Configuration of risk monitor system by plant defense-in-depth risk monitor and reliability monitor

YOSHIKAWA Hidekazu, LIND Morten, YANG Ming, HASHIM Muhammad, and ZHANG Zhijian

College of Nuclear Science and Technology, Harbin Engineering University, Harbin, 150001 China
(yosikawa@kib.biglobe.ne.jp)

Abstract: A new method of risk monitor system of a nuclear power plant has been proposed from the aspect by what degree of safety functions incorporated in the plant system is maintained by multiple barriers of defense-in-depth (DiD). Wherein, the central idea is plant DiD risk monitor and reliability monitor derived from the five aspects of (i) design principle of nuclear safety based on DiD concept, (ii) definition of risk and risk to be monitored, (iii) severe accident phenomena as major risk, (iv) scheme of risk ranking, and (v) dynamic risk display. In this paper, the overall frame of the proposed risk monitor system is summarized and the detailed discussion is made on major items such as definition of risk and risk ranking, anatomy of fault occurrence, two-layer configuration of risk monitor, how to configure individual elements of plant DiD risk monitor, and lastly how to apply for a PWR safety system.
Keyword: risk monitor; plant DiD risk monitor; reliability monitor; risk ranking; PWR safety system

1 Introduction

Nuclear power plant is a large-scale complex engineering system, and it is a typical example of safety-critical system because it contains and deals with dangerous radioactive materials. Therefore, maintenance of safety is strongly requested for the operation of nuclear power plants. The objective of the authors' presented study is to develop a systematic and comprehensive risk monitor system of nuclear power plant by the application of advanced ICT (information and communication technology) to enhance the safety of nuclear power plant throughout the whole process of design, operation and maintenance of nuclear power plant.

The authors of this paper had proposed a new concept of distributed human interface system to integrate various supporting functions for both operation and maintenance of nuclear power plant [1]. The first step of the proposed concept had been to develop an integrated method for constructing knowledge base (KB) system for proactive trouble prevention [2]. The major ideas employed to construct KB for proactive trouble prevention are: (i) structuring trouble KB for trouble prediction and prevention, (ii) realizing such KB by using web database, (iii) modeling plant system by the combinations of various shapes and composition of rigid things such as nuclear fuels, reactor vessel, piping tubes (*i.e.*, solid matters), and various liquid and gas to fill in the void space of the rigid things and flow through them *(i.e.*, non-solid matters), (iv) modeling such solid matters as object-oriented KB where described are how the solid matters are composed by the combination of structural components (pipe, vessels, *etc*.) and electrical circuits, their usage method and environmental conditions and knowledge on troubles, and further (v) modeling non-solid matters by the Multilevel Flow Model (MFM) to describe the semantic meaning of how the control system of process plants works functionally, by utilizing icons and symbols [3]. This MFM method had been applied for a prototype fast reactor Monju to describe the whole plant system with steady state power control system [4]. The MFM has been further being extended to be able to describe the change of control mode of the whole control system of Monju plant from its cold shutdown state to full power operation mode. [5]

The second subject of this paper is related with "risk" of nuclear power plant (NPP). Wherein, the authors of this paper followed the definition of "risk" of the NPP as "possibility of various hazard brought by

Received date: June 7, 2012
(Revised date: June 23, 2012)

severe accident". This definition is broader than the definition of "core melt frequency" employed in the level 1 PRA (probabilistic risk assessment) or PSA (probabilistic safety assessment) NPP.

The authors especially took notice on the concept of "risk monitor" in the actual application of PRA currently being used for the operation and maintenance management of NPPs. The authors expanded the risk monitor concept of normal operation to be applicable for various accident situations from prior to core melt to after core melt. The basic idea of the authors' risk monitor system is the division of "plant DiD risk monitor" and "reliability monitor" to monitor by what degree of safety functions incorporated in the plant system is maintained by multiple barriers of defense-in-depth (DiD) [6]. Wherein, how to comprise "plant DiD risk monitor" and "reliability monitor" was discussed from the four aspects: (i) design principle of nuclear safety to realize defense-in-depth concept, (ii) definition of risk and risk to be monitored, (iii) severe accident phenomena, and (iv) scheme of risk ranking. As will be explained later in this paper, the reliability monitors will be used to evaluate the reliability of individual sub-systems to comprise the whole safety system, while plant DiD risk monitor will serve to evaluate the intactness of the whole safety system by the result of individual reliability monitors.

The image of distributed human-machine interface system of plant DiD risk monitor and reliability monitor was also elaborated in [6] together with the discussion on how to visualize risk state intuitively as "dynamic risk monitor" as the display to human. Wherein, the method of reliability monitor was also examined for containment spray system in PWR plant by combining a failure mode and effect analysis method (FMEA) [7] and a dynamic reliability analysis method called GO-FLOW [8].

In this paper, the overall frame of the authors' proposed frame on risk monitor system will be first summarized in 2, and then the detailed discussion will continue in 3 with respect to the definitions of major terminologies of risk, risk ranking, anatomy of fault occurrence, two-layer configuration of risk monitor, how to configure individual elements of "plant DiD risk monitor" and lastly how to apply the two-layer configuration of risk monitor for a PWR safety system.

2 Risk monitor system

2.1 Definition of risk monitor

The word "Risk Monitor" traditionally used in nuclear application has been a specific application of a Living PSA [9] as a real-time analysis tool used to estimate the point-in-time "risk of core melt accident". Wherein, the real-time analysis is based on the actual plant configuration defined in terms of power operation or one of the shutdown modes, the components that have been removed from service, the choice of running and standby trains for normally operating systems, and setting the environmental factors. The term Risk Monitor has been defined by IAEA [10] as "a plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components. At any given time, the Risk Monitor reflects the current plant configuration in terms of the known status of the various systems and/ or components. The Risk Monitor model is based on, and is consistent with, the Living PSA. It is updated with the same frequency as the Living PSA. The Risk Monitor is used by the plant staff in support of operational decisions."

The authors' proposed risk monitor system is basically the same as the above definition of risk monitor, but the distinction lies in the definition of "risk". The range of risk is not limited in core damage accident but includes all kinds of dangerous states brought by severe accident. Accordingly, the configuration of the authors' risk monitor system should be different from the traditional living PSA tools as to the way of how to organize the risk monitor and how to display the risk on the human interface. The basic features of the authors' risk monitor system are introduced in the subsequent sections with respect to: (a) Definition of risk and risk ranking, (b) Anatomy of fault event occurrence, (c) Risk monitor by semiotic modeling, (d) Plant DiD risk monitor and reliability monitor, and (e) Visualization as dynamic risk monitor.

2.2 Definition of risk and risk ranking

2.2.1 Design principle of nuclear safety

The safety of NPP is based on the Principle of Defense-in Depth (DiD), *i.e.*, multiple barriers against radiological release to the environment. There

are four barriers of nuclear reactor: nuclear fuel, cladding, pressure boundary of reactor coolant including reactor vessel and containment. The intactness of individual barriers is assured by three safety functions of (a) STOP nuclear reaction, (b) COOL reactor, and (c) CONTAIN radiological release.

The reliability of individual safety functions is enhanced by adapting the principles of diversity, redundancy and physical separation, while aggravated by common cause factors in initiating failure events.

2.2.2 Risk to be monitored

There are many ways of defining "risk" brought by NPP operation, however the authors put the emphasis on safety protection of the environment, and define "risk" as the radioactive hazards as the outcome of various possible state of "Severe accidents by core melt".

2.2.3 Risk by severe accident

The researches on severe accident have been extensively conducted worldwide to obtain knowledge on what kind of phenomena occur to develop into severe accident in the light water reactor (LWR) and by what way it should be avoid by the basic safety design principles as well as additional introduction of various safety measures for severe accident management. By conducting on literature surveys on severe accident research world wide, the authors of this paper obtained basic knowledge on the major phenomena to be considered for the severe accident prevention and management as well as the related severe accident analysis codes.

(1) Summary of severe accident phenomena

A summary of major accident phenomena which are of interest for safety analysis of LWR is shown in Table 1. In Table 1, various phenomena appears in the safety analysis for the severe accident of LWR are listed up on major behaviors of nuclear fuel, coolant and violent material interaction on one hand while different types of accident (*e.g.*, transient over-power and loss of coolant accident) on the other hand. The various phenomena classification seen in Table 1 is based on possible losses of the three safety functions: STOP the nuclear fission, COOL the reactor and CONTAIN the radiological release.

(2) Phenomena progression in severe accident

With regards to the phenomena progression in severe accident, it can be roughly divided into three stages: (i) phenomena within reactor pressure vessel (RPV), (ii) phenomena within containment vessel (CV), and (ii) off-site fission product (FP) release and environmental consequences. The phenomena within

Table 1 Summary of various accident phenomena in the accident of light water reactors

Severe accident phenomena	Transient over-power	LOCA
Fuel behaviors which encompass fuel failure and meltdown	Fuel swelling Fuel failure and melting Pellet-clad interaction Fuel relocation/slumping	
Heat transfer and coolant behaviors which may lead to loss of coolability		Abnormal flow conditions in two-phase flow and natural circulation Departure from nucleate boiling (DNB) Blow-down, refill, quench, re-flooding Counter current flow limiting (CCFL)
Various violent interaction behavior mainly related to failure to contain radiological release by the ruptures of reactor vessel and containment vessel	Fuel coolant interaction (FCI) Zr-water reaction Hydrogen explosion Steam explosion Corium-concrete reaction Direct containment heating	

RPV would proceed by five stages of off-normal thermal-hydraulics, core melting, FP release from fuel, FP transport in reactor coolant system (RCS), and failure of RPV, whereas those within CV, molted core (debris) concrete interaction, FP release from debris, FP transport in containment, thermal/mechanical load to CV and finally CV failure.

Those phenomena progression in case of severe accident is indicated at the top part of Fig.1, where you can see the names of those phenomena from left to right with the progression of severe accident. There have been a lot of analysis codes developed around the world for severe accident related phenomena.

(3) Severe accident analysis codes

The start of systematic development of severe accident analysis codes for LWR may be at the time of Rasmussen report in 1975 on the probabilistic risk assessment (PSA) of commercial nuclear power plants in USA [11]. Since then the research and development of severe accident analysis codes has been progressed from the period in 1980'-90'after TMI accident and Chernobyl accident until these days. The historical trend of the severe accident analysis codes can be said that in the early days rather simple analysis methods for individual phenomena had been developed as independent computer codes, but these separate efforts had then integrated into the larger scale codes system with more accurate simulation tools to cover whole ranges of accident scenario and accident progression than before, with the progress of computer simulation technologies. The names of representative severe accident analysis codes developed thus far mainly in USA with a few examples research works by French researchers at IPSN (Institute Protection Surete Nuclaire) and Japanese researchers at JAERI (Japan Atomic Energy Research Institute) are shown in Fig.1 by classifying into individual source term codes, integrated code and detailed mechanistic codes with their simulating capabilities of specific severe accident phenomena.

(4) Comparison of different severe accident analysis codes

An example of comparative calculation of different severe accident analysis codes was made by A. Hidaka, *et al.* [11], for a small loss of coolant accident (LOCA) in a Boiling Water reactor (BWR) where the

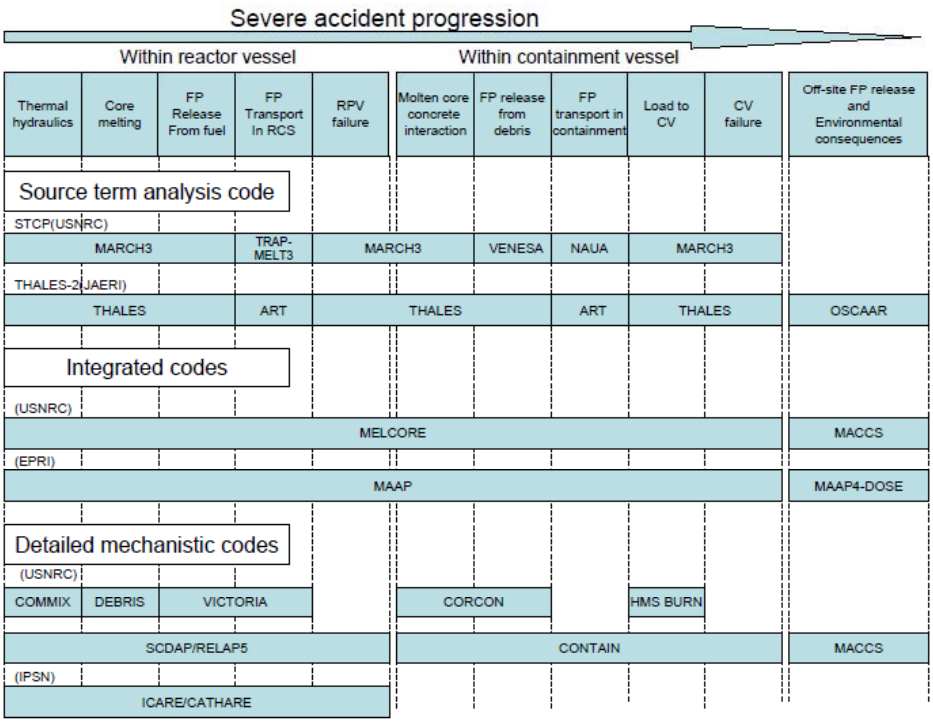

Fig.1 Severe accident sequence and the related severe accident codes.

utilized severe accident analysis codes were STCP [12], THALES-2[13], and MELCORE[14]. The inter-comparison of the three codes for the calculated event sequence and the timing is given in Table 2, where you can see that the progression of severe accident would proceed rather fast in time, although the code prediction by three codes differs with each other by the difference of physical models employed in each code. It is also seen from this Table 2 that fast detection of accident symptom as well as fast and sure provision of the effective counteraction is very important for the risk monitor to preclude the plant situation to develop into more serious state of severe accident.

Table 2 Calculated events sequence and its timing in case of small LOCA of a BWR

Events	STCP (min)	THALES-2 (min)	MELCOR (min)
Core uncover	5.3	14.6	18.8
Core melt initiation	40.3	46.6	55.2
Core support failure	59.6	60.4	90.9
Core collapse	56.7	123.5	---
Vessel failure	79.7	141.6	175.1
Containment failure	254.4	384.2	574.5

(Source of this table: reference [12])

2.2.4 Risk ranking

It is very important to have reliable instrumentation and control (I&C) systems in the plant, and it is also requested to I&C systems that can work even in off-normal accident situation. To decide which risk level the plant is, you should take into account of the following factors: (i) Status of individual subsystems and equipments for maintaining the safety function of STOP, COOL and CONTAIN, (ii) Degree of redundancy, diversity, physical separation, (iii) Kind of initiating events, common cause factors of internal event and external event, and (iv) Kind of reactor state.

The kinds of reactor state at normal plant operation are full power operation with/without online maintenance, various stage of shutdown maintenance. However in the authors' presented risk monitor study, you should also take into account of the accident situation including severe accident. The resultant definition of deciding the risk level is given in Table 3, where six-level risk ranking is taken from the eight combinations of STOP, COOL and CONTAIN. In Table 3 the number 1 of individual safety function means that it works successfully while the number 0 in failure state. According to this risk ranking, no risk state is level 0 while the highest risk state is level 5.

The risk ranking method shown in Table 3 is basically premature idea and it is not so rigorous one. First, you should be careful by what way to decide

Table 3 An example of risk ranking

Risk level	Stop	Cool	Contain	Possibility of severe accident
0	1	1	1	No risk Safely shutdown, cooled and no release
1	1	1	0	No severe accident phenomena but some problem in containment
2	1	0	1	Loss of not so serious cooling function Safely shutdown, but cooling failed but no release
3	1	0	0	Serious severe accident possible Safely shutdown, but both cooling and contain function failed
3	0	1	1	Severe accident may be suppressed by ESF function Shutdown failed but cooling and no release
3	0	1	0	Some contain function failed Shutdown failed , cooled but released
4	0	0	1	Serious though severe accident phenomena occurr because containment function succeeded Shutdown failed , cooling failed but no release
5	0	0	0	Worst severe accident because all safety functions failed

success (1) or fail (0) of each safety function of STOP, COOL and CONTAIN. Second, the risk levels 1 to 5 should be carefully decided by evaluating by what degree the plant would be damaged by the knowledge base on various severe accident phenomena, or by what degree each of the three safety functions of the plant are aggravated by initiating event.

However by Table 3, you can intuitively assign that the risk rank of Chernobyl accident in 1986 in former Soviet Union is the largest one of 5, because all three safety functions were lost by reactor excursion accident initiated by operator error. Whereas the rank of TEPCO's Fukushima Daiichi accident happened in Japan in 2012 was 3, where STOP nuclear reaction was successful even for the largest earthquake in Japanese recorded history, but all COOL functions were lost by the attack of tsunami as high as 13 meters and the ensuing reactor core melt with hydrogen explosion destroyed the CONTAIN functions of the plants.

By Table 3, the risk level of the accident reactor will change with the change of three safety functions during the accident and even after the cease of accident. You should also assign risk levels of Chernobyl reactor and all four reactors of TEPCO's Fukushima Daiichi station at their present post accident situation. Those reactors are and will be still risky state until their complete decommissioning in the future.

2.3 Anatomy of fault event occurrence

Risk situation (hazard) is brought by the disruption of individual safety functions by both factors of internal and external disturbance to the plant. Internal factors are various machine failures by inappropriate usage to cause fatigue, wastage, *etc*, as well as by human error. External factors are caused by various natural disasters such as earthquake, fire, flooding, tsunami as well as human-caused events such as sabotage, terrorism, airplane collision, *etc*. Please note that the cause of Chernobyl accident was internal factors (human factors) while that of Fukushima Daiichi accident, external factor (earthquake and tsunami) with the root cause being in common for the both big accidents is the lack of provision in safety design of the plant system. Therefore, it is very important to consider common mode failure (CMF) which would cause more risky situation by the superimposition of internal and external factors with respect to the spatial range of its influence, timing and frequency to bring more hazardous situation than by single independent event occurrence.

The treatment method of CMF and its application for the authors' risk monitor whether "plant DiD risk monitor" or "reliability monitor" can be summarized as shown in Table 4, by referring the procedure employed in probabilistic safety assessment (PSA)

Table 4 Viewpoint of treating common mode failure

Clearness of fault cause	Influencing span of fault cause	Types of fault cause	Coupling mechanism	Analytical treatment	Risk monitor
Clear Randomly or steadily Exist	Whole plant	Earthquake	Spatial	Explicit	Plant DiD Risk monitor
	Combined subsystem	Fire, flood, tsunami	Spatial	Explicit	
		Functional relation	Functional	Explicit	
		Common share of support equipment	Functional		
		Change of physical environment by equipment failure	Spatial		
Unclear	Single subsystem Individual equipment	Physical environment (high temp, high pressure,)	Spatial	Explicit Parametric	Reliability monitor
		Design, Fabrication	Human factors		
		Maintenance, Check,	Human factors		
		Human factors in operation	Human factors		

for NPP. In Table 4, the word "explicit" is here to treat the related CMF factors as individual "headings" of event tree analysis while "parametric" means treating CMF by utilizing various parametric modeling method such as beta factor method, MGL (multiple Greek letter) method, BFR (binomial failure rate) method. Also in Table 4 the authors assumed that the consideration of CMF over the whole plant or the several subsystems is treated in the "plant DiD risk monitor", while it is made for a single subsystem or equipment in "Reliability monitor".

2.4 Configuration of risk monitor

2.4.1 Risk monitor composed by two-layer system

The presented risk monitor would be a useful tool to manage the damaged plant in real severe accident situation. It is very rare that your plant would commit or encounter severe accident, but even if it is very rare it is good training to conduct always on (A) "mind thinking experiment" on what risk will bring about in the plant if something extraordinary situation happens, in addition to conduct on (B) "daily ordinary risk informed monitoring" of plant operation and maintenance for the whole plant system.

To cope with the both (A) and (B), the authors of this paper propose to compose the risk monitor by two-layer system. "Risk monitor" is organized as "plant DiD risk monitor" (for the layer A) to know potential risk state caused by severe accident phenomena to the plant system as a whole, from the daily monitoring of the reliability state of individual subsystems and equipments by "reliability monitor" at local worksite (for the layer B). "Plant DiD risk monitor" should know the risk state of plant system from the view whether or not the three safety functions of (a) STOP nuclear reaction, (b) COOL reactor, and (c) CONTAIN radiological release are maintained in advance as well as on time for both on power operation and shutdown phases.

2.4.2 Plant DiD risk monitor and reliability monitor

The image of the authors' distributed human-machine interface system of plant DiD risk monitor and reliability monitor is illustrated in Fig. 2. In Fig. 2, plant DiD risk monitor system is the user interface system in the main control room, while reliability monitor systems may be installed either on maintenance console or the maintainers' handheld computer at their workplace.

The knowledge base system of reliability monitor in Fig. 2 will be comprised by various knowledge information such as (i) Non-solid matter model of whole plant by revised MFM, (ii) Knowledge based solid matters models for individual subsystems and equipments, (iii) GO-FLOW Diagram and the related

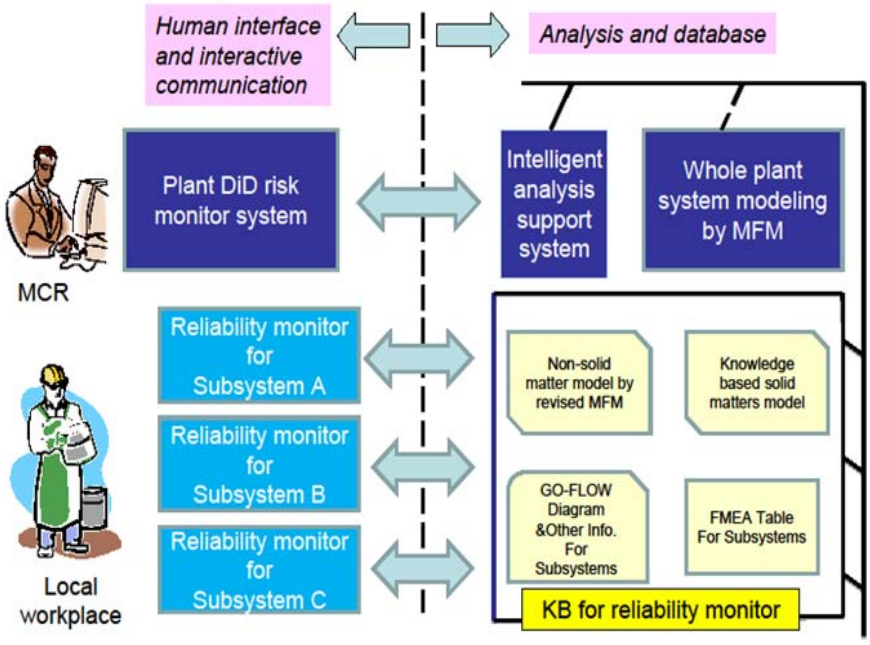

Fig. 2 Plant DiD risk monitor and reliability monitor.

information for individual subsystems, (iv) FMEA Table for individual subsystems, and so forth. The knowledge base system of reliability monitor would be in common use by all the users both in the main control room and the local workplace through the internet over the plant site. The detailed discussions on the knowledge base system of reliability monitor have been presented in the authors' previous papers [2, 5]. While on the part of plant DiD risk monitor, it will be separately discussed in Chapter 3 including intelligent analysis support system and whole plant system modeling by MFM.

3 Plant DiD risk monitor

In this chapter, the authors of this paper firstly introduce the basic ideas on how to compose the plant DiD risk monitor is first discussed for the parts of (i) Human interface and interactive communication and (ii) Analysis and database which are shown in Fig.2. Then they will proceed to an example practice on the plant DiD risk monitor for a safety system of PWR plant.

3.1 Human interface for interactive communication

3.1.1 Display as dynamic risk monitor

In the actual nuclear power plant, risk state will change in time and by operation mode, *i.e.*, start up and shutdown, steady state power operation, plant configuration change by online maintenance, shutdown maintenance, and abnormal/accident situation. The plant DiD risk monitor should estimate the time changing risk state of the whole plant with enough accuracy and fast computation time for visualizing risk state "by Defense-in-Depth manner" with the degree of severity of plant state. It is also important to visualize the time changing risk level of whole plant by the form intuitively understood by operators in the MCR as well as by the supporting staffs in the remotely located emergency response center in the event of severe accident.

The essential idea of the authors on how to display time changing risk level as "Dynamic risk monitor" for the operator in MCR is depicted in Fig. 3. In Fig. 3, time varying risk state is displayed as a moving point (trajectory of yellow point in Fig.3) on TL-plane, where T is Time margin until reactor becomes dangerous state and L is Safety margin of various plant parameters which represent the status of three safety functions of STOP, COOL and CONTAIN.

This display shown in Fig.3 is constituted by multiple sheet to visualize different risk level of risk ranking as shown in Table 3.The origin O of LT-plane means Danger point (L_0, T_0) within a risk ranking level 0, where T_0 and L_0 mean no time margin and no safety margin to go from a risk ranking level 0 to a more high level 1. Note that in case of Table 3, range of risk level is from 0 to 5. Therefore, the yellow point of this dynamic risk monitor display will change in

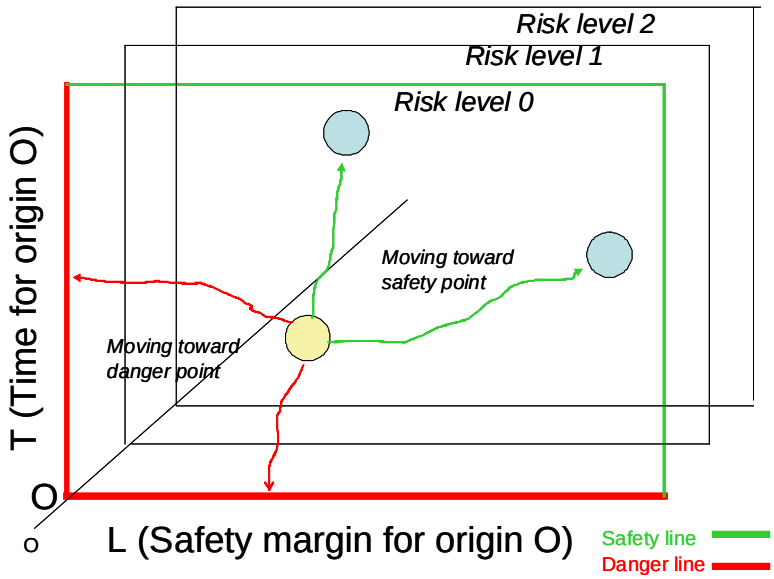

Fig. 3 Dynamic risk monitor as human interface.

accordance with the change of Defense-in-Depth (DiD), that is, degree of intactness of multiple barriers as well as the three safety functions. The yellow point shows estimated "risk value" for various risk ranking level in Table 3, for example, 0.1, 0.2, *etc*., in the risk ranking level 1, 1.1,1.2, *etc*., in the risk ranking level 2.

The dynamic risk monitor for the risk ranking level 0 corresponds to the risk monitor for a normal (no accident) state of plant during operation and shutdown. (Note: the risk ranking level larger than 1 describes the levels of accident in accordance with the severity of accident.) When the trajectory of risk state (indicated by yellow point on Fig.3) moves towards L-O axis or T–O axis it is approaching towards more dangerous state. (This means "risk value" will go up 0.3, 0.4, 0.6, *etc*., toward 1.0) And when the yellow point touches on the line of L-O axis or T–O axis, then the risk value at the risk ranking 0 is no more less than 1.0 and the risk ranking of the dynamic risk monitor will go up to a higher risk ranking level 1 or higher level than 1 depending upon the value of T_0 or L_0. And the yellow point on the dynamic risk monitor for new risk ranking level will change the position in the T-O-L graph.

But if the yellow point goes apart far away either from L-O axis or T–O axis it is in a safe state. In case of risk ranking level larger than 1, there may be a possibility of lowering the risk ranking level by the successful countermeasure of emergency management.

3.1.2 Where to apply dynamic risk display

The above idea is the basic display idea of dynamic risk monitor where you should consider that the risk ranking will be different in the plant operation mode as well as for different accident situation. It is also important when the plant configuration is intentionally changed from the normal operating condition as in the case of maintenance shutdown.

And further this dynamic risk monitor concept would become a useful tool to rate the level of severe accident by the way as shown in Table 3 of risk ranking. The estimation of the risk level of the damaged plant is made for both the progression and recovering phases of the accident by weighing the situation from the two aspects: that is, (i) by far the plant is severely damaged, and (ii) by what degree the makeshift recovery actions are successful for mitigating the radioactive release to the environment.

To sum up the above discussion on how to set parameters (T, L, O) (T: time margin, L: safety margin, and O: origin of T-O-L graph), the parameter L will change by Risk ranking as shown in Table 3, while the parameters T and O should be carefully defined by considering by what degree the safety barriers of nuclear reactor are damaged as well as how much time is left for the reactor state to reach fatal state. In order to prepare for the calculating module of the set of (T, L, O) in the dynamic risk monitor in the severe accident situation, it may be necessary to make full use of severe accident simulator. Considering those factors mentioned above, how to design dynamic risk monitor with effective computing module set of (T, L, O) will be the issues associated on the part of analysis and database as discussed in the subsequent part.

3.2 Analysis and database

3.2.1 Semiotic modeling by MFM

The essential ideas of how to apply the semiotic modeling for nuclear power plant has been already presented by the authors' papers [2, 5]. Non-solid matter model by the revised MFM developed by M. Lind [3] will be used to describe (i) Designer's Intention, and to infer (ii) Condition to cause Troubles, and (iii) Consequences of Troubles, wherein lower level break down to disassemble into subsystems and further into individual machines and equipments to describe cause and consequence of failure of subsystems and individual components by knowledge based solid matters model.

The MFM modeling method revised by M. Lind [3] to enhance the description capability of control system of the process plant and the proposed graphical method was applied for a complicated plant system of Japanese Fast Breeder Reactor Monju which includes the steady state plant control system [4].

However, the above MFM method is not direct way of configuring the Defense-in-Depth risk monitor, although it can describe graphically the whole plant system which is composed of (i) basic plant system and (ii) control and safety systems. The authors

extend the discussion on how to configure the Defense-in-Depth risk monitor, with concentrating on the point of what is defense-in-depth with respect to risk monitor.

3.2.2 What is defense-in-depth risk

The ultimate risk caused by nuclear reactor plant is the release of radioactive fission products (FPs) to the environment from the nuclear reactor. There are multiple barriers in nuclear power plants to prevent FP from releasing to the environment. They are fuel rod, reactor coolant system (RCS) including reactor vessel, and containment vessel.

The intactness of those barriers is maintained by originally implemented material design consideration with the appropriate safety design of the three safety functions of STOP, COOL and CONTAIN together with the adoption of appropriate safety principles such as functional diversity, physical separation, redundancy, *etc.*

So what is defense-in-depth risk? It is the degree of risk level in the risk ranking table as explained in 2.2.4, and it is determined by the intactness of multiple barriers, the state of three safety functions and the provision of appropriate safety principles.

To sum up, the displayed point by yellow color on the risk level plane 0 in Fig.3 is the output of plant DiD risk monitor, while the output of conventional risk monitor is the instantaneous core melt frequency given by living PSA.

3.2.3 How to determine degree of defense-in-depth risk

There are two factors to estimate defense-in-depth risk. The one is high-lightening where the multiple barriers lie in the integrated system of non-solid matters model by MFM with solid matter model. This part will correspond to “whole plant system modeling by MFM” in Fig.2.

Then the intactness of those barriers should be evaluated by some appropriate computing model where each state of three safety functions (STOP, COOL and CONTAIN) are employed as major parameters to decide the intactness by seeing the conditions of various flows (water, heat, FPs, *etc.*) and to know how to and by what degree individual barriers be affected. This part will correspond to “intelligent analysis support system” in Fig.2.

3.3 Example application for PWR safety system

The authors of this paper have been applying the basic idea of plant DiD risk monitor and reliability monitor as illustrated in Fig.2, for a PWR safety system as shown in Fig.4. As seen in Fig.4, this safety system of PWR plant is composed by two safety sub-systems of (i) emergency core cooling system (ECCS) and (ii)

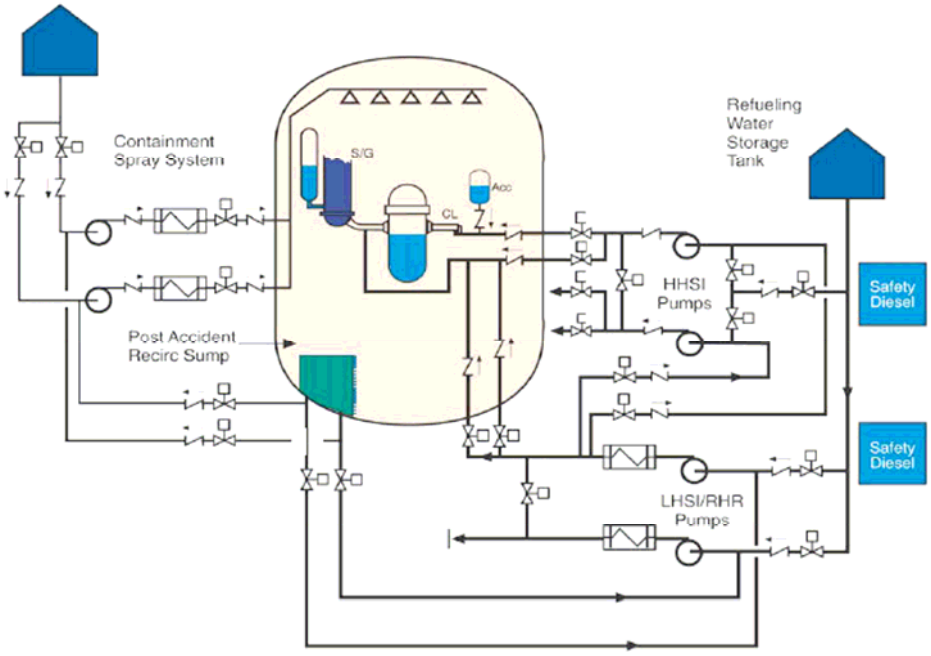

Fig. 4 Safety system of conventional PWR plant.

containment spray system.

3.3.1 Whole plant model by MFM

In the actual PWR plant, those two safety sub-systems are connected to the basic plant system which generate nuclear heat to produce high temperature water in the nuclear reactor, convey it through the primary loop, convert it to steam in the steam generator (SG), and then electric power is generated in the turbine by high temperature steam in the secondary loop. In addition, there are many basic components in PWR: pressurizer, chemical control volume system, various instrumentation and control systems, reactor protection system, air filter system, radioactive waste process systems, *etc*. Therefore, the whole PWR plant becomes very large and complicated system so that it will be very cumbersome work to write down the whole system by MFM.

3.3.2 Diagnosis of barrier intactness

On the other hand of describing the whole PWR plant system, the multiple barriers of this PWR system should be described as the hierarchical structure of the important components in the basic plant system in order to diagnose the intactness of individual barriers of the plant. Figure 5 is an example of how to describe the multiple barriers. As shown in Fig. 5, the components in the boxes (thick line and thin line) are important barriers which have to keep the intactness in the accident situations.

Those components constitute multiple barriers and if those barriers fail in sequence from left-hand to right-hand side, the risk of the plant will go up the level of the risk ranking as given in Table 3. In order to know how the individual barriers will be affected as to the intactness, you should basically notice the various physical and chemical conditions caused by flow of water and heat surrounding the respective barriers.

You can utilize those flow models drawn by MFM to reduce appropriate diagnostic algorisms to judge the intactness of the barriers in the initial phase of accident situation for online monitoring and diagnosis purposes. It is necessary to have various criteria to judge the breach of intactness. And it is necessary to consider various causes of troubles (Accident initiator) to hinder safety operation of nuclear power plant. You should also take into account of “common cause factors” for the accident initiators to give influences on the accident sequence as well as for the degradation of reliability of various components and subsystems.

3.3.3 Prognosis of accident progression

If the barrier would fail, then FP gas would blow out from the barrier. And the release of FP becomes concern for risk to the environment. Other situation may be that the geometry of solid matters comprising the component would distort or lost and if it becomes molten state, it will move upwards or downwards. However, you can no more apply MFM model for these severe accident situation. You will need severe accident analysis codes to evaluate the level of risk for those situations.

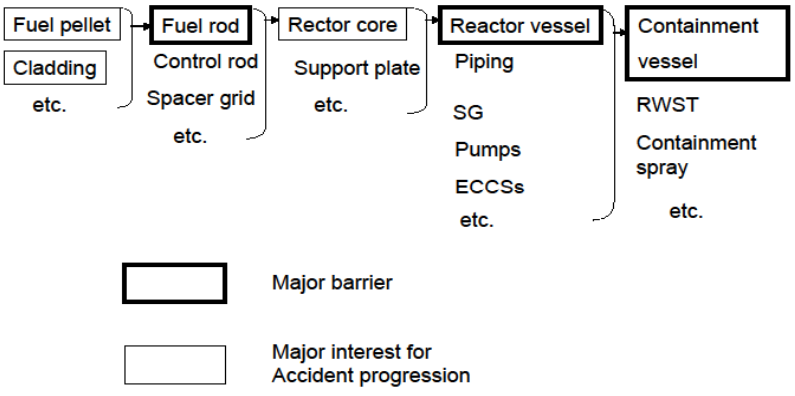

Fig. 5 Multiple barriers of PWR plant.

3.3.4 Condition setting to reliability monitors

The role of reliability monitor is to evaluate the risk of individual subsystems by utilizing FMEA and conducting GO FLOW analysis to estimate dynamic reliability of the individual subsystems. Here, you should notice that the preconditions for the evaluation by reliability monitors are all given by plant DiD risk monitor. Those conditions are such as (i) target subsystems, (ii) plant operation conditions and mode, (iii) types of accident initiators, (iv) common cause factors, (v) failure mechanism to be considered, (vi) failure data, *etc*.

Although not described further in this paper, some members of the authors of this paper have been starting to develop two reliability monitors of PWR safety sub-systems separately: one for containment spray system and the other for ECCS system, by utilizing GO FLOW program.

However, in case of conducting GO FLOW analysis for the both sub-systems, you should be careful about the available volume of water resources in the refueling water storage tank and containment sump to change from injection mode to recirculation mode in the event of loss of coolant accident.

4 Conclusion

A new method of risk monitor system of a nuclear power plant has been proposed by the authors of this paper from the safety aspect by what degree of safety functions incorporated in the plant system is maintained by multiple barriers of defense-in-depth (DiD). Wherein, the central idea is plant DiD risk monitor and reliability monitor derived from the five aspects of (i) design principle of nuclear safety to realize DiD concept, (ii) definition of risk and risk to be monitored, (iii) severe accident phenomena as major risk, (iv) scheme of risk ranking, and (v) dynamic risk display.

In this paper, the overall frame of the proposed risk monitor system was summarized and the details were described of major items such the definition of risk and risk ranking, anatomy of fault occurrence, two-layer configuration of risk monitor, and how to configure individual elements of plant DiD risk monitor. Further, the example application was introduced for applying the proposed risk monitor for a PWR safety system.

The authors' works until this paper have been mainly conceptual design for the whole risk monitor system, although they started to develop reliability monitors for the safety system of a conventional PWR plant.

In the next step, the authors will work further to develop MFM modeling for this safety system of PWR, intelligent support for diagnosing the intactness of multiple barriers, *etc*., in order to apply the proposed frame of plant DiD risk monitor for a specific issue of PWR plant.

Acknowledgment

The authors thank the financial support from National Natural Science Foundation (NFSC) of China (Grand No.60604036) and the 111 Project (Grand No. b08047).

References

[1] YOSHIKAWA, H.: Distributed HMI System for Managing all Span of Plant Control and Maintenance, Nuclear Engineering and Technology, 2009, 41(3): 237-246.

[2] 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, International Journal of Nuclear Safety and Simulation, 2011, 2(2)**:** 140-150.

[3] 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.

[4] LIND, M., YOSHIKAWA, H., JOERGENSEN, S.B., YANG, M., TAMAYAMA, K., and OKUSA, K.: Multilevel flow modeling of Monju Nuclear Power Plant, International Journal of Nuclear Safety and Simulation, 2011, 2(3):275-285.

[5] LIND, M., YOSHIKAWA, H., JOERGENSEN, S.B., YANG, M., TAMAYAMA, K., and OKUSA, K.:Modeling operating modes of the Monju nuclear power plant, Proc. ANS NPIC & HMIT2012, July 22-26, 2012, San Diego, U.S.A.

[6] YOSHIKAWA, H., YANG, M., HASHIM, M., LIND, M., and ZHANG, Z.: Design of Risk Monitor for Nuclear Reactor Plants, International Journal of Nuclear Safety and Simulation, 2011, 2(3): 265-273.

[7] As an example of FMEA method,
see URL: http://www.npd-solutions.com/fmea.html (As of January, 2010)

[8] MATSUOKA, T.: System Reliability Analysis Method

GO-FLOW for probabilistic Safety Assessment, CRC Sogo Kenkyusho, 1996. (In Japanese).

[9] FREEMAN, R., MOIR, R.: What is living PSA?, Nuclear energy, 1993, 32(6):355-362.

[10] IAEA-TECDOC-1106, Living Probabilistic Safety Assessment (LPSA), IAEA (1000).

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

[12] HIDAKA, A.: Comparative Study of Source Terms of a BWR Severe Accident by THALES-2, STCP and MELCOR, Proc. 1992 National Heat Transfer Conf.,HTC, 1992, 6:408-416.

[13] GIESEKE, J.A, *et al.*: Source Term Code Package: A User's Guide (Mod.1), NUREG/CR-4587(1986).

[14] KAJIMOTO, M., MURAMATSU, K., WATANABE, N.: Development of THALES-2, A Computer Code for Coupled Thermal-Hydraulics and FP Transport Analyses for Severe Accident at LWRs and Its Application to Analysis of FP Revaporization Phenomena, Proc. Int. Topical Meeting on Safety of Thermal Reactors, Portland, 1991:584-592.

[15] SUMMERS, R., *et al.*: MELCOR1.8.0: A Computer Code for Nuclear Reactor Severe Accident Source Term and Risk Assessment Analyses, NUREG/CR-5531 (1991).