Perspective to make nuclear power plants more resilient

GOFUKU Akio[1]

1. *Graduate School of Natural Science and Technology, Okayama University, 3-1-1 Tsushima-Naka, Kita-ku, Okayama 700-8530, Japan (fukuchan@sys.okayama-u.ac.jp)*

Abstract: By the impact of Fukushima Daiichi NPP (Nuclear Power Plant) accident, there are many critiques to nuclear power generation, especially in Japan. In order to respond the criticism, a great increase of the safety of NPPs is inevitable. Of course, extensive studies and developments have been conducted to increase the safety of NPPs. Almost all the studies and developments are to increase the resistance of an NPP according to the concept of defense in depth to prepare supposed abnormal events. However, it is impossible to suppose all situations and their combinations that may happen in the operation of an NPP. Therefore, a new approach should be developed and added to increase the safety of NPPs covering the hardware systems, staff organization, human-machine interfaces, operation procedures, and education and training of both operators and plant staffs. Recently, the concept of resilience engineering (RE) is becoming popular to prepare and respond an abnormal situation, especially in the fields of safety critical systems and health care. The concept does not exclude the previous approaches to increase the safety of a system but add a new viewpoint for system safety. The characteristic features of RE are expressed by the words of 'Safety II' and 'Work As Done' although researchers are dealing with the topics on how to apply RE in a real complex system and organization. This article first introduces resilient responsive actions of operators and plant staffs to protect a more catastrophic situation in the Fukushima Daiichi accident. Then, the concept of RE and its possibility to increase the safety of NPPs are introduced. The authors are now studying several works to develop techniques based on functional models to enable operators take resilient responsive actions in the operation of NPPs. They are an interface system to display useful information for operators in a computer-based procedure and a technique to generate plausible operation procedures in an accidental situation. The approach and current results of the latter work are also introduced.

Keyword: safety of nuclear power plants; resilience engineering; education and training

1 Introduction

As known well, in the Fukushima Daiichi accident, hydrogen explosion happened in Units 1 to 3 that were in full power operation before the happening of SBO (Station Black Out) by the serious tsunami. Then, they were seriously damaged and huge radioactive materials were released to the environment. In addition, fires happened in Unit 4 that had been in a shut down condition for maintenance due to the hydrogen that came from the stack of Unit 3.

As the lessons learned from the accident, the chairperson of the governmental investigation committee of the Fukushima Daiichi accident made his comments in the end of the final report of the investigation committee[1]:

1. Things that are possible happen. Things that are thought not possible also happen.
2. You cannot see things you do not wish to see. You can see what you wish to see.
3. Assume to the extent possible and make full preparations.
4. Creating a framework alone does not mean it will function. Frameworks can be constructed but goals not collectively shared.
5. Everything changes, respond flexibly to changes.
6. Acknowledge that risks exist, and create a culture able to debate the risks directly.
7. It is vital to be conscious of the importance of seeing with your own eyes, thinking with your own head, making decisions and taking action, and vital to cultivate such faculties.

The safety of nuclear power plants should be highly improved by considering these remarks. One of the basic and common approaches to ensure the safety of nuclear power plants is to follow the concept of defense in depth[2]. In the concept, there are five layers for 1) preventing the occurrences of anomalies and failures, 2) preventing the development to an

Received date: November 11, 2016
(Revised date: December 5, 2016)

"accident" of an anomaly and failure, 3) mitigating the affects of "accident", 4) taking measures to "accident that exceeds design criteria", and 5) taking measures to protect the public and the environment. Usually, the top three layers are emphasized.

For preventing an accident, abnormal events are first supposed as many as we can and to prepare the supposed events by developing and adding safety systems and necessary resources for counter measures, arranging a suitable organization, developing operation procedures for the events, introducing advanced technologies for human-machine interfaces, and improving education and training menus of operators and plant staffs.

However, it is impossible to suppose all situations and their combinations that may happen in the operation of an NPP (Nuclear Power Plant). In addition, from the lessons learned from Fukushima Daiichi accident, the layers 4 and 5 should be considered to improve the safety of nuclear power plants. This means that a new approach should be developed and added to increase the safety of NPPs covering the hardware systems, staff organization, human-machine interfaces, operation procedures, and education and training of operators and plant staffs.

2 Investigation of Fukushima Daiichi NPP accident from the viewpoints of human factors

2.1 Topics of investigation

In the Fukushima Daiichi accident, many faults and mistakes related with recognizing the situation in the plant, information sharing inside and/or outside the power station, decision making, education and training, instrumentation and control facilities, work environment, *etc.* were pointed out in various accident reports[1, 3, 4]. However, it is not enough only to criticize the faults and mistakes. Rather, we should learn from the accident as much as possible.

Under this motivation, the subcommittee of Human-Machine Systems Research of Atomic Energy Society of Japan established a subcommittee to investigate the problems related with human factors for the counter activities of the Fukushima Daiichi accident in order to have lessons. In the subcommittee, the investigation was made by referring various open documents, reports, data, and so on due to no authority to interview the staffs of the plant.

The topics of investigation are listed as follows:

1. grasping of plant conditions of Unit 1 and 2 by operators,
2. activities of plant staffs especially on recognizing operation condition of IC (Isolation Condenser) of Unit 1 and alternative injection of Unit 3,
3. problems in education and training of operators,
4. problems in communication and information sharing,
5. capability of accident management of organization, and
6. factors that obstruct counter activities in operation and field recovery actions.

In the following subsections, the topics of items 1, 3, and 6 are briefly introduced from the report of investigation[5].

2.2 Analysis of work conditions for operators

The environment around the plant was very bad for human activities. First, there happened aftershocks frequently. The aftershocks interrupted field activities for surveying the damage by the major shock of earthquake and caused uneasiness feeling to plant staffs. Second point is the continuation of big tsunami warning. This made difficulty and limiting the range of field activities. The third is the happening of SBO (Station Black Out). By the loss of all electricity, the lightning of MCR (Main Control Room) of Unit 1 and 2 was turned off and the methods to monitor and remotely control plant condition were lost. In addition, high radioactivity after around six hours from the happening of SBO by the partial core damage worsened the environment for human activities.

Figure 1 shows a summary of the happening time of aftershocks, condition of illumination of MCR, radioactivity level of MCR, and condition of sunshine in the time span for 4 hours from 14:30. At 14:46, the major shock of the earthquake happened at the plant. From this time chart, we can understand the deadly environment for human activities. In this time span, serious aftershocks at the level of the intensity scale of 4 and more happened for 23 times.

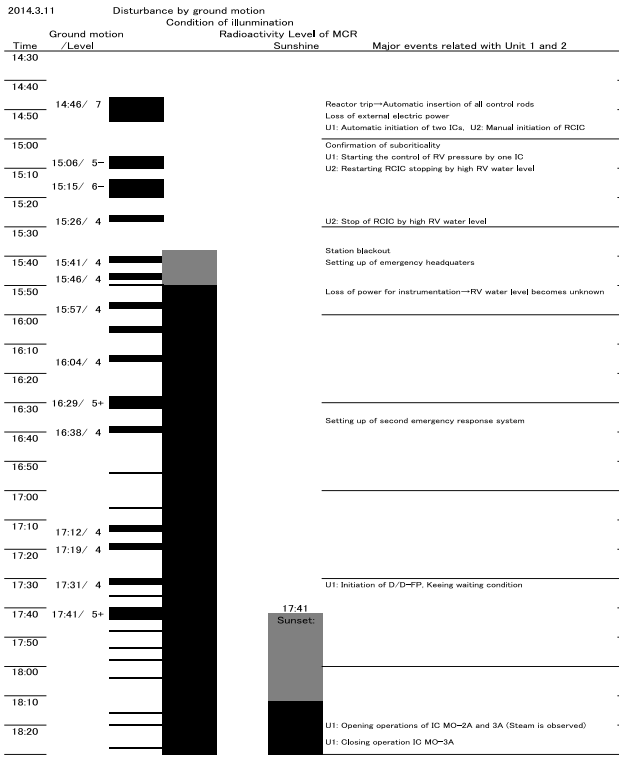

Fig. 1 Summary of work environment for operators.

In Japan, the shock level of earthquake is usually indicated using the JMA (Japan Meteorological Agency) intensity scale. The major shock is the intensity scale of 7. In this level of shock, wooden houses with low earthquake resistance are even more likely to lean or collapse. At the intensity scale of 4, most people are startled by the shock.

Although there was no suitable counter operation procedure and the conditions for recovery activities were bad, operators and plant staffs did their best using their knowledge and skill educated and trained. They recognized the necessity of alternative water injection in an early stage after SBO. They set up alternative water injection path using the piping inside buildings based on the experience of Kashiwazaki-Kariha NPP at the Chuetsu earthquake in 2004. They also found a recovery way of minimum electricity using a part of switchboard of Unit 2. In addition, they behaved in several creative ideas. Examples are using car batteries for instrumentation, serial connection of fire engines to obtain necessary head to inject sea water, and so on.

2.3 Operator training before the accident

The Japanese guideline of education and training of NPP operators before Fukushima Daiichi accident did not fully cover a long term SBO although a short term SBO is included in an accident to be considered. In fact, the guideline JEAG4802-2002[6] that specifies the education and training of nuclear power plant operators instructs a short term SBO as the accident to be considered and specifies the events of loss of power and loss of cooling functions as the malfunctions of training simulator.

2.4 Factors that obstruct counter activities

The factors that obstruct counter activities can be summarized as follows:

1) weak power source and service systems against tsunami resulting in loss of lightning of MCR and loss of monitoring and control system and SPDS (Safety Parameter Display System) functions of the anti-seismic building,
2) excessive dependence on remote control,
3) insufficient communication means for information sharing among MCR, emergency section, and head quarter of utility,
4) weakness of lightning and monitoring outside the buildings, and
5) insufficient tools to remove a heap of rubble by tsunami and/or hydrogen explosion.

3 Resilient activities in Fukushima Daiichi NPP accident

3.1 Resilient activities in the accident

In the serious accident of Fukushima Daiichi NPP, there were some resilient activities taken by operators and plant staffs. The factors why they could do should be analyzed and considered in the improvement of education and training of operators and plant staffs. Examples can be seen in the counter activities of 1) using car batteries to recover monitoring functions, 2) opening valves of fire fighting piping for injecting water into reactor vessel, 3) serial connection of fire engines to obtain necessary head of water for injecting sea water into reactor vessel, 4) drilling of venting hole of reactor building on the roofs of Units 5 and 6[7], and 5) emergent undocking of a tanker at the port in the site[7]. In the following, the examples 1 and 2 are briefly described.

The first one is using car batteries to recover monitoring functions. Operators carried out the difficult works to collect car batteries in the hard

working conditions of total darkness in MCR, under major tsunami warning, and a heap of rubble in the site. At 21:19 and 21:50 on March 11 after around 6 hours from the happening SBO, the water level of reactor vessel of Units 1 and 2 became to be intermittently monitored. The final recovery of electricity for measurement systems of Units 1 and 2 by a low-voltage power source car was at around 22:00 on March 12.

The second example of resilient activities is opening valves of fire fighting piping for injecting water into reactor vessel. Plant manager recognized the necessity of counter measures for a severe accident and instructed the investigation of injection by fire fighting piping and/or fire engines at 17:12 on March 11. Operators in MCR considered water injection into reactor vessel by the diesel driven fire fighting pumps in turbine building and made field works under the instruction of the head of operation crew. They finally ensured the injection line at 20:50 on March 11. The reactor core of Unit 1 could be finally cooled by water and sea water through the injection line to avoid a catastrophic situation of the unit.

3.2 Resilience engineering

In recent years, resilience engineering[8, 9] becomes popular in the fields of operating safety critical systems. The resilience engineering focuses on how humans respond to a thread flexibly and how humans recover the damaged system in a case of disturbance happening.

The resilience engineering points out two aspects that are not considered in the conventional safety engineering. The first aspect is the distinction between ‘safety I’ and ‘safety II’. The ‘safety I’ takes care not to happen an anomaly as the safety engineering do. On the other hand, the ‘safety II’ focuses on how things do well and try to learn ways to respond flexibly an anomaly from usual activities. The second aspect is to consider ‘work as done (WAD)’, that is, actual work instead of ‘work as imagined (WAI)’, that is, formal work.

The resilience engineering requires four abilities for a resilient system that is, anticipating, monitoring, responding, and learning. In order to evaluate the four abilities, a set of questionnaire called resilience ability grid (RAG) is proposed.

4 Making nuclear power plants more resilient

4.1 Approaches to make NPPs more resilient

There are several ways to make NPPs more resilient. One approach is the improvement of hardware by adding safety equipment, preparing mobile devices, and so on. The filter vent system, core catcher, and other additional hardware systems will contribute to make NPPs more fault tolerant.

Software tools to support the activities of plant staffs will be helpful for monitoring plant conditions, taking counter operations against unexpected events, supplying resources of counter measures, communicating among plant staffs, emergency response center, and head quarter of electric power company, and so on.

CBPs (Computer-Based Procedures) become to be introduced in future NPPs. There is an international standard, IEC62646[10], for designing CBP systems. The advantages of CBPs compared with PBPs are dynamic representation, navigational link, path tracking, supplementary information, and so on. However, there are several issues to be solved[11]: limited information displayed on the VDU, spending much time on a specific step, and tendency to skip procedure steps.

In addition, the improvement of education and training is important. The education and training should improve not only technical skill of operators and plant staffs but also non-technical skill of them. The non-technical skill means the one to do one’s best as a team member. In the field of aviation, the CRM (Crew Resource Management) training[12] is implemented for the training menus of flight crews to improve non-technical skill to respond an abnormal situation as a team. The introduction of the CRM training will improve the performance of operators and plant staffs as team members.

4.2 A technique to generate operation procedures

The authors are studying a technique[13, 14] to generate online candidates of operation procedures in order to

support operator activities in an unexpected plant situation. In this subsection, the technique is briefly introduced as a software system that will contribute to making NPPs more resilient.

The technique generates plausible counter operation procedure using functional information of plant components from the consideration that components have their own functions to contribute to the accomplishment of the goal/objective of a system, functions are realized in several components, and components may have behaviors that are not recognized as functions but can contribute to suppress the bad influence in an emergency plant situation. Multilevel Flow Modeling (MFM)[15-17] is used to construct a functional model. The MFM expresses the functional information of a target system as a graph. There are two kinds of node symbols. The symbols of objectives and threats are used to express the objectives of system components and threats. The functional primitives express the functions of system components. On the other hand, there are several arc symbols to connect node symbols and express their relations.

The necessary data and information to generate plausible counter operation procedure are summarized as follows:

1) a functional model, that is, MFM model as a base model,
2) inference propagation rules of MFM relations to infer the influence of an operation on the state of a functional symbol that expresses the condition of a component,
3) information of component states to map the influence of a trouble condition of component,
4) information of operations to find plausible operation that can change plant condition to a desirable one, and
5) re-describing rules of objective by changing viewpoint to search MFM objectives that have the same meaning of counter operation goal.

The flowchart to generate plausible counter operation procedures is shown in Fig. 2.

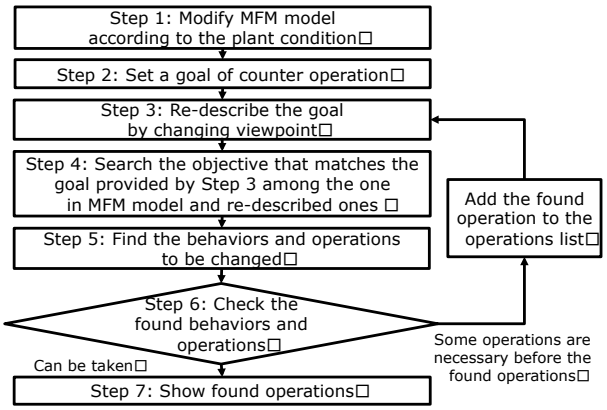

Fig. 2 Flowchart to generate plausible counter operation procedure.

The applicability of the technique was examined by the trials to derive counter operation procedures for a PWR plant. Three LOCA cases with failures of safety systems were considered. The applicability of the technique was confirmed because it derived some counter operation procedures including the operation procedures[18] called accident management prepared for a Japanese PWR plant.

4.3 Improvement of education and training

The authors have started a study to analyze the factors of education and training to cultivate the idea of resilient activities from the viewpoint of resilience engineering. Our research questions are

a) "what types of knowledge and skills can be obtained from usual activities ?" and
b) "what kinds of education and training are effective to cultivate such knowledge and skills ?".

The following approaches are considered:

Step 1: collection of resilient activities in accidental situations like Fukushima Daiichi NPP accident,
Step 2: relating knowledge and abilities to the resilient activities, and
Step 3: designing education and training menus to effectively obtain the knowledge and abilities.

6 Conclusions

In this article, the importance of considering human factors in the analysis of accidents is emphasized to make NPPs more resilient. It is important to develop computer support systems to support counter activities of operators in MCR and plant staffs. The improvement of education and training of operators and staffs in NPPs is also important to increase the

performance of counter actions as well as the improvement of hardware such as the capacity of components, component arrangement, and additional installation of components in order not to happen an accident and to mitigate the influence in the case of happening an abnormal event.

Acknowledgements

The author expresses his thanks for the members of Investigation Subcommittee of TEPCO Fukushima Daiichi NPP Accident established in the subcommittee of Human-Machine Systems Research of Atomic Energy Society of Japan for their sincere investigations and discussions.

References

[1] Investigation Committee on the Accident at Fukushima Nuclear Power Stations of Tokyo Electric Power Company, Final report, 2012.

[2] INSAG: Defense in depth in nuclear safety: INSAG-10, IAEA, 1996.

[3] INPO: Lessons learned from the nuclear accident at the Fukushima Daiichi nuclear power station, INPO-11-005 Addendum, 2012.

[4] IAEA: IAEA international fact finding expert mission of the Fukushima Dai-ichi NPP accident following the great East Japan earthquake and tsunami, IAEA Mission Report, 2011.

[5] Investigation Subcommittee of TEPCO Fukushima Daiichi Nuclear Power Plant Accident, Investigation of Fukushima Daiichi accident from the viewpoints of human factors, Subcommittee of Human-Machine Systems Research of Atomic Energy Society of Japan, 2015. (in Japanese)

[6] Nuclear Standards Committee of the Japan Electric Association, Guidelines of education and training of operators of nuclear power plants, JEAG4802-2002, 2002.

[7] YOSHIZAWA A., FURUHAMA H., OBA K., and KITAMURA M.: Improvement of organizational resilience based on Fukushima-Daiichi nuclear power plant accident - Analysis of structure for responding -, Proc. 2014 Annual Meeting of the Japan Society of Mechanical Engineers, 2014: Paper No. G2010102. (in Japanese)

[8] HOLLNAGEL, E., WOODS, D. D., and LEVENSON, N.: Resilience engineering: Concepts and percepts, Ashgate Publishing Ltd., 2006.

[9] HOLLNAGEL, E., PARIES, J., WOODS, D. D., and WREATHALL, J.: Resilience engineering in practice: A guidebook, Ashgate Publishing Ltd., 2011.

[10] IEC, Nuclear power plants - control rooms - computer based procedures, IEC 62646, 2012.

[11] SURYONO, T. J., and GOFUKU, A.: The desirable features of computer based emergency operating procedure for nuclear power operation, Proc. the 13th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Human-Machine Systems, 2016: Paper No. ThuE4-03.

[12] JENSEN R. S.: Pilot Judgment and Crew Resource Management 1995 Ashgate Publishing Ltd., 1995.

[13] INOUE, T., GOFUKU, A., and SUGIHARA, T.: A technique to generate plausible operation procedure for an emergency situation based on a functional model, Proc. of International Symposium on Socially and Technically Symbiotic Systems 2015 and International Symposium on Symbiotic Nuclear Power Systems 2015, 2015: 437-443.

[14] INOUE, T., and GOFUKU, A.: A technique to prioritize plausible counter operation procedures in an accidental situation of plants, Proc. 8th International Symposium on Symbiotic Nuclear Power Systems for 21st Century, 2016: Paper No. ISSNP 2016-002.

[15] LIND, M.: An introduction of multilevel flow modeling, International Journal of Nuclear Safety and Simulation, 2011, 2 (1): 22-32.

[16] LIND, M.: Control functions in MFM: basic principles, International Journal of Nuclear Safety and Simulation, 2011, 2 (2): 132-139.

[17] LIND, M., and ZHANG, X.: Functional modeling for fault diagnosis and its application for NPP, Nuclear Engineering and Technology, 2014, 46 (6): 753-772.

[18] The Japan Atomic Power Company, Overview of protecting measures that were established in AM examination report and AM maintenance report, Available: http://www.meti.go.jp/press/2012/04/20120419002/20120419002-6.pdf. [Access date: 2016. 2. 27]. (in Japanese)