EXPERIENCES IN FUKUSHIMA DAI-ICHI NUCLEAR POWER PLANT IN LIGHT OF RESILIENCE ENGINEERING

Atsufumi Yoshizawa [1], Kyoko Oba[2] and Masaharu Kitamura[3]

[1] Nuclear Fuel Transport Company

1-1-3, Shiba Daimon, Minato-ku, Tokyo, 105-0012 Japan

E-ail atsufumi_yoshizawa@nft.co.jp

[2] Japan Atomic Energy Agency

2-2-2, Uchisaiwai-cho, Chiyoda-ku, Tokyo, 100-5877, Japan

E-mail oba.kyoko@jaea.go.jp

[3]Research Institute for Technology Management Strategy (TeMS)

6-6-40-403 Aramaki-Aza-Aoba, Aoba-ku, Sendai, 980-8579 Japan

E-mail kitamura@temst.jp

Abstract

The conventional concept of safety had the objective to eliminate risk. However, the Fukushima Daiichi Nuclear Power Plant Accident exemplified that there is a region of safety that cannot be covered by such an approach. As is evident from the first author's experience on site during the Fukushima Accident, systems need to be resilient in order to secure safety even amidst large disturbances. Also, people in the field showed the ability to make an effort to achieve success (recovery) even when plagued by problems or adversity (resilience). This paper introduces a model for explaining the difference between conventional and new safety concepts. As this model requires the analysis of success cases, this paper focuses on incidents within the Fukushima Accident and analyzes two incidents that can be considered successes based on resilience engineering methodology. Based on this analysis, we attempt to structuralize the relationship between the four core capabilities of resilience engineering (Learning, Responding, Monitoring, and Anticipating) and complementary traits in order to utilize resilience engineering in real-world situations.

1 INTRODUCTION

The objective of the conventional concept of safety is freedom from unacceptable risk. In other words, the premise is that safety can be achieved if risk factors, which are unforeseeable, are removed from the system. However, the accident at the Fukushima Daiichi Nuclear Power Plant (Fukushima Accident) , which was caused by an M 9.0 earthquake triggered by an unprecedented motion of tectonic plates that caused a 15 m tsunami (estimated height at Fukushima Daiichi NPP), clearly demonstrated there are exigent circumstances for which this conventional approach does not apply (TEPCO, 2012, Chapter 3). This paper proposes the necessity for a new safety concept that transcends this conventional concept and reexamines the positioning of humans within safety concepts.

The first author was the Plant Manager of Fukushima Daiichi NPP Units-5/6 at the time of the Great East Japan Earthquake and was put in a position where he had to cope with the accident in a way that would ensure the safety of site personnel while providing a response to the site emergency. When the power plant lost power, lighting, communications, instrumentation and monitoring functions became severely impaired. These conditions combined with exploding buildings and spiking radiation levels plunged the power station into a situation that far exceeded plant design basis. Just maintaining the status quo required multiple tasks, including supplying fuel to fire engines and power trucks used to cool the reactors, which had to be carried out under extremely challenging conditions with limited resources. In addition, as various manuals with which plant operators had boasted compliance were being rendered useless, the author was put under enormous pressure to respond quickly and flexibly to the situation based on uncertain information.

It is clear that under such severe accident conditions the situation would have most certainly escalated to catastrophic proportions had it not been for the actions taken at the site. None of the critical actions taken at the site, including injecting water into the reactors, were done automatically—they were the sole response of the people at the plant. Everyone on-site knew that, "plant status will certainly deteriorate into more

dangerous conditions" and "taking the initiative to act independently was the only way to mitigate the danger to the plant and protect ourselves." However, conventional safety assessment methodology has always considered humans as "elements which threaten system safety by causing human error," so systems were designed to remove this fluctuating element from the system as much as possible. As the people on-site desperately coped with the accident I witnessed behavior that was completely opposite from what was defined by the conventional safety concept—they actually possessed the ability (resilience) to think and flexibly respond in order to restore systems in a changing environment (Hollnagel, et. al., 2008).

The Fukushima Accident showed us that a resilient system is a vital for securing safety, i.e., the system needs to be able to avoid catastrophic failure even amidst large disturbances and that this will eventually be achieved through human actions (Responding.) This is in perfect concert with the concept proposed by E. Hollnagel that states that "Resilient systems must have the ability to succeed under changing conditions" and that "humans are a necessary resource for flexible and resilient systems" (Hollnagel et. al., 2006, 2010) It also demonstrates the validity of Resilience Engineering methodology that puts forth the response by people (Responding) as one of its core capabilities.

This paper attempts to pursue higher standards of safety by focusing on the actions of the people who responded to the accident on site and evaluating specific events during the accident based on a new "people-focused" safety concept while referring to Resilience Engineering, which has been recently proposed and is in the process of development. It should be noted that the examples described in this paper will be categorized as Unexplained Events as per R. Westrum's Typology of Resilience (Westrum, 2006) and, accordingly, this paper examines the ideal state of resilience under such conditions.

2 Necessity for A New Safety Concept (Safety-II) and the Resilience Engineering Approach

In this section summaries of relevant preceding studies that evaluate the events that occurred on site during the Fukushima Accident will be provided along with an explanatory model used to deepen understanding of the differences between conventional thinking.

2.1 Concepts of Safety-I and Safety-II

In the past, safety was constructed on the basis of minimizing risk, i.e., safety will be achieved by predicting accident events, identifying the risks leading to such events, and removing such risks therby preventing accidents from happening(ISO/IEC, 2014). In this process, humans were considered as elements that threaten system safety by causing human error and therefore, many approaches have been taken to prevent human errors.Hence, humans are tretaed as Human Error Probability in risk assessments. Based on this concept, automation to remove instable human interaction was a justifiable approach to improving system stability.

If the focus is put on humans, then preventing human error becomes a prerequisite for securing safety. However, the question then becomes whether or not the goal of guaranteeing safety can be achieved by merely prevening human error. In orther words, by setting the goal of eliminating risks and assuming that "safety means a state where nothing happens ", efforts to ensure safety will be focused only on the prevention of failures and troubles, and will not generate any other added value. Flexibly responding in different ways during an emergency is only possible by humans and the organizations that they comprise, and as such, a new goal needs to be set that will nurture capabilities that can be applied in an agile manner.

The existing safety concept as Safety-I and the new safety concept as "Safety-II" (Hollnagel, 2014 defined). The latter is defined further as "safety as the ability to succeed under varying conditions"(Hollnagel, 2014,pp134). The target to achieve is described as "a condition where as much as possible goes right"(Hollnagel, 2014,pp134) and humans are considered as "a resource necessary for system flexibility and resilience" (Hollnagel, 2014,pp147) This new notion of safety differs from Safety-I that emphasizes the minimization of risk in that it focuses rather on identifying those actions that increase the chance of success and exemplifies the capabilities displayed by the people and organizations at the site of Fukushima Accident.

2.2 Importance of Learning from Successes Hidden within Larger Events

A typical definition of Safety-I is"Freedom from risk which is not tolerable (ISO/IEC Guide 51)", according to which safety is constructed with a focus on risk and failure. Analyzing failures and preventing recurrence by

removing the cause is a typical application of Safety-I, which is based on the “hypothesis of different causes“ that considers failure and success to be the resultants of different factors(Hollnagel, 2014,pp52).

However, in large-scale socio-technical systems such as nuclear power plants, things are more complicated. Figure 1 shows a concept diagram during normal times and emergencies. The iceberg depicts a collection of actions and examples. In complex systems, it is appropriate to express incidents as a collection of many actions and examples. The water surface depicts the competence of the organizations and people. As shown in Figure 1, during normal times aseries of actions are conducted within the capacity of people and organization in order for the system to function, and fluctuation can be absorbed.

This figure shows that two approaches are necessary to ensure safety during a single event. The first is to ensure prior preparation so that failure, as depicted in Figure 1 by the portion of the icebergiceberg above the water’s surface, does not occur again. The second is to equip [the system] with capabilities that will enable the success of various tasks to be processed smoothly and effectively , as depicted by the portion of the icebergiceberg below the water’s surface, and to minimize the portion of the iceberg above the surface. Actions taken during the Fukushima Accident that were below the surface were, for example, cooling the reactors by injecting seawater using fire engines and providing power to instruments in the control room using car batteries(TEPCO, 2012, Capter8). Detailed examples will be described in 3.1 and 3.2.

As described in the second approach to ensuring safety, the height of the water surface in Figure 1 (span of capability) can change significantly according to the situation and the interaction between the organizations and teams that respond to the accident. In other words, people are doing their best as every moment passes by and making decisions based on bounded rationality with the information available at the time. The distinction between failure and success can only be made after the fact and are not necessarily the result of separate factors (parity of success and failure.) Therefore, failure events can be viewed as having failed by chance under a certain situation. As the concept of Safety-II shows, it is not appropriate to think that causes for failure and success are different by applying the hypothesis of different causes to the upper and lower parts of the iceberg.

Based on the experience of the Fukushima Accident, the first author confirmed the necessity for a paradigm shift from the conventional Safety-I that pursues safety by focusing on failures to Safety-II that aims to elicit efforts to maximize the chance of success.

Note thatfailures within the portion of the actions and events that run the system and usually go on unnoticed under water but that “emerge” above the surface during a disaster, provide an opportunity to notice issues. It is important to have the capability to learn from these opportunities by discovering resilient events that hide behind the shadow of failures.

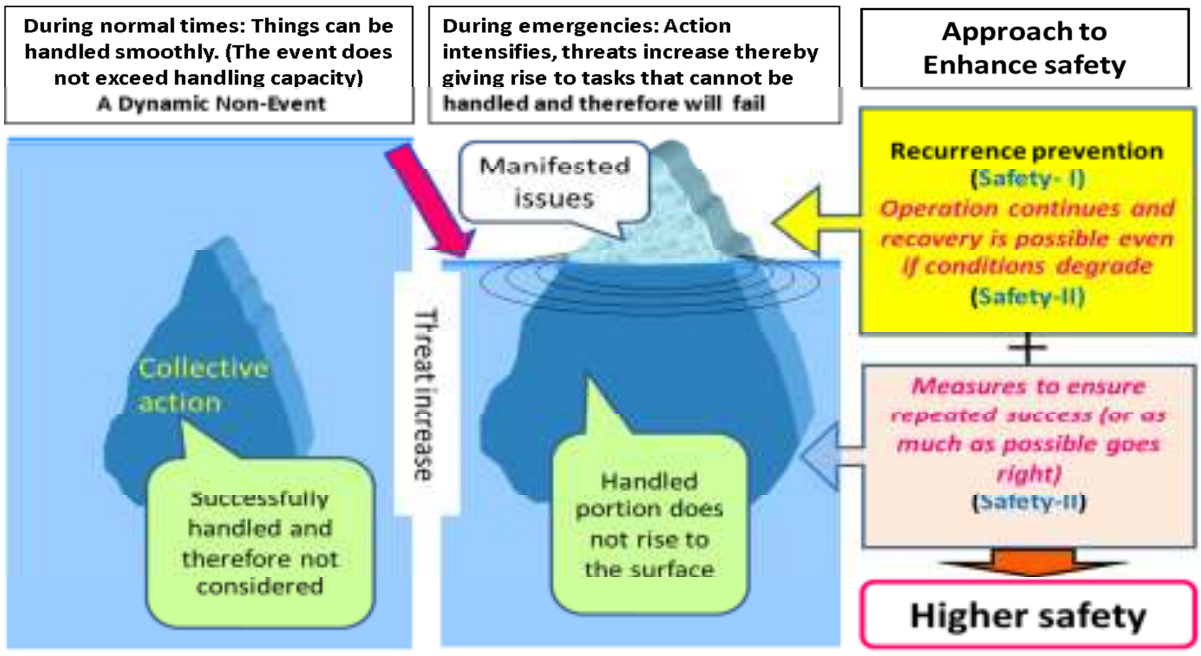

Figure 1. *Comparison model of approach to enhance safety between Safety-I and Safety-II*

Disasters visualize social systems for what they really are, and provide opportunity discovering resilient events

2.3 Resilience Engineering and its Components

Resilience Engineering has recently been widely recognized as a methodology to pursue safety based on Safety-II. The purpose of resilience engineering boils down to how to bring about resilience (elasticity and recoverability) to systems.

It is well known that resilience engineering defines the following four elements as core capabilities (Hollnagel, et al. 2009)

Learning, Responding, Monitoring, Anticipating

These four capabilities are not independent of each other but rather interact. The capabilities of Responding and Anticipating can be improved through study and practice. If anticipation is successful, response capability improves. Conversely, extremely high response capability can in some cases make up for a lack of anticipation. However, even if there is a difference in the degree of aptitude between them all four capabilities are necessary for a system to have resiliency.

However, further complementary requirements need to be met in order for these four capabilities to effectively function. . Hollnagel, et al., pointed out that deficiencies in time, knowledge, competence, and resource will force a system to lose control and noted that resolving such deficiencies is a condition for resiliency. (Hollnagel and Woods、 2006, Epilogue) The authors summarized these conditions as complementary prerequisites as follows:

As system is forced to operate in a passive mode when time runs out, so it is important to increase system anticipation and take proactive measures to secure time. Knowledge and competence are prerequisites for making decisions on how to respond, but to make such decisions, learning from successes, as mentioned in 2.2, is also important. Knowledge and competence means knowing what to do and how to do it, but the appropriate allocation of resources is critical in order to take necessary action. It is pointed out that the capability to notice subtle changes is necessary in order to initiate the functions of responding and monitoring,.(Lay,2010, chapter 7) Given the above discussion, this study will focus on proactive actions, learning from successes, preparation and the appropriate allocation of resources, and the capability to take notice as four complementary prerequisites. Although knowledge and skill (competence) are equally important, it is not a prerequisite specific to resilience engineering but rather to operational safety in general. Therefore, these are treated as more basic prerequisites compared to the four complementary prerequisites.

Note, however, that proactive measures may well end up being unnecessary. Organizations that stress resilience need to have a business strategy that accepts decisions to make sacrifices. (Woods, 2006).

3 The Case of Fukushima Daiichi NPP

In this section, the , relationship between the four core capabilities of resilience engineering described in Chapter 2 and the four complementary prerequisites will be examined based on actual case events at the Fukushima Daiichi NPP. As mentioned before, disasters enable us to visualize systems and provide opportunities to notice various elements. Numerous reports were made after the accident but the vast majority of them focus on failures with very few discussing successes. This section will shed light on successes that have not been studied in any report and will be evaluated based on first-hand experience on site by the first author.

3.1 Case 1: Emergency Evacuation of a Heavy Oil Tanker (TEPCO, 2012, Appendix 2, pp.7)

When the earthquake occurred a tanker was moored in the power plant port where heavy oil was being transferred from it to a tank via a pipeline. When the earthquake struck, the onshore manager (experienced with operating ships) and the captain of the ship anticipated the arrival of the tsunami based on their experience (learning effect.) The captain immediately made the decision to evacuate the tanker from the port and move it out to sea. At the time, the captain also made the decision to prioritize emergency departure from the shore and to cut and abandon the pipeline and oil fence, based on the time required to take such actions. The tools (resource) required to cut the oil fence were on-hand. As a result of this quick decision-making and maneuvering of the ship amidst sea currents that were already being affected by the approaching tsunami, collisions with other ships and floating debris (coping and monitoring) were avoided and the tanker was moved out of the port just in time to prevent damage from the tsunami.

If the evacuation had been delayed and the tanker had been stranded onshore, not only would it have become an obstacle for the emergency response, but it could have also caught on fire and exacerbated the situation. As such, this is an important case that contributed to preventing further deterioration of the conditions on site.

3.2 Case 2: Explosion Prevention at Fukushima Daiichi NPP Units 5 and 6 Reactor Buildings (TEPCO, 2012, Appendix 2, pp.151)

Among the six units at Fukushima Daiichi NPP, Units 1 to 4 incurred severe damage. However, Units 5 and 6 were also far from safety. Fortunately, an air-cooled emergency diesel generator installed in Unit 6 survived the tsunami and was able to operate continuously. This enabled the supply of power, albeit insufficient, to Unit 5 that had lost all AC power. Thanks to this generator just enough power was provided to keep monitoring instruments in the main control room working and restore the residual heat removal system. In hindsight, enabling water levels in the reactors and spent fuel pools to be maintained prevented the generation of hydrogen gas. However, when the building for Unit 4, which was undergoing periodic inspection just like Units 5 and 6, exploded, the cause of the explosion was unknown and it was not unreasonable to assume that Units 5 and 6 might suffer the same fate. Also since power was supplied by an emergency diesel generator that was vulnerable to singular failure the possibility that aftershocks could disable water injection and heat removal functions was foreseeable. Hence, in the early morning of day seven, holes were drilled in the concrete roofs of the Unit 5 and 6 reactor buildings using boring machines. Although worker safety was of the utmost concern, the decision to carry out the task was made from a more macro-safety point of view. This eliminated the risk and concern of hydrogen explosion thereby enabling work to bring the units to cold shutdown on day nine to continue. This measure was flexible, proactive and significantly different from normal safety procedures.

In the process of carrying out this task, large construction companies turned down TEPCO's request for personnel support and only provided other resources, such as equipment. Just when TEPCO personnel started to take actions on their own they ran into the office manager of a local building contractor, who volunteered to help. Thanks to inter-organizational team work and determination another crisis was avoided.

3.3 Voices from the Field

In order to explain responding to avoid extreme conditions, there are cases in which the four complementary prerequisites described in Section 2 fall short. Case 2 is a clear example. When the office manager of a building contractor happened to run into TEPCO personnel on their way to drill holes in the building roofs, there was no reason for him to volunteer to help with such a dangerous task especially since he was in the process of evacuating. Later, he reflected on his decision to help saying that he felt that if he did not volunteer to go along he wouldn't be worthy enough to work at the power plant again for the rest of his life. It is apparent that this decision was made because of the feeling of unity between TEPCO employees and contractors that had been cultivated through daily operations.

There are other similar anecdotes. Below we examine these incidents using excerpts from interviews with the people involved.

1. "For operators to leave the control room, it means giving up control of the reactor. That means abandoning the evacuated local residents who have put their faith in us as well as our own families. It is we, the people on site, who needed to respond. That is why we cannot just leave. " *–Quote from shift manager addressing his subordinates and then bowing deeply.* (Takahashi, 2015, In Japanese)
2. I will do anything. I am prepared to throw myself into the jaws of the power station. If there's anything that needs to be done, just tell me. I want to show you that operators have guts if it's the last thing I do. (Veteran TEPCO personnel with much experience in operation)(TEPCO, 2012, Appendix 2, pp184)
3. With a sense of mission as a plant contractor and the knowledge of how hard Masao Yoshida was fighting to save the plant, I simply could not abandon him. (Chief of local office of a plant contractor) (Takahashi, 2015, In Japanese)
4. I begged them to take actions to prepare for water injection, such as removing rubble and replacing hoses for minimal injection. What truly moved me was that everyone volunteered to go into the field after I asked them to do this. (Site Superintendent Yoshida)(Japanese Government Accident Investigation Committee,2011,In Japanese)

What can be seen from these words is that it was the optimistic attitude of the workers involved in this situation that enabled various tasks to be carried forward. This "Attitude" was cultivated by various factors including the sense of mission and solidarity of field workers to restore systems anyway they could amidst accident condition, and the sense of attachment to their local community in Fukushima. From among the four core capabilities of resilience engineering emphasis should be placed on the importance of Attitude as it is a critical factor for facilitating an effective response., as (Komatsubara, 2008)(Oba, et. al., 2014)(Yoshizawa, et. al.,2014).

Figure 2 shows the four capabilities and four complementary prerequisites discussed in the previous section along with the important factor of Attitude identified in the case analysis. The four major capabilities are shown in a hexagon. The four elements shown in clouds indicate mental activities while appropriate resource allocation is shown in a circular platform that serves as the foundation for tangible elements such as facilities, equipment, tools, protective gear, and personnel. Knowledge and skill are shown in a similar icon as they are the intellectual foundation for all activities.

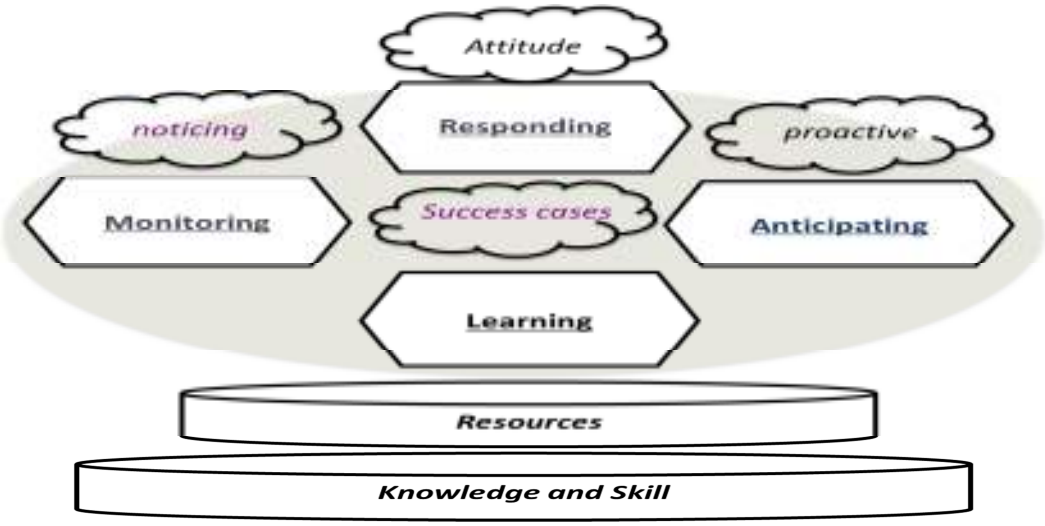

Figure 2. *Structure of 4 Core Capability and Complement Factors of Resilience Engineering*

3 Discussions and Conclusions

Since the wake of the Fukushima Accident, numerous discussions have been ongoing with regard to the concept of safety for large-scale socio-technical system. The conventional concepts of safety had the objective of freedom from unacceptable risk and considered system risk factors could be anticipated with the assumption that safety could be achieved by eliminated them. However, the Fukushima Accident illustrated that there is a region of safety that cannot be covered by such an approach and that there is a need for a new safety concept that transcends this conventional concept. As is evident from the experience on site during the Fukushima Accident, systems need to be resilient in order to secure safety and these system need to be able to avoid catastrophic failure even amidst large disturbances. This is in perfect concert with the concept proposed by E. Hollnagel that "safety is the ability to succeed under varying conditions (Safety-II)".

Historically, humans had been treated as "elements which threaten system safety by causing human error ." However, workers in the field during the Fukushima Accident desperately fought the accident and possessed the ability (resilience) to flexibly think and take action to restore systems in a changing environment. It was concluded that resilience engineering as a methodology for achieving Safety-II that identifies four core capabilities, and complementary prerequisites that nurture such capabilities, for humans and organizations, is an effective method for leveraging the lessons learned from first-hand experience during the Fukushima Accident.

This paper introduced a model to explain the difference between Safety-I and Safety-II concepts. A model showed the necessity to focus on successes and also showed that failures and disasters have enabled systems to be visualized and have provided opportunities to recognized hidden events that are resilient.

The paper also focused on smaller events within the Fukushima Accident and analyzed two successes based on resilience engineering methodology. The importance of Attitude as a trait that complements the four core capabilities was pointed out. Furthermore, an attempt was made to structuralize the relationship between core capabilities and complementary traits in preparation for practical application.

Acknowledgements

We would like to express our heartfelt apologies to the many people who still are leading lives as evacuees due to the Fukushima accident as well as for all the inconvenience and anxiety the accident has caused the local community and Japanese society as a whole. In addition, we would like to express our appreciation for the support of so many people who devoted themselves to responding to the accident under such severe conditions, and our condolences to the families of the two colleagues who made the ultimate sacrifice in the line of duty and Site Superintendent Masao Yoshida, who spearheaded the initial response.

REFERENCES

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

Hollnagel, E., Nemeth, C.P. and Dekker, S.(eds.) (2008). Remaining Sensitive to the Possibility of Failure, Resilience Engineering Perspectives, Vol.1, Ashgate (2008)

Hollnagel, E.(2009); *The Four Corner Stones of Resilience Engineering, Chapter 6* of Nemeth C.P., Hollnagel E.and Dekker, S. (eds.) Preparation and Restoration, Resilience Engineering Perspectives, Vol.2, Ashgate (2009)

Hollnagel, E., Pariès, J., Woods, D. and Wreathall, J. (2010). Resilience Engineering in Practice : A Guidebook, *Prologue*, Ashgate Publishing Ltd. (December 2010)

Hollnagel, E. (2014). Safety-Ⅰ and Safety-Ⅱ, The Past and Future of Safety Management, *Chapter 3 and 7*, ASHGATE. (2014)

The International Organization for Standardization and the International Electrotechnical Commission (2014). Safety aspects- Guidelines for their inclusion in standards, Guide 51 (2014)

Japanese Government Accident Investigation Committee Interview Record (2011). *Masao Yoshida Interview Results*, July 29, 2011, (In Japanese)

Komatsubara, A.(2008) ; *When Resilience does not Work, Chapter 7* of Hollnagel, E., Nemeth, C.P. and Dekker, S.(eds.) Remaining Sensitive to the Possibility of Failure, Resilience Engineering Perspectives, Vol.1, , Ashgate (2008)

Lay, E.(2010). *Practices for Noticing and Dealing with the Critical. A Case Study from Maintenance of Power Plants, chapter 7* of Hollnagel, E., Pariès,J., Woods, D. and Wreathall, J. (2010). Resilience Engineering in Practice : A Guidebook, Ashgate Publishing Ltd. (December 2010)

Oba, K., Yoshizawa, A. and Kitamura, M. (2014). Enhancement of Organizational Resilience in Light of the Fukushima Daiichi Nuclear Power Plant Accident (II) – Promoting of Attitude Building Measures -, *The Japan Society of Mechanical Engineers, Proceedings of the 2014 Annual Conference, G2010103.* (In Japanese)

Takahashi, H., Kyodo News Nuclear Accident Coverage Team Editor (2015). “Remembrances of the Loss of All Power Supply,” Shodensha (March 6, 2013). (In Japanese)

Tokyo Electric Power Company, Inc. (2012). Fukushima Nuclear Accident Investigation Report, *Chapter 3 and Appendix 2* ,June 20, 2012

Woods, D.D.(2006). *Essential Characteristics of Resilience, Chapter 2* of Hollnagel, E., Woods, D. and Leveson, N.(2006). Resilience Engineering : Concepts and Precepts, Ashgate Publishing Ltd.(February 2006)

Westrum, R. (2006), *Typology of Resilience, Chapter5* of Hollnagel, E., Woods, D. and Leveson, N.(2006). Resilience Engineering : Concepts and Precepts, Ashgate Publishing Ltd.(February 2006)

Yoshizawa, A., Furuhama, Y., Mutou, K., OBA, K., and Kitamura, M. (2014). Enhancement of Organizational Resilience in Light of the Fukushima Daiichi Nuclear Power Plant Accident (I) – Analysis of Responding Structure -, *The Japan Society of Mechanical Engineers, Proceedings of the 2014 Annual Conference, G2010102*. (In Japanese)