Challenges for Nuclear Safety from the Viewpoint of Natural Hazard Risk Management

Tatsuya Itoi and Naoto Sekimura

Abstract Lessons learned from the Fukushima Daiichi NPP accident and challenges for enhancement of the concept of nuclear safety are summarized from the viewpoint of risk management as well as the concept of defense in depth, for the protection against natural hazards, i.e., design against natural hazards and emergency response combined with regional disaster prevention and mitigation. The concept of resilience is also discussed, as a means for refining the fundamental concept of nuclear safety.

Keywords Fukushima Daiichi NPP accident · Earthquake · Tsunami · Nuclear safety

1 Introduction

It is well understood among the public as well as engineers that the use of nuclear energy involves potential risk associated with accidents. This is clearly recognized by experiences in which the potential risk has become obvious, e.g., during the Fukushima Daiichi NPP accident. Analysis of the experiences before, during, and after the accident is considered essential to discuss the safety of nuclear power in the future. In this chapter, future challenges addressed by several reports on the Fukushima Daiichi NPP accident are summarized from the viewpoint of natural hazard risk management. It is also discussed that the fundamental concept of nuclear safety, i.e. defense in depth, can be enhanced by introducing the concept of risk as well as resilience.

T. Itoi (✉) · N. Sekimura
The University of Tokyo, Tokyo, Japan
e-mail: itoi@n.t.u-tokyo.ac.jp

N. Sekimura
e-mail: sekimura@n.t.u-tokyo.ac.jp

J. Ahn et al. (eds.), *Resilience: A New Paradigm of Nuclear Safety*,
DOI 10.1007/978-3-319-58768-4_6

2 The Great East Japan Earthquake Disaster and the Fukushima Daiichi NPP Accident

The 2011 Tohoku earthquake and tsunami caused 19,335 deaths and 2,600 people are still missing [1]. Spatially distributed damage is also the characteristic of the earthquake and tsunami. Almost a hundred thousand people were forced to evacuate as a result of the Fukushima Daiichi NPP accident, whereas almost 300,000 people in total were evacuated in the aftermath of the earthquake and tsunami. In terms of fatalities, a number of people died related to the Fukushima Daiichi NPP accident, e.g., two plant workers due to tsunami, and more than 20 hospital patients during and after evacuation, though no people died because of radiation effects due to the release of radioactive material. Large negative impacts to society have also been caused by the nuclear accident as well as by the earthquake and tsunami. Some have pointed out that the evacuation orders following the nuclear accident prevented rescue activities for people under collapsed houses in the areas surrounding the Fukushima Daiichi and Daini NPPs, which may have caused more fatalities.

3 Challenges Identified in Light of the Fukushima Daiichi NPP Accident

Risk management is a process that consists of identification, analysis, evaluation, treatment, and monitoring of risk. If risk is evaluated to be high, it has to be reduced by introducing a countermeasure to be retained. A contingency plan is also needed to prepare for the retained risk, if it should be realized. Risk analysis can be effectively used only if it is organically integrated into a risk management process. In our society, however, risk analysis of nuclear power plants, i.e., estimation of the probability that an accident will occur, tends to be used only to judge whether the risk is acceptable or not. Afterwards, simply speaking, nuclear plant operators together with regulators may fail to prepare a contingency plan in the case when the risk becomes obvious, and may also fail to implement an effective mechanism to continuously manage risk.

3.1 Risks of Nuclear Power Plant Accidents

Conventionally, risk R has been defined as the mean value of the possible adverse consequences, i.e., consequence times its frequency, as follows:

$$R = \sum_i C_i P_i \tag{1}$$

where, C_i is the consequence and P_i is the probability of occurrence of C_i for the i-th scenario. This definition of risk, however, represents only one aspect of risk, which is complex in nature.

It is described in ISO 31000 [2] that organizations face internal or external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is defined as "risk." The objective of nuclear safety is to protect people, individually and collectively, as well as the environment from the harmful effects of ionizing radiations [3]. Therefore, the risks of nuclear power plant accidents are the effect of uncertainty in the various predecessors of accidents, e.g., earthquakes, fires, flooding and human errors, etc., on the objective of nuclear safety.

Analysis of risk is to attempt to envision what will happen if a certain course of action, including inaction, is taken [4]. Therefore, risk is defined as an answer to the following questions [4]:

- What can go wrong? (Scenario)
- How likely is it? (Likelihood)
- What might its consequences be? (Consequence)

The importance of the scenario, in addition to the consequence and the likelihood (or frequency), is more emphasized in this definition to describe the characteristics of risk. It is also emphasized that the risk information should include information about what is within/out of scope and how uncertain the result of the risk assessment is. The consequences that are assessed by risk assessment are not limited to fatalities due to radiation exposure, but include other consequences related to quality of life, e.g., environmental damage. It should also be noted that the actual fatalities related to nuclear power plant accidents are not always limited to radiation effects but may include other factors as discussed above, which should be included in the scope of the risk assessment of nuclear power plants.

3.2 Risk-Informed Decision Making

The purpose of probabilistic risk assessment is not limited to discussions whether a certain nuclear power plant is safe enough based on the estimated value of accident occurrence probability. We can also identify the weak points of the plant and contribute to an improved quality of decision making related to the introduction of safety-enhancement measures. Examples of required decision-making qualities are reasonability, accountability, openness, and transparency.

On the other hand, assessment of the risk due to external factors, e.g., earthquakes, fires, flooding, and aircraft impact, is hampered by an inherently large uncertainty. Therefore, an integrated framework to deal with these kinds of risks, i.e. a decision-making process under large uncertainty [5], is essential to ensure the safety of nuclear power plants now and in the future. Key elements for the

integrated decision-making process include deterministic consideration, e.g., defense in depth, good practices, operating experiences, and organizational considerations [5], some of which are discussed briefly below.

Uncertainty due to lack of knowledge, e.g. uncertainty related to modeling or insufficient amount of data, is called "epistemic uncertainty", which is distinguished from inherent randomness, i.e. aleatory uncertainty. Appropriate methodologies to analyze risk depend on the magnitude of epistemic uncertainty. Epistemic uncertainty is related to the amount of knowledge about accident scenarios and their consequences as well as their probability.

It has been discussed, e.g. by Stirling [6], that decision makers who receive the results of risk assessment as well as engineers who provide the results of risk assessment have a tendency to simplify and trivialize the characteristics of risk so as to make them easier to analyze and evaluate. However, when considering the basic purpose of risk analysis, i.e. to contribute to rational decision making, the result of such simplified risk assessment may be one of reasons that the decision is wrongly distorted. To avoid this distortion, it is recommended to use various methodologies in addition to probabilistic risk analysis, e.g., sensitivity analysis, deliberation among experts, and enhancement of diversity as well as resilience capacity, to tackle the entire range of risk including ignorance.

3.3 Defense in Depth

"Defense in depth" is an approach to designing and operating nuclear facilities that prevents the occurrence and mitigates the consequences of accidents. The approach consists of multiple levels of defense to compensate for potential failures [7]. Table 1 shows the objectives and essential means for each of five levels of defense defined by IAEA INSAG [8]. Defense in depth is considered to be the fundamental concept to achieve nuclear safety under uncertainty, especially for installation of nuclear power plants, and is regarded still important after the Fukushima Daiichi NPP accident. Meanwhile, it is sometimes said that the Fukushima Daiichi NPP accident, which occurred due to a severe natural event, is a challenge to the defense in depth concept. It was conventionally considered that natural hazard risks can be avoided through appropriate siting criteria and conservative design, i.e. up to the first level of defense in depth, without much consideration of higher levels of defense in depth, though it is discussed in IAEA INSAG-25 that the concept of defense in depth includes consideration of external hazards. A typical example is that the accident management introduced at NPPs in Japan was prepared mainly for accidents from internal event, i.e., random failure of components, and consideration of external events in case of accident management was not discussed before the Fukushima Daiichi NPP accident. It can be said that there was no effective mechanism to evaluate and reduce the risk from both internal and external events continuously in Japan.

Table 1 Objectives and essential means of defense in depth (IAEA, 1996)

Level of defense in depth	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

It is natural and reasonable, even if the Fukushima Daiichi NPP accident had not occurred, that external events including natural events should be considered among the main factors for nuclear power plant accidents. In case of natural events, e.g., earthquakes and tsunamis, simultaneous occurrence of damage to many structures, systems and components, both on-site and off-site, must be considered to prepare for accident management and for off-site emergency response to the conditions that are most likely to occur. Probabilistic risk assessment is considered one of the effective approaches for estimating reasonable and realistic plant conditions.

The fourth and fifth levels of defense in depth are the on-site and off-site response, respectively, to mitigate the impact of the accident. Though these measures are not hardware-oriented but management-based, it should be assumed that structures, systems, and components, e.g., mobile equipment for accident management or access routes to a nuclear power plant from off-site, related to the fourth and fifth levels of defense in depth, may become unavailable due to prior damage to these components related to the second and third levels of defense in depth. This is because usually the on-site and off-site facilities other than the reactor building are designed to resist natural events at a smaller scale than the reactor itself; this is discussed in the following section. Accident management and emergency response plans should be prepared to be effective under these kinds of severe conditions.

3.4 Design Against External Hazards Such as Earthquakes

Hardware design of nuclear power plants plays a central role in their systems safety. Major direct factors of the Fukushima Daiichi NPP accident are considered to be

lack of preparation for beyond-design events as well as underestimation of design tsunami height, i.e., both lack of contingency planning and deficiency in design. The former issue is related to the importance of identification and resolution of the "cliff edge effect."

There are two background factors that led to the underestimation of design tsunami height. One is an insufficient understanding of the importance of following the most up-to-date scientific knowledge, where paradigms occasionally shift dramatically, as our knowledge of natural hazards is expanded; the other is an over-insistence on valid historical evidence to take preventive action. Design earthquake ground motion and tsunami are evaluated for supposed active faults and subduction zone earthquakes. For subduction zone earthquakes, the supposed earthquake characteristics are determined based on the historical records for only several hundreds of years, while geological data over a longer period of time can be available for active faults.

Table 2 shows a reference probability level of design ground motions for different categories of structure, such as NPP and ordinal civil structure. For the earthquake resistant design of NPP, an earthquake that has not been experienced in history has to be assumed in some cases, because the reference probability level for NPP design is quite small, one-tenth of that for ordinary civil structures and sometimes smaller than that for disaster preparation for a nation.

It may also be added that nuclear power plant design against external events such as earthquakes tends to focus on prevention of component failure. From the viewpoint of implementation of defense in depth, however, the concept of systems

Table 2 Examples of reference probability level for earthquake-resistant design

		Annual probability of exceedance	Cf. Exceedance probability in 50 years (%)
Design ground motion of NPP	Level 1	10^{-2} (mean) (IAEA)	40 (mean) (IAEA)
	Level 2	10^{-4}–10^{-3} (mean) (IAEA) 10^{-5}–10^{-4} (median) (IAEA)	0.5–5 (mean) (IAEA) 0.05–0.5 (median) (IAEA)
Design ground motion for ordinal civil structure	Service ability limit state	1/500-1/25 (AS/NZ) 1/50-1/20 (Japan)	5–86 (AS/NZ) 63–92 (Japan)
	Ultimate limit state	1/2500 (US) 1/2500-1/250 (AS/NZ) 1/500-1/1000 (Japan)	2 (US) 2–20 (AS/NZ) 5–10 (Japan)
Cf. Regional disaster prevention & mitigation		$<10^{-3}$ (Japan)	<5 (Japan)

design, i.e. performance-based design, related to the second and third levels of defense in depth should be more emphasized, to control abnormal operations or accidents effectively when external events occur.

3.5 Accident Management

Provisions for management of severe accidents are required for the fourth level of defense in depth. For nuclear power plants in Japan, accident management was planned and introduced as a countermeasure for severe accidents around 2000 by operators as voluntary basis without regulatory requirements. Reports on probabilistic risk assessment for internal events were published in 2002 to confirm the effectiveness of introducing severe accident countermeasures. However, it has been recognized among experts that the main source of risk is not from internal events but from external events such as earthquakes. Therefore, a standardized method was prepared and published as AESJ (Atomic Energy Society of Japan) standard for seismic risk assessment by 2007. Risk assessment due to natural hazards, i.e. individual plant examination for external events, was not published for each specific plant in Japan before the Fukushima Daiichi NPP accident in 2011. Accident management was not yet reinforced to suppose natural hazards by continuous efforts.

3.6 Regional Disaster Prevention/Mitigation

It is of significant concern for the public whether they can survive, e.g. by successfully evacuating in case of a nuclear accident. For this purpose, we need to provide information on the likelihood, timing, and possible amount of radioactive material released for possible accidents. Because all units may suffer from identical external events, multi-unit risk assessment is necessary considering the disturbance of on-site and off-site activities related to mitigate the consequences of the accident, as was observed in the hydrogen explosion in the Fukushima Daiichi accident.

Considering off-site emergency response, it is critically important that we recognize that off-site facilities may suffer damage from a nuclear accident due to natural events occurring simultaneously. There are many kinds of possible interactions. A first point of consideration is the difficulty for local residents to evacuate and also the difficulty for external organizations to provide support to the nuclear site, due to the spatial distribution of damage to the infrastructure (see the examples of damages for surface transportation around the Fukushima Daiichi NPP shown in Figs. 1 and 2) and other factors. A second point of consideration is that the rescue activity for people affected by the severe natural event may be disturbed because of the forced evacuation due to nuclear accident, such as when a rescue team is forced to leave the site. Additionally, people are discouraged from multiple damages repeatedly by the natural event as well as by the nuclear accident.

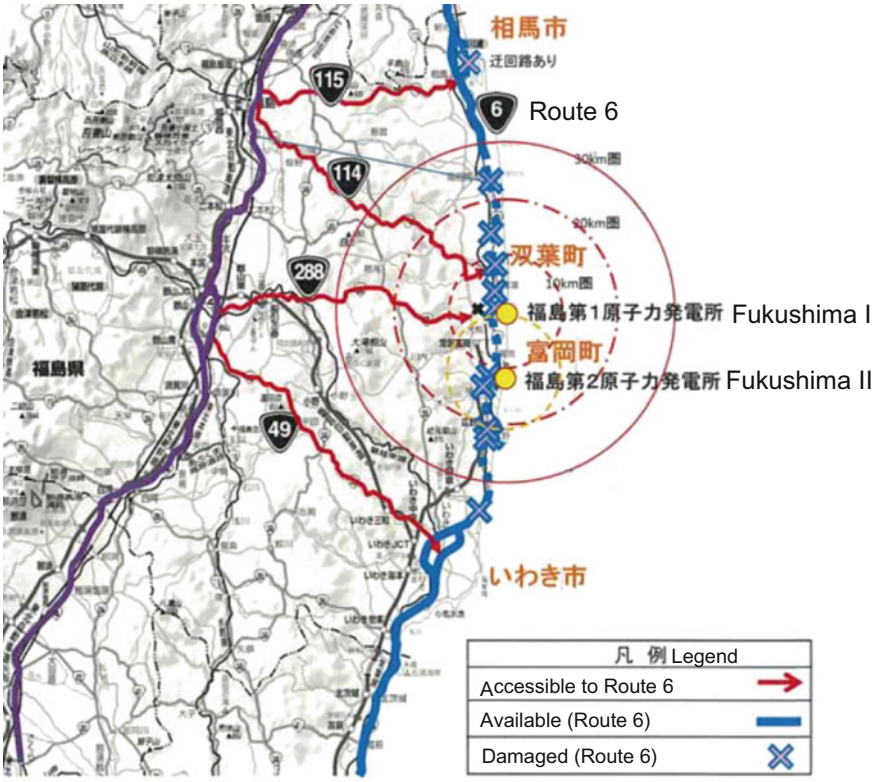

Fig. 1 Location of damage along Route 6. http://www.thr.mlit.go.jp/road/jisinkannrenjouhou_110311/dourohisaijyoukyou.pdf

Fig. 2 Collapse of road surface due to ground motion (Route 6). http://www.thr.mlit.go.jp/road/jisinkannrenjouhou_110311/dourohisaijyoukyou.pdf

4 Resilience in the Field of Nuclear Safety Engineering

The term "resilience" is understood among nuclear engineers as a concept for enhancing nuclear safety. It is, however, used to describe a wide range of perspectives. Consensus is required about the meaning and the role of the term in the field of nuclear safety engineering. In this chapter, the role of resilience is discussed from the viewpoint of enhancing nuclear safety.

The concept of resilience is considered important when dealing with risk under large uncertainty as discussed above. The concept of resilience is not introduced when risk is simply regarded as the possibility that something untoward may happen, but when it is regarded as something whose occurrence is rare but inevitable, to be managed when it in fact does occur. In such case, the importance of understanding the characteristics of the scenario when the risk becomes obvious is more emphasized, including the temporal sequence. Conventionally, as discussed heretofore, defense in depth is fundamental to nuclear safety, and was gradually refined to include lessons learned from the Three Mile Island accident as well as the Chernobyl accident. Resilience is considered to be a concept that can further refine and enhance the concept of defense in depth.

4.1 Resilience Engineering for Possible Future Nuclear Accident

Resilience can be defined as the ability to prepare for and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events [10]. In this sense, resilience is a concept that is relevant in the context of emergencies, such as nuclear accidents. Figure 3 schematically shows the accident sequence with respect to time, from occurrence to conclusion of nuclear accidents, all of which are in the scope of resilience engineering. The vertical axis of the figure shows the function, i.e. malfunction of barrier in each level of defense in depth, while the horizontal axis represents time. The temporal sequence to deal with abnormal and accidental conditions until recovery, e.g., accident management, off-site emergency response, decontamination and decommissioning, is illustrated in the figure.

To protect both the public and the workers, defense in depth is a widely accepted approach combining both prevention of incidents and accidents, and mitigation of their consequences, as discussed above. The safety barriers and procedures installed based on the concept of defense in depth are to prepare for, mitigate and respond to the accident, which are within the scope of resilience engineering.

In other words, from the viewpoint of nuclear safety engineering, resilience is a concept that expands the concept of defense in depth by enlarging the scope of nuclear safety engineering from only preventing accidents and mitigating consequences to responding to and recovering from accidents in the medium and long term.

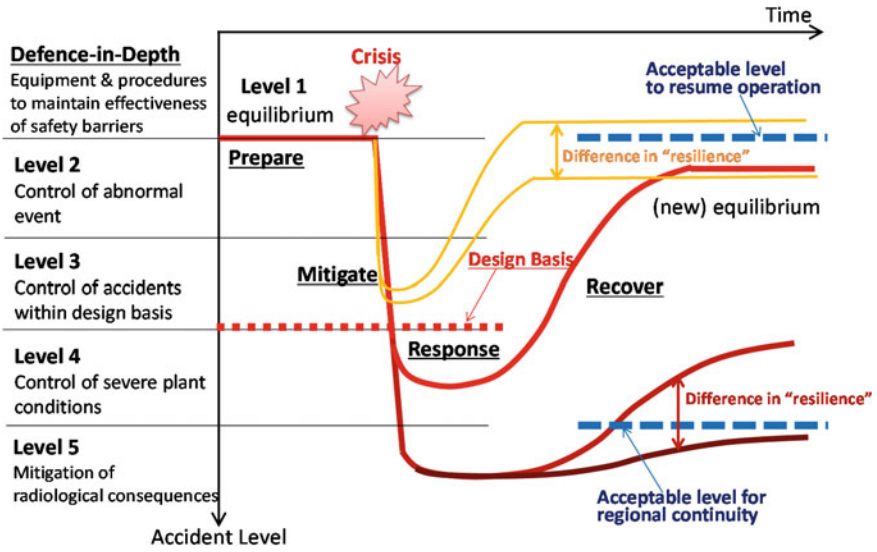

Fig. 3 Relationship between defense-in-depth and resilience from the viewpoint of nuclear safety engineering [11]

4.2 Resilience Engineering for Integrated Risk-Informed Decision-Making Process

It has been discussed that resilience is not restricted to a systems' response to crisis, but also includes adapting to slow and long-term changes. In other words, resilience can be defined also as the adaptive capacity of systems to maintain, through proactive maintenance, functions that deteriorate over time, the capacity of systems to evolve by remaking itself in order to adapt to existing and future environmental challenges, and the capacity of a system to become more robust by learning from past failures or from recent findings. In other words, maintenance science and technology should be effectively integrated into the decision-making process associated with continuous improvement of nuclear safety. This type of resilience is related to the first level of "defense in depth."

Hollnagel [13] suggests that the conventional safety perspective that defines safety as the condition where the number of adverse outcomes is as low as possible (i.e. safety-I) has some limitations, and a new safety perspective should also be emphasized, which defines safety as the condition where the number of intended outcomes is as high as possible (i.e. safety-II). This framework is considered to be important when the decision-making process with continuous improvement is discussed. Resilience engineering needs to include resilience for both safety-I and safety-II.

5 Summary

In this chapter, the challenges for nuclear safety with respect to natural hazard risk management were summarized from the viewpoint of a risk-informed framework, defense in depth, design, and regional disaster prevention/mitigation.

The application of the resilience concept to nuclear safety and maintenance science and technology was discussed. Resilience engineering is considered to be a discipline that broadly applies theories and technologies related to safety, which can especially refine and enhance the concept of defense in depth, the fundamental concept of nuclear safety. Roles of stakeholders (public, utilities, vendors, regulatory bodies, government, academia, etc.) need to be discussed in this context, to reconsider the conventional procedures for nuclear safety.

References

1. http://www.fdma.go.jp/bn/higaihou_new.html (in Japanese) Accessed 20 Sept 2015
2. International Organization for Standardization: ISO 31000:2009, Risk management—Principles and guidelines, (2009)
3. International Atomic Energy Agency: Fundamental Safety Principles, Safety Fundamentals, No.SF-1 (2006)
4. S. Kaplan, B.J. Garrick, On the quantitative definition of risk. Risk Anal. **1**(1), 11–27 (1981)
5. International Atomic Energy Agency: A Framework for an Integrated Risk Informed Decision Making Process, INSAG-25, A report by the International Nuclear Safety Group (2011)
6. A. Stirling, Keep it complex. Nature **468**, 1029–1031 (2010)
7. United States Nuclear Regulatory Commission, http://www.nrc.gov/reading-rm/basic-ref/glossary/defense-in-depth.html. Accessed 20 Sept 2015
8. International Atomic Energy Agency, Defence in Depth in Nuclear Safety, INSAG-10, A report by the international safety advisory group (1996)
9. Joint Editorial Committee for the Report on the Great East Japan Earthquake Disaster, Report on the Great East Japan Earthquake Disaster Nuclear Engineering Volume (in Japanese with English abstract) (2015)
10. The National Academies: Disaster Resilience: A National Imperative (2001)
11. N. Sekimura, H. Miyano, T. Itoi, Resilience Engineering: New Discipline for Enhancement of Nuclear Safety, Proceedings of ICMST-Kobe 2014 (2014)
12. Committee on Increasing National Resilience to Hazards and Disasters; Committee on Science, Engineering, and Public Policy; The National Academies: Disaster Resilience: A National Imperative (2012)
13. E. Hollnagel, *Safety-I and Safety-II The Past and Future of Safety Management* (Ashgate, 2014)