How the Fukushima Daiichi Accident Changed (or not) the Nuclear Safety Fundamentals?

Kazuo Furuta and Taro Kanno

Abstract In this chapter, the fundamentals of nuclear safety that the Fukushima Daiichi accident did and did not change will be discussed. While the most basic strategy of defense-in-depth principle is still valid, some problems have emerged after Fukushima, preparedness for all-hazards and multiple disasters, and importance of the administration of emergency response. From this observation, enhancing the resilience of nuclear systems is a critical issue after Fukushima. The safety enhancement measures considered in nuclear facilities will be reviewed referring to the elementary characteristics of systems resilience, and a new framework will be proposed for dealing with unsafe events, where unsafe events are classified into three categories.

Keywords Defense-in-depth · Residual risk · Beyond design-basis · Resilience · Category 2 events

1 Introduction

After the Great East Japan Earthquake (*Tohoku Earthquake*) and the Fukushima Daiichi accident (*Fukushima*), people used a word "unanticipated" for describing the disaster. It is true that the up-to-date seismology at the time of disaster could not foresee that such a huge earthquake and tsunami can ever occur in the area, and the main cause of the accident was insufficient preparedness of the plants against tsunamis [1]. It seems an improper remedial action, however, just reevaluating the risk of tsunamis more precisely and increasing the height of seawalls. It seems wrong also to think that the fundamentals of nuclear safety has broken down and it should be replaced with another one. Having reviewed the experiences of the

K. Furuta (✉) · T. Kanno
School of Engineering, The University of Tokyo, Tokyo, Japan
e-mail: furuta@rerc.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_3

disaster, what we have to do is rather renovating the basic strategy of nuclear safety, defense-in-depth principle, from a viewpoint of systems resilience.

2 What Did not Change After Fukushima

After Fukushima, many people including the press condemned that the myth of nuclear safety was over and the thoughts of experts were totally wrong. The accident, however, has shown clearly that the most basic strategy of defense-in-depth principle is still valid, because the accident was caused exactly from the lack of defense-in-depth. The single safety barrier that had protected the Fukushima Daiichi plants against tsunamis was the seawalls. Since the largest scale of tsunamis that may possibly occur in the area is uncertain, multiple barriers should have been implemented for protecting the plants against tsunamis. In this situation, the tsunami caused by Tohoku Earthquake that exceeded the design basis was fatal.

In addition to the seawalls of an insufficient height, the areas of safety-relevant equipment in the plants were not watertight. The emergency power supply such as metal clad switchboards as well as diesel generators were located under the ground level. All these equipment were therefore submerged and lost functions just after the tsunami hit the plants. The backup systems against station blackout were insufficient, either, both in the emergency power supply and the means of water injection.

Safety barriers were not well prepared for mitigation of the consequence of an accident. Before the JCO criticality accident (JCO) [2], which occurred in 1999, emergency response that requires evacuation of nearby residents had been a taboo in Japanese nuclear development. As an aftermath of JCO, Act on Special Measures Concerning Nuclear Emergency Preparedness was enacted, and emergency response drills were enforced in each prefecture of major facility sites. It was revealed, however, in Fukushima that these efforts were totally ineffective, because the scale of accident was far beyond the prescribed scenarios of emergency response plans.

As described above, the disaster of Fukushima occurred, not because the very basis of nuclear safety was wrong, but because it was not implemented and maintained properly. Defense-in-depth is the most basic strategy of nuclear safety that had been established at an early stage of nuclear development, before sophisticated methods of risk-informed safety management were introduced. After Fukushima, some people claim that we should rely more on risk-informed methods for safety management and we should evaluate more precisely the risks of external hazards. It is necessary to do so, but only introducing more sophisticated risk-informed methods is not the final answer.

Figure 1 shows an overview of the safety management based on a probabilistic concept of risk, which is a combination of the scale and probability of damage. A certain risk limit can be chosen as the curve shown on the scale-probability plane in the figure. The region above this curve is called an unacceptable region, and that

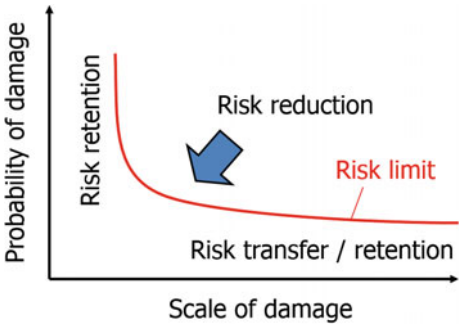

Fig. 1 Safety management based on a probabilistic concept of risk

below the curve an acceptable region. If the system status is located within the unacceptable region, one must make all efforts to reduce the risk. Safety management on a probabilistic concept of risk is actually more complicated. A tolerable region will be introduced often between the unacceptable and acceptable regions with an upper and lower risk limits. As low as reasonably practicable (ALARP) principle is applied in this region. In addition, the risk profile of a complex system cannot be treated with a risk limit presumed under the assumption of normal distribution, because it shows a long tail and rare events may occur more frequently than expected. Anyways, Fig. 1 shows the first-order approximation of the risk-based approach of safety management.

Even if the system status is located in the acceptable region, however, it does not mean that the risk has vanished. The risk that still remains after having satisfied the risk limit is called the residual risk. We also have to deal with the residual risk after having satisfied the risk limit. Occurrence of an unanticipated event often leads to further reduction of the risk limit and then to elevation of safety regulation, but this process is an endless loop. Management of the residual risk is performed by risk retention and risk transfer, which are often out of the scope of ordinary safety regulation, and the strategy of their application is to be established. In a social setting, risk transfer is performed usually by insurance, and risk retention by disaster preparedness, compensation of damage, and so on. The method of risk retention, however, for damage that exceeds the scale of commercial insurance is disputable.

Renovating deterministic approaches following the defense-in-depth principle will be a key. After Fukushima, the Nuclear Regulation Authority (NRA) of Japan enforced new regulatory standards for commercial power reactors in July 2013. The new standards request enhancement of design basis, protection against earthquakes and tsunamis, and new requirements for severe accidents. In order to fulfil the standards, Japanese utility companies are now taking remedial actions to their plants and installing various safety measures such as follows [3, 4], and these measures are in line with enhancement of defense-in-depth rather than introducing new principles.

Measures to Prevent Damages from Natural Disasters: The maximum seismic motion and height of tsunamis are reevaluated based on the up-to-date knowledge of seismology, and the hazards of active faults close to the plant site are reexamined. The seawalls are reconstructed and reinforcement structures are added to the plant components, if necessary. Countermeasures are also taken against other natural disasters such as tornados, volcanic eruptions, and external fires.

Installation of Watertight Structures and Countermeasures Against Internal Flooding: Watertight doors are installed to the reactor building. The structures of ventilation openings are redesigned to prevent water invasion. Countermeasures against internal flooding are also taken by installing pipe and cable penatration seals, water protection covers, weirs, and so on.

Reinforcement of Emergency Power Supply and Water Injection: Not only permanent but also mobile equipment are installed for emergency power supply and water injection considerig beyond-design-basis situations. The capacity of these equipment are designed with enough margins to compensate for maintenance outage and equipment failres. The storage locations and connection points for the mobile equipment are diversified. Water injection to the spent fuel pits is also reinforced.

Prevention of Reactor Containment Damage: Auxiliary containment spray systems are installed, which can be supplied by permanent and mobile water injection pumps. Water injection lines to the bottom of containment vessel are considered for cooling core debris. Filtered containment venting systems are installed to prevent damage of the containment vessel from overpressure. Measures to prevent hydrogen explosion are taken by monitoring, evacuation, and recombination of hydrogen gas.

Preventing Dispersion of Radioactivity: Measures to prevent hydrogen explosion in the reactor building are taken as well. Water cannon trucks are equipped for mitigating dispersion of radioactivity in case the containment vessel or the spent fuel pits are damaged. Pollution control screens are installed at the drainage canal exits.

3 What Changed After Fukushima

3.1 All-Hazards and Multiple Disasters

Though the basis of nuclear safety did not change even after Fukushima, some problems have emerged that caused the lack of defense-in-depth. We should learn lessons on these points and reflect them in taking concrete measures for safety enhancement.

Firstly, we must be concerned more about preparedness for all-hazards and multiple disasters than had been. The safety barriers against tsunamis were very fragile, because people in the nuclear industry were so concerned about seismic

motion that less attention was paid to the risk of tsunamis. Almost all of the equipment for emergency power supply and emergency water injection were located below the ground level, because the location is the best for protecting them from seismic motion. Such consideration, however, did harm for protecting them from tsunamis. We should have been more concerned about natural disasters other than seismic motion.

The backup systems against station blackout were insufficient, because the reliability of power grid is extremely high in Japan. The industry had made all efforts to maintain the reliability of power grid as high as possible, and they are too confident of it to think station blackout for a long period of time probable before Fukushima. The multiple disasters over a very wide area after Tohoku Earthquake easily denied such expectation and the external power supply from the grid became completely unavailable. Relying just on the quality of power grid is vulnerable in front of such multiple disasters.

Preparedness for all-hazards, unrestricted to natural disasters, is now a critical issue of nuclear safety in Japan after Fukushima. Aircraft crashes and terrorists' attacks should be considered also. Progress of these events may easily exceed the conventional event scenarios, and it is difficult to take preventive countermeasures to achieve prescribed design bases, in particular by installing some hardware equipment. It is therefore unsuitable to cover all these hazards by safety regulation. Meteorite strikes are out of the scope of design bases at present, but some response scenario should be imagined as an unforced activity. What can we do if most of the plant staff are down due to pandemic? Such questions must be asked behind the nominal scene of regulation.

3.2 Administration of Emergency Response

Secondly, we should attend more to the administration of emergency response rather than preventive measures with hardware equipment. While no casualties from radiation exposure have been reported, many people died during or just after evacuation due to improper evacuation planning and operation in Fukushima.

An offsite center, which is expected to be the local headquarter of nuclear emergency response, was constructed in each area of major nuclear facility sites after JCO. But the offsite center in the Fukushima area did not function at all due to the blackout and a high radiation dose. The administrator failed to collect monitoring data of radiation dose and could not use SPEEDI (System for Prediction of Environmental Emergency Dose Information) for decision-making in evacuation planning, in particular for deciding which areas to be evacuated. It is because data necessary for operating SPEEDI could not be transferred from the Safety Parameter Display System (SPDS) at the plant site due to the loss of external power supply. The Nuclear Safety Technology Center, which is an organization under the regulatory body, calculated the likely atmospheric dispersion of radioactive materials using SPEEDI assuming a unit radioactivity release from the Fukushima site and

reported the results to relevant organizations. It was recognized afterwards that the calculation results were useful for evacuation planning, but none of the organizations used them due to improper information strategy by the government.

In addition, information sharing was so poor between different organizations such as TEPCO, the central government, Self-Defense Force, police, and the local governments, that evacuation planning and operation were carried out on an ad hoc basis. The most symbolic and miserable case of the consequence from the poor administration was 19 deaths in the evacuee patients from Futaba Hospital. Following the evacuation order, 209 patients who could walk on their own and almost all hospital staff left the hospital boarding five busses dispatched by the town on March 12, but some 130 patients of Futaba Hospital, 98 people staying at the related nursing home, two facility staff, and the hospital director stayed behind. Okuma Town, however, misjudged that the evacuation from the hospital was completed. Two days later, a squadron of the Ground Self-Defense Force Liaison transferred all 98 people from the nursing home and 34 patients from Futaba Hospital to Iwaki-Koyo High School. It took around 11 h due to confusion in deciding the facility to accept these evacuees, and 8 patients died meanwhile. Transfer of the patients remaining at Futaba Hospital delayed for the reported critical situation of the nuclear reactor as well as poor information sharing between the relavant organizations, and the operation was completed early morning on March 17. The delay resulted in additional deaths of 11 patients.

The disaster described above would have been avoided if we had elaborated the administration of emergency response considering accident scenarios that really match the crisis. Different from engineering design of hardware equipment, however, no systematic or technical design methods have been established for the administration of emergency response. Techniques for optimal planning or normative decision-making have been developed in Operations Research and applied to emergency response problems such as evacuation planning. Most of them do not work in ill-structured situations of emergency, because they rely on complete and accurate information to set up mathematical models and obtain solutions. In addition, the conventional mathematical methods cannot deal with organizational interactions, which play a very important role in emergency response as described so far.

Some new approaches of administration design therefore are expected such as agent-based organizational simulation or application of bio-inspired design of complex social systems. Kanno, Morimoto, and Furuta proposed agent-based organizational simulation for emergency response planning [5]. Figure 2 illustrates the proposed simulation architecture of organizational emergency response. The simulation model consists of many agents representing various organizations relevant to emergency response. The scenario manager is a controller, which provides messages on the progress of disaster to the agents following a particular scenario. The simulation system outputs logs of communications, actions and resource consumptions for each agent. One can evaluate the total performance of emergency response by analysing these logs. The time required for executing some task, for example, can be a measure of the effectiveness and efficiency of the task execution.

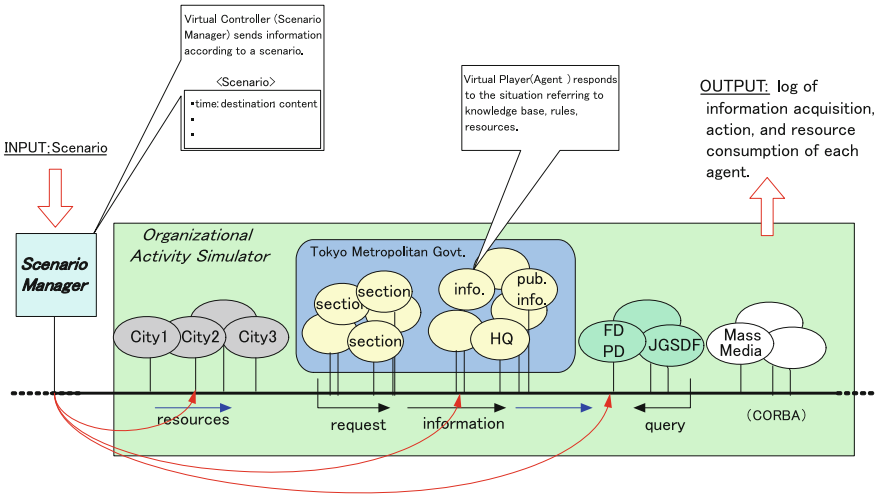

Fig. 2 Simulation architecture of organizational emergency response

Bottlenecks of the system in terms of the workload or information sharing can be identified as well by comparing the amount of executed tasks or processed information by each agent. Comaring simulation results by changing the action rules of agents and the disaster scenario will give us useful insights for rational emergency response planning.

4 Enhancing Resilience

Resilience, which is the ability of a system to absorb changes and to maintain its functionality, has attracted interests of experts in many areas after Tohoku Earthquake and Fukushima. While the conventional safety design of artifacts focuses just on the within design-basis region, resilience sheds light also on the beyond design-basis regions. Resilience of a system is often represented by the speed of recovery from a degraded state of system functionality after a crisis. It is, however, multifaceted features of a system, and Woods enumerated the following four essential characteristics of resilience [6]:

Buffering capacity — the size or kinds of disruptions the system can absorb or adapt to without a fundamental breakdown in performance or in the system's structure;

Flexibility — the system's ability to restructure itself in response to external changes or pressures;

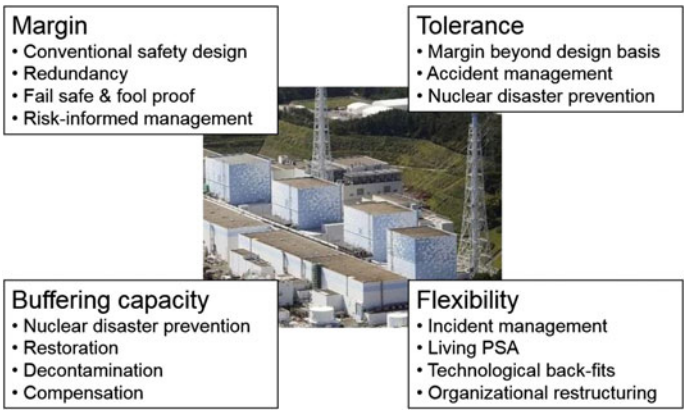

Fig. 3 Resilience enhancement measures in nuclear power plants

Margin	how closely or how precarious the system is currently operating relative to one or another kind of performance boundary;
Tolerance	how a system behaves near a boundary, whether the system gracefully degrades as stress/pressure increase, or collapses quickly when pressure exceeds adaptive capacity.

Following his proposal, Fig. 3 shows a summary of how the safety enhancement measures adopted in Nuclear Power Plants (NPPs) before and after *Fukushima* contribute to enhancing resilience. The conventional within design-basis approaches of safety design contribute to enhancing margin. Accident management is a typical enhancement measure of tolerance for beyond design-basis events. Nuclear disaster prevention appears at two places in this figure, tolerance and buffering capacity. The scale of disasters targeted in the two differs and they correspond respectively to the 4th and 5th level of defense-in-depth. Buffering capacity is related to the recovery process from damaged conditions after a disaster, while flexibility contributes to the improvement above the previous performance level by organizational learning and reengineering. The remedial actions undertaken by the utility companies for satisfying the new regulatory standards can be classified in the same manner.

5 Three Categories of Unsafe Events

Though the basic strategy of nuclear safety has not changed even after Fukushima, now we are requested to deal with a wider scope of events including beyond design-basis. This situation is described in Table 1, where unsafe events that occur in NPPs are classified into three categories.

Table 1 Three categories of unsafe events

	Category 1	Category 2	Category 3
Manifestation	Work accidents or single failures	Systemic or organizational accidents	Design basis events or anticipated incidents
Frequency	Relatively high	Extremely low	Very low
Scale of damage	Local and limited	Medium ∼ devastating	Devastating
Primary victims	Interested people	Interested people and/or third party	Interested people and/or third party
Complexity of scenarios	Simple	Complicated and non-linear	Complicated but linear
Variety of scenarios	Diverse but classifiable	Extremely diverse	Limited and finite
Quantitative risk assessment	Statistically possible	Impossible	Theoretically possible
Safety goal	ALARP[a]	ALARP[a]	Absolute risk limit
Countermeasures	Quality assurance and work management	Systems approach	Engineered safety features
Trade-off with economy	Compatible	Partly compatible	Conflicting
Status in nuclear industry	Already resolved	Unresolved	Already resolved

[a]*ALARA* As low as reasonably practicable

The author made the original version of this table shortly after JCO. Category 1 corresponds to unsafe events of relatively a high frequency and low consequence and they do not differ from work accidents in the ordinary industries. The risk of these events can be evaluated statistically and remedial actions are taken in ergonomics and work management. In contrast, Category 3 includes design basis events of a low frequency and high consequence, and they are unique to the nuclear industry. The countermeasures for this category are evaluating their risks theoretically and installing some engineered safety features. Category 2 is a new type of unsafe events that emerged in the past decades. This category includes complex events of systemic or organizational accidents, and they sometimes exceed the design bases.

A locus of interest will be the trade-off of safety measures with economy. Since NPPs are protected from Category 3 events with engineered safety features, most of which are out of service during the normal operation, their enhancement conflicts with the plant economy. In contrast, safety enhancement measures for Category 1 events often contribute also to the improvement of efficiency and productivity of works, and they can be compatible with the plant economy. It differs from the natural image that safety and economy are in a trade-off relationship. Those for Category 2 are located between the both, i.e., if safety enhancement measures using engineered safety features are necessary, the investments are costs. Otherwise, they

are sometimes compatible with the plant economy through the improvement in work efficiency.

When this table was created, a term of resilience was unknown among the community of nuclear safety, but now it has become clear that enhancement of resilience contributes to solving a problem how to prevent and mitigate Category 2 events. General principles as well as practical methods, however, to do so are not yet enough established, and resilience engineering should challenge to solve this issue.

6 Conclusions

The Fukushima Daiichi accident was caused mainly by the breach of defense-in-depth against tsunamis, which is the very basis of nuclear safety, and it is unnecessary to substitute it with a new concept. The accident rather showed that defense-in-depth is effective even in unanticipated emergency conditions of beyond design-basis, and the remedial actions now undertaken by the utility companies in Japan are in line with the principle. It must be taken into consideration, however, that the breach occurred due to insufficient preparedness for all-hazards and multiple disasters. The administration of emergency response rather than preventive measures by hardware equipment should be more concerned about than before. Enhancing the resilience and renovating the defense-in-depth of NPPs are crucial and Category 2 unsafe events will be the targets of these efforts.

References

1. Final Investigation Report, *Investigation committee on the accident at the Fukushima nuclear power stations* (2012) http://www.cas.go.jp/jp/seisaku/icanps/eng/final-report.html. Accessed 23 July 2012
2. K. Furuta, K. Sasou, R. Kubota, H. Ujita, Y. Shuto, E. Yagi, Human factor analysis of JCO criticality accident. Int. J. Cogn. Technol. Work **2**(4), 182–203 (2000)
3. S. Kanaida, N. Itou, A. Ueno, Y. Takabayashi, Strategy of installation of permanent and mobile equipment for countermeasures against severe accident at Tokai-2, in *Proceedings of ICMST-Kobe 2014*, Kobe, Japan, Japan Society of Maintenology, 2–5 November 2014
4. H. Uehara, T. Kawamoto, S. Kaneda, K. Ishikawa, K. Numata, Safety measures at Tomari nuclear plant, in *Proceedings of ICMST-Kobe 2014*, Kobe, Japan, Japan Society of Maintenology, 2–5 November 2014
5. T. Kanno, Y. Morimoto, K. Furuta, A distributed multi-agent simulation system of emergency response in disasters. Int. J. Risk Assess. Manag. **6**(4/5/6), 528–554 (2006)
6. D.D. Woods, in *Resilience Engineering: Concepts and Precepts*, ed. by E. Hollnagel, D.D. Woods, N. Leveson (Ashgate, Aldershot, UK, 2006), p. 21–34