activated and the emergency core cooling systems began operating. Approximately one hour later after the earthquake, a giant tsunami of about 14 meters in height hit the plant, incapacitating diesel generators and seawater pumps, making it impossible to remove the decay heat of the core fuel to cool it down.

Despite water injection into the reactors, fuel failure occurred. Some damage to the pressure vessels and containment vessels is deemed to have occurred, and hydrogen explosions occurred due possibly to the accumulation of hydrogen within the reactor buildings. As a result, radioactive material has been released from the reactor buildings and reached areas outside the plant's premises. In other words, cooling and containment of the nuclear reactors were not achieved, and as a result, radioactive material from the plant has been released to areas outside the plant site and contaminated surrounding areas. All-out efforts to bring under control the situation at the Fukushima daiichi nuclear power plant are still currently in progress.

RESIDUAL RISK IN DESIGN REVIEW GUIDELINE OF NPP

Current Seismic Design Review Guideline of NPP

The basic requirement of the current seismic design review guideline of nuclear facilities, which was revised in 2006, states (NSCJ, 2006),

To avoid any risks of serious radiological exposure to the public in the vicinity of the Facilities due to the external disturbance initiated by an earthquake, by appropriately formulating 'the ground motions' for the seismic design, which could be postulated appropriately to occur with a very low probability during the service period of the Facilities and which could seriously affect the same.

The basic principle regarding seismic safety is the same as the previous one (NSCJ, 1981), however, the probabilistic statement such as "a very low probability during the service period of the facilities" has been adopted in the current guideline, which is the quite contrast to the absolute expression of the previous one. This indicates the current guideline adopts the probability concept into the seismic design since there exists large uncertainty in the phenomena of earthquakes. The most important attitude towards safer NPPs is to do every effort to recognize, to identify and to assess various uncertainties in all engineering processes. Furthermore, the guideline continues to mention use of PSA (Probabilistic Safety Assessment) of NPPs with the concept of residual risk.

Incentives to introduce the PSA approaches for safety evaluation have been accommodated in the current guide. It requests that: the operators strive to minimize the residual risk as far as practically affordable; and also outlines the exceedance probabilities of the design basis ground motion to be referred to in each safety review case. It continues to state that approaches based on the residual risk will lead to future risk-informed regulation for NPPs.

Risk concept for earthquake and tsunami

Japanese seismic design review guideline for Nuclear Power Facilities (2006) states that reflecting the fundamental performance requirement of NP facilities should be avoidance of any risks of serious radiological exposure to the public in the vicinity of the facilities, as is shown in the above. More concretely, to ensure safety of NP, the primary requirement are to stop, to cool down a reactor and to confine all radioactive materials within a reactor. Unfortunately, these fundamental requirements could not be accomplished at the event of Fukushima Daiichi Nuclear power plants.

The current seismic design review guideline has introduced "residual risk " which allows a small probability that the seismic design ground motion is exceeded during the plant life. This is indeed an important paradigm shift in the revision, while the old guideline had required only absolute safety for nuclear power facilities. This new concept "residual risk", however, has not been intensively implemented regarding how to treat it, how to assess it, and how to utilize it after no intensive discussion has been made since the revision of the guideline. Another important point of the 2006 revision of the seismic design review guideline is to state an inclusion of earthquake-induced phenomena, i.e., slope failures and tsunamis. If the latter phenomenon was treated properly, we might have avoided the serious accident of the Fukushima Daiichi Nuclear Power Plants.

The current guideline clearly states to make every effort to reduce any residual risks that still exist beyond the design basis, which has originally been proposed for the provision of setting the design basis seismic ground motion Ss. The same concept should be applied to the residual risk due to tsunami beyond the design basis. There could be variety of measures to reduce the residual risk due to future tsunamis. A fundamental treatment should be, of course, based on the concept of "defense in depth", i.e., prevention of initiation of accidents, prevention of development of accidents and mitigation of consequence due to the accidents. One of practical but effective risk evaluation is implementation of a tsunami PSA, similar to seismic PSA, which in principle consists of a tsunami hazard assessment, a fragility evaluation and CDF (Core Damage Frequency) estimation of an NPP.

The fragility of NPP systems against tsunamis should cover mechanical failure, electrical component failure due to inundation, both of which require extensive and detail information and technical lessons from the Fukushima event.

RISK CONCEPT AND RISK MANAGEMANT

Risk concept

It is well recognized that it is not feasible to achieve higher safety of engineering systems only by following the design guideline and relevant regulations. Safety should be understood as not an index expressing discrete states; safe or not safe, but continuous quantity expressing the degree of the safe state. It then follows that probability or risk concept has been introduced to take rigorous consideration of various uncertainties specially lying in natural phenomena. Risk, by engineering definition, R is the combination, sometime, the product of the probability P and the consequence of the event C, as follows.

$$R = PC \tag{1}$$

C could be the loss of disaster in monetary unit, or in the numbers of casualties. Since the definition (1) is quite effective in the respect that the risk takes into consideration of the likelihood and the consequence of a event by using a single scalar quantity. In case that the probability is small and the consequence is also small, such a event can be ignored. However, in case that P is small but C is very large, such an extreme event is not allowed to ignore. The threat such as the 2011 Great East Earthquake Disaster should not be ignored even if the probability is very small, but very large consequence may come.

Risk management

One of the advantages of the risk expression is that we can directly compare the threat of various types of disasters from various causes, with different probabilities and consequences. The risk due to large earthquakes can be compared with those due to typhoons or heavy rainfall. From such comparative basis, more rational decision can be done in any engineering problems. The design or more general term such as risk management of NPPs should be more based on the concept of risk in order to make more rational decision.

Superior property of the risk as mentioned in the above can be emphasized in the followings. It is possible to treat various risks on the common basis, and to quantify safety due to various risks. The former advantage should be more emphasized that because the risk comparison can provide useful basis regarding prioritization of investment under various practical constraints. In other words, the risk is a quite useful index on which more rational and higher level decision can be made, which is called “risk management”. Table 1 shows the overview of the whole risk management processes according to the document Guide 73 (ISO, 2002).

In case that the present risk is high and not acceptable to society, the risk should be reduced appropriately. Figure 5 shows how to reduce the risk on the basis of definition of the risk, and there are basically two ways to reduce the risk; one is to reduce the relevant probability, the other is to reduce the consequence. The examples of the former way is to reinforce a building or build a safer building in the seismic design, while the latter is to ensure the evacuation plan during earthquakes. It is desirable to reduce either P or C with an appropriate balance. The best way of risk reduction for earthquakes must be different from that for tsunamis.

Quantification of safety is essential in the engineering. Concept of absolute safety has often been prevailed even in the engineering community, especially in the nuclear industry in Japan, which would come from subjective and emotional way of people’s feeling. The concept of absolute safety indeed

sounds very comfortable as if human beings could conquer the nature with modern technology. It brings great relief for us, and then we get to think that we would be free from any danger, and in the end we completely forget the disaster, what the disaster would be like. The disaster of the 2011 Great East Earthquake teaches us that the comfort coming from the concept of absolute safety paralyzes us. It indicates that we should bear in mind that there is various risks surrounding us and we should not ignore some of risk with low probability but large consequence such as nuclear power plant accidents.

Table 1 Overview of Risk Management (ISO, 2022)

Risk management			
	Risk assessment		
		Risk analysis	
			Hazard identification
			Risk estimation
		Risk evaluation	
	Risk treatment		
		Risk avoidance	
		Risk optimization	
		Risk transfer	
		Risk retention	
	Risk acceptance		
	Risk communication		

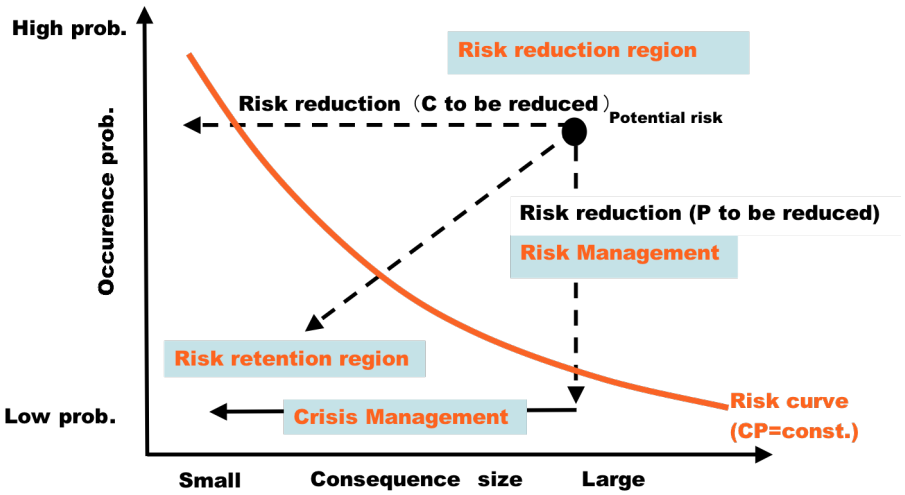

Figure 4 Way of Risk Reduction

ROBUSTNESS AND RESILIENCE

As is mentioned earlier, the notable characters of the disaster due to the 2011 Great East Japan Earthquake are the followings. One is that the devastated area is very wide, say, 500 km long coastal area which were heavily affected and simultaneously damaged by the huge tsunami. The other is the disaster compound with a huge earthquake and the following tsunami. Focusing on the Fukushima daiichi NP, the earthquake ground motion with the same order of ground motion intensity level as the design level hit the wide region, by which non-critical facilities, off-site power supply, access roads to

the site, etc. were heavily and simultaneously damaged in a relatively wide region surrounding the site. The report says the Fukushima accident occurred due to the loss of all off-site electrical supply, main cause was an excessive shaking and tsunami inundation, which is a quite severe combination which was not intensively been taken into consideration at the design stage around 40 years ago. A special accident investigation committee on the accident at the Fukushima plant chaired by Dr. Hatamura recently submitted an intermediate report on the accident. Dislike the random failure of electrical devices, the earthquake and tsunami generally affect a wide region where we cannot rely on any emergency aid from the surrounding area because those area are also equally affected at the same time.

Secondly, most of NPP's locate only the sea shore lines in Japan, were struck by the huge earthquake with the earthquake magnitude of nine and the tsunami wave following after forty minutes later in the Fukushima site. Then, off-site electric power supply was down, and plant emergency diesel generators were activated, but tsunami wave with 15 meter height disabled the diesel generators and seawater pumps. Finally, the plant failed to cool down the four reactors. Despite the desperate recovery emergency activity, radioactive materials have been released from the reactor. These series of time-dependent transition plant state have been made in the plant. Many operators intervention control were done; automatically shutting down the reactor, electric supply immediately switched to the battery, then automatically DG were activated, after approximately 40 minutes from the main shock, a huge tsunami inundated the facilities and sea-water operated pumps located at the lower floor of the turbine building closer to the seashore. Finally the plant became in the state of SBO (Station-Black-Out), which was the direct cause of the following hydrogen explosion. From this observation of the accident, the physical state of all plants at Fukushima daiichi site had been transitioned very quickly in time. For each time instant, the most appropriate action to be taken were not the same to prevent the worst scenario o the NPP. In other words, the risk itself possesses time-dependent nature, involving human actions and non-static hazard.

From the above-mentioned feature of the Fukushima accident, new concept extended from the risk concept such as simultaneous failures, i.e., common cause failure and temporal evolution of failure, equivalently, time-dependent risk evolution are needed. It can be claimed that modern engineering systems possess multiple functions rather than a single function, their system configuration are no more a single element constituent than complex systems, and their systems are not independent but mutually dependent and inter-related systems. Namely, a very complex system assembled or integrated by many dependent subsystems.

Safety burst

Consequently, safety of such modern systems should be evaluated in much more integrated and multi-disciplinary approach, which does not seem to be the one in the past. To incorporate the above into the engineering activities, the following new concept has been named by Dr. Shibata and been proposed as "concept of safety burst" by the authors. "Safety burst", a quite new word, was clearly defined as in the following.

Safety burst indicates the physical state that after either a single failure of a part or simultaneous failures of portions of a huge, complex engineering system with possible large failure consequence is initiated, further damage is propagating and extending and finally the expected performance of the system becomes out of control.

The report shows some past examples: black out of North America in 2003, an accident of JCO in Tokai village in 1999, Fire of subway trains in Seoul in 2003, etc. All of accidents are related to huge modern engineering systems and human activities.

Figure 5 shows the new concept related to the safety burst, in which key words are shown in the two categories; chain-reaction type and simultaneous failure. The former is progressive failure of system, which can be understood by using "resilience" which originally means elasticity, vitality and capability of immediate recovery against external disturbance. By definition, the system should be

resilient. It means that even if the system is damaged, it is easy to recover, which is indeed the extension of risk concept into the one in time domain. The resilience may be related to dynamic risk management strategy, FT/ET analyses, all of which is implemented in a time domain.

The robustness, which is recently often used, describes how strong, insensitive, stable and stiff the system is. If we consider all wider regional infrastructure system including power plants as a huge complex system, simultaneous failures occurring in more than two places drastically reduce the preventive measure against common disturbances such as earthquakes or tsunami like natural hazards. Indeed, earthquakes can shakes very wide regions simultaneously. It is so called "common cause failure" used in engineering systems. The relevant concept is a fail-safe system, defense in depth, etc. This category is related to the risk in special domain.

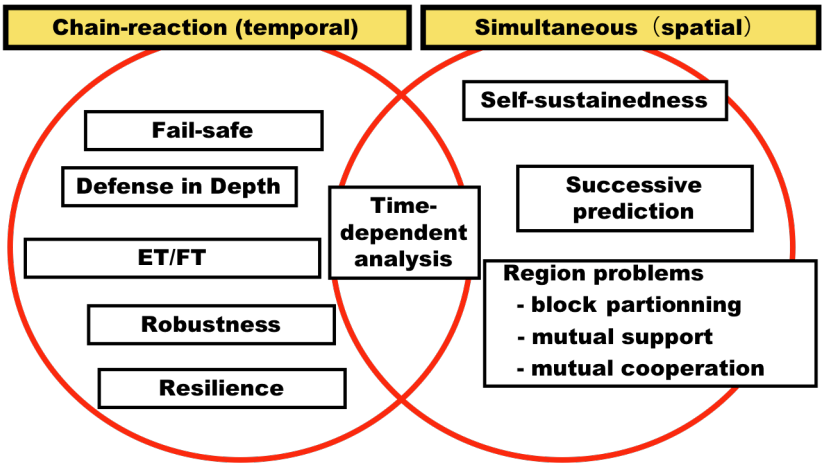

Figure 5 General layout of Fukushima Daiichi NPP (Takada, 2005)

CONCLUSIONS

The clearer paradigm shift that based on the risk concept, from the old engineering discipline that design to prevent any accidents to the new disciple that design and countermeasure based on the probability of having accidents. Furthermore, the result risk-oriented consideration can help to feed back the result of risk analyses to design, to ensure safety for operating plants. And further extension of the risk concept, robustness and resilience are stressed. The former is related to the risk in space, while the latter is the risk in time. This concept is necessary for modern engineering systems such as NPP's, which are typically multi-functional, mutually dependent complex systems.

REFERENCES

ADEP web page, Acceleration observed taken from ADEP web page, 2011

ERI, Location of Aftershocks taken from ERI Web page of the University of Tokyo, 2011

Joint Investigation group of the Tohoku earthquake and Tsunami, 2011

Takada, T., What Engineering should be after the Unprecedented Disaster, WG for Emergency Engineering Vision, Scholl of Engineering, University of Tokyo, 2011

Nuclear Safety Commission of Japan (2006) Revision of Regulatory Guide for Reviewing Seismic Design of Nuclear Power Reactor Facilities, NSC 2006-59

ISO/IEC Guide 73: Risk management-Vocabulary- Guidelines for use in standards, 2002

Takada, T., "Safety Burst", WG report, EAJ Information No.121, March, 2005