JESK J Ergon Soc Korea 2018; 37(3): 301-315
http://dx.doi.org/10.5143/JESK.2018.37.3.301
http://jesk.or.kr eISSN:2093-8462

Analysis of Fukushima Accident in Resilience Engineering Perspective Using the FRAM (Functional Resonance Analysis Method)

Dong Yeon Lee, Hyun-Chul Lee

Korea Atomic Energy Research Institute, 34057

Corresponding Author
Dong Yeon Lee
Korea Atomic Energy Research Institute, 34057
Mobile : +82-10-3075-2218
Email : ldy15@kaeri.re.kr

Received : May 04, 2018
Revised : May 09, 2018
Accepted : June 01, 2018

Objective: The aim of this study is to investigate the combination of function variability that has affected the development of the Fukushima accident and to identify potential risks of the emergency response system that directly related the Fukushima accident using the functional resonance analysis method.

Background: From a traditional perspective (safety-1), safety management is implemented in a way that finds and solves the direct cause of the accident. In the Resilience engineering (safety-2), perspective, accidents or adverse outcomes are considered to emergent from the variability of performance rather than a linear causal relationship. The FRAM is a method of modeling system functions and finding potential risks in the system.

Method: This study used the FRAM to analyze the accident response of the Fukushima case. In order to identify the accident response system of the Fukushima, we investigated the existing Fukushima accident reports and analyzed the nuclear power plant structure report. Based on these results, we modeled the accident response system of Fukushima accident. Through the FRAM model, we analyzed the variability of the system functions and identified the risks that the combinations of variability might cause.

Results: Through the retrospective analysis, we identified the effect of the combinations of variability of system functions on the accident development process. In this study, we present two instantiations. In addition, we conducted the prospective analysis to identify the potential risks of accident response system of the Fukushima that were not reported in actual Fukushima accident.

Conclusion: This study suggested that how the variability of the functions of system connected and contributed to the expansion of the accident. The FRAM can be used to reduce the risk of system-wide hazards through analyzing the combination of variability of system functions, identifying the potential risks related to safety.

Application: The FRAM will be a systematic method of analysis for in-depth risk management.

Keywords: Resilience engineering, Safety-2, FRAM, Fukushima accident, Accident investigation method

1. Introduction

1.1 Research background

1.1.1 Fukushima nuclear power plant accident

The Fukushima nuclear accident was a disaster due to the Great East Japan Earthquake and the following tsunami. On March 11, 2011, an earthquake and tsunami hit the northern Tohoku region of Japan. As a result, Fukushima Dai-ichi Nuclear Power Plants located on the adjacent shore in the epicenter were directly affected. Immediately after the earthquake, the active reactors automatically shut down their sustained fission reactions. Just after earthquake, tsunami reached a height of approximately 15 meters, then all of the six reactor buildings were flooded to 4~5 meters in height from Units 1 to 3, as well as Units 4 to 6, which were undergoing regular inspections. Then Fukushima NPP lost all electrical power. As a result, core meltdown and hydrogen explosion damaged the reactor containment vessel, causing a large amount of radioactivity to leak. This accident was ultimately declared a Level 7 "Severe Accident" by the International Nuclear Event Scale (INES).

The Fukushima nuclear power plant was prepared for existing types of incidents, but the loss of all ac and dc power due to the earthquake and tsunami was beyond the anticipated range of accident. Immediately after the earthquake, all reactors automatically shut down as designed, but the reactor cooling functions that remove residual heat from core could not work properly due to the loss of all electric power in plant. However, the tsunami disabled the alternative power source such as emergency diesel driven generators that would have provided power to control and operate the coolant systems. Loss of cooling and the difficulty of using alternative safety functions have directly contributed to nuclear meltdown and the release of radioactivity.

In addition to the problem of these plant safety facilities, there have been many problems in the incident response process of Tokyo Electric Power Company (TEPCO) and Japanese government agencies. When the accident occurred, the chairman and president of TEPCO were both absent, so critical decision making on the emergency response was delayed. Furthermore, there are a lot of confusions in emergency response order because communication between the plant site and the emergency response center (ERC) was not smooth.

The Japanese government has also failed to carry out its role of gathering accident-related information and providing it as a basis for emergency decision making. They took a passive posture and failed to issue evacuation orders for residence. That is, the government was not able to deal with the accident adequately. Moreover, several factors such as the intervention of the Prime Minister were appeared in human and organizational response process.

1.1.2 Traditional safety approach

The goal of most existing research of system safety and accident model was to identify the relevance of human errors to safety accidents and to analyze the nature, pathways, and causes of those accidents or failures (Reason, 1990). With this approach, researches have been conducted in various methods from various perspectives. These studies on human errors and accident models have contributed to the reduction of human errors and interpretation of safety. However, such findings reveal many limitations in modern large-scale system environments that are dominated by complexity and uncertainty (Hollnagel and Goteman, 2004).

Representative limitations include the simplification of accident analysis due to linear causal relationship, insufficient consideration about contextual information in analysis of error/accident, the expertise required for error analysis, and difficulty of risk prediction in unstructured work situations (Ham, 2011).

In traditional approach, safety is defined as the absence of accidents and incidents or as an acceptable level of risk. In this perspective, which is termed Safety-I, safety is considered to be a state where as few things as possible go wrong. According to Safety-I, things go wrong due to technical, human and organizational causes, that is failures and malfunctions. The safety management principle is to respond when accident occurs or unacceptable risk recognized. Accordingly, the purpose of accident investigation is to identify the causes and contributory factors of adverse outcomes. These approaches then try to eliminate causes or improve barriers or both (Hollnagel and Goteman, 2004). New types of accidents have similarly been accounted for by introducing new types of causes relating to technological, human, or organization. Safety efforts focus on what goes wrong, and this focus is reinforced in many ways. Numerous models try to figure out how things go wrong and a considerable number of methods are offered to identify and address the causes. The general solution is known as 'find and fix': look for failures and malfunctions, try to find their causes, and then eliminate causes and/or improve barriers. Few audits and surveys may include a focus on strengths. However, on the whole, models, methodologies, and data are much less compared to finding the things go wrong (Hollnagel and Goteman, 2004).

In summary, safety can be defined as a reduced number of negative events from a traditional perspective. A negative outcome is caused by a system failure or malfunction. Accidents or incidents are considered to have a specific root cause. Thus, the purpose of traditional safety management is to find the root cause of the accident, and to eliminate it, or to prepare countermeasures.

1.1.3 Resilience engineering

The resilience engineering is new perspective of safety, which is termed Safety-2. Resilience engineering focuses on how systems or humans adapt to environmental changes in order to maintain a stable system state (Costella et al., 2009). In this perspective, the success of a system refers to a state in which risk is anticipated and prevented in advance, so that the system is continuously under control to avoid risky state. Resilience engineering also emphasizes the ability of the system to quickly recovery its original state, when the system failure or risk occurs. Thus, system resilience can be defined as the ability to anticipate and prevent system failures or risks and to respond effectively to the original state when the negative events occur.

In perspective of resilience engineering, variability in performance of individuals or organizations is inevitable. In modern complex systems, it is impossible to predict all conditions at all. Therefore, an individual or an organization must respond momentarily and adaptively to internal and external situational changes. In this case, due to complexity and time constraints, the response strategy may not be perfect. Thus, the response to the environment may succeed, but it may fail. In other words, the variability of performance is inevitable.

In other words, resilience engineering proposes that all outcomes whether negative or positive are due to the variability of performance, whether individual or collective. In other words, positive and negative outcomes happen in the same way. That is, both failures and normal performance may be either successful of unsuccessful depending on variability of everyday performance. Thus individual or organization should adjust their daily performance to the current condition so that they can adapt to changes in environments or situations that are not predefined. In other words, it is necessary to adjust performance according to the current condition rather than preparing for specific causes. Outcomes are emergent rather than resultant that based on cause-effect relationship.

The concept of resilience engineering provides requirements for the methodology to overcome the limitations of traditional accident analysis. In particular, the fact that the origins of success and failure of performance are the same raises the need to systematically understand this variability and to analyze accidents and risks based on this systematic understanding.

Modern complex systems, such as Socio-technical system can be defined as composed of a number of subsystems, which may

include multiple functions. Although the technical and human system components are designed to function in a reliable and predictable way, performance always has variability to a smaller or larger extent (Hollnagel and Goteman 2004). The risk of these large-scale complex systems can be 'emergent' by a combination of variability of multiple functions. Traditional approaches to safety have limitations in analyzing these risks in large-scale complex systems.

1.1.4 FRAM (Functional Resonance Analysis Method)

The Functional Resonance Analysis Method is developed by Erik Hollnagel (Hollnagel, 2004), which models non-linear interactions of system functions to understand and predict the emergent process in which an accident occurs. FRAM analyze the potential risks that may arise from the functional resonance such as combination of variability. FRAM describes system failures or adverse events as the outcome of a functional resonance arising from the variability of everyday performance (Hollnagel, 2013).

Resonance is defined in physics as an increase in amplitude of oscillation of an electric or mechanical system exposed to a periodic force whose frequency is equal or very close to the natural undamped frequency of the system (Hollnagel and Goteman, 2004). The resonance principle is applied to explain how asymmetric huge effects may come from small or insignificant variations, and the emphasis is on dynamic dependencies rather than failure probabilities.

Functional resonance in FRAM is the concept that explains the process of developing weak variability of various signals that are not easily detectable, (but which are implicit in the adverse outcome,) as a signal of a detectable event through unintended interactions.

As mentioned earlier, complex socio-technical systems consist of many subsystems and include various components and functions. Some safety accidents may be explained by a failure of the technical element of the system or system function, but in many cases it is not possible. In most cases, accidents occur when the interactions between system components are made in a way that is unpredictable due to performance variability. The variability of small components or functions can be combined at a particular point in time to produce disproportionately large effects, and this phenomenon of combining functions in the system can be called functional resonance. Functional resonance does not provide the definitive explanation of why accident happened, but it can serve as a useful analogy to think about accidents and understand how large effect can occur (Hollnagel and Goteman, 2004). In summary, Functional resonance means that each function in the system is combined in an unexpected way at an unexpected point, resulting in outcomes.

In conclusion, the outcome of the event occurs in a way that is difficult to explain by the principle of linear causality, especially in modern, large and complex systems, such as socio-technical systems. A socio-technical system consists of numerous functions, and these functions are connected complexly and can affect each other. Therefore, even if small variability occurred in each function, it can be expanded to critical consequence that is unpredictable in the process of combining and propagating the variability at a specific point in time. Although there are simple cases in which the linear causal relationship can be grasped in the system, but it is impossible to anticipate and prepare for every situation. Therefore, there is a need for a method to identify potential risks for unexpected events in addition to existing prescriptive safety management.

1.2 The purpose of the research

After the Fukushima accident, number of reports around the world has analyzed the cause of the Fukushima accident. Most studies examined the reason why the safety system associated with Fukushima nuclear power plant did not respond effectively to the accident. As a result, there have been many improvements in terms of preparation for safety in the nuclear power plant all over the world.

However, it is practically impossible to anticipate all possible situations and prepare for that in terms of the design. Furthermore, it is difficult to identify potential risks that may arise during the accident response process by using a linear analysis of casual relationships. This is related to the fact that nuclear power plants are the large scale complex systems mentioned above. Nuclear power plants are made up of diverse systems, which are largely automated and incorporate in-depth defense concepts for safety. However, minor human errors of operator may lead to accident or breakdown of system. Major accident of the past, such as TMI and Chernobyl accidents were cases that have developed in unexpected ways, leading to severe accident.

Therefore, it is necessary to analyze not only the cause of a specific accident, but also the potential risks that may arise in the system's accident response process. The FRAM is a method of analyzing and modeling all the functions of the whole system to understand the variability and combination of each function. Through analysis of this variability and combination, FRAM can serve as analytical methods to identify potential risks in the system. FRAM can be used either to analyze existing accident cases or to identify potential risks of the future system. Retrospective analysis, the method of analyzing past events is similar to the traditional root cause analysis, but it can identify various factors that affected the progress of the accident unlike the simple analysis. Prospective analysis is the method used like a risk assessment to analyze the potential risks that may arise in the future system.

The purpose of this study was, using the FRAM, to investigate the combination of function variability that has affected the development of the Fukushima accident and to identify potential risks of the emergency response system that directly related the Fukushima accident.

2. Method

Two ergonomic experts, one nuclear power plant driving expert, and one psychology expert participated in FRAM modeling of the Fukushima accident response system.

2.1 FRAM steps

The FRAM is typically done in four steps. The first step is to identify the essential functions of the system and to characterize these functions into six aspects. The second step is to characterize the variability of the functions that constitute the FRAM model. This step should address the situation-dependent performance variability. The third step is to identify possible functional resonances based on dependencies and relationships between system functions. Since each function in FRAM is characterized in six aspects, each function is connected and interacted in various ways. An instantiation represents a concrete instance of the model for given (actual or assumed) situations and sets of conditions. The details provided by the instantiation makes it possible to identify precisely about whether and how the potential variability can come about. The final step is to develop measures and requirements to monitor variability that can pose a threat to safety, and to provide countermeasures or barriers to deal with them.

2.2 Identify and describe the functions

The first step of FRAM is to identify and define all relevant functions of the system. Once the purpose of the modeling has been determined, the system functions have to be identified. There is no specific method in the function identification and definition phase. Any analytical method which identify the functions of the system can be used. Established work analysis techniques such as Hierarchical Task Analysis (HTA) or Work Domain Analysis (WDA) can also be used in this step. It is not necessary to grasp the hierarchy of functions, but it is essential to identify and connect every function of the system. Hollnagel (2013) recommends starting with the task analysis or official documents of the relevant organization (e.g., procedure) for the identification of the functions. The information collected in this way needs to be reviewed by domain experts. To ensure the quality of the FRAM model, the process of function identification is very important.

After the function identification, each function can be defined in terms of six aspects: Input, Output, Precondition, Resource, Time, and Control. Each aspect defined by Hollnagel (2013) is as follows.

- Inputs (I), which are needed to perform the function. Inputs constitute the links to previous functions and can be either transformed or used by the function in order to produce the outputs.
- Outputs (O), that are produced by the function. Outputs constitute the links to subsequent functions.
- Resources (R), representing what is needed by the function to process the input (in terms of, e.g., hardware, procedures, software, energy, manpower).
- Controls (C), or constraints, that serve to supervise or restrict the function (to monitor it and adjusts it when it goes astray). Controls can be active functions or just plans, procedures and guidelines.
- Preconditions (P), which are system conditions that must be fulfilled before a function can be carried out. A common precondition is that another step or process has been completed or that a specific system condition has been established.
- Time (T), which can also be considered a special kind of resource. All processes take place in time and are governed by time. Time can also be a constraint in the sense that there is a time window for an activity (a duration).

The first phase of this study was identifying and defining all functions relevant to Fukushima accident. In principle, it is necessary to identify and connect all functions of the whole system for FRAM analysis. However, due to the limitations of the information gathering process, it was impossible to grasp all the functions of Fukushima Power Plant, TEPCO, and Japanese government agencies. Thus, in this study, we referred to the existing report on the structure of nuclear power plants to identify the safety functions of the power plant. Then we investigated and defined the functions directly related to the development of Fukushima accident such as Core cooling, Limit pressure rise functions through reviewing existing Fukushima accident reports. Also, we investigated and analyzed emergency response functions of the TEPCO, the government, and the prime minister by refer to the report of the National Assembly of Japan.

The identification of the safety function of Fukushima power plant was conducted based on technical report of the Korea Atomic Energy Research Institute (KAERI): Function Analysis of Nuclear Power Plants for developing of Man-Machine Interface System for Korean Next Generation Reactor (KAERI, 1995). Although the type of reactor analyzed in this report was a PWR structure, which is different from the BWR type Fukushima power plant, there is no significant difference in core cooling and power system. Since it was impossible to grasp the entire system structure of the Fukushima NPP, we used this report to identify and connect the safety functions of nuclear power plant. This analysis and subsequent modeling steps were carried out with the help of an experienced operator of nuclear power plant. TEPCO and the Japanese government, and the Prime Minister's accident response functions are identified by reviewing the relevant reports such as the official report of the Fukushima nuclear accident independent investigation commission, and the Fukushima Daiichi accident report of IAEA (The National Diet of Japan, 2012; INPO, 2012; Lipscy et al., 2013; Amano, 2015; EPRI, 2015).

2.3 Modeling

The second step of study was to model the accident response functions associated with the Fukushima accident by linking the functions identified in the previous step. Six aspects of each function can be represented in a graphical form using a hexagon module as shown in Figure 1. While the identification of each function and its variability is mostly involved in a table format, the FRAM model can also be represented in a graphic format for easy understanding (Frost and Mo, 2014). The modeling process expresses each function as a hexagonal module, and links the related aspects with lines. In this process, we used the FRAM Modeling Visualizer (FMV) which developed by Erik Hollnagel. Once the label and six aspects of each function are entered into the software, FMV renders it graphically. Also, the variability data of each function can be noted.

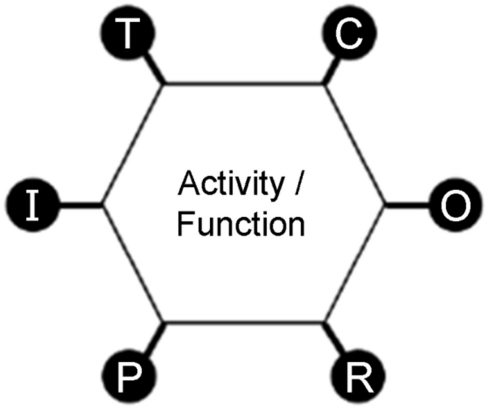

Figure 1. FRAM function module

2.4 Identification of variability

The third step is to identify the variability of each function in FRAM model. The FRAM model describes the possible couplings between functions, and is therefore also the basis for describing the potential variability of functions (Hollnagel, 2012). In this step, the factors that may cause the variability of each function itself and the variability of output of each function are identified. One of two ways can be used to determine the variability of the output. First, a simple way is to examine the possibility of the variability of output in terms of time and accuracy. This solution defines how the output of the function can be varied according to two criteria. The elaborate way is to use failure mode to determine how the output of the function can be varied in terms of Timing, Duration, Sequence, Object, Force, Direction, Speed, Distance, and so on. In this study, we analyzed the variability of the output of each function using failure mode.

For example, if 'the evacuate residents function' is analyzed using the failure mode, one of the criteria of failure mode, timing, can be the starting point. In case of too early in terms of timing, it can cause anxiety of residents, but it does not cause any negative result in terms of safety. However, if 'the evacuate residents function' is actuated too late or omitted, safety-related negative consequences may occur and therefore this function can be considered to have negative variability. In the case of sequence criteria, repetition or intrusion may cause confusion in the evacuation of residents. Thus, this also has negative variability. In addition, there may be variability in terms of Direction and Distance. The criteria of Duration, Object, Force, and Speed are not relevant for analysis of this function's variability.

In this way, by analyzing all functions, the variability that can appear in each function can be grasped and predicted.

2.5 Aggregation of variability

The final step is to analyze the potential risk that may arise from the combination of variability through aggregating the variability of each function of the FRAM model. In other words, this step is to determine how performance variability combines and to figure out how to create non-linear outcomes. As mentioned earlier, the retrospective analysis can be used to examine the evolving process of performance variability into a risk in particular time point.

In this study, the variability of each function of Fukushima FRAM model was integrated to figure out the resonance between system functions that appeared in the accident response of Fukushima case. That is, we identify the instantiations where the

variability of the functions combined and had a negative effect on the accident response.

For example, as a result of modeling in this study, the supply AC power function was connected to resources aspect of safety function such as steam release, core cooling, and monitoring plant status. The supply AC power function may exhibit variability in terms of timing. The technological function has little variability except for a complete failure of malfunction. However, this function was totally lost due to natural disaster in the Fukushima accident. Thus, the output of the supply AC power function is subject to variability (omission). On the other hand, variability has also occurred in the function of emergency response of operators/workers. Due to the trouble in using the plant monitoring function and delays in on-site command, it failed to function normally, and the variability in the aspect of timing, object, and sequence occurred.

The core cooling function which associated with these two functions was influenced by the combination of the variability of the two functions. With the loss of AC power, the main cooling function was not working properly. Also, the emergency response of the operator was delayed. So, it was impossible to respond appropriately to rapid change of situation. This series of processes has severely damaged the safety of nuclear reactors and containment vessels, the ultimate purpose of safety functions.

We also examined the potential risks that did not occur in the actual case through the FRAM model. Assuming that the variability occurs simultaneously in the number of functions and combining the possible consequences of the variability, it is possible to anticipate what risks might occur. This analysis shows how to use the FRAM model as a prospective analysis. Analysis and aggregation of variability steps were conducted through discussion of researchers.

3. Results

Figure 2 illustrated the FRAM model of Fukushima NPP accident. The model shows 27 functions for accident response of Fukushima NPP and TEPCO and Government.

The Fukushima power plant lost its existing cooling function due to power loss, which affected the containment condition maintenance function. Eventually, this caused damage to the containment vessel and radiation leakage. The FRAM model on Fukushima in Figure 2 connects from the power supply function to containment vessel maintenance function, and includes other functions directly related to Fukushima accident.

In addition, the FRAM model of this study includes functions such as ERC operation, report of field situation, emergency response decision making, and communicate with cooperating institutions as to response functions of TEPCO.

Finally, the model includes functions such as determining response strategies, field situational understanding, press announcement, and make evacuation order at the government level.

3.1 Retrospective analysis

Retrospective analysis on Fukushima accident was conducted using FRAM model.

3.1.1 Instantiation 1

In the FRAM analysis, functions are classified into three types: Technological function, human function, organizational function. In principle, the technological function is considered to have little variability unless it is completely failed. However, in the Fukushima case, the variability of AC and DC power supply function was affected by earthquake and tsunami (Force-Omission). The power

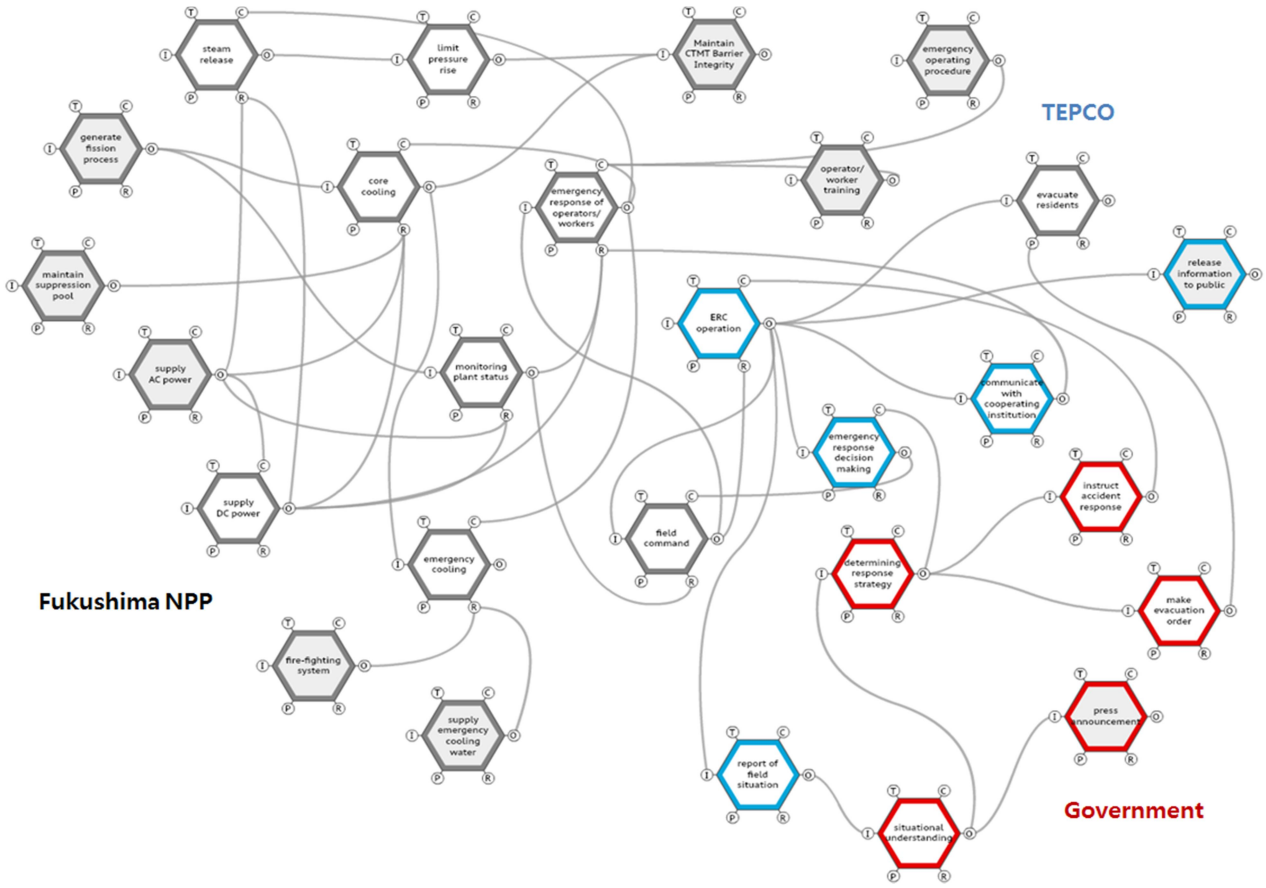

Figure 2. FRAM model on Fukushima NPP accident

supply function affects almost functions of the power plant. In the FRAM model of this study, steam release function, core cooling function, and monitoring plant status function were directly affected, and thus most function of them were lost. Loss of the cooling and limiting pressure functions affected the function of maintain Containment Vessel (CTMT) barrier integrity. Loss of major functions for maintenance of reactor temperature has led to situations that alternative methods such as emergency core cooling using a fire pump are needed. In addition, the loss of plant monitoring functionality has also affected operator and worker emergency responses.

However, the variability of the emergency response of operators/workers function also occurred. The loss of most safety functions due to earthquakes and tsunamis was unpredictable. Thus, the response personnel were unable to respond as predefined and trained. The delay of the operation of ERC (Timing: Too late), and confusion of decision-making of the response strategies (Sequence: repetition), unavailability of plant monitoring features (Force: Too little) have combined and made it difficult for the operators to properly respond to emergency (Timing: too late / Force: too little / Object: wrong object). The response personnel were not able to quickly identify what response was needed and the emergency response function was not properly performed. This variability coupled with the variability of the loss of AC/DC power supply functions, and then it has severely damaged major safety maintenance functions.

In addition, the emergency cooling function itself also had variability. The diesel-driven emergency generator could not be used

due to the tsunami, and other emergency power vehicles and fire pumps were also not available due to tsunami debris. The variability of the regular safety functions of the plant combined with the variability of emergency safety functions resulted in damage to the containment vessel. Thereafter, reactor overheat and hydrogen explosion occurred. Finally, radiation leakage occurred (The National Diet of Japan, 2012; INPO, 2012; EPRI, 2015).

3.1.2 Instantiation 2

At the time of the Fukushima accident, although there was a predefined reporting route between the site - TEPCO headquarters - government, the Prime Minister directly intervened in the incident response process, and caused various problems. The Prime Minister asked for a direct report of the accident, thus the variability of report of field situation function of the TEPCO has occurred (sequence: repetition). Because of this, communication about the accident situation of site was too late (timing: too late), and the same contents had to be repeatedly reported to various higher agencies. (sequence: repetition) In other words, efficient communication between responsible organization was difficult. Therefore, the government was not able to quickly grasp the situation in the site and functions of government response (e.g., situational understanding, determining response strategy) also had variability, for instance, to instruct that did not fit the field judgement (object: wrong object, sequence: intrusion).

Decisions of evacuation area also lacked evidence and planning reviews. In this situation, the evacuation order was not systematically issued and the Prime Minister also issued evacuation orders without discussing with government agencies. This has caused confusion in the evacuation of residents. Indeed, some residents have evacuated to dangerous areas.

Due to the negative variability in the functions of government's response strategy decision, emergency response decision of TEPCO was also delayed (timing: too late), which delayed the activation of ERC and caused confusion in the field command. Consequently, TEPCO, the government, and the Prime Minister did not help on-site response, but rather caused confusion. As a result, the response personnel in the field were not able to respond quickly and appropriately (The National Diet of Japan, 2012).

3.2 Prospective analysis

In this study, the FRAM model was used to identify the potential risks of existing systems that were not reported in actual Fukushima accident. The analysis of the potential risks was based on the knowledge and experience of the researchers about the development process of the existing nuclear accident and malfunction cases. In most cases of the major severe accident and domestic nuclear accident or breakdown, the main cause of accident starts with small malfunctions or human errors.

The combinations of small variability not always lead to major accidents. Defects of mutually unrelated functions are not solely risky and are simply resolved. The combination of mutually unrelated functions can be solved simply without developing into a great risk.

Based on the experience of the analyst with the accident and malfunction in the nuclear domain, it is possible to infer the possibility that the combination of function variability can be a potential risk to the system. In particular, it is easy to identify combinations of variability with the potential to lead to greater risk using the FRAM model which links all of the system functions.

3.2.1 Instantiation 1

Figure 3 illustrates instantiation 1. First, if the operator and worker training function is not properly performed, it may be difficult for workers to accurately understand the state of the systems of the power plant during maintenance work. Meanwhile, there may be situations where it is impossible to grasp some status of power plants, due to a partial failure of the plant monitoring instrument.

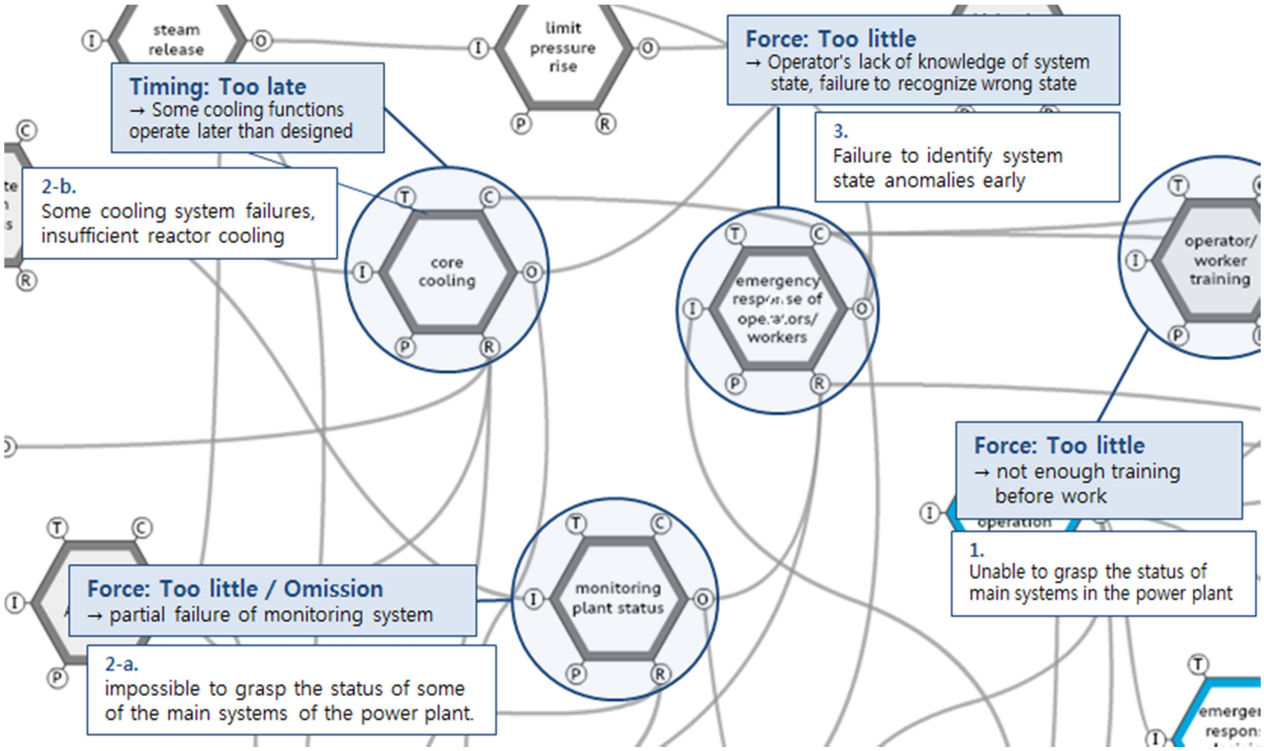

Figure 3. Instantiation of prospective analysis 1

Finally, a small failure in one component of the cooling system can cause a situation that requires maintenance. These small variabilities are not a big problem per se. But if they occur at the same time and these variabilities are combined, they can produce significant negative outcomes. Even if these variabilities are combined, the occurrence of a specific accident cannot be predicted. Because it is a potential risk rather than a particular cause. Nevertheless, if the system can handle each of these variability, the potential risk of this combination of variability can be eliminated or minimized.

3.2.2 Instantiation 2

It can be assumed what the situation would be like through the FRAM model if the variability in the Fukushima accident response process was positive. Figure 4 illustrate this instantiation. The emergency response center was operated immediately after the accident occurs, and the reporting system is up and running as quickly as is predefined. Therefore, the government can accurately understand the situation of the site and establish an appropriate strategy for the current situation. According to this strategy, the emergency response center command a consistent and systematic response order and site personnel can recover the suspended safety system or apply alternative safety function so that they prevent or delay the spread of accident until the cooperating agencies can help.

4. Discussion

The FRAM allows to analyze potential risks within complex socio-technical systems. In this study, we used FRAM to analyze how variability of functions of related systems in Fukushima accident contributed to the expansion of accident. As mentioned earlier, the FRAM analysis needs to identify and model all the functions related to the system. However, in this study, the FRAM model

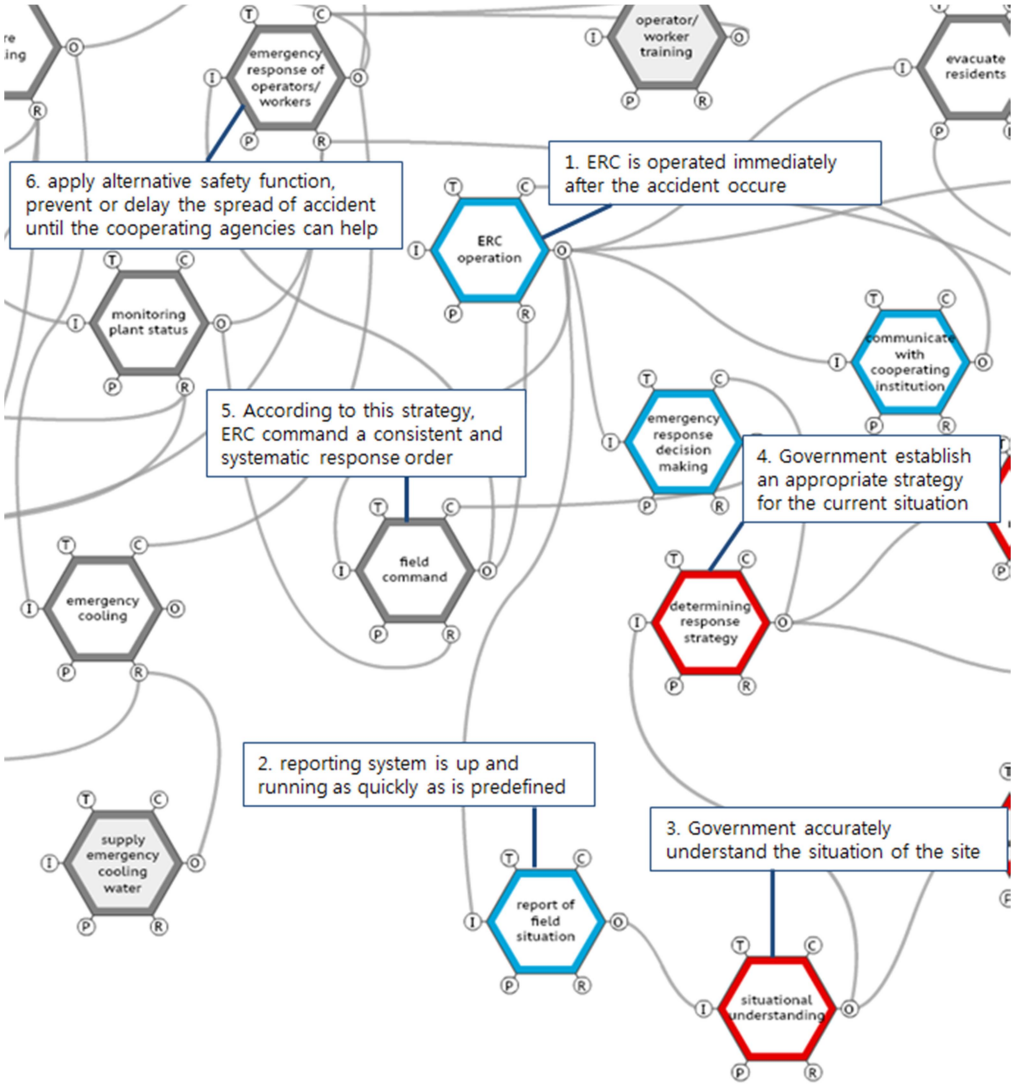

Figure 4. Instantiation of prospective analysis 2

was developed using only the functions directly related to the accident due to the limitation of the information gathering process.

For this reason, the retrospective analysis of this study was conducted in a similar way to the traditional linear accident analysis. Nevertheless, unlike the traditional linear analysis, the analysis using the FRAM model has the advantage that the effect of the combination of functions can be investigated explicitly. In traditional root cause analysis, the variability of functions without noticeable failure is easy to overlook in the analysis process.

Through analysis of human and organizational response function, it was found that the alternative incident response process was not smooth since the variability of technological function and human response function occurred at the same time. In fact, in the Fukushima accident, even when the safety systems and equipment that prepared for the nuclear power plant was not available, the judgment and effort of field workers and operators recovered some safety functions. Even if the plant safety system was disabled, it would have been possible to delay or prevent development of accident if the response commander, such as TEPCO or

government, gave prompt instructions.

In this study, in addition to retrospective analysis, we carried out prospective analysis using FRAM model. Through the FRAM model developed in this study, we were able to grasp other potential risks that did not occur in actual Fukushima accident case. The phenomenon assumed in the results such as 'insufficient worker training' or 'breakdown of small components of system' are frequently reported in Korean nuclear accident / failure cases in actual. It should be noted that when these variabilities occur separately, they only result in small failures but if they occur at the same time and coupled, it can have a disproportionately large negative impact.

We also proposed assumptions about what would happen if the variability in the accident case was positive. As mentioned earlier, we can't suggest that if we were able to deal with the variability that emerged from actual accident cases, we could have stopped the expansion of the Fukushima accident in certain. However, if the risk of each function's variability could be minimized, it would have been possible to respond more properly. In other words, by eliminating or mitigating the variability that may occur in each function, the potential risk of a combination of variability can be reduced.

In conclusion, this study analyzed Fukushima accident using FRAM. We identified the variability of various functions that had a negative impact on the development of the accident. Also, we analyzed other potential risks using the developed model. It seems obvious that mutually related functions can affect each other in the event or accident. However, in a complex socio-technical system, it may not be easy to identify the connection of each function. The socio-technical system consists of many subsystems, and each component can have multiple functions. FRAM model has the advantage of graphical representation that expresses complex connections between system functions explicitly. To develop FRAM model, all the functions of the system and the connections of all functions have to be identified. Graphical representations based on these analytical results help clarify connections with other functions that can affect one function.

The existing Fukushima accident analysis focused on analyzing the factors that directly affected the accident. Since the Fukushima accident, global nuclear safety management trends have investigated areas of vulnerability in the accident and prepared follow-up actions. This is consistent with the above-mentioned safety-1 perspective. Identifying risk factors directly related the accident and preparing countermeasures are also an important safety management. For instance: reinforcing barriers to prevent tsunami flooding, strengthening facilities to withstand earthquakes, or supplementing mobile facilities.

From the perspective of resilience engineering, besides strengthening existing preparedness, it is important to anticipate what is going to happen and to be flexible in coping with it. The FRAM can be used as a way to extensively anticipate the situation. The FRAM is a tool that helps identify potential risks that are not explicitly exposed. Addressing these potential risks is consistent with the resilience engineering perspective. From this perspective, small factors such as maintenance of the incident response organization, checking of the communication system, training of the operator, and substitution of each function of the system can be a critical factor.

The FRAM requires large amount of data for analyzing the system. The analysis and connection of all the functions of the system is very complex process. Therefore, it takes a long time to analyze and the expertise of the analyst is critical. For large-complex systems such as nuclear power plant, the analytical difficulty can be even greater. This study has been conducted through discussion of experienced nuclear power plant operator and ergonomics experts for analysis. However, since the FRAM is a subjective analysis method, the accuracy and reliability of the analysis still remain a limitation.

Although the FRAM can identify the variability of each function that can create a potential risk, the preparation or implementation of countermeasures is another matter. In some cases, it is possible to deal with the variability of a function in a simple way, in

other cases, difficult measures such as modifying system design may be necessary. In order to resolve the variability identified through FRAM, additional search for solutions should be carried out.

5. Conclusion

This study analyzed the response process of Fukushima accident by FRAM, and suggested that how the variability of the functions of the systems connected and contributed to the expansion of the accident. Unlike many of the existing studies that have examined specific causes, we analyzed the outcomes of the combined variability of each function. We also provided an analysis of the potential risks. It may be possible to reduce the risk of system-wide hazards through analyzing the combination of variability of system functions, identifying the potential risks related to safety, and providing mitigation measures to reduce or eliminate the variability of functions.

After the Fukushima accident, countries around the world are conducting the complement in various aspects to establish multidimensional safety. The FRAM will be a systematic method of analysis for in-depth risk management.

Acknowledgements

This research was supported by Nuclear R&D Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (Grant No. 2017M2A8A4017947).

References

Amano, Y., The Fukushima Daiichi accident. Vienna, Austria, IAEA, 2015.

Costella, F., Saurin, A., Guimaraes, B. and de, M., A method for assessing health and safety management systems from the resilience engineering perspective, *Safety Science*, 47, 1056-1067, 2009.

EPRI, Technical Report, Severe Nuclear Accidents: Lessons Learned for Instrumentation, Control and Human Factors, 2015.

Frost, B. and Mo, J., System Hazard Analysis of a Complex Socio-Technical System: The Functional Resonance Analysis Method in Hazard Identification, Australian System Safety Conference, Melbourne Australia, 28-30, 2014.

Ham, D.H., Research Trends of Cognitive Systems Engineering Approaches to Human Error and Accident Modelling in Complex Systems, *Journal of the Ergonomics Society of Korea*, 30, 41-53, 2011.

Hollnagel, E. and Goteman, O., The functional resonance accident model. *Cognitive System Engineering in Process Control*, 2004.

Hollnagel, E., FRAM: the Functional Resonance Analysis Method, ASHGATE, 2012.

Hollnagel, E. An Application of the Functional Resonance Analysis Method (FRAM) to Risk Assessment of Organisational Change, Swedish Radiation Safety Authority, 2013.

INPO, Special Report, Lessons Learned from the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station, 2012.

KAERI, Technical Report: Function Analysis of Nuclear Power Plants for developing of Man-Machine Interface System for Korean Next Generation Reactor, 1995.

Lipscy, P., Kushida, K. and Incerti, T., The Fukushima Disaster and Japan's Nuclear Plant Vulnerability in Comparative Perspective, *Environmental Science and Technology,* 47, 6082-6088, 2013.

Reason, J., Human Error, Cambridge University Press, New York, 1990.

The National Diet of Japan, The official report of The Fukushima Nuclear Accident Independent Investigation Commission, 2012.

Author listings

Dong Yeon Lee: ldy15@kaeri.re.kr
Highest degree: MA, Department of Psychology, Chung-Ang University
Position title: Researcher, Nuclear ICT Research Division, KAERI
Areas of interest: Human Factors, Industrial Psychology, Interface Design

Hyun-Chul Lee: leehc@kaeri.re.kr
Highest degree: Ph.D. Nuclear and Quantum Engineering, KAIST
Position title: Principal Researcher, Nuclear ICT Research Division, KAERI
Areas of interest: Human Factors, Systems Engineering, Security/Protection System