Available online at www.sciencedirect.com

ScienceDirect

IFAC-PapersOnLine 49-19 (2016) 245–250

Lessons Learned from Good Practices During the Accident at Fukushima Daiichi Nuclear Power Station in Light of Resilience Engineering

Atsufumi Yoshizawa*. Kyoko Oba**
Masaharu Kitamura***

** International Research Institute for Nuclear Decommissioning, 2-23-1, Nishi-shimbashi, Minato-ku, Tokyo, 105-0003 Japan (Tel: +81-3-6435-8601, E- mail: atsufumi-yoshizawa@irid.or.jp)*
*** Japan Atomic Energy Agency, 2-2-2, Uchisaiwai-cho, Chiyoda-ku, Tokyo, 100-5877, Japan (Tel : +81-3-3592-2341,E-mail : oba.kyoko@jaea.go.jp)*
**** Research Institute for Technology Management Strategy (TeMS), 6-6-40-403 Aramaki-Aza-Aoba, Aoba-ku, Sendai, 980-8579 Japan (Tel: +81-22-393-4884, E-mail: kitamura@temst.jp)*

Abstract: The accident at the Fukushima Daiichi Nuclear Power Station, which was triggered by the Great East Japan Earthquake, has presented significant issues about in which the safety of massive socio-technical systems is structured. We must derive the greatest number of lessons possible from this accident to ensure the safety of systems in the future, but the lessons learned so far have mainly focused on risks and been deduced from an analysis of failures that led to the accident. Meanwhile, with regard to the many actions executed in the field that allowed any "further catastrophe" to be avoided despite such a possibility having been assumed in circumstances where equipment and manuals could not be relied on, there has been almost no analysis, assessment nor lessons gleaned. This paper references the approach of Resilience Engineering which aims to extend successes in a changing environment, and focuses on the actions that prevented "further catastrophe" through an analysis of the Fukushima accident and derives new lessons to improve the capability to handle "unforeseen contingencies."

Keywords: Fukushima Daiichi Nuclear Power Station, Resilience Engineering, Four Cornerstones, Responding, Attitude, Emergence, Unforeseen Contingencies

1. INTRODUCTION

The accident at the Fukushima Daiichi Nuclear Power Station (hereinafter, "Fukushima accident"), which was triggered by the Great East Japan Earthquake that struck on March 11, 2011, has presented significant issues about how to ensure the safety of complex socio-technical systems. Many institutions have conducted analyses of the Fukushima accident and derived lessons to be learned, but most of these have been devoted to analyze factors that resulted in the accident and deduced lessons from such factors. This is due to the fact that the basic approach to safety is "freedom from risk which is not tolerable" as stated in ISO/IEC Guide 51, which the Science Council of Japan considers its foundation. According to this definition, because the approach demands that any "risks" a system has be brought to light and expunged or reduced to an acceptable level so that safety many be ensured, this approach requires that anything that has gone wrong in the past be prevented from reoccurring.

On the other hand, according to Westrum's typology, the Fukushima accident is synonymous with on unexampled event that clearly surpasses any irregular threat (Westrum, 2006), and it is also an event that calls into question how safety is to be ensured at times when such horrific unanticipated events are faced. Although the Fukushima accident is a major accident despite any "further catastrophe" having also been anticipated (Investigation Committee, Interview Records, 2012), then Prime Minister Noda declared that Fukushima Daiichi had reached a state of cold shutdown on December 16, 2011 after the strenuous efforts of those involved (Prime Minister of Japan and His Cabinet HP, 2011). Nevertheless, in these important reports, there has been insufficient extraction of data, which may prove to be lessons to be learned, from the perspective of why this "further catastrophe" was able to be avoided.

Yotaro Hatamura, Chairperson of the Investigation Committee on the Accident the Fukushima Nuclear Power Stations of Tokyo Electric Power Company, stated in the Chairperson's Remarks to the Final Report, "The events that occurred within the nuclear power station after it was flooded as a result of the tsunami were a series of incidents that people involved with nuclear power generation in Japan had never encountered before, and without the actions of those involved in dealing with the accident at the facilities, who risked their lives, the accident would have worsened further and radioactive materials might well have dispersed over a clearly much wider area than at present" (Investigation Committee, Final Report, 2012). These remarks point to the importance of the activities conducted by the workers who remained on-site in the extreme conditions of a very hazardous working environment, including high levels of radiation. Many of the workers were from the local communities, and the reality was that a "further catastrophe" was able to be avoided through a series of tasks which were

2405-8963 © 2016, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2016.10.537

executed while it was still unclear whether their families were safe or not.

Based on the experiences of the first author who was actually engaged in the response to the Fukushima accident on-site, this paper references the approach of Resilience Engineering (Hollnagel, 2006), which has garnered attention in medical emergencies and other such situations since the accident, and focuses on the “things that went right” in the field which contributed to staving off any “further catastrophe” as mentioned by Chairperson Hatamura and regarding which almost no analysis has been conducted to deduce new lessons to be learned that focus on “people.” Also, a safety concept will be examined so that these lessons may be derived and put to use systematically.

2. NECESSITY FOR A NEW SAFETY GOAL

As stated in the previous section, safety has so far been constructed mainly in terms of prevention through risk minimization. This is founded on the idea that safety is ensured by assuming accidents or other such events, bringing to light the risks entailed in such incidents and reducing them down to an acceptable level. Erik Hollnagel, a pioneer in organizational safety research, has termed this sort of risk removal-type safety “Safety-I” (Hollnagel, 2014, pp.49-52). In so doing, many approaches have been adopted where people are regarded as a “factor threatening the safety of systems” in the effort to prevent human error. That is why probabilistic risk assessments (PRA) for nuclear power consider people a “human error probability.”Although preventing human errors is of course a necessary act in ensuring safety, setting a goal in which “safety is a state where nothing happens” tends to direct the energy, which could be put into improving safety, towards preventing accidents and problems before they happen (Hollnagel, 2011).

The first author experienced the Great East Japan Earthquake in the field as a plant manager (for Units 5 & 6) at Fukushima Daiichi Nuclear Power Station, and was in a position where he had to respond to the accident at the plant while ensuring the safety of station personnel. The power station, which had lost power and whose lighting, communications, instrumentation, monitoring and other such functions were significantly damaged, was an environment where adverse conditions were present exceeding those anticipated at the time of plant design, including hydrogen explosions in buildings, and where radiation levels were also rapidly rising. Nevertheless, while under extreme pressure and pressed for time and with the manuals, which personnel had intended to observe, utterly useless, there were workers who held their ground and executed a response adapted to the situation at hand, without the use of any manuals, as they also operated under severe conditions where they had to surmise what the situation was based on limited data and execute a response that was grounded in their knowledge and experience. To cite a few specific examples, “people” conceived of and took all actions to secure a line injecting cooling water into the core prior to the radiation level inside the building at Unit 1 reaching a fatal level. People restored instruments using batteries from employees’ cars. People injected cooling water into the reactor using fire engines and cooling water into the spent fuel pool using a concrete pumper vehicle and measured the spent fuel pool water level. People achieved a cold shutdown of Units 5 & 6 using a temporary seawater pump (TEPCO, 2012). Planned and executed such actions had been responded beyond prepared organizational rules by personnel to meet the situation in the field with limited resources and uncertain information. Total system resulted in resilient to avoid “further catastrophe” by those “emergent” functions (Pariès, 2006) ..

Not only during the Fukushima accident, but also in “unforeseen contingencies” which change in a variety of ways, a “flexible response” in the field is indispensable. However, such a response is not able to be programmed in advance, but “emerges” according to the way in which an event unfolds, its environment, what resources are foreseeable and usable as well as other factors. It is also assumed that these actions will at times entail significant “Sacrifice Judgment” (Woods, 2006).

The Fukushima accident has clearly indicated, as an important element in ensuring safety, that it is necessary to “avoid catastrophic damage even though a large disturbance is sustained,” that such avoidance is ultimately the work of “acts of people (responding),” and that it is important to enhance the possibilities for actions and responses to “emerge.” So, how should a goal be configured that yields “added value” to foster the ability in people and organizations to be able to “adapt as desired” in response to events that exceed our experience and assumptions. In regard to this issue, Erik Hollnagel has called this new success improvement-type safety concept “Safety-II” and defined “safety as the ability to succeed under varying conditions.” Also, the goal to be achieved is “a condition where as much as possible goes right,” and, within that context people are positioned as “a resource necessary for system flexibility and resilience” (Hollnagel, 2014, pp.145-148). This differs from Safety-I which aims for risk minimization, and is a concept that attempts to bring out actions improving success, which was superbly expressed in the ability needed from people and organizations in the field during the Fukushima accident.

In this way, although Safety-II affords a new safety objective, it is not a concept that conflicts with Safety-I, but it is reasonable to consider it as effectively an extension of Safety-I which already ensures safety to a certain high level. Resilience Engineering is positioned as an engineering methodology for pursuing this goal (Kitamura, 2014).Large-scale socio-technical systems, such as nuclear power are amazingly complex. Figure 1 shows a conceptual model explaining responses during normal times and during emergencies (Yoshizawa, et al., 2015b). The iceberg represents the aggregation of actions. With complex systems, it is suitable that events are expressed as an aggregate of many acts. Also, the area underwater represents the competence of organizations and individuals.

As shown in Figure 1, during normal times, a series of acts to make a system function are performed within the scope of