Precepts of Resilience Engineering as Guidelines for Learning Lessons from the Fukushima-Daiichi Accident

Masaharu Kitamura[1, 2]
[1] Research Institute for Technology Management Strategy (TeMS) Ltd., 6-6-40-403, Aramaki-Aza-Aoba, Aoba-ku, Sendai, Japan
kitamura@temst.jp
[2] New Industry Creation Hatchery Center, Tohoku University, 6-6-10, Aramaki-Aza-Aoba, Aoba-ku, Sendai, Japan

Abstract. Applicability of the precepts of Resilience Engineering as guidelines to derive lessons from the severe accident at the Fukushima-Daiichi Nuclear Power Station is assessed in this article. Two reports published by official investigation committees have been mainly analyzed as data sources for fact-finding. Through the analysis, the four main capabilities proposed by Resilience Engineering, i.e. responding, monitoring, anticipating and learning, are found to be extremely useful and cost-effective in preventing or mitigating nuclear power plant accidents. In addition, a sensible response to warnings is found to be critically important to ensure accident preparedness. The derived lessons are well-organized and systematized so as to be applicable to the prevention of accidents resulting not only from tsunamis but other trigger events as well. The observations obtained through the present analysis clearly highlight the applicability and effectiveness of Resilience Engineering in accident analysis and learning activities.

1 INTRODUCTION

The disaster of Fukushima-Daiichi Nuclear Power Station (NPS) resulted in tremendous damage in Japan and caused serious concerns about nuclear safety throughout the world. Accident investigations have been conducted by a number of organizations to identify the causes of the Fukushima nuclear accident and to propose effective countermeasures to prevent future accidents. The reports published thus far cover a wide variety of findings related to the accident and corresponding recommendations.

Most investigations have been carried out based on a linear cause-and-effect approach, i.e., listing up adverse events experienced during the accident to identify the causes of each adverse event, with countermeasures then being recommended to eliminate the identified causes. A basic idea behind the cause-and-effect approach is that a high level of safety can be achieved by eliminating the causes of the accident. From a viewpoint of Resilience Engineering (Hollnagel, Woods, Leveson 2006; Hollnagel et al. 2011), the basic idea is equivalent to the traditional approach to safety, which is to pay attention to things that have gone wrong. Without doubt, the traditional approach has been widely employed in almost all investigations of the Fukushima-Daiichi accident.

It should be recognized, however, that the traditional approach tends to focus too much on the specific accident scenario experienced at the Fukushima-Daiichi NPS. As far as a huge tsunami is concerned, the recommendations might by quite sufficient (or possibly more than sufficient) to prevent another severe accident. But the triggering event of a future severe accident could be something other than a tsunami. A historical reflection of serious accidents in nuclear and non-nuclear industries indicates that every severe accident is unique as far as the identified cause-and-effect relationships are concerned. It is better to examine the specific accident scenario to derive generic lessons that can be applied to prevent or mitigate future accidents caused by a triggering event different from a tsunami. In addition, it would be worthwhile to reduce and organize the large number of various recommendations in order to obtain a systematic view of the recommendations. This paper describes an attempt to meet this need by applying the precepts of Resilience Engineering (Hollnagel, Woods and Leveson 2006; Hollnagel et al. 2011) to attain Safety-2 (Hollnagel 2013) rather than Safety-1.

2 TYPICAL RECOMMENDATIONS IN PREVIOUS REPORTS

Among various investigative groups, the Investigation Committee on the Accident at Fukushima Nuclear Power Stations of TEPCO (also called the Hatamura Committee), and The Fukushima Nuclear Accident Independent Investigation Commission founded by The National Diet of Japan, (also called the Kurokawa Commission) are regarded to be the most influential ones as they were founded by official organizations. Based on highly intensive field studies and interviews, these groups have published reports, which are herein called the Hatamura report (Hatamura 2012), and the Kurokawa report (Kurokawa 2012), respectively. The recommendations provided by the Hatamura report are listed below:

- Recommendations for a basic stance for safety measures and emergency preparedness
- Recommendations for safety measures regarding nuclear power generation
- Recommendations for nuclear emergency response systems
- Recommendation for damage prevention and mitigation

- Recommendations for harmonization with international practices
- Recommendation for relevant organizations
- Recommendations for continued investigation of accident causes and damages

The Kurokawa report provided a similar set of recommendations. It differs from the Hatamura report in that it places more emphasis on reforming regulatory bodies and laws related to nuclear safety. It should be noted that each recommendation in both of the reports consists of multiple sub-recommendations, and many of the sub-recommendations consist of multiple sub-sub-recommendations. Therefore, the number of corrective actions to be made is quite large. Actual implementation of the recommended measures would be extremely costly and time-consuming. As mentioned earlier, the purpose of these recommendations and measures is to eliminate each of the causes identified through the investigation of the accident. Within the framework of probabilistic risk assessment (PRA) (Kumamoto and Henry 1996), this approach to the elimination of the causes of the accident is practically equivalent to avoidance of occurrence of possible cut sets. An alternate approach, which is equivalent to the assurance of availability of path sets, is possible as well as reasonable. The applicability of the alternate, i.e., success-oriented, approach is examined in light of Resilience Engineering methodology.

3 GUIDELINES FOR LEARNING

The fundamental precepts proposed based on the framework of Resilience Engineering are briefly summarized below as guidelines for learning.

(1) Safety-2 is more appropriate than Safety-1 fin ensuring the safety of socio-technical systems such as a NPS.

(2) The four capabilities, i.e. responding, monitoring, anticipating and learning, are necessary for resilient systems.

(3) Preparation and allocation of proper resources are critically important for resilient systems.

(4) A constant sense of unease (Hollnagel 2006b) is necessary to maintain the resilience of systems.

(5) Warnings must be carefully examined and proper sacrifice judgments (Woods 2006) must be made as necessary.

Precepts (1) through (4) can be understood as guidelines naturally derived from the basic knowledge of Resilience Engineering. Guideline (5) could be less obvious. However, it is a natural lemma of guideline (4). It is a well-known empirical heuristics that warnings are usually available if cautiously monitored. Examples can be found in

the accident at Three Mile Island NPS (Leveson 1995; Kemeny 1979), and in well-known severe non-nuclear accidents such as the Titanic, Bhopal and Therac-25 (Leveson 1995). Although more precepts are available from the perspective of Resilience Engineering, the five precepts mentioned above are regarded to be the most important and basic ones.

4 APPLICATIONS

By applying the four guidelines to review of the accident, a set of observations has been derived as follows.

- Consideration of nuclear safety from the viewpoint of Safety-2 was practically absent. Since tremendous efforts had been spent on prevention of anomalies, which is equivalent to pursuing Safety-1, both Tokyo Electric Power Company (TEPCO) and The Nuclear and Industrial Safety Agency (NISA) were unaware of the importance of severe accident management as an essential component of defense-in-depth.
- Among the four capabilities, the learning capability was particularly insufficient. The impact of external events such as earthquakes and tsunamis on nuclear safety had been widely recognized from the viewpoint of PRA (Kumamoto and Henley 1996). In addition, threats of tsunami and flooding were experienced in foreign countries. On December 27, 1999, an unexpectedly strong flooded the Blayais NPS in France, resulting in water damage of pumps and containment safety systems. Also, on December 26, 2004, the Sumatra tsunami attacked the Madras NPS in India, resulting in an emergency shutdown due to tsunami-induced damage to the seawater pump. The chance of learning had been available, but disregarded because of complacency and ignorance of Safety-2.
- Other capabilities, i.e., monitoring, anticipating and responding, were obviously poor because the poor learning capability overwhelmed the organization and, as a natural consequence, no attention was given to maintaining and enhancing these capabilities, which are critically important in managing severe accidents.
- Preparation of resources was obviously insufficient. Though TEPCO personnel at the Fukushima-Daiichi site struggled very hard after the station blackout to obtain electricity and fresh water, they were not successful. They actually collected and utilized batteries from trucks and personal cars to measure critical safety parameters such as the water level in the reactor core and pressure in the containment vessel. Such a desperate effort evidently indicates poor preparedness for severe accidents.

- Responses to warnings were also very poor. It is now clear that TEPCO and the NISA had received several warnings from reliable sources concerning the

likelihood of the occurrence of a gigantic tsunami in Fukushima and adjacent prefectures. Nevertheless, the importance of such warnings was underestimated because of the misunderstanding that the probability of such a huge tsunami was practically negligible.

These observations can be transformed into lessons in a straightforward manner. For example, the first observation can be transformed into a lesson that greater attention must be paid to Safety-2 for upgrading the safety of NPSs. The second observation of insufficient learning capability can be simply transformed into a lesson that unusual events experienced in foreign countries and in Japan must be treated seriously. Other observations are also transformed into lessons without any difficulty. It should be recognized that the lessons derived from each of the observations are in essence related to ensuring certain success paths.

5 DISCUSSION

The observations mentioned above provide us with an organized set of lessons along with the guidelines from Resilience Engineering. Even a subset of the above-mentioned lessons can be sufficient to prevent the occurrence of a Fukushima-like nuclear disaster. In the official reports published in Japan, TEPCO personnel are criticized for not responding to the warnings because expected countermeasures such as a huge seawall, an extra high-performance diesel generator, etc. would have been too expensive. If TEPCO personnel had been aware of the importance of Safety-2 and of the precepts of Resilience Engineering, they might have tried to prepare some basic resources such as extra batteries and fire engines. Such resources are far less expensive than a huge seawall but would have been sufficient to significantly reduce the severity of the accident.

The author does not intend to criticize the official accident reports. Nor does he intend to claim advantages of the success-oriented lessons over other lessons and recommendations. Implementation of a large number of recommendations proposed by the official committees is definitely desirable for attaining an excellence of nuclear safety in Japan. The present approach has been conducted with the intention of providing an alternate practical way to achieve a higher level of safety in light of Resilience Engineering. As far as the widely acknowledged concept of Occam's razor (Rissanen 1978), also known as the law of parsimony (Akaike 1974), is concerned, out of two possible theories, the simpler is to be preferred from a scientific viewpoint. However, the exhaustive list of recommendations proposed by the investigation committees should be implemented in order to meet the public concerns (Kitamura 200).

Last but not least, consideration is given with the reference to the remarkable interpretation provided by K. Kurokawa, the chairman of the National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission. He stated; "What

must be admitted – very painfully- is that this was a disaster 'Made-in-Japan' Manmade accident". Then he continued that "Its fundamental causes are to be found in the ingrained convention of Japanese culture: our reflexive obedience; our reluctance to question authority; our devotion to 'sticking with the program'; our group-ism; and our insularity".

Japanese people would admit that the message from the chairman is to some extent valid. However, this interpretation can introduce significant side effects. One is the possibility of gradual neglect of the message in Japan. As the fundamental causes of the accident are so strongly attributed to Japanese culture, it is obvious that any attempt to eliminate the causes will demand tremendous efforts of various kinds. For any individuals and organizations, this would be too demanding, resulting in gradual neglect. Another is a possibility of neglect caused by the obstacle of distancing through differencing (Cook and Woods, 2006). If the fundamental cause of the accident is attributed to Japanese culture, people in other countries might feel that the cause is irrelevant to them. But such a view is absolutely wrong. The culture-oriented interpretation must be treated carefully by paying attention to commonalities rather than differences.

6 CONCLUDING REMARKS

The Fukushima-Daiichi accident must be studied in detail to prevent another severe accident. A large number of lessons leading to hardware/software improvements and organizational reforms must be seriously implemented. It is, however, certainly informative and desirable to look at the large number of improvements from different perspectives and try to restructure them in a systematic manner. The precepts of Resilience Engineering are highly effective to realizing this. It would be worthwhile to pursue improved safety of nuclear power plants and of other high-hazard processes as well on the basis of this recognition.

REFERENCES

Akaike, H. (1974). A new look at the statistical model identification. *IEEE Transactions on Automatic Control,* AC-19, 716-723.

Cook, R. I. and Woods, D. D.(2006), Distancing through differencing: An obstacle to organizational learning following accidents. In Hollnagel, Woods and Leveson (Ed.), *Resilience Engineering: Concepts and Precepts* (pp.329-338). Aldershot. UK: Ashgate Publishing.

Hatamura, Y. (Chairman) (2012). *The Final Report of Investigation Committee on the Accident at Fukushima Nuclear Power Stations of TEPCO*. Available at http://www.cas.go.jp/jp/seisaku/icanps/eng/final-report.html [accessed: 7 May 2013]

Hollnagel, E. (2006b). Epilogue. In Hollnagel, Woods and Leveson (Ed.), *Resilience Engineering: Concepts and Precepts* (pp.345-378). Aldershot. UK: Ashgate Publishing.

Hollnagel, E. (2013). A tale of two safeties. *International Electronic Journal of Nuclear Safety and Simulation*, vol.4. 1-9.

Hollnagel, E. , Woods, D. D. , Leveson, N. (2006). *Resilience Engineering: Concepts and Precepts*. Aldershot. UK: Ashgate Publishing.

Hollnagel, E., Paries, J, Woods, D.D., Wreathall, J. (2011). *Resilience Engineering in Practice, A Guidebook*. Aldershot. UK: Ashgate Publishing.

Kemeny, J. G. (Chairman) (1979), *Report of The President's Commission on the Accident at the Three Mile Island*, Available at http://www.threemileisland.org/downloads/188.pdf [accessed March 28, 2013]

Kitamura, M. (2009), The Mihama-2 accident from today's perspective, In E. Hollnagel (Ed.), *Safer Complex Industrial Environments* (pp.19-36). Boca Raton, FL: CRC Press. 19-36.

Kumamoto, H. and Henley, E.J. (1996). *Probabilistic Risk Assessment and Management for Engineers and Scientists*, Second Edition, IEEE Press.

Kurokawa, K. (Chairman) (2012), *The Official Report of The National Diet of Japan by Fukushima Nuclear Accident Independent Investigation Commission.* Available at http://warp.da.ndl.go.jp/info:ndljp/pid/3856371/naiic.go.jp/en/report/ [accessed April 3, 2013]

Leveson, N. (1995). *Safeware – System, Safety and Computers.* Addison-Wesley Publishing Co.

Rissanen, J. (1978). Modeling by shortest data description. *Automatica* 14 (5), 465–658

Woods, D.D. (2006). Essential characteristics of resilience. In Hollnagel, Woods and Leveson (Ed.), *Resilience Engineering: Concepts and Precepts* (pp.21-33). Aldershot. UK: Ashgate Publishing