Design of risk monitor for nuclear reactor plants

YOSHIKAWA Hidekazu[1], YANG Ming[1], HASHIM Muhammad[1], LIND Morten[2], and ZHANG Zhijian[1]

1. College of Nuclear Science and Technology, Harbin Engineering University, Harbin, China (yosikawa@kib.biglobe.ne.jp, yangmingheu@yahoo.com.cn)

2. Department of Electric Engineering, Technical University of Denmark, Kongens Lyngby, Denmark (mli@elektro.dtu.dk)

Abstract: In this paper, the method of how to comprise a concept of "plant Defense-in-Depth (DiD) risk monitor" and "reliability monitor" for nuclear power plant is discussed in detail. The discussion starts on the definition of risk and risk ranking on the items of (i) design principle of nuclear safety, (ii) risk to be monitored, (iii) severe accident phenomena, and (iv) risk ranking. After analyzing the anatomy of fault event occurrence from the view of common mode failure and considering the semiotic modeling of nuclear power plant as a whole by utilizing multilevel flow model (MFM), the image of distributed human-machine interface system of plant DiD risk monitor and reliability monitor is introduced. Also discussion is made on how to visualize risk state intuitively as "dynamic risk monitor" as the display to human. Then an example practice is presented for containment spray system of PWR by the proposed concept of "reliability monitor" with the application of FMEA and GO-FLOW analysis. The formation of "plant DiD risk monitor" by utilization of revised MFM will be the next step study for configuring the proposed concept for the "plant DiD risk monitor".

Keywords: risk monitor; risk ranking; FMEA; GO-FLOW; MFM

1 Introduction

It is needless to say that the operation and maintenance (O & M) for nuclear power plant (NPP) should be high safety and reliability with improved efficiency. To look at the technical trend of NPP around the world, digital instrumentation and control (I&C) and maintenance rationalization have been progressing: Digitalization of not only non-safety but also safety-grade I &C systems with full computerized Main Control Room (MCR) is prevailing around the world. Moreover, a new trend has appeared in Full Digital MCR in a Japanese PWR[1] as well as in French PWR[2]: Addition of maintenance console layers in Full digitalized MCR in addition to the operator console layers for operation and large screen display for information share.

Concerning plant maintenance of NPP, it has been shifting from traditional time based maintenance to condition based maintenance. The operation strategy of long time power operation with online maintenance and short time outage will be advantageous but it will necessitate frequent change of plant configuration not only during plant shutdown but also at power operation. This will lead to the following issues:

(i) Necessities of introducing plant configuration monitors, condition monitor tools and risk monitors, in addition to the already implemented various operator support system, (ii) Information share between operators and maintainers is needed in MCR to improve communication and work support among O&M staffs in MCR, roving operator, and maintainer at local machine site, and (iii) Operation support system should be more "distributed" in plant (MCR and local sites in the plant) and "connected" with each other.

This will lead to the introduction of new interface devices and display methodologies both for MCR and local workers. The authors had made proposal of a new network-integrated O & M support environment by connecting MCR and many local workplaces of machine maintenance by the introduction of advanced Information Communication Technology (ICT). The central idea on this network-integrated O & M support environment was Distributed HMI System as were presented at Refs.[3, 4]. And then they proposed a new idea of knowledge base system for proactive trouble prevention in Ref.[5]. In this paper, the authors will

Received date: August 16, 2011
(Revised date: September 15, 2011)

discuss on how to design, develop and implement the risk monitoring system, mainly for pressurized water reactor (PWR) plants.

2 Distributed HMI system

The proposed concept of distributed HMI system is a network-integrated O & M support environment by connecting MCR and many local workplaces of machine maintenance as illustrated in Fig. 1. In fact, the authors' idea of such networked support environment comes from the distributed diagnostic system which is developing at Monju plant[6]. The major items in the proposed concept are summarized as follows;

(a) Online plant data distributing over Plant Intranet with Cyber security and Reliability through Middleware from various sensors and equipments by intranet protocols,
(b) Online Plant Monitor & Diagnosis toolkits,
(c) Reliability Monitors for Various Subsystems and Equipment,
(d) Plant Defense-in-Depth (DiD) Risk Monitor for the whole plant,
(e) Proactive trouble prevention KB, and
(f) Human interface system both for MCR and local workers.

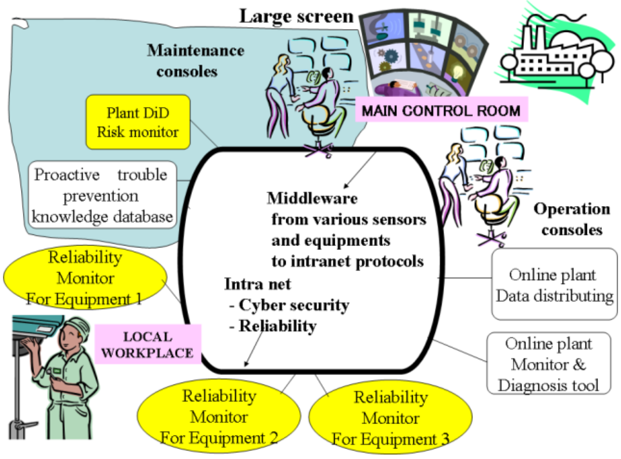

Large screen
Maintenance consoles
Plant DiD Risk monitor
MAIN CONTROL ROOM
Proactive trouble prevention knowledge database
Middleware from various sensors and equipments to intranet protocols
Intra net
- Cyber security
- Reliability
Operation consoles
Online plant Data distributing
Reliability Monitor For Equipment 1
LOCAL WORKPLACE
Online plant Monitor & Diagnosis tool
Reliability Monitor For Equipment 2
Reliability Monitor For Equipment 3

Fig. 1 Whole scheme of distributed HMI.

As seen in Fig.1, human interfaces for the MCR are (i) operator consoles with the software of online plant data distributing and online plant monitoring and diagnosis toolkits, (ii) maintenance consoles with plant DiD risk monitor and proactive trouble prevention knowledge database, and (iii) large display to share the information in the MCR. The human interfaces for the local workplaces may be various handheld tools of the maintainers with reliability monitors of individual equipments. The major subject of this paper is how to design and develop the risk monitoring method for PWR as “Plant DiD risk monitor” in MCR while as “Reliability Monitor” for individual subsystems and equipments at local workplace.

3 Risk monitor

Although not presented in this paper, the authors of this paper assume that “Plant DiD risk monitor” will be configured by the semiotic functional modeling method called “Multilevel Flow Model (MFM)” [7 - 9] which has been developed by M. Lind as the integrated risk monitor system for whole plant system. The “Plant DiD risk monitor” assembles and analyzes all the information given by “reliability monitor” for individual subsystems and equipments at local places. The “Reliability monitor” gives the qualitative evaluation by the way similar to FMEA (Failure Mode and Effect Analysis)[11] with the quantitative reliability evaluation method called GO-FLOW method[12] which has been developed by T.Matsuoka.

In this chapter, the authors will discuss on how to configure the risk monitor from the following aspects: (a) How to evaluate the degree of risk state of plant, (b) How to deal with the common mode failure related with initiating fault event, and (c) How to configure “plant DiD risk monitor” by the MFM model of whole plant and to correlate it with “Reliability monitor”. Discussion will be extended in the next chapter 4, on how to visualize risk state intuitively as “dynamic risk monitor” as the display to human.

3.1 Definition of risk and risk ranking

3.1.1 Design principle of nuclear safety

It is well known that the safety of NPP is based on the Principle of Defense-in Depth (DiD), *i.e.*, multiple barriers against radiological release to the environment[10]. 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, *i.e.*, common mode failure in initiating failure events.

3.1.2 Risk to be monitored

There are many ways of defining “Risk” which is brought by NPP. In this paper the authors define it as the possibility as well as the consequence of “Severe accident by core melt”. “Risk monitor” should be organized as “plant DiD risk monitor” 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. “Plant DiD risk monitor” should know the actual 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 for designing as well as on time for both on power operation and shutdown phases.

3.1.3 Severe accident phenomena

The researches on severe accident have been extensively conducted worldwide to obtain knowledge on what kind of phenomena would occur and develop into severe accident in the light water reactor (LWR) and by what it should avoid by the safety design as well as the introduction of various safety functions in the plant. The authors have conducted a literature review on the major phenomena to be considered for the severe accident prevention and management as well as the related severe accident analysis codes. Although not mention in detail, a summary of major severe accident phenomena is shown in Table 1. In Table 1, various severe accident phenomena in LWR are classified by a matrix form with behaviors of fuel, coolant and violent material interaction on one hand while different types of accident (transient over-power and loss of coolant accident) on the other hand. As will be discussed in the next 3.1.4 as well as in chapter 4, the details of those severe accident phenomena and the related analysis codes on severe accident would be utilized as the knowledge bases to define risk level and to develop dynamic risk monitor.

Table 1 Major severe accident phenomena in LWR

Severe accident phenomena	Transient over-power	LOCA
Fuel behavior mainly related to failure to stop the nuclear reaction	Fuel swelling Fuel failure and melting Pellet-clad interaction Fuel relocation/slumping	
Coolant behavior mainly related to failure to cool the reactor		DNB Two-phase flow Natural circulation Blowdown-refill-quench-reflood CCFL
Various violent interaction behavior mainly related to failure to contain radiological release	FCI Zr-water reaction Hydrogen explosion Steam explosion Corium-concrete reaction	

3.1.4 Risk ranking

To decide which risk level the plant is, you should take into account 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 which includes full power operation with/without online maintenance, various stage of shutdown maintenance. An example of deciding the risk level is given in Table 2, where six level risk ranking is taken from the eight combinations of STOP, COOL and CONTAIN. In Table 2, the number 1 of individual safety function means that it works successfully while the number 0 in failure. According to this risk ranking, no risk state is level 0 while the highest risk state is level 5. The risk levels 1 to 5 should be decided by evaluating by what degree the plant would be damaged by the knowledge base on various severe accident phenomena, if the three safety functions are aggravated by the fault initiating event to the plant.

Note that Fukushima Daiichi accident which occurred in March 11, 2011 is considered to be in Risk level 3 since although reactor shutdown was successful, both safety functions of COOL and CONTAIN were subsequently lost by the attack of big tsunami. While the risk level of Chernobyl accident in 1986 was 5 because all three safety functions were destroyed by uncontrollable reactivity insertion to the reactor.

Table 2 An example of risk ranking

Risk level	Stop	Cool	Contain	Possibility of severe accident
0	1	1	1	No risk Safety 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 Safety shutdown, but cooling failed but no release
3	1	0	0	Serious severe accident possible Safety 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 occur because containment function succeeded Shutdown failed, cooling failed but no release
5	0	0	0	Worst severe accident because all safety functions failed

3.2 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, hurricane, *etc*., as well as human-caused events such as sabotage, terrorism, airplane collision, *etc*.

Importance of considering common mode failure(CMF) which might 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" is shown in Table 3, by referring the procedure employed in the area of probabilistic safety assessment (PSA) for NPP.[12] In Table 3, the word "explicit" is here to treat the related CMF factors as individual "headings" of event tree analysis while "parametric" means various parametric modeling method such as beta factor method, MGL(multiple Greek letter) method, BFR (binomial failure rate) method. Also in Table 3 the authors allocated that the consideration of CMF over the whole plant or the several subsystems is treated by the "plant DiD risk monitor" while it is made by "Reliability monitor" for a single subsystem or equipment.

Table 3 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 Unclear	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		
	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		

3.3 Risk monitor by semiotic modeling

The essential ideas of how to apply the semiotic modeling method for nuclear power plant has been already presented by the authors' paper[13]. There are two types of object items to configure the target plant system. One type of the object items is solid matter which can be classified as structural element such as reactor vessel, mechanical pump, pipe, *etc*., and electrical element such as electric motor, control unit, *etc*. Various facilities, systems and components in the nuclear power plant can be described as the form of knowledge base model of the solid matter which is composed by (i) knowledge on specification of object item, (ii) knowledge on endowed conditions to object item, and (iii) knowledge on general failure mode of object items.

On the other hand of solid matter object items, there are many non solid matters such as fluid flow, electric flow (electric current, electric power), and information flow (signal flow from sensors, to processors for control and safety purpose and actuators for automatic action or to displays for operators manual processing).Those various flows running through the plant system are important to realize and maintain the function of the plant system. The modeling of non-solid matter is to describe those various flow running through the plant system with correlating with their meaning in terms of "functions" to be realized. The authors had already presented in their previous paper that a revised multilevel flow model (MFM)[9] could be used for such purpose.

To sum up for realizing the concept of risk monitor as described in 3.1, the authors will utilize the functional modeling method MFM for the semiotic modeling of target plant by highlighting three safety functions of (a) STOP, (b)COOL and (c)CONTAIN as “useful functions” . Non-solid matter model by the revised MFM 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.

3.4 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 risk monitor in Fig. 2 is 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 information for individual subsystems, (iv) FMEA Table for individual subsystems, and so forth. The knowledge base system of risk monitor would be in common use by all the users both in the main control room and the local workplace through the intranet over the plant site.

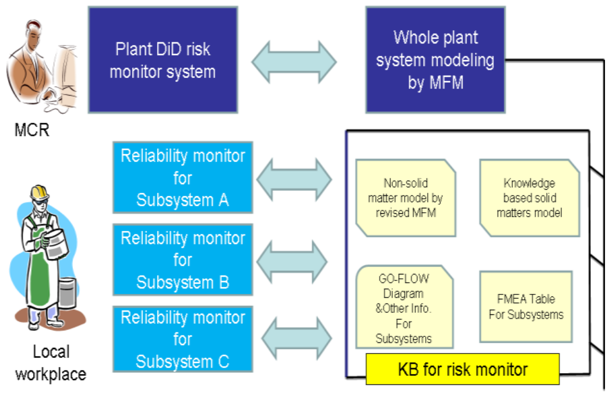

Plant DiD risk monitor system
Whole plant system modeling by MFM
MCR
Reliability monitor for Subsystem A
Reliability monitor for Subsystem B
Reliability monitor for Subsystem C
Local workplace
Non-solid matter model by revised MFM
Knowledge based solid matters model
GO-FLOW Diagram &Other Info. For Subsystems
FMEA Table For Subsystems
KB for risk monitor

Fig. 2 Plant DiD risk monitor and reliability monitor.

3.5 Visualization 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 as discussed in the previous subsection **3.4** should estimate the time changing risk state of the whole plant with enough accuracy and fast computation time. And it is also important to visualize the time changing risk level of whole plant by the form intuitively understood by operators in the MCR.

The essential point of the authors’ idea on how to display the time changing risk level as “Dynamic risk monitor” for the operator in MCR is depicted in Fig. 3, for visualizing risk state “by Defense-in-Depth manner” with the degree of severity of plant state. 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.

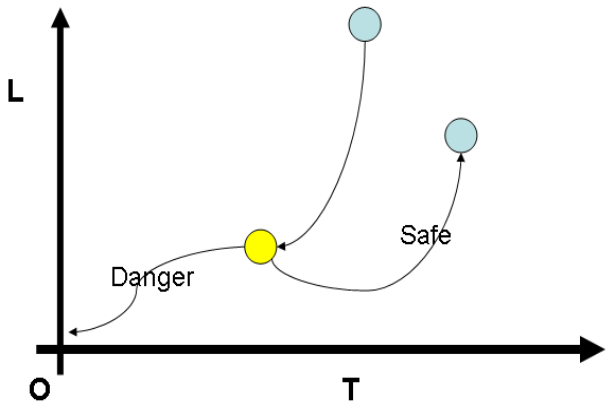


Fig. 3 Dynamic risk monitor as human interface.

The origin O of TL-plane means Danger point (T_0, L_0) within a risk ranking range I, where T_0 and L_0 mean no time margin and no safety margin to go from a risk ranking state I to a more high state I+1. Note that in case of Table 3, range of I is from 0 to 5. Therefore, the yellow point of this dynamic risk monitor display will change in 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 2, 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) plant operation and shutdown. 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 an appropriate countermeasure of emergency management.

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. 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 tool to rate the level of severe accident by the way as shown in Table 2 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 y far the plant is severely damaged and by what degree the makeshift recovery actions are successful for mitigating the radioactive release to the environment.

To sum up the above discussion from 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 2, 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, it may be necessary to 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 also included as one of the future issues of developing Plant DiD risk monitor.

4 Example practice of a reliability monitor

4.1 Description of containment spray system

As an example practice of reliability monitor by using FMEA and GO-FLOW, a reliability monitor was constructed for containment spray system used in the conventional pressurized water reactor (PWR). The configuration of containment spray system employed in the conventional PWR plant is illustrated in Fig. 4. In Fig. 4, there are two parallel lines of injecting water by Containment Spray Pump (CSP) from Refueling Fuel Storage Tank (RWST) and NaOH addition from spray additive tank and re-circulating water from the sump. Also you can see a test line in Fig. 4.

The existence of those two parallel lines and test line may enhance the reliability of the containment spray system in the actual operation and maintenance of the system, but it is simplified by a single line in the authors’ example practice as shown in Fig.5. The meanings of several abbreviations used in Fig.5 are as follows: RWST stands for refueling water storage tank, SAT spray additive tank, CSHEX containment spray heat exchanger, CSP containment spray pump and M1 to M4 are motor-operated valves. The components RWST, SAT, CSHEX, Spray header are passive component while CSP and motor-operated valves M1 to M4 are active component.

The role of containment spray system is to suppress the pressure of containment in the event of loss-of-coolant accident (LOCA) of PWR and wash down the radioactive fission product gas in the containment by spraying the water with adding NaOH. When LOCA occurs, water in the RWST added by NaOH in SAT is injected by CSP to the containment from the spray header (injection mode), and when the water in RWST is exhausted the water collected in the sump of containment is pumped by CSP and then charged by CSP to containment (re-circulation mode). In re-circulation mode, the residual heat from reactor vessel is removed by CSHEX.

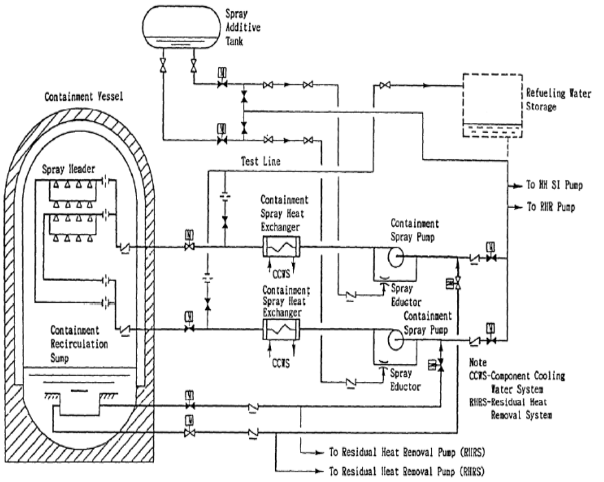

Spray Additive Tank
Containment Vessel
Refueling Water Storage
Test Line
Spray Header
To HH SI Pump
To RHR Pump
Containment Spray Heat Exchanger
Containment Spray Pump
CCWS
Spray Eductor
Containment Recirculation Sump
Note
CCWS-Component Cooling Water System
RHRS-Residual Heat Removal System
To Residual Heat Removal Pump (RHRS)
To Residual Heat Removal Pump (RHRS)

Fig. 4 Containment spray system in PWR plant.

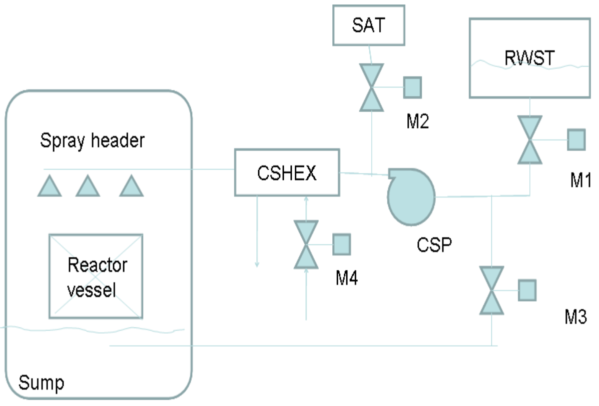


Fig. 5 Simplified containment spray system used in example practice.

The operation of containment spray system for LOCA is explained in Table 4, where major active and passive components in the containment spray system is listed. You can see the change of the operation mode from injection mode to re-circulation mode is mainly controlled by changing the open-close state of the four motor-operated valves M1 to M4.

Table 4 Operation of containment spray system for LOCA

Equipments	Injection mode	Recirculation mode
M1	Open	Close
M2	Open	Close
M3	Close	Open
M4	Close	Open
CSP	On	On
CSHEX	Passive	Passive
Spray header	Passive	Passive

4.2 FMEA for containment spray system

Concerning FMEA for the containment spray system, the authors employed an FMEA sheet as shown in Table 5, where most of the components comprising the containment spray system are listed up and then action mode, failure mode, effect to the plant and degree of its fatalness are described for each of the component. In Table 5, the fatalness of individual failure of a certain component was noted as “large-large” or “large” from the aspect whether or not the failure of corresponding component may develop into a dangerous state of severe accident and the consequence of the corresponding state is worrisome one or not. Although not yet composed, those kinds of trouble knowledge of various components can be easily reduced from the already constructed solid matter knowledge base of various components.

4.3 GO-FLOW analysis for containment spray system

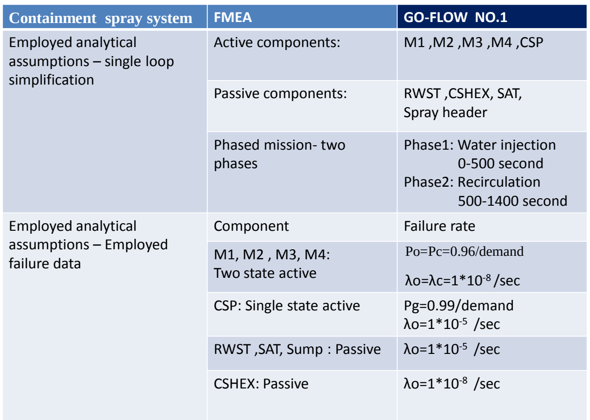
The objective of conducting the GO-FLOW analysis is versatile from the aspect of risk monitor which may range from the reliability evaluation and planning the maintenance program of a specific safety subsystem in the plant. The authors have conducted on GO-FLOW trial analysis to obtain the dynamic reliability curve for the simplified containment spray system as shown in Fig.5. From the viewpoint of the relation between Plant DiD risk monitor and reliability monitor as shown in Fig.2, the main subjects of GO-FLOW analysis from the risk monitor aspect are the summarized information of why (objective), how (assumption and procedure) and what (result of analysis) of individual GO-FLOW practice for a specific subsystem should be compiled as the useful knowledge base. In view of the above,

Table 5 FMEA sheet for containment spray system

Containment spray system			FEMA	GO-Flow
Subsystem/parts	Action mode	Failure mode	Effect to plant	Degree of fatalness
M1	Injection	Fail to open	Cannot change	Large-Large
	Recirculation	Fail to close	Enough pumped water may not go to spray	
M2	Injection	Fail to open	Cannot add NaOH	Large
	Recirculation	Fail to close	Enough pumped water may not go to spray	
M3	Injection	Fail to open	RWST water may go to sump	
	Recirculation	Fail to close	Cannot be circulated	Large-Large
M4	Injection	Fail to open	May be permitted	
	Recirculation	Fail to close	Cannot remove residual heat	Large-Large
CSP	Injection	Fail to start	Cannot charge	Large-Large
	Recirculation	Fail to start	Cannot be circulated	Large-Large
CSHEK	Passive	Leak from primary to second	May not only charge enough water also removal heat	Large
Spray header	Passive	Deformation of spray	Non effective spray effect	
SAT	Passive	Not enough NaOH	Cannot add enough NaOH	
RWST	Passive	Not enough water	Cannot charge water	
Sump	Passive	Leak	Not only enough water to circulate but also leakage of radioactive water	Large-Large

the example practice of the example GO-FLOW analysis for the simplified containment spray system is summarized as three sheets as shown in Figs.6-8.

The analytical assumptions used for the example practice are summarized in the GO-FLOW analysis sheet No. 1 as shown in Fig.6. Selection of active and passive components with their individual failure rate values and the time scheme of phased mission are indicated in Fig. 6.



Containment spray system	FMEA	GO-FLOW NO.1
Employed analytical assumptions – single loop simplification	Active components:	M1 ,M2 ,M3 ,M4 ,CSP
	Passive components:	RWST ,CSHEX, SAT, Spray header
	Phased mission- two phases	Phase1: Water injection 0-500 second Phase2: Recirculation 500-1400 second
Employed analytical assumptions – Employed failure data	Component	Failure rate

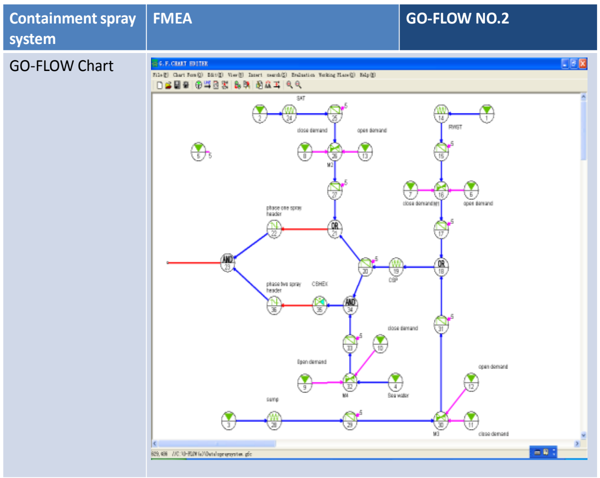
	M1, M2 , M3, M4:
	Two state active
		Po=Pc=0.96/demand
		λo=λc=1*10^{-8} /sec

	CSP: Single state active	Pg=0.99/demand
		λo=1*10^{-5} /sec

	RWST ,SAT, Sump : Passive	λo=1*10^{-5} /sec
	CSHEX: Passive	λo=1*10^{-8} /sec

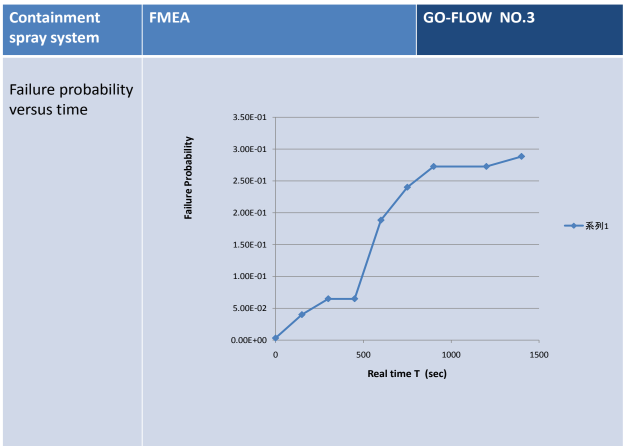
Fig. 6 GO-FLOW analysis sheet No.1.
(1) Employed analytical assumptions

The employed GO-FLOW chart and the calculated time history of the failure probability for the containment spray system are shown in Figs.7 and 8, respectively. It is seen in Fig.8 that the failure probability of the containment spray system would increase with time and the increase rate becomes larger in the recirculation phase than in initial water injection phase.



Containment spray system	FMEA	GO-FLOW NO.2
GO-FLOW Chart		

Fig. 7 GO-FLOW analysis sheet No. 2.
(2) Employed GO-FLOW chart



Containment spray system	FMEA	GO-FLOW NO.3
Failure probability versus time		

Fig. 8 GO-FLOW analysis sheet No. 3.
(3) Obtained failure probability versus time

The above presented GO-FLOW analysis is not a rigorous evaluation for a real containment spray system in the nuclear power plant with respect to the analytical assumptions and the obtained failure rate curve. The way of making the summary of

GO-FLOW analysis presented in Figs. 6-8 is only an example. You should device the way of making the summary for the cases of sensitivity analysis, uncertainty analysis and consideration of common mode failure, and so forth, depending on the objective of your GO-FLOW analysis. By this way, you can expand the knowledge bases of risk monitor as shown in Fig.2.

5 Concluding remarks

In this paper, the method of how to comprise a concept of "plant DiD risk monitor" and "reliability monitor" for nuclear power plant was discussed in detail. The discussion started on the definition of risk and risk ranking on the items of (i) design principle of nuclear safety, (ii) what is risk to be monitored, (iii) severe accident phenomena to bring the risk, and (iv) risk ranking. After analyzing the anatomy of fault event occurrence from the view point of common mode failure and considering the semiotic modeling of nuclear power plant as a whole by utilizing multilevel flow model (MFM), the image of distributed human-machine interface system of plant DiD risk monitor and reliability monitor was introduced.

Then an example practice was presented for containment spray system of PWR by the proposed concept of "reliability monitor" with the application of FMEA and GO-FLOW analysis.

The formation of "plant DiD risk monitor" by utilization of revised MFM will be the next step study for configuring the proposed concept for the "plant DiD risk monitor".

Acknowledgment

The study is supported by the 111 project on Nuclear Power Safety and Simulation (b08047).

References

[1] MORIKAWA, H., and WATANABE, H.: The Main Control Board Upgrade Project at the Ikata Power Station for Units 1 and 2, Proc. 7th International Topical Meeting on Nuclear Power Plant Instrumentation, Control and Human Interface Technologies (NPIC6HMIT 2010), Las Vegas, U.S.A., November 7-11, 2010.

[2] FILIPPI, G., NORROS, L., PIRIUS, D., and DIONIS, F.: NMOTION Project, the European Project for Defining the Research Roadmap on HF, I&C and HIS for NPPs, ibid.

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

[4] YOSHIKAWA H., and YANG M.: Study on Integrated Method for Constructing Proactive Trouble Prevention Knowledge Base, Proc. 18 th International Conference on Nuclear Engineering (ICONE18), Xi'an, China, May 17-21, 2010.

[5] YOSHIKAWA, H., YANG, M., LIND, M., TAMAYAMA, K., and OKUSA, K.: Development of Semiotic Framework of Proactive Trouble Prevention Knowledge Base System and Its Application for FBR Prototype Plant "Monju", Proc. 7th International Topical Meeting on Nuclear Power Plant Instrumentation, Control and Human Interface Technologies (NPIC6HMIT 2010), Las Vegas, U.S.A., November 7-11, 2010.

[6] MIZUNO, M., OKUSA, K., and TAMAYAMA, K.: Human Interface of Distributed Plant Monitoring and Diagnosis System at "Monju", Proc. International Symposium on Symbiotic Nuclear Power Systems for 21st Century (ISSNP), Tsuruga, Japan, July 9-11, 2007.

[7] LIND M.: Modeling Goals and Functions of Complex Industrial Plants, Applied Artificial Intelligence, 1994, 8(2):259-283.

[8] LIND, M.: Knowledge Representation for Integrated Plant Operation and Maintenance, Proc. 7th International Topical Meeting on Nuclear Power Plant Instrumentation, Control and Human Interface Technologies (NPIC&HMIT 2010) ,Las Vegas, U.S.A., November 7-11, 2010.

[9] 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, Valenciennes, France, August 31- September 3, 2010.

[10] PETRANGELLI, G.: Nuclear Safety, Elsevier Butterworth-Heinemann, 2006.

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

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

[13] 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):140-15