1. Introduction

After the TEPCO Fukushima Daiichi Nuclear Power Plant (1F) accident that occurred in March 2011, in Japan, regarding the safety improvement and the regulation for nuclear power plants, the utilization of risk information using the knowledge of Probabilistic Risk Assessment (PRA) has been promoted more than before [1-3]. Meanwhile, based on the lessons learned from the 1F accident, the scope of safety regulatory requirement was expanded from the level 3 (control of accidents within the design basis) of Defense in Depth (DiD) [4-5] to the level 4 (measure of severe accident), and measures related to the level 5 (off-site emergency response) were strengthened [6-10].

Nuclear facilities usually take multiple measures against various accidents, and it is unlikely that a single component failure or a single human error will lead to a large-scale accident. In the DiD level 4 and 5 accidents that exceed the design basis, it is assumed multiple component failures and/or multiple human operation failures occur simultaneously, and it is necessary to take measures considering such situations. As one of causes of such simultaneous occurrence failures, there is external event such as natural hazard, typically a large-scale earthquake. As an example of measures against such a situation, there is a measure against a severe accident at a nuclear fuel fabrication facility. In this accident scenario, it is assumed that simultaneous fires occur at multiple places in the facility due to an earthquake, and human operations greatly contribute to its accident measures [11].

In order to perform risk assessment for such accidents and measures, it is necessary to consider the feedbacks of the influences of human operations, etc. and the interactions among multiple events. However, since conventional PRA methods (Fault Tree Analysis (FTA), Event Tree Analysis (ETA) and Hazard and Operability Study (HAZOP), etc.) focus on individual component failures and individual human errors, these methods are insufficient for analysis considering such interactions including feedbacks.

In order to enable such analysis, the authors proposed introduction of the accident model [12], Systems Theoretic Accident Model and Process/System Theoretic Process Analysis (STAMP/STPA) method, based on the system theory proposed by Nancy G. Leveson [13-15]. The STAMP/STPA method is a hazard analysis method that is constructed based on the idea that an accident occurs when the interactions, specifically the necessary control instructions, among the *Elements* (Here, the "*Elements*" means components, operators, general public, organizations, regions and so on, that can constitute the system.) do not work properly, and this method is suitable for analyzing dynamic interactions and the feedbacks among the *Elements*. For this reason, this method is utilized a lot for the safety analysis and design of the system needing the complicated control in socio-technical systems such as the power grid and water distribution networks, and in the various industries such as the aviation industry, the shipping industry and so on [13, 16-19].

However, the analysis using the STAMP/STPA method is analyzed from the viewpoint of "control" among *Elements* constituting the entire system. Meanwhile, in the DiD level 4 and level 5, not only the malfunction of the controls but also the physical influences on the systems and/or components, should be major factors to be considered. Especially, in order to analyze influences of the simultaneous occurrence of multiple events, it is necessary to extend the relationship among systems and/or components to relationship concerning physical influences and substances movements and so on.

Meanwhile, the risk assessment at the DiD level 4 and level 5 requires information on the possibility of individual component failures and the magnitude of their impact. For this reason, it is necessary to provide a prescription that links the conventional PRA methods, which is good at such evaluation, with the STAMP/STPA method.

As an example of linking the conventional PRA methods and the STAMP/STPA method, a multi-layer model using the STAMP/STPA method has been studied [20, 21]. This study intends for evacuation of residents at the time of a nuclear accident and focuses on interaction between people and organizations through decision-making and actions. Meanwhile, the authors constructed a multi-layer model that focused

on feedbacks of the influences of human operation in a severe accident and on interactions among the *Elements* and created a procedure for the hazard analysis using this model [12].

2. Risk assessment model considering interaction including feedback

2.1 Issues of conventional methods and introduction of STAMP/STPA method

As mentioned above, since the conventional PRA methods focusing on individual component failures are based on the premise that individual components do not interact directly or indirectly [15], it is insufficient to take into account such interactions including feedbacks.

The STAMP/STPA method focuses on the relationship of controls (including information feedbacks) as shown in Fig.1, and enables analysis of the hazards of the target system and their causes while confirming the behavior of the entire system. Therefore, by introducing this method, it is possible to respond to the feedback to the event by human operations, which is one of the issues.

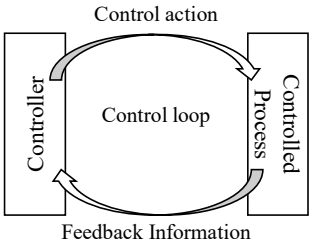

Fig. 1– Conceptual diagram of STAMP/STPA

On the other hand, considering the interactions related to the simultaneous occurrence of multiple events, it is considered that the STAMP/STPA method can be extended as follows.

- Regarding the relationship among components, humans, organizations, etc. of the analysis target system, the relationship of "acting side and affected side" of physical influence is considered in addition to the relationship of "controlling side and controlled side".
- The relationship of "moving source and moving destination" is considered when substances move among *Elements*.
- The analysis target system is extended from a single system related to "control" to a combination of a plurality of systems in which there is the above-described relationship.

2.2 Multi-layer construction

In order to link the conventional PRA methods and the STAMP/STPA method, the authors proposed a method that multi-layer was constructed associating a plurality of layers with each other [12]. These layers are constructed by analyzing the target systems from the viewpoint of each method.

Fig.2 shows an example of a multi-layer. Using the extended STAMP/STPA method described in 2.1, the first and second layer are respectively created from viewpoint of control and physical influences. Using conventional PRA methods, the third layer is created as a fault tree (FT) whose top event is accident of the facility. The information of events occurring on the *Element*s of the first and second layer is delivered to the third layer.

2.3 Outline and implementation procedure of risk assessment model considering interactions

2.3.1 Hazard analysis

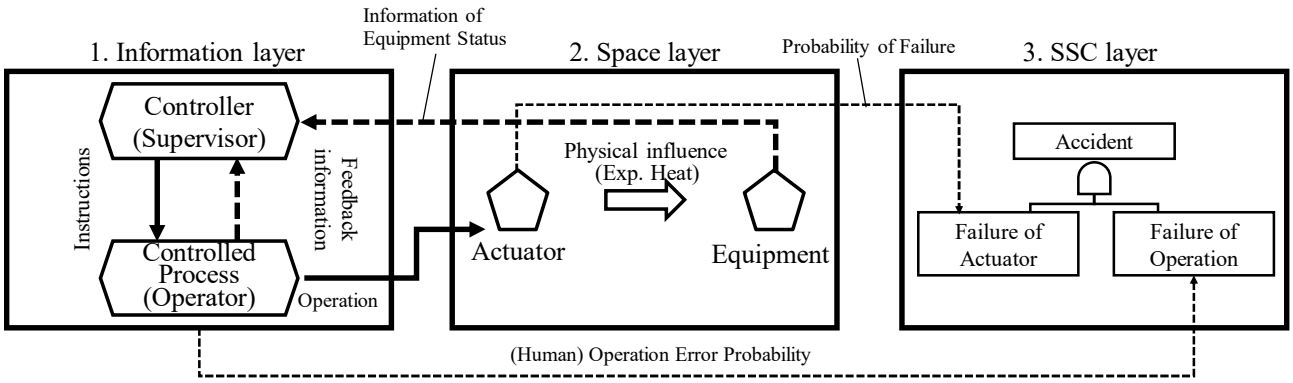

Fig. 2– Example of multi-layer

Fig. 3 shows the procedure for conducting a risk assessment using the multi-layer method. In STEP2 hazard analysis, conventional hazard analysis is performed (STEP2-1). The analysis results obtained in STEP2-1 are used for hazard analysis focusing on the entire system (STEP2-2). In STEP2-2, a multi-layer model is used in the following manner.

(A) Multi-layer construction

At first, the scope of the entire analysis target system is defined, and all the *Elements* constituting the entire system are extracted. Next, the attributes of these *Elements* are clarified from the viewpoint of the type of actions (control, transfer of instructions and information, physical influences, substances movements and so on.), and several layers are defined according to these attributes, and each *Element* is allocated on each layer according to the attribute. Furthermore, in each layer, the *Element* that gives the action and the *Element* that receives the action, are connected by a line (herein referred to as "*Line*"). In addition to these layers, the "Structures, Systems and Components (SSC)" layer is defined to systematize the event progression from the basic event to the facility accident using the conventional PRA methods. Finally, a multi-layer is constructed by associating these layers each other. Specifically, layers are associated by connecting *Elements* that are in different layers and are related to each other through the action.

(B) Hazard analysis of basic Loop

From each layer and the multi-layer, all the *Line* connections that constitute a basic loop starting from the *Element* causing accident (herein referred to as basic "*Loop*") and all the *Line* connections that do not constitute a *Loop* (herein referred to as "*Unclosed Line*"), are extracted. Here, *Loop* and *Unclosed Line* are referred to as "Event Progression Line (*EPL*)". Fig.4 shows an example of the *EPL* that constitutes *Loop*.

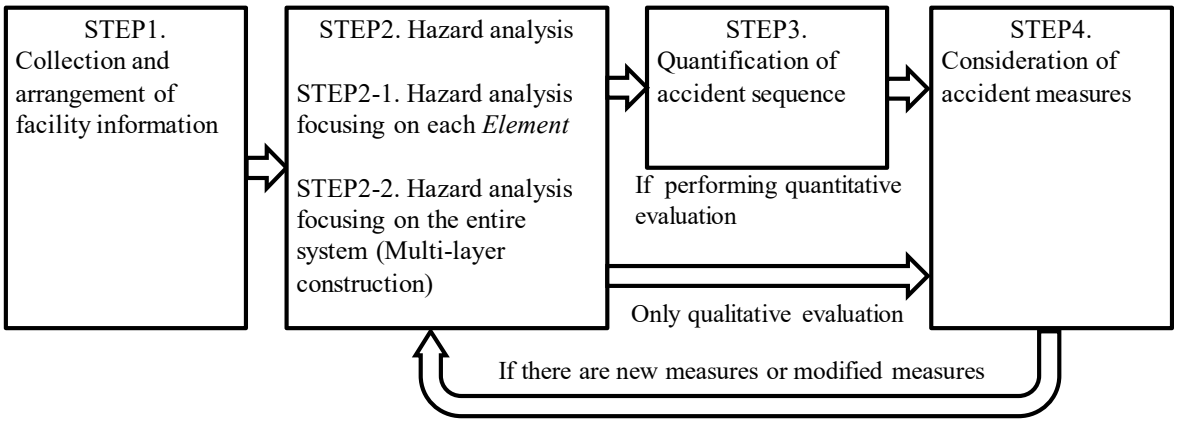

Fig. 3– The risk assessment procedure using the multi-layer method

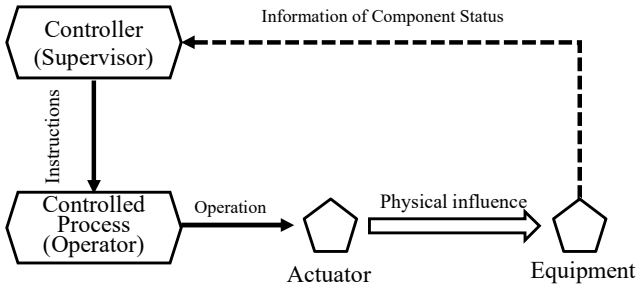

Fig. 4– Example of *EPL*

The *EPL* is an important unit when considering accident measures. For example, an *Unclosed Line* event does not receive feedbacks to end this event and does not take measures to prevent the expansion of the accidents and to mitigate the influence. Therefore, it is necessary to take measures to configure a *Loop*.

In this hazard analysis, the actions among the *Elements* of the *EPL* are focused on. Next, the unsafe actions (e.g., *Loop* breaks) leading to hazards, the causes of such unsafe actions and the hazards resulting from them are analyzed. At that time, the unsafe actions are extracted by using the guide words (See Table 2) of the STAMP/STPA method [13-15].

(C) Hazard analysis considering the interaction of multiple events

Among a plurality of *EPL*s, there may be a plurality of combinations of time steps depending on the timing of the interactions. Here, all possible time steps are extracted. If necessary, a plurality of multi-layers corresponding to the time steps are created. Hazard analysis is performed based on the created multi-layers in the same manner as in (B).

2.3.2 Quantification of accident sequence

If quantitative evaluation is performed, models for quantitative evaluation (for example: a fragility curve, a human reliability analysis model, etc.) are assigned to each *Element* on the layers created using the STAMP/STPA method. The evaluations of the influences of feedbacks and interactions are performed in these layers. The evaluation results are delivered to the SSC layer, and the calculation of the occurrence probability of the top event of FT is performed. However, the development of specific framework for the quantitative evaluation that dynamically integrates the quantification model of each *Element* will be a future issue.

2.3.3 Consideration of accident measures

Based on the above analysis results, the equipment, people, etc. to be introduced for accident measures are considered. At that time, focusing on the configuration of the *Loop*, if there are *EPLs* which do not constitute the *Loop*, introducing new *Elements* and actions are considered to prevent accidents, to prevent expansion of accident and to mitigate their influences. In addition, the *Lines* entering and exiting the *Element* are checked, the reliability and the type of the *Loop* and the magnitude of the load on each *Element* are grasped. If necessary, adding backup *Lines*, *Elements* and *Loops* are considered. When introducing new equipment and measures, the hazard analysis of STEP2 is performed again.

3. An example of implementation of risk assessment model considering interaction

In order to confirm the effectiveness of the risk assessment model that took into account the interactions shown in Chapter 2, hazard analysis is conducted assuming the simultaneous occurrence of two glove box (GB) fires caused by an earthquake in the process room at a hypothetical nuclear fuel fabrication facility. However, for simplicity, the operation of the equipment and the role of humans are assumed to be simple,

and the accident response procedure is also simple as follows. Fig.5 shows an overview of the equipment and personnel layout.

- A fire detector for the GB is installed near the GB. A fire detector detects a fire by heat.
- Information on the fire detected by the detector is sent to the supervisor waiting in the central monitoring room.
- The supervisor who recognizes the occurrence of a fire issues fire extinguishing instructions to the Accident Response Crews (ARCs) in the central monitoring room.
- The ARCs who have received instructions to extinguish fire go to the processing room via the access route. At that time, the ARCs report the situation to the supervisor and receives instructions from the supervisor.
- The ARCs who arrive at the processing room extinguish the fire with a fire extinguisher installed in the processing room.

In addition to the above measure procedure, the following conditions are added assuming that two GB (GB A and GB B) fired simultaneously due to the earthquake.

- GB A and GB B are in the same processing room and are relatively close to each other, but they must be accessed by different routes for fire extinguishing. These access routes are referred to as access route A and access route B, respectively.
- Fire detector A and fire detector B (both are temperature detectors) are installed near GB A and GB B, respectively.
- The supervisor who recognizes the occurrence of a fire issues an instruction to extinguish fire to ARCs A for GB A fire and to ARCs B for GB B fire.
- ARCs A and ARCs B who have been instructed to extinguish fire go to the processing room through access route A and access route B, respectively.
- ARCs A and ARCs B arriving at the processing room extinguish fires using fire extinguishing equipment A and fire extinguishing equipment B installed near GB A and GB B, respectively.

Based on the above conditions, a hazard analysis focusing on individual components and a hazard analysis focusing on the entire system are performed. Based on these results, the multi-layer shown in Fig. 6 is created.

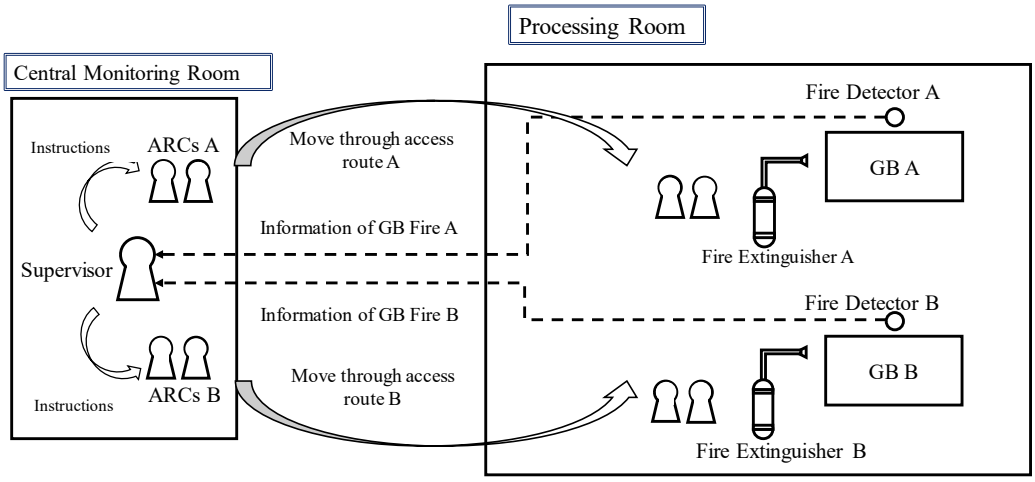

Fig. 5– Overview of equipment and personnel layout

Fig.7 shows one example of the *EPL* extracted from this multi-layer. In this *EPL*, a fire breaks out from GB A and the heat propagates through the processing room. The propagated heat is detected by the detector A, and the temperature information of the processing room is transmitted to the supervisor. The supervisor instructs ARCs A to extinguish the fire, ARCs A extinguish the GB A fire by operating the fire extinguisher A in the processing room and releasing the fire extinguishing agent from the fire extinguisher A while reporting the situation to the supervisor. The supervisor recognizes the fire extinguishing status of GB A by the information from detector A and the report of ARCs A. The heat in the process room affects the ARCs A and the fire extinguisher A. This *EPL* forms a *Loop*. Table 1 shows extract of examples of hazards in this *EPL* extracted using guide words used in STAMP/STPA.

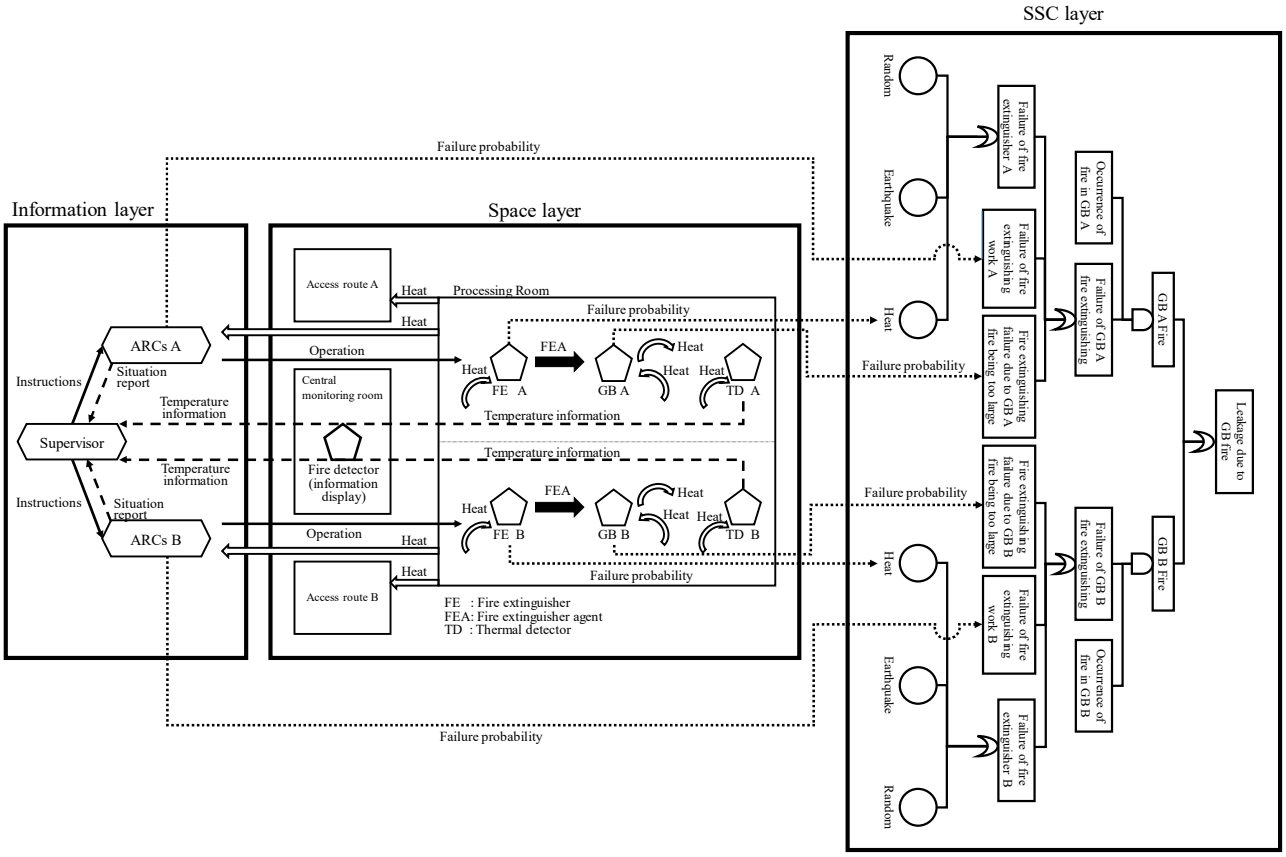

Fig. 6– Example of multi-layer

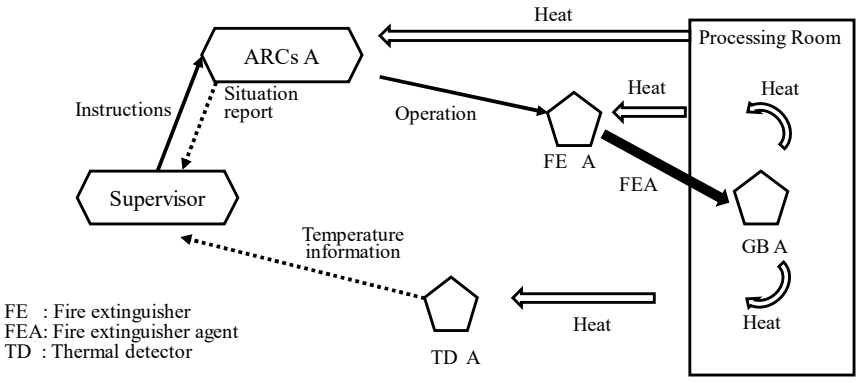

Fig. 7– Example of *EPL*

Table 1 Example of result of hazard analysis for *EPL* (extract)

Control Action	From	To	Not Providing	Providing Causes hazard	Too early/Too late	Stop too soon/ Applying too long
Thermal radiation	GB A	PR	---	Heat affects equipment and humans.	---	---
Thermal radiation	PR	TD	The TD cannot detect the fire.	---	---	---
Transmission of temperature information	TD	SP	The SP cannot recognize the fire.	---	Since transmission of temperature information is delayed, the instructions of SP are delayed.	Since transmission of temperature information stops early, the SP cannot recognize the fire, or the instructions of SP are delayed.
Instructions	SP	ARCs A	The FEWs are not performed.	Since incorrect instructions are given, the FEWs are delayed or not possible.	Since the instructions of SP are too early (instructions are given before the ARCs gather), the ARCs can't perform the FEWs sufficiently. Since instructions are delayed, the FEWs are delayed.	Since the instructions of SP are too long, the FEWs are delayed.
Operation for FE A	ARCs A	FE A	The fire is not extinguished.	Since incorrect operation is performed, the fire cannot not be extinguished, or the fire extinguished is delayed.	Since operation is too late, the fire progresses, and the fire extinguished is delayed.	Since operation is too long, the fire progresses, and the fire extinguished is delayed.
Release of FE agent	FE A	GB A	The fire is not extinguished.	---	---	Since FE agent spray is too short, the fire cannot not be extinguished

ARC: Accident Response Crew / SP: Supervisor / PR: processing room / TD: Thermal Detector / FE: Fire Extinguisher / FE agent: Fire Extinguishing agent / FEW: Fire Extinguishing Work

Furthermore, as an example of a hazard analysis taking into account the interaction of multiple events, the interaction between the above-mentioned *EPL* and the *EPL* with the same progression as the above-mentioned *EPL*, but the target is GB B, is analyzed. Fig.8 shows the interaction between the two *EPLs*. Table 2 shows extract of examples of analysis for hazard related to interactions.

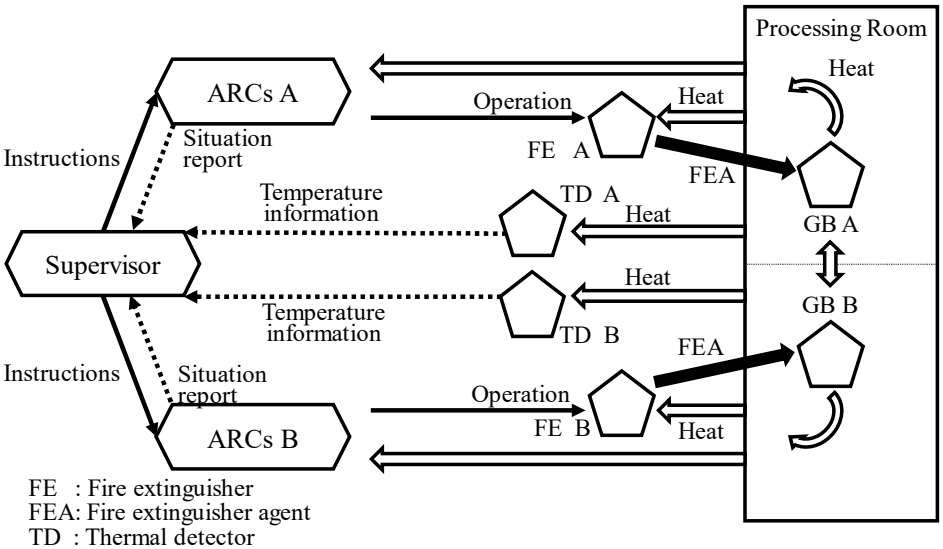

Fig. 8– Example of hazard analysis in the interaction of multiple events

Table 2. Example of interaction between GB A fire event and GB B fire event (extract)

Interaction	Example of hazard
The supervisor's processing of for the GB A and the GB B is performed simultaneously.	・ An error occurs in the fire extinguishing instruction for the GB A fire. ・ The fire extinguishing instructions for the GB A fire are delay. ・ An error occurs in the fire extinguishing instruction for the GB B fire. ・ The fire extinguishing instructions for the GB B fire are delay. ・ The fire extinguishing instructions for the GB B are not given.
The heat from the GB A fire affects the GB B through the space of the processing room.	・ The GB B fire continues.
The heat from the GB A fire affects the fire detector B through the space of the processing room.	・ Exceeding the allowable heat capacity of the fire detector B, it breaks down and the supervisor cannot recognize the GB B fire. ・ In this case, the importance of the report from the ARCs B increases, and psychological load on them increases, and an error or delay occurs in their operation.
The heat from the GB A fire affects the ARCs B through the space of the processing room.	・ The ARCs B cannot perform the fire extinguishing works. ・ The fire extinguishing works of the ARCs B are delayed. ・ The psychological load on the ARCs B increases, resulting in errors and delays.
The heat from the GB A fire affects the fire extinguisher B through the space of the processing room.	・ The fire extinguisher B fails, and the fire extinguishing works cannot be performed.

4. Conclusion

In risk assessment for the DiD level 4 and 5 at nuclear facilities, it is necessary to consider the feedbacks of influences to events by human operations, etc. and the influences of simultaneous occurrence of multiple events. The conventional PRA hazard analysis methods are not sufficient to take these into account. For this reason, the authors introduced the accident model STAMP/STPA method based on the system theory proposed by Nancy G. Leveson, and proposed a method using a multi-layer model that is linked to the conventional PRA methods with STAMP/STPA method. In this paper, through the case analysis, it is shown that this method can identify interactions and hazards that occur among events. The conventional PRA methods alone can't identify these interactions and hazards. Furthermore, it is shown that this method can perform qualitative hazard analysis for the DiD level 4 and 5. However, this method has the following issues, which need to be studied in the future.

- Efficient method for identification of combination of timing of interaction among multiple events
- Construction of a framework for dynamic quantitative evaluation of the influences of feedback and interaction among multiple events

6. Acknowledgements

This research was carried out with grants from Grants-in-Aid for Scientific Research. The authors would wish to thank the Japan Society for the Promotion of Science which supported us, and the Tokyo City University which allowed us to receive the grant.

7. References

[1] T. Fuketa, "Use of risk information in regulations," Nuclear Risk Research Center Symposium 2015, Otemachi Sankei Plaza Tokyo, Sept. 2, 2015, https://criepi.denken.or.jp/jp/nrrc/event/pdf/pd2_fuketa.pdf [in Japanese].

[2] S. Kaneko, "Toward the implementation of regulations using risk information," Nuclear Risk Research Center Symposium 2018, Yurakucho Asahi Hall Tokyo, Feb. 2, 2018, https://criepi.denken.or.jp/jp/nrrc/event/pdf/2018_kouen2kaneko.pdf, [in Japanese].

[21] K. Goto, Y. Ohtori, H. Muta and A. Omoto, "1N07 Analysis of evacuation during the JCO accident by safety analysis method STAMP/STPA," Proceedings of AESJ 2019 Annual Meeting", 2019 Mar. 20-22, Ibaraki University Mito Campus, Japan, p.1N07 [in Japanese].

