A new functional modeling framework of risk monitor system

YOSHIKAWA Hidekazu[1], LIND Morten[2], MATSUOKA Takeshi[3], HASHIM Muhammad[4], YANG Ming[5], and ZHANG Zhijian[6]

1. College of Nuclear Science & Technology, Harbin Engineering University, 145-1 Nantong Street, Nangang District, Harbin, 150001, Heilongjiang, P.R. China (yosikawa@kib.biglobe.ne.jp)
2. College of Nuclear Science & Technology, Harbin Engineering University, 145-1 Nantong Street, Nangang District, Harbin, 150001, Heilongjiang, P.R. China (mli@elektro.dtu.dk)
3. College of Nuclear Science & Technology, Harbin Engineering University, 145-1 Nantong Street, Nangang District, Harbin, 150001, Heilongjiang, P.R. China (mats@cc.utsunomiya-u.ac.jp)
4. College of Nuclear Science & Technology, Harbin Engineering University, 145-1 Nantong Street, Nangang District, Harbin, 150001, Heilongjiang, P.R. China (hashimsajid@yahoo.com)
5. College of Nuclear Science & Technology, Harbin Engineering University, 145-1 Nantong Street, Nangang District, Harbin, 150001, Heilongjiang, P.R. China (myang.heu@gmail.com)
6. College of Nuclear Science & Technology, Harbin Engineering University, 145-1 Nantong Street, Nangang District, Harbin, 150001, Heilongjiang, P.R. China (zhangzhijian@hrbeu.edu.cn)

Abstract: A new risk monitor system has been developed which can be applied not only to prevent severe accident 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 fundamental assumption of such risk monitor system, the method of configuring the whole system by plant Defense in Depth (DiD) risk monitor and reliability monitor, and the progress of development thus far conducted are first summarized. Then the result of preliminary study on how to configure the Plant Defense in Depth Risk Monitor by functional modeling approach is presented. .Lastly, a preliminary study is conducted on applying the integrated functional modeling for Plant Defense in depth risk monitor for passive safety system of AP1000.
Keyword: severe accident prevention; risk monitor; functional modeling; reliability monitor; plant DiD risk monitor; passive safety AP1000

1 Introduction

The WASH-1400 report of probabilistic risk assessment (PRA) for nuclear power plant had been first published in 1975 by U.S. Nuclear Regulatory Commission.[1] PRA has been alternatively called PSA(Probabilistic Safety Assessment). Since WASH-1400 and the progress of PRA methodology, the usage of PRA has been expanded into many nuclear developing countries around the world in order to improve safety management to avoid core melt accident. With the maturity of PRA, living PSA has been developed in U.S.A. as a methodology for improving the efficiency of plant shutdown management together with maintaining the plant safety. These days living PSA is also called as risk monitor. According to the definition of IAEA, risk monitor is a plant specific real time analysis tool used to determine the instantaneous risk of a core melt accident based on the actual status of the systems and components.[2]

However, according to the authors' understanding, usage of PRA and living PSA in nuclear industries have been mainly intended to the prevention of core melt accident, and no consideration has been made on how to mitigate the consequence of core melt accident once it happens. On the other hand of PRA, the INES scale (international nuclear event scale) has been introduced among the member countries of the IAEA nuclear safety treaty, and the degrees of INES have been announced public at every time any trouble or accident happens in nuclear facilities.[3] The INES covers any big severe accident, and the largest INES scale 8 corresponds to both Chernobyl and Fukushima Daiichi accidents.

The background of the author's study is that it is necessary to develop a new risk monitor system 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, by experiencing the Fukushima Daiichi accident in Japan happened in March 2011 which still plagues Fukushima citizen and Japanese society. It is expected to foster resilient capability of the nuclear personnel so that they can predict the dangerous risk and create proper countermeasures in (i) preventing occurrence of severe accident, (ii)prompt recovery from emergent situation, and (iii)long-term management of post-severe accident consequences.

In what follows, progress of the authors' study thus

Received date: October 9, 2013
(Revised date: November 5, 2013)

far conducted will be first summarized in section 2., and then the result of the author's preliminary study on how to configure the Plant Defense in Depth Risk Monitor by functional modeling will be presented in section 3. And lastly discussion on developing a plant DiD risk monitor will be made in section 4 for passive safety system of AP1000.

2 Overview of risk monitor system

In the authors study, the definition of risk and the way of calculating the risk is different from the IAEA definition. 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.) Also not only the ranking of risk level (like the INES scale) but also "dynamical change of risk ranking with the degree of risk to be visualized for easy grasp" is taking into account.

Therefore, the author's risk monitor concept can be applied not only daily management of normal operation and maintenance by the operating staffs but also for emergency situation and post-severe accident management mitigating the radiological consequence to the environment.

The proposed Risk Monitor System is constituted by two layered systems as depicted in Figure 1, although the detailed configuration of the whole system have not yet fixed at the present stage. However basically it is composed by a Plant Defense in Depth (DiD) Risk Monitor for the whole plant and several Reliability Monitors for individual subsystems.[4] The basic concept of this risk monitor system and the progress of the works done until at present are summarized in the subsequent sections of this chapter.

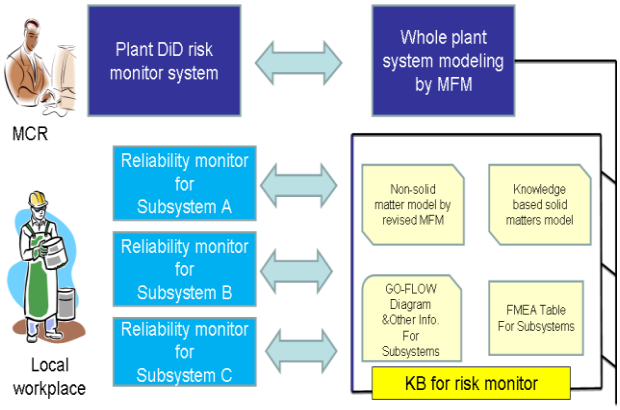

Fig. 1 Authors' proposed risk monitor system.

2.1 Design principle of nuclear power plant safety

According to the authors' risk monitor system, it is assumed that the ultimate risk of a nuclear reactor is the radioactive hazards resulting from various possible states of severe accidents. The design principle of nuclear power plant safety is defense in depth: multiple barriers are provided against radiological releases to the environment. And there are four barriers against severe accidents; nuclear fuel, cladding, pressure boundary of reactor coolant including reactor vessel, and containment. And in case of troubles, intactness of those barriers is assured by three safety functions: STOP nuclear reaction, COOL reactor, and CONTAIN radiological release.

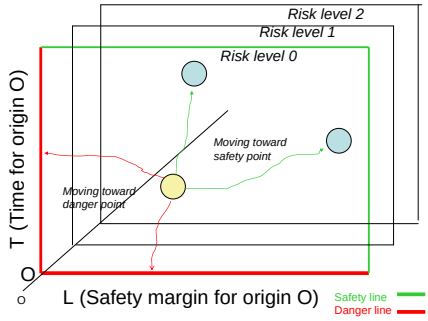

Fig. 2. Dynamic risk monitor as human interface to visualize risk state.

2.2 Risk monitoring and visualization

According to the authors' risk monitor system, evaluation of risk state is made by two step procedure; First, Risk levels should be decided by (i) seeing the intactness of three safety functions. Concretely, there are 2x2x2 = 8 cases by considering whether or not each safety function is intact (1) or lost (0) and the 8 cases are then classified into several risk levels by taking into account of different situations.

Risk level 0 is the situation when all safety functions are intact. But even if the Risk level is 0, the reliability of the plant in operation will change from time to time depending on how the redundancy, diversity and physical separation of the individual equipments and components are maintained and on the margin of plant parameters to the safety limit.
In case risk level larger than 1 where either or all safety functions will be lost, the Degree of risk should be decided by (ii) evaluating by what degree the plant would be damaged based on accident phenomena and their consequences.

According to the authors' proposed risk monitor system it serves as human interface for risk visualization. The Dynamic risk monitor should visualize risk ranking as "risk level" (0,1,2,…), while the degree of risk state in a specific risk level as

shown in Figure 2.In Figure 2, there are two parameters to quantify the risk state in the same risk level: (i)Time margin to reach the point of no return, and (ii)Degree of physical damage no more to be recovered.

2.3 Plant DiD risk monitor and reliability monitor

In Figure 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[5].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.

2.4 Application study of the Reliability Monitor

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[6], where a parametric study of the sensitivity analysis, uncertainty analysis, and analysis of common mode factors by parametric model have been also conducted.

3 Functional modeling for Plant Defense in depth Risk Monitor

The following ideas have been utilized in order to configure the 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 error should be considered as failure mechanism, and
(iii) Basic idea of graphical representation method for human-machine interaction will be utilized in order to reorganize it by integrated functional modeling method for Plant Defense in depth Risk monitor.

3.1 Whole plant system model with implementing failure mechanism[7]

How to model the whole plant system with implementing failure prediction mechanism? It is basically by the combination of solid matters model and non solid matters model, as described in the subsequent sections.

3.1.1 Solid matters model

It describes the rigid form matters and their configuration as an object-oriented knowledge base (KB) system with the combination of (i)3D-CAD model of structural components and (ii)Computer-aided design model of electrical circuits such as LSI circuit. Versatile KBs are also correlated with the 3D-CAD and LSI models on (i)various physical, chemical mechanisms to bring about the trouble and failure of the equipments, components, and parts, (ii)detection methods of failure, and (iii)countermeasures to prevent, repair and replace the failed parts and equipments.

3.1.2 Non-solid matter model

Basically Non-solid matter model describes liquid and gas matters flowing through solid matters. However, functional modeling method such as Multilevel Flow Model (MFM)[8] to be employed in this study can describe not only various mass and energy flows of liquid and gas, but also information flow for control/safety system. The graphical representation method used in MFM can describe the semantic meaning of such flow components with implementing Goals and Means, Objectives and functions, *etc*. In the authors' presented study, the central issue in this non-solid matter model is how to deal with complex control/safety systems implemented in the process plant. This issue is discussed in the next subsection.

3.1.3 Functional model of control/safety systems

Control/safety systems constitute the central nerve system which will guide the whole process plant to work in a coordinate way to attain the operational requirement by using various subsystems which serves versatile elementary functions in the whole system. And individual sequential action mode to fulfill a specific objective of the control/safety systems is realized by changing several basic elements which comprise the control/safety system. This function of sequential action mode to fulfill a specific objective is equivalent to "phased mission problem" which is said to be difficult to handle by FTA employed in the conventional PRA method. (It is one of the advantages that the GO FLOW method is easy to handle. phased mission.)

By the author's functional modeling approach, those characters of automatic control/safety systems will be modeled by using knowledge based system by object-oriented representation. (This means, basic process/task elements will be treated as "instance"

while "phased mission" processes be "subclass".) These methods can also be applied for manual operation procedure by operators.

3.1.4 Model of predicting failed case

The other specific function to realize "risk monitor" will be that it is necessary to develop a function of "predicting risk state" as mentioned in 2.2. The Reliability monitor as mentioned in 2.4 will be utilized to estimate the reliability of individual subsystems conducting their missions successfully along the preset temporal sequence. But it is also necessary to implement additional "thinking machine" to consider and predict the failed cases such that if failed what will be the situation, how to prevent the failure, *etc*.

3.2 Important factors influencing system failures

There are two aspects in considering the cause of the troubles and accidents and the span of the consequence of accident. They are (i) common mode failure caused by internal and external factor, and (ii) human error. In this study, the ranges of treating those two factors are considered both for plant DiD risk monitor and reliability monitor. Table 1 shows the character of common mode failure and the coverage of the risk monitor system, while Figure 3 for human error.

3.3 Graphical method for human-machine interaction

As a basis for realizing the functional model for the control/safety system in the process plant as discussed in 3.1.2, the author reviewed his past research result on the modeling of human-machine mutual interaction in the actual nuclear power plant operation where both the automatic machine system and manual operator action are mingled together[9]. In what follows, the method of modeling is first summarized in 3.3.1 and then exemplified in 3.3.2.

3.3.1 Modeling of human-machine mutual interaction

The method proposed by the authors for modeling human-machine mutual interaction consists of three graphical representations: (i)Task transition diagram, (ii)Hierarchical task analysis diagram and the related action mode analysis table, and (iii) Operators configuration and the communication path diagram. The essential points of the three representations are summarized below.

Table 1. Character of common mode failure and the coverage of risk monitor system.

Clearness of fault cause	Type of fault cause	Span of fault cause	Coupling mechanism	Analytical method	Risk monitor
Clear	Earthquake	Whole plant	Spatial	Explicit	Plant DiD risk monitor
	Tsunami, fire, flood, tornade	Combined subsystems	Spatial	Explicit	
	Functional relation		Functional	Explicit	
	Common share of support equipments		Functional		
	Change of physical environment by equipment failure		Spatial		
Steadily or randomly exists	Physical environment (high temperature, high pressure, etc.)	Single subsystem	Spatial	Explicit	Reliability monitor
Unclear	Design, fabrication		Human factors	Parametric	
	Maintenance, check	Individual equipment	Human factors		
	Human factors in operation		Human factors		

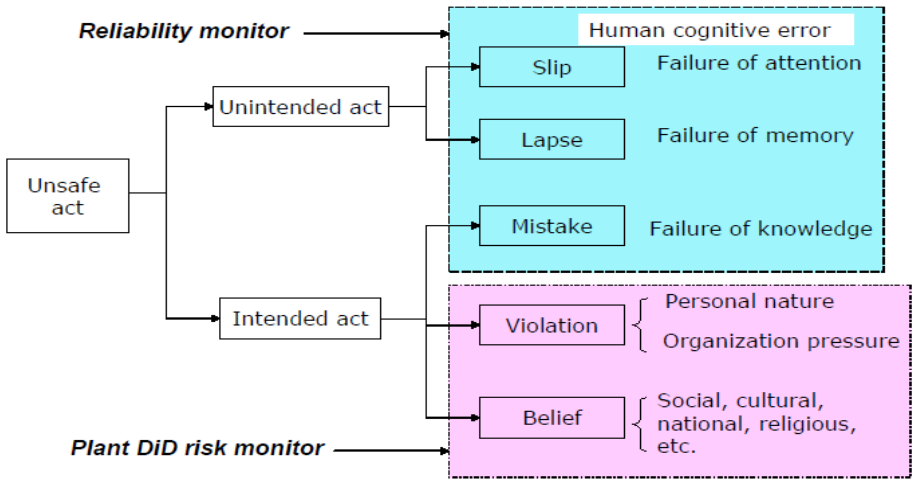

Fig. 3 Error classification of human factors and the coverage of risk monitor system.

(1)Task transition diagram

- Event development paths during plant recovery work are described by using a sort of block chart for the chain of successful task phase (state) transition.
- Clear definition of task phases and its objective, procedure, *etc*., are also described in the chart.
- Special considerations on the consequence of task failure are also described by noticing such as severity of plant state, automatic startup of backup safety systems, *etc.*

(2)Hierarchical task analysis diagram

It describes the operator procedure in detail for each phase of the task transition diagram by:

- Hierarchical expansion of task goal into sub-goals of sub-tasks,
- Clear description of procedure ("action program") by sequence and contents, and
- Clear description of control logics by "rule description".

The related "action mode analysis table" is the same as "Failure Mode and Analysis (FMEA)" table.

(3) Operators configuration and the communication path diagram

The operators configuration and the communication path diagram will describe how operating staffs such as shift supervisor, reactor operator, turbine operator, roving operators, safety engineer, are organized and the way of their task allocation, means of mutual communication and the contents to be communicated.

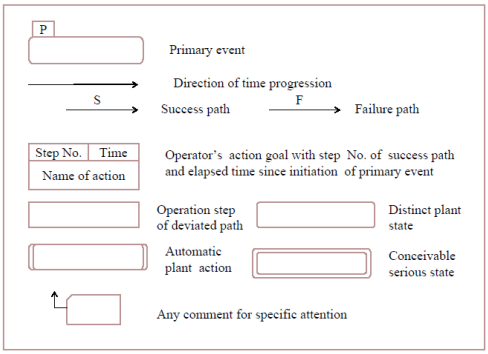

Fig.4 Symbols used for task transition diagram.

3.3.2 Example practice

As an example demonstrating the author's proposed method is taken the actual operation procedure used by BWR operators coping with LOCA. First, symbols used for describing the task transition diagram are explained in Figure 4. The meaning of task transition diagram is that it describes the way of successful management of plant state in the event of accident expected for the operators, with addition of what would happen if deviated.

By using the symbols in Figure 4, the task transition diagram for BWR operators coping with LOCA is illustrated in Figure 5, with the example operators configuration and the communication path diagram in Figure 6. An example hierarchical task analysis diagram for success path No.3 of Figure 5 is shown in Figure 7, with its action mode analysis table in Table 2. From this example, it is observed that: (i) existence of parallel tasks even in the successful procedure for failed plant condition (Task allocation between operators may consider), and (ii) preparation of backup measures in case of task failure by either automatic safety systems or operator's manual operation. (There is possibility of going to severe accident if failed in manual operation or failure of automatic system.)

3.4 Human-machine interaction model with risk monitor system

Then what is this model related with risk monitor system? First, the role of reliability monitor is to evaluate the rate of possibility of various success path chains seen in the task transition diagram.

Then, what is the role of plant DiD risk monitor? The answer is "it should present the equivalent information by more flexibly and usable form than those that are described here for the task transition diagram and the related ones as mentioned in the previous subsection 3.3.1."

It is also expected that the plant DiD risk monitor can estimate "dynamic risk" state, *that is*, risk level and the degree of risk (T and L), by using the results of reliability monitor and other information.

The hardware and software of human-machine system and the correspondence to the functional modeling methods can be described as shown in Table 3.

It is one of the subjects of the author's study to consider how to implement the software of operation rules and procedures in Table 3 for plant did Risk monitor. This subject will be separately discussed in the next subsection 3.5.

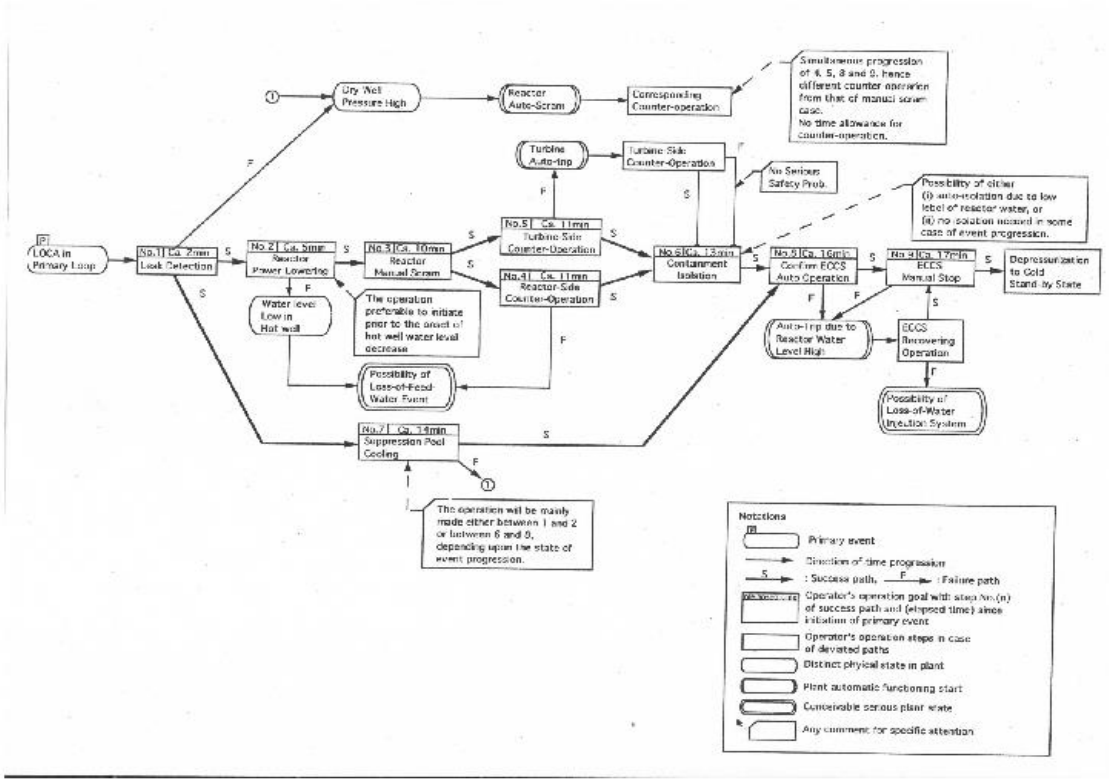

Fig. 5 Example task transition diagram for BWR operators coping with LOCA.

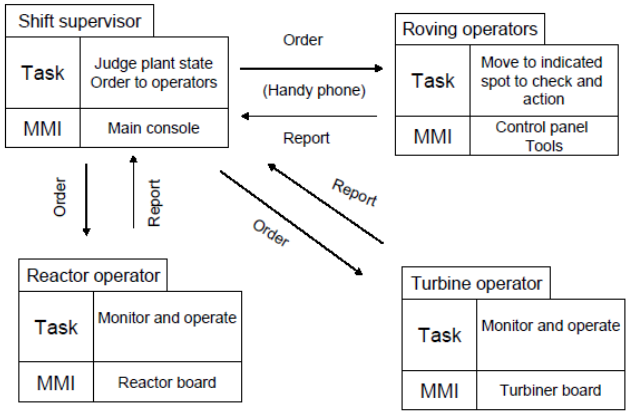

Fig. 6 Example operators configuration and the communication path diagram.

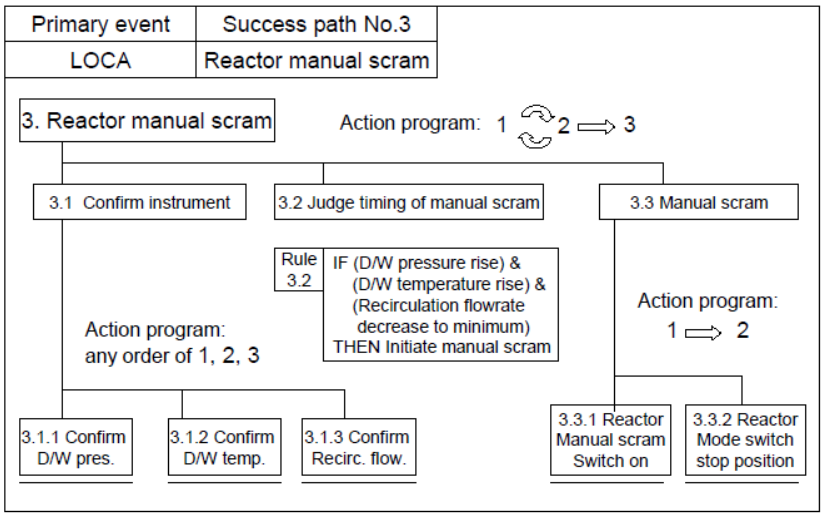

Fig. 7 Example hierarchical task analysis diagram for success path No.3 of Figure 5.

Table 2. Example action mode analysis table for success path No.3 of Figure 5.

Time m:s	MMI response	Action No.	Human error	Recovery step	Hazard propagation
00:10	D/W Pres. Hi. alarm		Skill based Slip such as misread, timing and selection		Possibility of no judgment of reactor Manual scrum
00:15	D/W Pres. Rising D/W Temp. Rising	3.1.1 Confirm D/W Pres.		3.1.2 3.1.3	
01:30	Recirc. flow change	3.1.2 Confirm D/W Temp.		3.1.3 3.1.1	
02:00		3.1.3 Confirm Recirc. flow		3.1.2 3.1.2	
04:00		3.2 Judge manual scram	Rule based misdiagnosis	Automatic scram by D/W Pres. High	No concern even if no manual scram
05:00		3.3.1 Reactor manual scram	Skill based slip of switch on	Automatic scram by D/W Pres. High	No concern even if no manual scram
05:05	Reactor scram alarm				
08:00		3.3.2 Reactor mode switch to stop position	Skill based slip of switch rotation	None	No change of interlock if no reactor mode change

Table 3. 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

3.5 Discussion on prerequisites of developing functional modeling method

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". Figure 8 shows a classification of operation modes for nuclear power plant operation which corresponds to types of analysis scenario.

<table>
<tr><td colspan="3">Classification of operation modes</td></tr>
<tr><td rowspan="4">A. Design basis</td><td rowspan="2">Normal operation</td><td>Start-up, Power change and Shutdown</td></tr>
<tr><td>Refueling and maintenance testing</td></tr>
<tr><td>Off-normal</td><td>Anticipated transient/accident</td></tr>
<tr><td colspan="2">Design basis severe accident</td></tr>
<tr><td colspan="3">B. Beyond design basis situations which include imaginary situations</td></tr>
</table>

Fig. 8 Classification of operation modes for nuclear power plant.

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 Figure 8) and "out of normal imagination" situations (B in Figure 8).

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 are what is called "emergence" (A new property or a new function will give rise from the existing partial property and function) in the case of occurring unfamiliar situation and the way of creating proper countermeasures to judging the monitored situation and preventing or mitigating the consequence of the accident situation.

It is difficult to consider all the problems at the present stage of the development, and therefore only the issue of how to configure human-machine interaction model as the basis of plant DiD risk monitor for any types of analysis scenario. Concretely, they are composed by (i)State transition diagram, (ii)Basic task element diagram, and (iii)Composite task element diagram. The basic ideas on how to develop those three diagrams will be explained in the subsequent section 3.6. Also a short discussion on proper user interface of plant DiD risk monitor for managing those diagrams and for analyzing specific application problem is given in the last part of section 3.6.

3.6 Integrated functional modeling for Plant Defense in depth risk monitor

This section summarizes software elements necessary to configure Plant Defense in depth risk monitor.

3.6.1 State transition diagram

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

- Relation between Original state, external input or disturbance and Outcome state should be semantically described.
- The state transition will be caused by either autonomous machine behavior or human-machine interaction. Then trigger condition of state transition should be described.
- Each state should assign both the risk level and the degree of risk (L, and T) by some computational means.
- The "hardware model" (*i.e.*, both solid matter and non-solid matter models) should be formulated in accordance with the analysis scenario.

3.6.2 Basic task element diagrams

These are also realized as object-oriented knowledge bases for individual basic task elements seen in the related operation procedure, where the following conditions should be equipped:

- Name ; Explain its meaning
- Input; what to see and by what way to judge
- Means; what to do for which by what way
- Right outcome; what's target result by what criterion to judge as right and what to do next
- Unwanted outcome; what will be the said states and what to do next.

3.6.3 Composite task element diagrams

This is realized as an object-oriented knowledge base to generate a complex task element by

composing from individual basic task elements, where the following conditions should consider:

- Name ; Explain its meaning of the composite task
- Method of how to synthesize the composite task.

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

- Input; what to see and by what way to judge
- Means; what to do for which by what way
- Right outcome; what's target result by what criterion to judge as right and what to do next
- Unwanted outcome; what will be the said states and what to do next.

3.6.4 User interface of plant DiD risk monitor

The discussion in this subsection corresponds to the software part of the functional modeling approach as listed in the previous Table 3. There are at least two different subjects for developing the user interface of plant DiD risk monitor. They are: (i)user interface for knowledge base management to register, update and delete various kinds of diagrams as mentioned in 3.6.1 to 3.6.3, and (ii)user interface for analyzing various aspect of risk problem on the target plant system by a selected analysis scenario from Figure 8. Regarding the latter interface of (ii), issues to be in concern were already discussed in the second paragraph of subsection 3.5.

4 Preliminary study on Integrated functional modeling for Plant Defense in depth risk monitor for AP1000

The authors would like to explain the reason why selecting AP1000 as the target for developing a plant DiD risk monitor in the first place. It is said that the AP1000 employs passive safety systems while reducing the number of active safety systems in order to significantly improve the plant safety design, simplification, cost reduction, *etc*.[10]. The major reason of adopting many passive safety systems in the AP1000 is to decrease the possibilities of hardware failure and human error. The authors of this paper have been conducting on the developing reliability monitor for the safety system of AP1000 to evaluate its reliability in the event of large break loss-of-coolant accident (LBLOCA) with comparing that of conventional PWR[11]. And the authors' study will proceed to the developmental study of plant DiD risk monitor in the next step also for AP1000.

In the second place, it is also necessary to explain the different roles of reliability monitor and plant DiD risk monitor by using the task transition diagram of BWR for LOCA as depicted in Figure 5. It is the role of the reliability monitor that it can analyze the success probability values of individual phases along the success sequence from the onset of LOCA until some safely standby condition. The GO FLOW method is used to evaluate the dynamic reliability values for individual phases as well as that for whole success sequence path, while FMEA evaluates the possible failure factors and the severity of its failure consequence.

On the other hand of reliability monitor, plant DiD risk monitor will give various preconditions to the reliability monitor, which will be decided by selecting a specific analysis scenario as listed in Figure 8. This means that plant DiD risk monitor will assume specific internal and external factors of common cause failure, based on which condition the reliability monitor should conduct on FMEA and GO FLOW calculation. Another role of plant DiD risk monitor is that it can deal with the risk evaluation of various blocks in Figure 5, in order to help conducting "emergence simulation" on "IF failed THEN what happen or how to detect, counteract, *etc*.".

Therefore, the authors' developmental study along the above stated direction will proceed roughly by the following steps:

(i) Write P&ID of AP1000 including its safety systems and convert them to MFM model with GO-FLOW chart,

(ii) Construct task transition diagram and the relevant diagrams and tables for the case of AP1000 for LBLOCA,

(iii) Convert the above diagram information to the three diagrams as mentioned in 3.6.1 to 3.6.3 to be usable as proper knowledge base,

(iv) Designing the first user interface function for handling the data as mentioned in (iii),

(v) Designing the second user interface function to conduct on interactive analysis with reliability monitor, and lastly

Develop the function of conducting "emergence simulation" of "what will happen, what will be the consequence, *etc*.".

5 Concluding remarks

The progress of the author's developmental study on a new risk monitor system was 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 fundamental assumption of such risk monitor system, method of configuring the whole system by plant Defense in Depth (DiD) risk monitor and reliability monitor, and the progress of development thus far conducted are first summarized, and then the result of preliminary study on how to configure the Plant Defense in Depth Risk Monitor by object-oriented software system based on functional modeling approach is presented as central subject of this paper.

Further study will be conducted for the conceptual design of the proposed method. And then, the study of how to apply the concept for AP1000 will be started in parallel to the development study of reliability monitors of AP1000. The concrete image of plant DiD risk monitor will be emerged and materialized step by step during the evolutional process of AP1000 application study.

References

[1] USNRC: Reactor Safety Study An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400, NUREG-75/014 (1975).

[2] IAEA Training Course on Safety Assessment of NPPs to Assist Decision Making: Risk Monitoring tools: Requirements of Risk Monitoring tools: relation with the Living PSA, applications of Risk Monitors. (http://www-ns.iaea.org/downloads/ni/training/specific_expert_knowledge/safety%20assessment/IV%203_11.6%20Risk%20Monitoring%20tools%20(coment1).pdf) (As of September 25. 2013).

[3] IAEA and OECD/NEA: The International Nuclear and Radiological Event Scale. User's Manual. 2008 Edition (2009).

[4] YOSHIKAWA, H., LIND, M., YANG, M., HASHIM, M., and ZHANG, Z.: 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.

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

[6] HASHIM, M., MATSUOKA, T., YOSHIKAWA, H., and YANG, M.: 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.

[7] YANG, M., ZHANG, Z., YOSHIKAWA, H., LIND, M., ITO, K., TAMAYAMA, K., and OKUSA, K.: Integrated method for constructing knowledge base system for proactive trouble prevention of nuclear power plant, Nuclear Safety and Simulation, Vol. 2, Number2, June 2011: 140-150.

[8] LIND, M.: A Goal-Function Approach to Analysis of Control Situation, Proc. 11th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design and Evaluation of Human-Machine Systems, August 31-September 3, 2010, Valenciennes, France.

[9] YOSHIKAWA, H.: An investigative study towards constructing anthropocentric man-machine system design methodology, Proc. Post ANP' 92 Conference Seminar on Human Cognitive and Cooperative Activities in Advanced Technological Systems: 25-36 (1992).

[10] SCHULZ, T.L.: Westinghouse AP1000 advanced passive plant, Nuclear Engineering and Design, 2006 (236): 1547-1557.

[11] 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.