Resilience Engineering, High Reliability Organization, and Risk Literacy

Dr. Hiroshi Ujita

The Canon Institute for Global Studies, 11F, Shin-Marunouchi Bldg., 5-1 Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-6511, JAPAN

ujita.hiroshi@canon-igs.org

Abstract. It is important to 'establish the feedback system on organization learning in ordinal time' And it means that it is important to establish the system admitting violation of order. The decision at on-site are given priority than other ones. The representative example is the decision of sea water infusion continuation which was given priority at on-site, even though the official residence and the main office TEPCO had ordered to stop the infusion.

The many failure cases are defined under national government level and nuclear industry level which are the problems of rare event awareness and of organization culture. The ordinal time training at on-site also work in emergency situation at the accident, while the level of administration department and government didn't work well.

Keywords: Resilience Engineering, High Reliability Organization, Risk Literacy, Fukushima Accident, Bounded Rationality, Information Limitation, Context

1 Introduction

The results of Fukushima Daiichi Accident investigation with diversified characteristic are released until now. Based upon the analyses of the investigation, the success and failure cases for emergency responses are analyzed concerning to personal- response capability, organizational-response capability, and communication ability with external organizations, and then the problems of responses are extracted. The action of sea-water infusion on Fukushima Daiichi nuclear power plant No.1 was paid attention and analyzed based on the 'Accident Analysis Report of Fukushima Nuclear Accident' [1] (Accident Report) by TEPCO, Tokyo Electric Power Company, especially focus on the decision making of continuation of pouring sea water.

2 Bounded Rationality in Context vs. Judge by God

In the field of cognitive science and the cognitive system engineering, the human being is considered as to think and judge it reasonably along context while there is information limitation. Sometimes the decision may be judged as an error by the outside later. It is called "bounded rationality in the context" vs. "judge by God". The absurd action of the organization was often explained in human illogicality until now, but the approach had recently come out to think that the human being rationality was the cause.

Table 1 shows three approaches from Organizational (Behavioral) Economics, business cost theory (reluctant to do), agency theory (information gap), and proprietary rights theory (selfishness).

business cost theory Action of opportunity principles, agency theory burying cost moral hazard, adverse selection (lemon market), proprietary rights theory, Externality. The common supposition "is bounded rationality and effect maximization".

It is necessary to find the social context that the error is easy to cause in the engineering for human beings in the future. In other words I do not analyze something with the error, and a way of thinking changes in the direction analyzing the social context that is easy to wake up an error. Because this direction is beyond a conventional ergonomic range treating the contents of the error basically, it is a fact to be difficult.

However, you should recognize it now if you do not analyze an error in the relative viewpoint with the environmental element to surround security and a human being when it is in the times not to be tied to measures. You should match the measures with a human rational characteristic to have.

Business cost saving system (collection of friend - right type - decentralization of power type organization)

Agency - cost cut system (objectification of the information)
Internalization system (proprietary rights distribution) of the externality

3 Accident model and Error model.

Table 2 shows Accident model and Error model.

I summarize the change of the model of an accident and the error in table 2. A conventional accident model is the domino model who I analyze the causation of trouble and the error, and takes measures. In the model, I use the slip which is the classification of the non-security act to occur by on-site work, lapse, mistake. Design thought of the depths protection has been established, and the accident to occur is caused by the excellence of the error of a variety of systems recently. The analysis of the organization blunder is necessary for the analysis by this Swiss cheese accident model in addition to conventional error analysis, too.

An organization accident is a problem in the organizations, and the cause reaches it before, as a result, the accumulation of what I think basically with the best of intentions and did shakes an organization, and the association with the safety problem (it is an act of the good will, but becomes the error) is high. As for the organization accident, the interdependence between the inside of the organization or the organization is accumulated by an error of the depths protection, and it is with a problem of the deterioration of the security culture in its turn. The organizational management based on the organization analyses such as behavioral sciences will be necessary for these measures.

4 The methodology on Resilience Engineering, High Reliability Organization, and Risk Literacy

Resilience and safety management Resilience is the intrinsic ability of a system to adjust its functioning prior to,
during, or following changes and disturbances, so that it can sustain required
operations under both expected and unexpected conditions.
A practice of Resilience Engineering / Proactive Safety Management requires that
all levels of the organisation are able to:
Monitor
Learn from past events
Respond
Anticipate

High Reliability Organization: Organizational Process by Nakanishi
Preparedness for Emergency Situation in Ordinal Time:
Carefulness (Confirmation),
Honesty (Report),
Sensitivity (Observation),
Emergency Response in Emergency Situation:
Alert (Concentration),

Flexibility (Response),

Ability of Risk Literacy:
Analysis power
Collection power
Understanding power
Predictive power
Communication power
Network power
Influence power
Practical power
Crisis Response Power
Radical Measures Power

5 The analysis based on Resilience Engineering, High Reliability Organization, and Risk Literacy

5.1 Chronological analysis

The analysis for the detail of sea-water infusion to Fukushima-Daiichi No.1

Chronological analysis was drawn up from "The main chronological analysis of Fukushima Daiichi nuclear power plant No.1 from earthquake occurrence to the next day" and "The status response relating to pouring water to Fukushima Daiichi nuclear power plant No.1", which came from the 'Accident Report.

The chronological analysis shows that the preparation of sea-water infusion is decided and ordered concurrently with pouring freshwater, and also shows that continuation of sea-water infusion is decided as on-site judgment although an official residence and the main office of TEPCO directed to stop the infusion. The necessity of continuation of sea-water infusion was recognized consistently by on- site judgment, and these measures were taken. However the main office of TEPCO directed to stop the infusion in taking into consideration of the intention of official residence. This means that the main office of TEPCO and the official residence viorate the fundamental principle which on-site judgment should be preceded in emergency situation.

5.2 Organizational factors analysis

The process of sea-water infusion on Fukushima Daiichi No.1 is analyzed from the point of resilience capability, high reliability organization capability, and risk-literacy capability [2-6]. The analysis example by risk-literacy capability is shown in Table 1 from the viewpoint of risk-management, which is described in 'Introduction of Risk Literacy- Lessons Learned from Incidents' [6]. The definition of risk literacy capability which can extract communication power that is important both for ordinary time and for emergency situation is the most appropriate for analysis. The horizontal axis shows response capabilities which are suggested in each study, and the vertical axis shows each level of individual, organization and correspondence to outside. The gothic font in green means success case, while the italic font in red means failure case.

The analysis of emergency correspondence like this kind of huge accident cannot be analyzed enough using conventional framework. As a whole of one organization, the classifications were reviewed and revised from two points. One is that the differences in correspondence and the problems in cooperation between on-site and administration department cannot be clarified. And the other one is that communication power has two sides which are the information cooperation in ordinal time and collaboration in case of emergency situation. The analysis power and information transmission power correspond to ordinal time, and the influence power and normal time skill correspond to the case of emergency situation. In this analysis, the contact with official residence and the cooperation inside government are also included in correspond to external organizations.

6 Success and failure cases

From the viewpoint of Resilience Engineering, the case of success and failure are listed and analyzed.

6.1 Good case of Resilience response

The good cases of resilience response are observed in individual base and organizational base as below.

- The effectiveness of insight on accident cases (inundation in Madras, 9.11 terrorism- B.5.b.) and of the risk evaluation.
  - Decision of continuation of sea water infusion (individual base)
- Reflection of the experience on Chuetsu-Oki Earthquake
  - Improvement of seismic building which is equipped emergency power source system and air conditioning system (organizational base)
  - Deployment of fire engines (organizational base)
- The effectiveness of command system in ordinal time (on-site of organizational base)
- Support by cooperation companies and manufacturers (designers and site workers of organizational base)

The reason why the good cases are occurred in on-site, the officers and workers always felt that their mission is to carry out with the sense of ownership and also with critical mind. They had trained the accident management in ordinal time, which works effectively in emergency situation, which is the just significant frame derived from the development of safety culture. It is important to 'establish the feedback system on organization learning in ordinal time'. But there were a little lack of information between control room and emergency response room, they will be able to solve by taking physical measures to clarify the circumstances at on-site. The TV conference system of Fukushima Daini nuclear power plant had worked effectively to communicate among on-site, the main office of TEPCO and the outside organizations. Furthermore using the white board for information sharing, which is the good case that the resilience works well, could prevent the confusion at on-site..

The continuations of emergency training in ordinal time with assuming the severe accident progression is considered to be the effective way. As many lacks in emergency correspondence in management department and in national government level are observed, and then the emergency training is necessary in management level, in which responsibility assignment is regularly taken, the incident seriousness is evaluated, and the mode is switched from ordinal time to emergency situation.

6.2 The failure of comprehensive power in organization, the fallacy of composition of risk awareness

The many failure cases are defined under national government level and nuclear industry level which are the problems of rare event awareness and of organization culture. Although everyone had same recognition for the risk of power loss and Tsunami, the accurate decision had not been made by national government level, just only made by individual level. The ordinal time training at on-site also work in emergency situation at the accident, while the level of administration department and government didn't work well.

- Risk misrecognition of Loss of offsite power and damage by Tsunami (national government level, industry level)
- Confusion of command system (organization base- between on-site and the main office of TEPCO)
- Confusion of command system (external correspondence base- national government level, and organization base- among official residence, regulation, and the main office of TEPCO)

The true nature of the problem in Japanese organization that doesn't change from when the 'Truth of Failures' [7], in which Japanese military operation failures in the World War II were analyzed, is written by Tobe, Nonaka, et. al.. Failure cause is described as standpoint of irrationality in Japanese on this book. But the problems in organization are not able to be resolved by irrationality in Japanese. It should be explained using by bounded rationality which Kikusawa advocate in 'Absurdity of Organization' [8]. His idea is that decision making which are made under limited circumstances based on limited information will end in failure from the eye of God. He also advocates destroying the bounded rationality for failure measures. It means that it is important to 'establish the system admitting violation of order in emergency situation'. The decision at on-site are given priority than other ones. The representative example is observed in the decision of sea water

infusion continuation, the decision at on-site were given priority even though the official residence and the main office TEPCO had ordered to stop the infusion. Otherwise it is the failure case that occur delay of PCV vent, for time loss to get the permission of national government and local government.

6.3 Consideration on Organizational problem

It is important to 'establish the feedback system on organization learning in ordinal time'.

The continuations of emergency training in ordinal time with assuming the severe accident progression is considered to be the effective way.

The emergency training is necessary in management level, in which responsibility assignment is regularly taken, the incident seriousness is evaluated, and the mode is switched from ordinal time to emergency situation.

Truth in Japanese organization still does not change when 'Truth of Failures'（Tobe, Nonaka, et.al.;）was written. - irrationality

Japanese organization should be described using by bounded rationality in 'Absurdity of Organization' (Kikusawa)

Destroying bounded rationality

'Establish the system admitting violation of order in emergency situation'.

The decision at on-site are given priority than other

Decision of continuation of sea water infusion

The problems as above can be explained by "Homogeneous way of thinking" and "Concentric Camaraderie", which are the hindrance on safety pursuit in Japan. 'Bottom-up decision making structure' connects to 'Absence of top management', and then becomes to 'Delay of decision making and Lack of understanding on valuing safety'. Due to the Japanese are excellent as noncommissioned officer, they often show their ability at emergency situation. But Japanese are short of management abilities, they often make heavy intervention or omission.

'Multilayered faction structure' makes 'Organization from Gesellschaft to Gemeinschaft', and then 'Adhesion and back-scratching' are spread in the organization. For the "Concentric Camaraderie", the feedback system in organization learning leads to the failure due to be preceded to internal logic than social common sense even in national government level or nuclear industry level.

7 Discussion

The "Privatization by National Policy" has been destroyed by large-scale disasters Fukushima Daiich nuclear power plants. Anyway, rare event has occurred on one occasion, measures had to be taken here after. National nuclear policies of many countries are being reexamined along with the safety evaluation. Safety design principle is "Defense in Depth" concept, which should be further reconsidered reflecting the accident causes. Usual systems focus on the forefront function, such as preventing damage, expansion mitigation, or incident prevention, while safety critical systems increases attention to back-up functions such as incident expansion mitigation or environmental effects mitigation, if it has a large enough impact on the environment. Common Mode Failure of External Initiating Event such as Earthquake or Tsunami, which is usually Rare Event, or auxiliary systems failure such as Off-site Power, EDG, Buttery, or Sea Water Cooling loss was difficult to install to Defense in Depth design, while it should be.

Rare Event is high consequence with low frequency. Low consequence with high frequency event is easy to treat by commercial reason, while it is very difficult to handle the rare event even the risk is just the same. "Unexpected event" has been used frequently, but it is the risk-benefit issues to assume or not. Tsunami Probabilistic Risk Analysis has been carried out, and safety related personnel knew the magnitude of the effect well.

Regardless of the initiating event, lack of measures to "Station blackout" is to be asked. According to the "Defense in Depth" concept reflecting Fukushima accident, we should consider three level safety functions; usual normal system, usual safety system, and newly installed emergency system including external support functions. Anyway the diversity is significantly required for not only future reactor concept but also existing plant back-fit activities.

Swiss Cheese Model proposed by Reason, J indicates operational problem other than design problem [2]. Fallacy of the defense in depth has frequently occurred recently because plant system is safe enough as operators becomes easily not to consider system safety. And then safety culture degradation would be happened, whose incident will easily become organizational accident. Such situation requires final barrier that is Crisis Management as shown in Fig.1.

Concept of "Soft Barrier" has been proposed here [3]. There are two types of safety barriers, one is Hard Barrier that is simply represented by Defense in Depth. The other is Soft Barrier, which maintains the hard barrier as expected condition, makes it perform as expected function. Even when the Hard Barrier does not perform its function, human activity to prevent hazardous effect and its support functions, such as manuals, rules, laws, organization, social system, etc. Soft Barrier can be further divided to two measures; one is "Software for design", such as Common mode failure treatment, Safety logic, Usability, etc. The other is "Humanware for operation", such as operator or maintenance personnel actions, Emergency Procedure, organization, management, Safety Culture, etc.

8 Conclusion

The good cases of resilience response are observed in individual base and organizational base as below.

- The effectiveness of insight on accident cases (inundation in Madras, 9.11 terrorism- B.5.b.) and of the risk evaluation.
  - Decision of continuation of sea water infusion (individual base)
- Reflection of the experience on Chuetsu-Oki Earthquake
  - Improvement of seismic building which is equipped emergency power source system and air conditioning system (organizational base)
  - Deployment of fire engines (organizational base)
- The effectiveness of command system in ordinal time (on-site of organizational base)
- Support by cooperation companies and manufacturers (designers and site workers of organizational base)

It is important to 'establish the feedback system on organization learning in ordinal time' And it means that it is important to establish the system admitting violation of order. The decision at on-site are given priority than other ones. The representative example is the decision of sea water infusion continuation which was given priority at on-site, even though the official residence and the main office TEPCO had ordered to stop the infusion.

The many failure cases are defined under national government level and nuclear industry level which are the problems of rare event awareness and of organization culture. The ordinal time training at on-site also work in emergency situation at the accident, while the level of administration department and government didn't work well.

- Risk misrecognition of Loss of offsite power and damage by Tsunami (national government level, industry level)
- Confusion of command system (organization base- between on-site and the main office of TEPCO)
- Confusion of command system (external correspondence base- national government level, and organization base- among official residence, regulation, and the main office of TEPCO)

Nuclear energy will play an important role from the necessity of mitigating climate change, as well as improve energy security. However, the Fukushima Daiichi Accident raised a new challenge of securing the safety of utilization. Following the safety design principle of "Defense in Depth", three level safety functions should be considered for the hardware. Those are, the usual normal system, usual safety system, and emergency system including external support function. On the other hand, software for design including common

mode failure treatment, safety logic, and usability should be improved together with the humanware for operation including personnel actions, emergency procedure, organization, management, and safety culture.

References

[1] TEPCO: 'Accident Analysis Report of Fukushima Nuclear Accident', 2012.6.
[2] Reason, J.: 'Managing the Risks of Organizational Accidents', Ashgate, 1997.
[3] Ujita, H.: 'Research on Error Management', Quality Assurance Study Group 2009 Annual Report, 2010.6 (in Japanese).
[4] Hollnagel, E.: Safety Culture, Safety Management, and Resilience Engineering, ATEC Aviation Safety Forum, 2009.11.
[5] Weick, K. E., Sutcliffe, K. M., 'Managing the Unexpected', Jossey-Bass, 2001.
[6] Lin, S.: 'Introduction of Risk Literacy- Lessons Learned from Incidents', NIKKEI-BP, 2005 (in Japanese).
[7] Tobe, Nonaka, et.al.; 'Truth of Failures', DIAMOND, 1984 (in Japanese).
[8] Kikusawa, K.: 'Absurdity of Organization', DIAMOND, 2000 (in Japanese).

Table 1. Accident model and Error model.

Accident Model	Error Model	Analysis Method	Measure
Domino (Failure Chain)	Human Error (Individual)	Cause-Consequence Link	Encapsulation, Seek & Destroy
Swiss Cheese (Diversity Loss)	System Error (Organization)	Risk Analysis	Defense & Barrier
Organizational Accident (Pitfalls of Defense in Depth)	Safety Culture Degradation	Safety Culture Check List	Monitor & Control on Organizational Culture

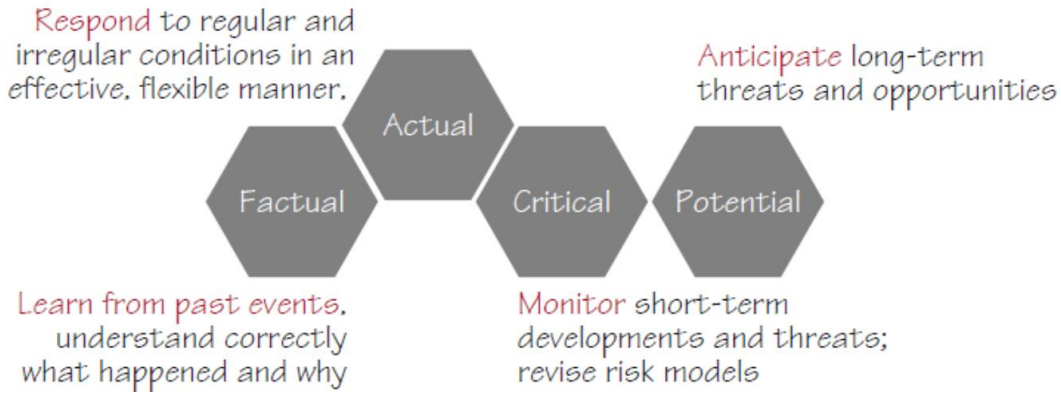

Fig.1. Resilience and safety management.

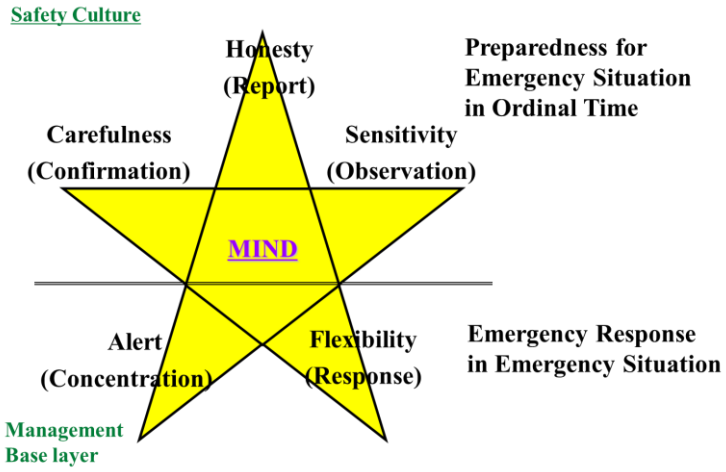

Fig.2. High Reliability Organization: Organizational Process.

Table 2. Evaluation of response capability from the viewpoint of risk literacy: The analysis of sea water infusion process on Fukushima Daiichi No.1.

Risk literacy / Analysis level	In Ordinal Time				In Emergency Situation		
	Analysis Power			Communication Power		Practical Power	
	Collection Power	Comprehensive Power	Predictive Power	Information Transmission Power	Influence power	Crisis Response Power	Radical Measures Power
Individual	**•Damage of Tsunami**	**•Risk recognition of Tsunami damage**	**•Risk recognition of Power Loss**	—	—	**• Continuation of Sea water infusion**	**• Training for emergency**
	・Collection of accidents: ・Jyogan-Tsunami	・Earthquake ・Tsunami ・Evaluation of influence range by PSA	Recognition of accidents damage	**•Information sharing at on-site**	**•Command system (on-site)** •Centralized at seismic building *•Contact between Control Room & Emergency Response Room*	**•Infusion of fresh water and sea water** •Vent •Prevention of damage expantion	**•Preparation of seismic building and fire engines** **•Command system** •AM measures
	•Collection of accident •Jyogan-Tsunami •JNES Tsunami PSA •Infusion at Le Blayais & Madras	*•Risk misrecognition of Tsunami damage*	*•Risk misrecognition of Power Loss*	*•Information sharing between main office and on-site*	•TV conference system (2F site) *•Confusion in command system between main office and on-site*		•Review the education and training system
External correspondence (official residence, etc.)	•Anti- terrorism in overseas •Collection of example : 9.11 terrorism- B.5.b.	•Classification of importance on accidents *•Risk misrecognition of earthquake and Tsunami*	•Importance of external events *•Risk misrecognition of infrastructure damage*		*•Media, local government, publicity to overseas* *•Confusion in command system among official residence, main office, & on-site*		**•Support by vendor and cooperation company** **•Support by external organizations** *•Drastic measures : Structure reform (Regulation/ Electric power company)*

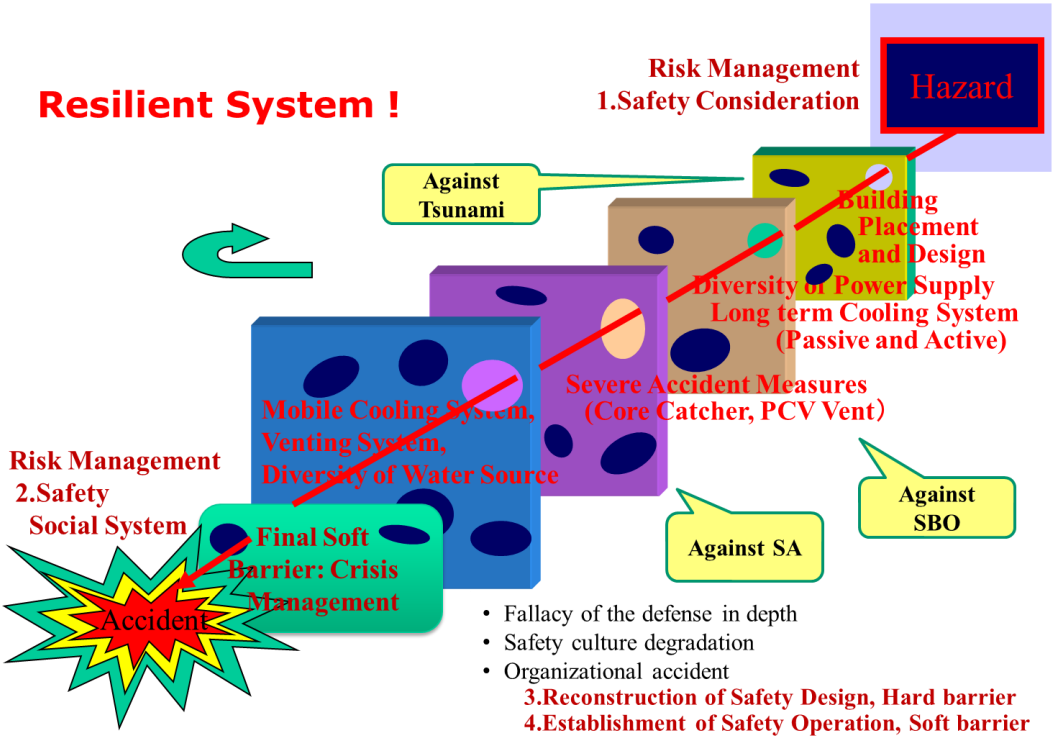

Fig. 3. Defense in Depth and new safety concept.