Integrated functional modeling method for NPP plant DiD risk monitor and its application for conventional PWR

YOSHIKAWA Hidekazu [1], YANG Ming [2], and ZHANG Zhijian [3]

1.College of Nuclear Science and Technology, Harbin Engineering University, China(yosikawa@kib.biglobe.ne.jp)
2. College of Nuclear Science and Technology, Harbin Engineering University, China (myang.heu@gmail.com)
3. College of Nuclear Science and Technology, Harbin Engineering University, China (zhangzhijian@hrbeu.edu.cn)

Abstract: The development of a new risk monitor system is introduced in this paper, which can be applied not only to severe accident prevention in daily operation but also to serve as to mitigate the radiological hazard just after severe accident happens and long term management of post-severe accident consequences. The summary of the fundamental method is given on how to configure the Plant Defense in-Depth (DiD) Risk Monitor by object-oriented software system based on functional modeling approach. Following the authors' preceding preliminary study for AP1000, the way of realizing the proposed method of configuring the plant DiD risk monitor was investigated for a safety-enhanced Japanese PWR design to meet with the tight anti-severe accident requirements set by national regulation in Japan after Fukushima Daiichi accident. The result of this example practice of the presented preliminary study for Japanese PWR was for the level 4 of the DiD in case of beyond design basis accident, that is, loss of all AC power + RCP seal LOCA, against the former case of AP1000 for level 3 DiD in case of large LOCA.

Keyword: defense-in depth; severe accident measures; risk monitor system

1 Introduction

The authors of this paper have been developing a new risk monitor system, in order not only to prevent severe accident in daily operation but also even to serve as to mitigate the radiological hazard just after severe accident happens and long term management of post-severe accident consequences.[1] The conspicuous features of the proposed risk monitor to be compared with the existing risk monitors basically lie on the two points: (i)The range of risk is not limited to core melt accidents but includes all kinds of negative outcome events, i.e., not only precursor troubles and incident but also any types of hazard states resulting from a severe accident, and (ii)The whole system of the proposed risk monitor system consists of plant Defense-in Depth (DiD) risk monitor and reliability monitor. The relation between the both monitors was discussed [2] and the method of how to apply a success tree oriented reliability analysis method GO-FLOW [3] had been extensively studied for the reliability monitor of the real safety systems of PWR plants as the practical example. [4, 5]Then, the method of how to configure the plant DiD risk monitor by functional modeling approach was first presented in [6], with a preliminary study being conducted on applying the integrated functional modeling for Plant Defense-in-depth risk monitor for passive safety system of AP1000.

The similar preliminary study on how to configure Plant DiD risk monitor is the subject of this paper for active safety system of conventional PWR in Japan. Wherein, the safety functions of Japanese PWR has been being reinforced by reflecting the lessons from Fukushima Daiichi NPP accidents in 2011.The objective of this study is to compare the Plant DiD risk monitors for both types of PWR, in order to consider on what will be effective software method to construct the Plant DiD risk monitors with correlating the relevant reliability monitors.

In which follows, a brief summary of the authors' proposed risk monitor system for NPP is given in 2. The functional model of plant DiD monitor is given in 3. The result and the discussion of the preliminary study will be given in 4 for the plant DiD risk monitor of the reinforced active safety system of a conventional PWR in Japan.

Received date: September 16, 2014

2 Brief summary of the authors' proposed risk monitor system for NPP

The authors' proposed risk monitor system is constituted by two layered systems as depicted in Fig. 1, although the detailed configuration of the whole system have not yet been fixed at the present stage. It is basically composed by a Plant Defense in Depth (DiD) Risk Monitor to predict and valuate plausible risk state from the perspective of whole plant, and several Reliability Monitors to evaluate the reliability of individual subsystems to fulfill their expected functions successfully under the prescribed conditions, wherein the prescribed conditions to the reliability monitor are given by the Plant DiD Risk Monitor.

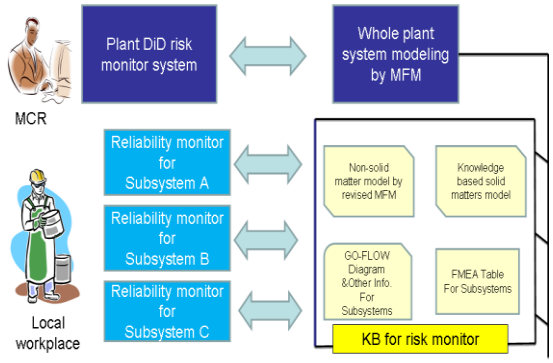

Fig. 1 Author's proposed risk monitor system.

In Fig. 1, the plant DiD risk monitor will identify every potential risk state caused by any conceivable event in the plant system as a whole where not only internal events but also external events arising from common cause factors and human factors should be taken into account.

Reliability evaluation for a sub-system is made by the Reliability monitor using a combination of FMEA and GO-FLOW. Reliability is normally defined as the successful rate of a system's performance that will fulfill its expected function when it is requested. In the safety design of nuclear power plant, reliability of safety functions is enhanced by principles of diversity, redundancy and physical separation.

The developmental study has been extensively conducted on reliability monitors for ECCS system and containment spray system for a conventional PWR plant by utilizing FMEA and GO-FLOW, where a parametric study of the sensitivity analysis, uncertainty analysis, and analysis of common mode factors by parametric model have been also conducted.

Since plant DiD risk monitor will be utilized to analyze and evaluate various risks cause by operation of nuclear power plant, it will be necessary to introduce a certain comprehensive framework to describe "types of analysis scenario". Table 1 shows a classification of operation modes for nuclear power plant operation which corresponds to types of analysis scenario.

There are very many cases to consider in advance on different types of operation modes of plant process both in normal and in design-basis off-normal situations (A in Table 1) and "out of normal imagination" situations (B in Table 1).

Table 1 Classification of operation modes for nuclear power plant.

Classification of operation modes		
A. Design basis	Normal operation	Start-up, Steady state operation, Power change and Shutdown
		Refueling, and maintenance testing
	Off-normal	Anticipated transient/accident
	Design basis severe accident	
B. Imaginary emergency situation		

On the other hand of various operation modes, it is well known in the field of human factors research that the operator's action becomes automated by proper training on the basis of acquired knowledge base on versatile behaviors of machines and plant systems. However, there remain unfamiliar situations when operators have to cope with it by problem solving from scratch. Therefore, it is said in human factors area that there are two types of human task: skill and rule based routine task and non-routine knowledge based task. Here the authors of this paper think that the problem solving in the unfamiliar situation is what is called "emergence" (this word means that a new property or a new function will give rise from the existing partial property and function when encountering unfamiliar situation), and the way of

creating proper countermeasures to judge the monitored situation and to prevent or mitigate the consequence of the accident situation.

The authors of this paper would like to start the issue by considering how to configure human-machine interaction model as the basis of plant DiD risk monitor for any types of analysis scenario. Concretely, they utilizes a graphical method to describe human-machine interaction model which one of the authors utilized to develop computerized human operator at the human-machine interface of main control room in the nuclear power plant [7]. The major idea this time is to convert the essential information in this graphical representation method into three knowledge-based entities of (i)State transition diagram, (ii)Basic task element diagram, and (iv)Composite task element diagram.

3 Functional model of plant DiD monitor

To sum up, the following ideas have been utilized as the basis of integrated functional modeling for Plant Defense-in-depth risk monitor:

(i) The whole plant system should be modeled by the combination of "solid matters model" and "non solid matters model",

(ii) Common mode factors both of internal and external events including human factors issue should be taken into account, and

Basic idea of graphical representation method for human-machine interaction will be utilized to reorganize it for knowledge-based software system for Plant DiD risk monitor.

Table 2 Correspondence between hardware and software of human-machine system and the functional modeling method.

	Human-machine system	Method of functional modeling and information representation
Hardware	Plant system including automatic and safety system	Solid matter models (3D CAD, LSI model)
	Human-machine interface equipments	Non-solid matter model (MFM, Goal-Mean)
Software	Configuration of operation staffs	Operators configuration and the communication path diagram
	Operation rules and procedures	Task transition diagram with Hierarchical task analysis diagram and the related action mode analysis table
	Various operation support tools	Emergence simulation method with AI reasoning

According to the author's idea, the hardware and software of human-machine system of the nuclear power plant and the correspondence to the functional modeling methods can be described as shown in Table 2. It has been one of the subjects of the author's study to consider how to implement the software of operation rules and procedures in Table 2 for plant DiD Risk monitor. The summaries of the author's study are given below on software elements (A), (B), (C), and (D) which are necessary to configure plant DiD risk monitor.

(A)State transition diagram

This is to be realized as an object-oriented modules for the abstracted state transition of machine and plant system by the principle of machine, where the following conditions should be equipped:

(i) Relation between Original state, external input or disturbance and Outcome state should be semantically described.

(ii) The state transition will be caused by either autonomous machine behavior or human-machine interaction. Then trigger condition of state transition should be described.

(iii) Each state should assign both the risk level and the degree of risk. The risk level distinguish the risk state in accordance with whether or not three safety functions of STOP, COOL and CONTAIN are maintained, while the degree of risk gives quantitative risk state by appropriate computational method.

The "hardware model" (*i.e.*, both solid matter and non-solid matter models) should be formulated in accordance with the analysis scenario.

(B)Basic task element diagram

This is also to be realized as object-oriented modules for individual basic task elements seen in the related operation procedure, where the following conditions should be equipped:

(i) Name ; Explain its meaning

(ii) Action; what to see and by what way to judge

(iii) Means; what to do for which by what way

(iv) Right outcome; what's target result by what criterion to judge as right and what to do next

(v) Unwanted outcome; what will be the said states and what to do next.

(C) Composite task element diagram

The tasks performed either by machine or human are normally the combination of many elementary tasks, and those elementary tasks are described by basin task element diagram. If the composite task element is represented by the same form of the elementary task element, this composite task element can be also utilized as a basic task element. To sum up, the composing task element will be generated by the combination of individual basic task elements, where the following conditions should consider:

(i) Name; Explain its meaning of the composite task

(ii) Method of how to synthesize the composite task from the selected basic task elements.

Additional parameters are needed by the synthesis of selected elemental tasks which originally have the following parameters:

(i) Action; what to see and by what way to judge

(ii) Means; what to do for which by what way

(iii) Right outcome; what's target result by what criterion to judge as right and what to do next

(iv) Unwanted outcome; what will be the said states and what to do next.

(D)User interface of plant DiD risk monitor

There are at least two different subjects for developing the user interface of plant DiD risk monitor. They are:

(i) User interface 1 for knowledge base management to register, update and delete various kinds of diagrams as mentioned in (A), (B) and (C), and

(ii) User interface 2 for analyzing various aspect of risk problem on the target plant system in a certain analysis scenario which is selected from Table 1.

4 Plant DiD risk monitor for Japanese conventional PWR

AP1000 uses a lot of passively working equipment and also employs the control systems by which exclude human intervention. In the authors' former study for configuring the plant DiD risk monitor of AP1000, the target scenario was for the case of large break LOCA where the successful workings of passive core cooling system and passive containment cooling system are main concern. The failures of the both system may lead to core melt and damage of containment. Therefore, it is within the range of level 3 of defense-in-depth since those failures of the safety systems are outside of the plant DiD risk monitor in consideration.

In Japan after TEPCO's Fukushima Daiichi accident happened in March 2011, only the nuclear power plants which reinforce anti-severe accident measures would be permitted to restart the operation by National Regulatory Agency (NRA). In this paper, the authors will try to configure the plant DiD risk monitor for a conventional type PWR of thermal output 2,652 MWth in Japan, which have reinforced its safety design in accordance with the revised safety standards and is now under reviewing by NRA.

4.1 Safety reinforced conventional PWR in Japan

Overall hardware feature of the safety reinforced Japanese conventional PWR is illustrated in Fig. 2. The revised framework of the operational procedure of the corresponding PWR in Japan is also shown in Fig.3, where the organizational strengthening to the emergency situation to cope with severe accident is indicated. After when the reactor would commit core melt accident, not only the operators in the committed plant unit but also the emergency response team hastily summoned to the on-site center will work together to cease the fire of severe accident. The whole organization of the emergency response team and their work place and the task allocation are illustrated in Fig. 4.

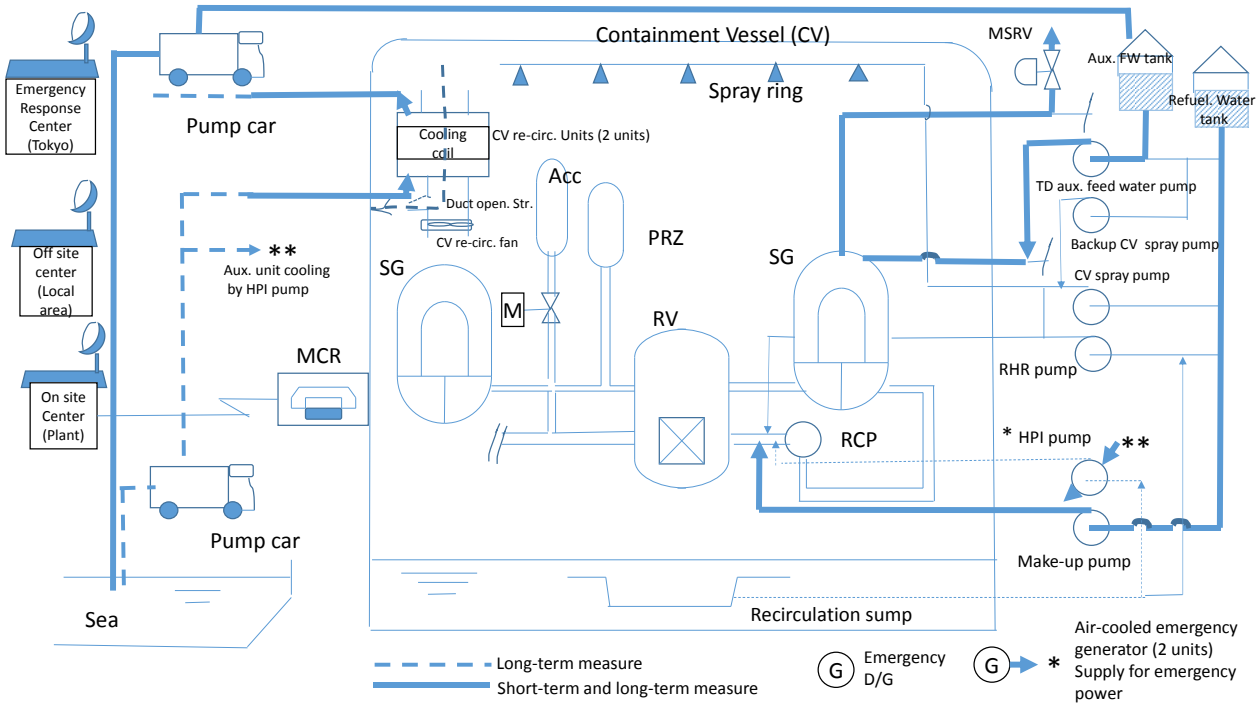

Fig. 2 Overall hardware feature of the safety reinforced Japanese conventional PWR.

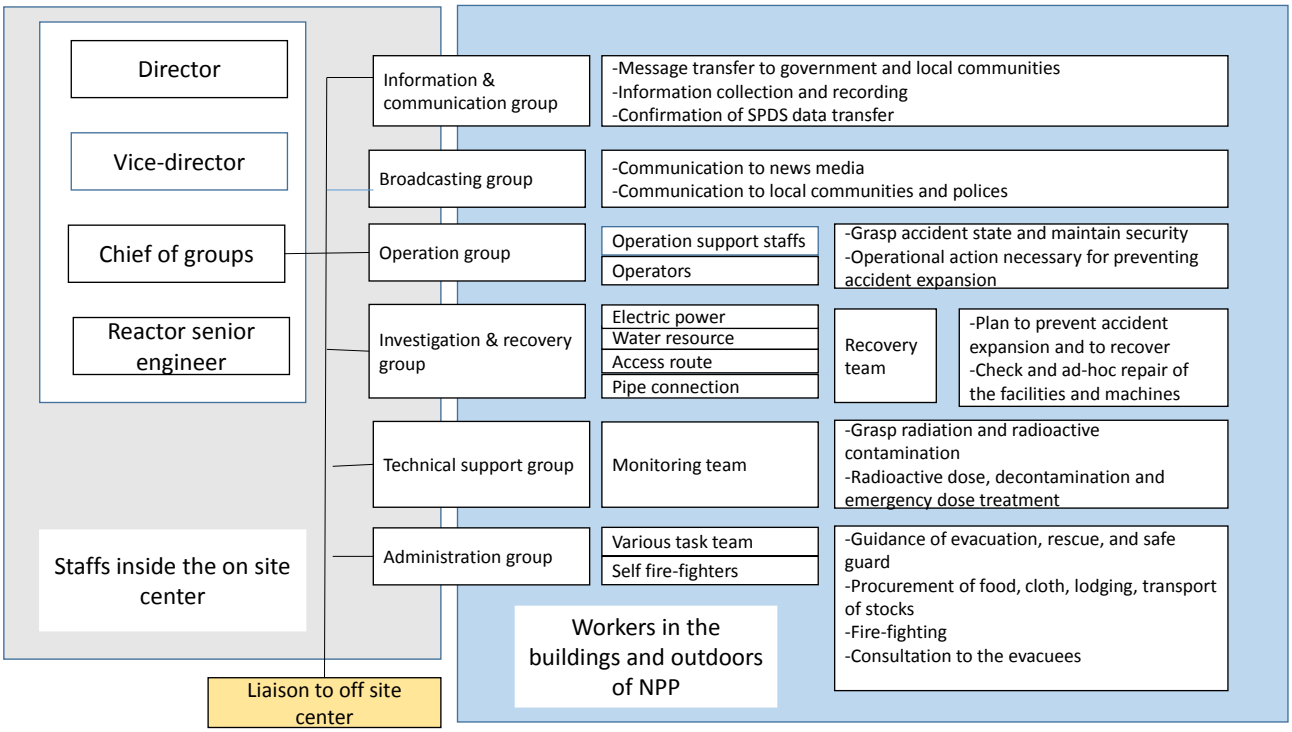

Fig. 3 Whole framework of operational procedure for safety reinforced Japanese conventional PWR.

Accident level and the goal of responsive action :			
	Design basis event	Prevent core damage	Prevent containment vessel (CV) rupture
Main control room (MCR)	-Alarm handling procedure -Trouble and accident handling procedure (Part I) : Event base procedure for design basis event	--Trouble and accident handling procedure (Part II) : Maintain intactness of nuclear fuel in cases of design basis events (Safety function based procedure and event based procedure)	-Trouble and accident handling procedure (Part III) : Prevent radioactive release to the environment by maintaining CV intactness in cases of leading to reactor core damage
Onsite emergency response center	Emergency response procedure		Accident management guideline
	-Securing nuclear reactor facilities in cases of severe accident occurrence and large scale destruction of the facility: Significant damages of reactor core, nuclear fuels in the spent fuel pit, and large-scale damage of the reactor and the by the collision of large airplane and the terrorist attack.		-Integral management guideline to prevent accident progression and mitigating the consequence in case of core damage when the above Part III procedure will no more succeed. -Two types of guidelines exist: monitoring function based guideline and that of whole evaluation of accident progression.

Fig. 4 Whole organization of emergency response team and their work place with task allocation.

4.2 Assumed accident scenario and accident management method

Similarly as was happened at Fukushima Daiichi accident in March 11, 2011, it is assumed that a severe initiative event is assumed to occur in the safety enhanced conventional Japanese PWR. It is here assumed that all alternating current (AC) power are lost, with no start-up of emergency diesel generators but the DC power sources can still maintain. Loss of water for cooling auxiliary machines is also assumed to occur and subsequently it will bring about loss of coolant accident through the seal of reactor coolant pump (RCP). To cope with this serious situation, it is assumed to manage the failed plant to settle down towards the safely cold shutdown state by the following approaches:

(i) In order to avoid reactor core melt, both the pressure and temperature of both the primary and the secondary sides of the PWR should be decreased gradually by the manual operation of the main steam relief valve and water charging by make-up pump within ca. four hours after the initiating event.

(ii) In order to maintain the confinement capability of radioactive materials generated in the reactor, the pressure and temperature of the containment vessel (CV) are manipulated so that they may not exceed their upper limit values.

4.3 Configuration of plant DiD risk monitor

The correspondence of the temporal event sequences is shown in Fig. 5, between the desirable plant parameters and the human task allocation in the emergency response team to manipulate the plant condition rightly. The more detailed picture than this Fig.5 can be illustrated as shown in Fig.6, by the block chart of right human-machine interaction to cope with the accident. This is the similar way of the graphical representation of task transition diagram which will give the basic information to the plant DiD risk monitor to be configured.

As seen in Fig.6, there are three cases as below, depending on whether or not successful response at the initial phases of accident:

a. In case AC power can be promptly recovered,

b. Loss of all AC power without reactor scram, and

c. Loss of all AC power and large break LOCA.

In Fig. 6, no consideration is made for the further progression of event sequence. However, it is thought that both cases of b and c would be severe of accident with difficult counteraction while rather easy accident management in the case a.

Further, all the rest event sequences in Fig.6 are based on only "success-tree based description". Therefore, if any failure in any step of action may bring different event sequences. Therefore, this chart would be more complicated ones if you take into account of any possibility of action failure in Fig.6.

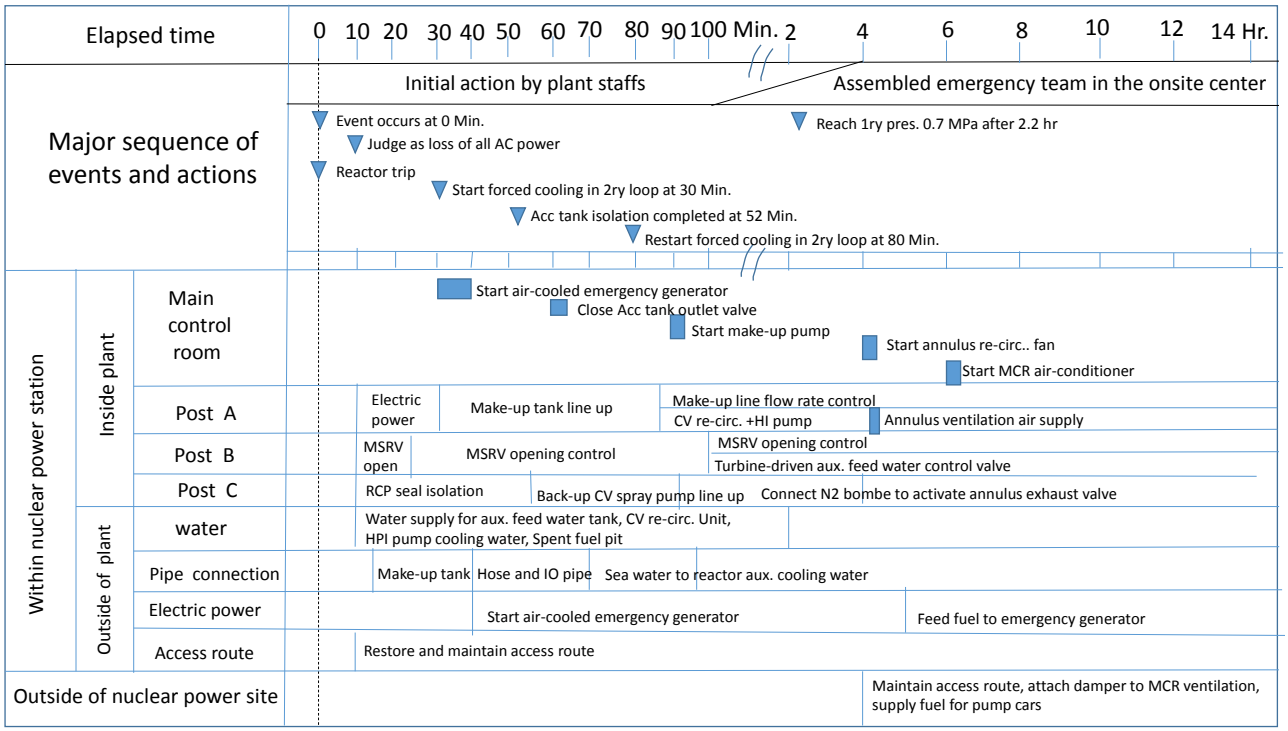

Fig. 5 Correspondence of temporal event sequences between desirable plant parameters and human task allocation.

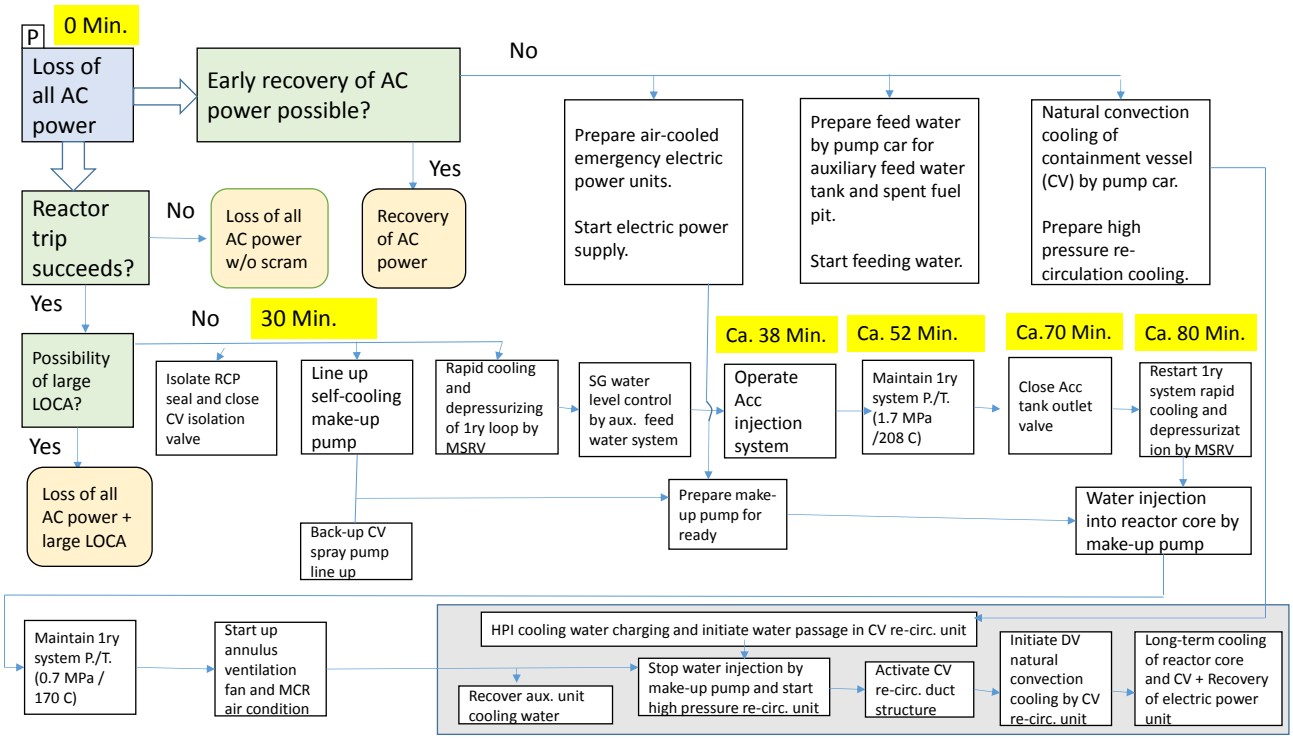

Fig. 6 Task transition diagram to manage the severe accident in conventional PWR.

Next, the plant DiD risk monitor for the Japanese conventional PWR as discussed in this paper will be compared with that of AP1000 which was presented in Ref. [5]. To be compared with so-called “built-in” type AP1000 which improved the safety design from scratch by employing passive safety principle with excluding human intervention, it is generally thought that the configuration of plant DiD risk monitor for safety reinforced Japanese PWR studied in this paper would become rather complicated. That is, the way of safety enforcement in Japanese conventional PWR is called “add-on” type where various severe accident countermeasures both hardware and software are additionally implemented to the existing PWR design.

Lastly, it should be also pointed out that the designing of software systems of plant DiD risk monitor would be different in accordance with the objective or the usage of the risk monitor system.

5 Concluding remarks

The progress of the author's developmental study on a new risk monitor system was introduced, which can be applied not only to severe accident prevention in daily operation but also to serve as to mitigate the radiological hazard just after severe accident happens and long term management of post-severe accident consequences. Then, the fundamental method was summarized on how to configure the Plant Defense in-Depth Risk Monitor by object-oriented software system based on functional modeling approach. Following the preceding preliminary study for AP1000, the way of realizing the proposed method of configuring the plant DiD risk monitor was investigated for a safety-reinforced Japanese PWR design to meet with the anti-severe accident requirement set by national regulation in Japan after Fukushima Daiichi accident. The example practice of the presented preliminary study for Japanese PWR was for the level 4 of the DiD in case of beyond design basis accident of loss of all AC power + RCP seal LOCA, against the former case of AP1000 for level 3 DiD in case of large LOCA. In the next step of this study, the authors will proceed to develop the software system to generate plant DiD risk monitor system usable for any types of accident scenario, although it should be taken into account that the design of the risk monitor system depends on what purpose it will be used in actual situation.

References

[1] YOSHIKAWA Hidekazu, LIND Morten, YANG Ming, HASHIM Muhammad, and ZHANG Zhijian: Configuration of risk monitor system by plant defense-in-depth risk monitor and reliability monitor, Nuclear Safety and Simulation, Vol. 3, Number 2, June 2012,140~152.

[2] YOSHIKAWA Hidekazu, LIND Morten, MATSUOKA Takeshi, HASHIM Muhammad, YANG Ming, and ZHANG Zhijian: A new functional modeling framework of risk monitor system, Nuclear Safety and Simulation, Vol. 4, Number 3, September 2013,192~202.

[3] MATSUOKA T.: System Reliability Analysis Method GO-FLOW for probabilistic Safety Assessment, CRC Sogo Kenkyusho, 1996. (In Japanese).

[4] HASHIM Muhammad, MATSUOKA Takeshi, YOSHIKAWA Hidekazu, and MING Yang: Dynamical reliability analysis for ECCS of pressurized water reactor considering the large break LOCA by GO-FLOW methodology, Nuclear Safety and Simulation, Vol. 3, Number 1, March 2012, 81~90.

[5] HASHIM M., YOSHIKAWA H., and YANG M.: Addressing the fundamental issues in reliability evaluation of passive safety of AP1000 for a comparison with active safety of PWR, Nuclear Safety and Simulation, Vol.4, No.2, June 2013: 147-159.

[6] YOSHIKAWA H., YANG M., LIND M., and MATSUOKA T.: Integrated functional modeling method for configuring NPP plant DiD risk monitor and its application for AP1000, (ICONE22-30987) Proceedings of the 22nd International Conference on Nuclear Engineering (ICONE22), July 7-11, 2014, Prague, Czech.

[7] YOSHIKAWA H., SHIMODA H., Ishii H., NAKAGAWA T., WU W., FUMIZAWA M., and MONTA K.: Development of Integrated Simulation System SEAMAID for Human-Machine Interaction in Nuclear Power Plants; Its Practical Application and Future Prospect, Proc. The 8th IFAC/IFIP/IFOR/IEA Symposium on Analysis, Design, and Evaluation of Human-Machine Systems, pp.535-540, 2001.