Development of a functional platform for system reliability monitoring of nuclear power plants

YANG Ming[1], WANG Wenlin[1], YANG Jun[1], and YOSHIKAWA Hidekazu[1]

1. *College of Nuclear Science and Technology, Harbin Engineering University, No. 145 Nantong Street, Harbin 150001, China (yangming@hrbeu.edu.cn)*

Abstract: This paper presents MFM builder, a platform based on Multilevel Flow Modeling (MFM), which provides a graphical interface for modeling functions of complex artificial systems such as nuclear power plant with emphasizing the designed purposes of systems. Several algorithms based on MFM have been developed for dynamic system reliability analysis, fault diagnosis and quantitative software reliability analysis. A Reliability Monitoring System (RMS) of PWR nuclear power plant was developed by integrating above algorithms. Experiments by connecting RMS with a full scale PWR simulator showed that it took 16 seconds for RMS calculating the reliability changes over time of safety-related systems according to given system configurations in the 31 days by one computer run. The proposed reliability monitoring system can be used not only offline as a reliability analysis tool to assist the plant maintenance staffs in maintenance plan making, but also online as a operator support system to assist the operators in Main Control Room (MCR) in their various tasks such as configuration management, fault diagnosis and operational decision making.
Keyword: functional modeling; reliability analysis; fault diagnosis; risk monitort

1 Introduction

Probabilistic Risk Assessment (PRA) plays valuable roles in Nuclear Power Plant (NPP) varying from design, manufacturing and licensing, to construction, operation, decommissioning, and regulation. However, the insights obtained from PRA analyses may become out-of-date because the system design, safety criterion, operating procedures and reliability data will no doubt change throughout the life cycle of a nuclear power plant. This has led to the development of "Living PSA" technology [1]. The main idea of Living PSA is to keep the PSA models up to date with the changes in nuclear power plant.

Risk monitor[2] is an application of Living PSA. A major difference between Living PSA and risk monitor is that the latter reflects not average, but instantaneous risk of nuclear power plant. Risk Monitor is based on Living PSA models, but with a particular emphasis on actual plant operation conditions and configurations.
Risk monitor can be applied offline and online. An online risk monitor was proposed by the authors of this paper [3]. Two key points of proposed risk monitor are: (1) monitoring operation conditions by a Real Time Fault Management System (RTFMS); and (2) updating system reliability calculation by a Reliability Monitoring System (RMS). Different with traditional PRA which is based on Event Tree/Fault Tree (ET/FT) , the reliability calculation in the proposed RMS is based on GO-FLOW[4] methodology. A "Living PSA" modeling technology based on GO-FLOW methodology was proposed, which utilizes a generic model for describing various states of equipment. This technology not only enables analysts to fast construct system reliability models, but also enables safety engineers and operators to quickly and easily update system reliability models without the need of understanding the details of GO-FLOW models.

This paper presents a new design of RMS. The authors propose to apply Multilevel Flow Modeling (MFM)[5] as the fundamental modeling method for the risk monitor development. MFM can provide a hierarchical knowledge representation on the behaviors of NPPs with a special emphasis on the designed purposes or goals. Based on the system knowledge represented by MFM, G2, a rule-based expert system, was utilized in RTFMS for automatic fault diagnostic reasoning. Under the guidance of a graphical MFM chart, can clearly understand what functions a system serves and how a function failure may propagate its effect on the other functions and ultimately endanger the system to achieve its designed goals. Furthermore, an algorithm for mapping MFMs into GO-FLOW models were

Received date: October 21, 2014

developed[6]. Since the RTFMS and RMS models are exactly same, coordinating operation conditions monitoring with reliability calculation updating becomes easier.

In the later part of this paper, the framework of the proposed risk monitor will be firstly presented. Then the design and development of MFM Builder will be introduced. Next, the key technologies for fault diagnosis and reliability calculation will be addressed. Finally, evaluation results of risk monitor performance and HMI simulation experiments will be summarized.

2 Framework of risk monitor

As shown in Fig. 1, the new risk monitor consists of six systems.

(1) MFM Builder: The MFM Builder provides a graphical interface for constructing and modifying MFMs. The MFMs can be saved as two kinds of data format including (a) the XML format in accordance with the specifications of G2 expert system; and (b) the text format in accordance with the specification of GO-FLOW program. Two data communication interface programs were designed to export MFMs into G2 expert system and GO-FLOW program for fault diagnostic reasoning and reliability calculation, respectively. The MFMs and reliability parameters can be updated automatically according to the real operation conditions.

(2) Plant Information Management System (PIMS): PIMS processes collection and recording of plant data. Plant data is stored in historical operation data database which contains the following two types of data. (a) real time operation data, is automatically collected by instrumentation and control system, and (b) nonreal time data, such as the data from experiment, test and routine inspection activities, is manually recorded by field workers.

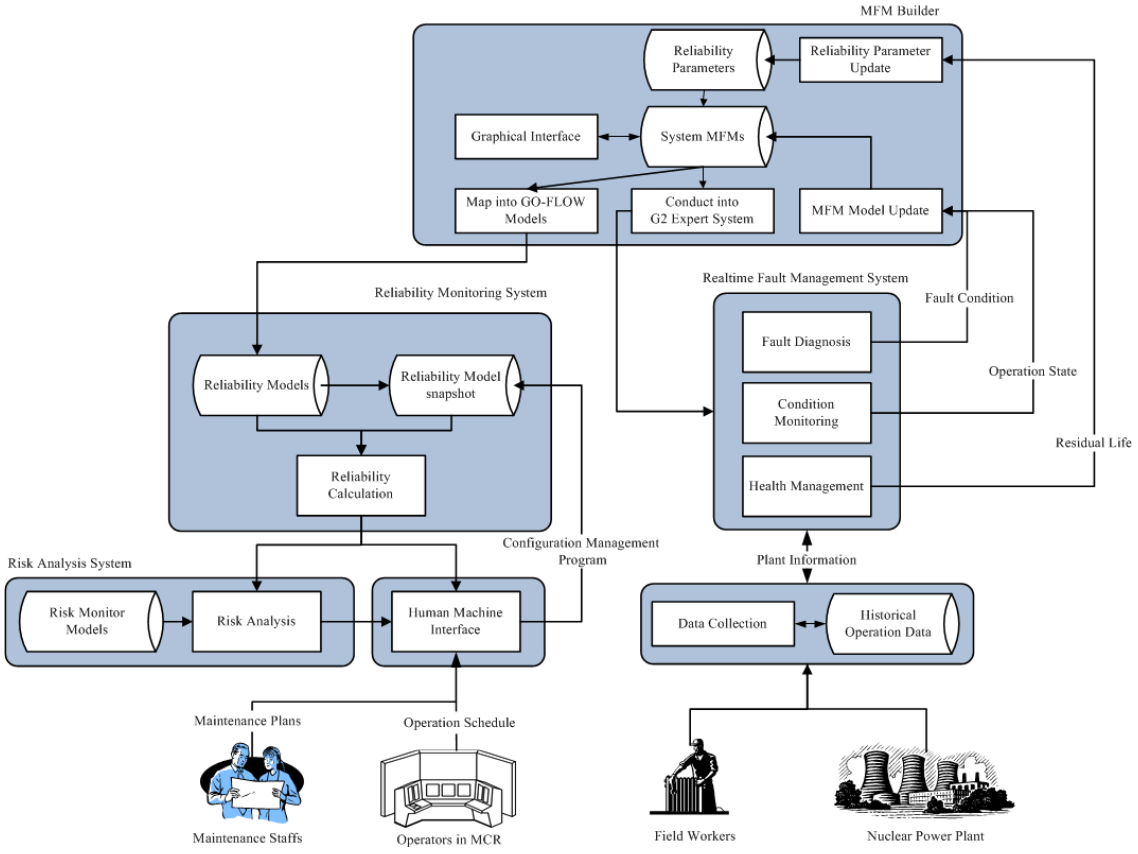

Fig.1 Framework of risk monitor.

(3) Real Time Fault Management System (RFMS): RFMS performs three functions according to the information provided by PIMS, that is, (a) condition monitoring, to detect configuration change such as status change of a valve from on to off by fault or operator's action; (b) fault diagnosis, to identify causes of failure including fault or accident type, location and level, in the case of plant being in an abnormal state; and (c) health management, to predict the residual life of component or equipment by performance monitoring and degradation analysis. The MFM Builder will utilize this information to update MFM models and reliability parameters, so that MFMs can keep accordance with the real status of equipment detected by RFMS.

(4) Reliability Monitoring System (RMS): RMS calculates the probabilities that plant systems will be successful or failed to perform their designed functions under the given conditions for a period of time. Initial modeling conditions for each equipment, such as equipment state, failure rate, average maintenance time and maintenance plans, are finalized manually by operators or safety engineers.

(5) Risk Analysis System (RAS): RAS calculates Instantaneous Core Damage Frequency (ICDF) based on accident sequences which are obtained by event tree analysis. The probability of each heading event in the event trees is calculated by RMS.

(6) Human Machine Interface (HMI): HMI provides the information on equipment states, system configurations, system reliability and risk levels with time progress. Operators and safety engineers can also update equipment states manually for evaluating the effects of their intended operation actions or maintenance schedules.

3 Design of MFM builder

As shown in Fig. 2, the MFM Builder which was programmed by Microsoft Visual C++6.0 under Windows XP environment provides a graphical interface for constructing MFMs. The MFM builder provides the following functions:

(1) System management: This function enable user to build, open, save, export and print a MFM model file.

(2) MFM chart drawing: A MFM chart can be easily built by selecting an element from the element bar, clicking the drawing area and connecting elements in turn according to the inflow and outflow sequence. Elements will be auto-numbered. The arrow direction of a transport icon that indicates the flow direction will be automatically identified according to the spatial relationship between the transport and its inlet function in the drawing area.

(3) Icon edit: An icon of MFM element in the drawing area can be selected, moved, removed, resized and marked in different colors which will be helpful for expressing the cause-effect consequence when MFM is used for fault diagnostic reasoning.

(4) Grammar check: MFM Builder will deny an illegal connection between two MFM elements according to the predefined MFM grammar, for example, a source function can be only connected a transport function at outlet.

(5) Operation parameter setting: The operation related parameters of a MFM function, including alarm threshold, alarm state, causality, failure modes and operation state, can be predefined and manually input though a dialog box by double clicking on the icon of a MFM function in the drawing area. The parameters of a function will be online updated automatically if the RTFMS detect any change from the predefined equipment state.

(6) Reliability parameter setting: The reliability related parameters of equipment or components, such as, fault probability, failure rate and main time to repair, are recorded in a reliability parameter database. The mapping relationship between MFM functions and equipment or components will be predefined. In addition to reliability parameters, a timetable is defined to each MFM function. The timetable consists of several discrete time points which can be used for describing the dynamic behavior of equipment. The time interval between two adjacent time points is set as 24 hours.

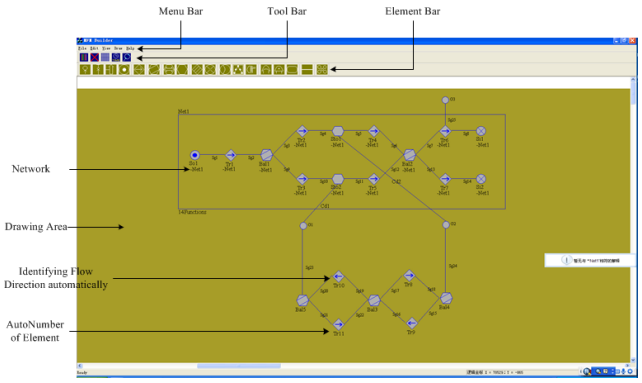

Fig.2 MFM builder.

4 Reliability calculation and updating

In the proposed risk monitor, system reliability calculation is performed by GO-FLOW program. A GO-FLOW model is a success-oriented and directed acyclic graph. Operator and signal are two basic elements of a GO-FLOW model. Each operator represents a fundamental reliability logical relationship and a signal may represent a mas flow, energy flow or control command.

Each MFM function can be basically mapped into a generic GO-FLOW model. As shown in Fig.3, the generic model of equipment combines 5 basic models (indicated in different colors) which represents the reliability characteristics of equipment in operation, standby, maintenance, test and failure. Switching equipment state from one to another is controlled by turning demand signals between 1 and 0 to open or block the relevant logic branches. If a MFM function doesn't have so many states, it can be mapped into a simplified GO-FLOW model by removing the relevant logical branches from the generic model.

GO-FLOW methodology enables probability calculation of a system at different time points by one computer run. The version of GO-FLOW program that the authors use supports 31 time points. By utilizing this ability, time span between time points is defined as 24 hours. That means the proposed RMS can analyze system reliability change day-by-day within one month.

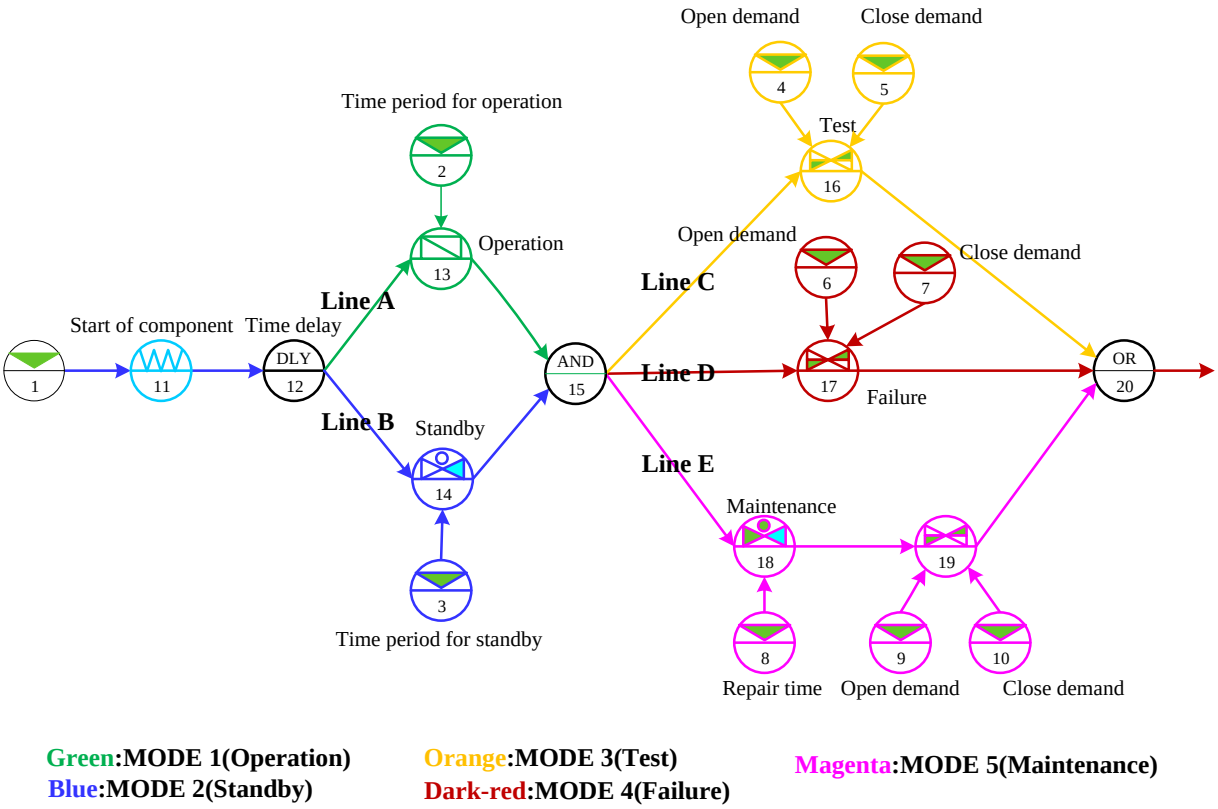

Fig. 3 Generic model of equipment with living PSA conception.

5 Fault management

The alarm state of each MFM function is discretized into either the type of two-state or the type of three-state. A typical type of two-state MFM function is realized by switch type components featured by on/off characteristic. A function featured by process parameters, such as temperature, flow rate and pressure, are processed to have three alarm states including high state, normal state and low state. The causalities between two adjacent functions are classified into three types including active causality, negative causality and none. For example, if a function A has an active causality to a function B, then the function A will cause the function B in the same alarm state with the function A. The MFMs for various plant systems together with the alarm thresholds, causalities and failure modes will be organized in a XML format date file in accordance with the specifications of G2 expert system. The G2 expert system will merge the plant information with these models for reasoning root causes that may cause plant systems abnormal.

Obtaining effective information on equipment state is a key issue of reliability monitoring. If the systems, for example engineered safety systems, contain many undetectable equipment, a large number of reasonable root causes may be inferred. To solve this problem, the developed Risk Monitor is considered to connect with a plant information management system which obtains plant information not only from I&C system, but also from authorized field staffs who could manually input valuable plant information from their maintenance, experiment and routine inspection activities. In China, this kind of plant information management system has been developed by China Guangdong Nuclear Power Group and applied in several nuclear power plants. The information management system can provide nearly 30,000 sampling points from DCS and field observation which will benefit an effective reliability monitoring on a level of plant systems.

6 Design of HMI

A graphical HMI was designed and developed in order to assist plant operators and safety engineers in operation decision-making and maintenance schedule planning.

As shown in Fig. 4, the main screen of HMI is designed into five major areas for offering equipment information, system configuration, system reliability level, fault message, and operation execution.

(1) Equipment Information Area (Area I): A pull-down menu will be available by clicking the "Reliability Monitoring" button in the toolbar. The system to be monitored can be then selected and the main information of relevant equipment, including equipment ID, name, state, start and end date for each state, and identifier in system reliability model, will be shown in the form of a table. For more detailed information of equipment, a complete table can be available by double clicking any place within this area. Operators or safety engineers, if they want to evaluate the effects of their intended operation actions or maintenance activities on system reliability, can change a new state of equipment manually. Four functional buttons are set up to guide users modify equipment information, confirm modification, withdraw a last modification, and reload a last saved model. After confirming modification, the new state will be mapping into a combination of control signals. A background process was designed to utilize this control signals for modifying the relevant model in the model database. By this way, users can update system reliability models without the need of understanding the details of GO-FLOW models.

(2) System Configuration Area (Area II): This area shows the configuration of a selected system in the form of a table which contains several lines and 31 columns, while lines correspond to equipment and columns represent days. Each block is colored by green, blue, orange, magenta or red, representing equipment in a state of in-service, standby, under test, failed or in maintenance, respectively. Thus, a block in the table represents a certain condition of equipment in a certain day. Combination of blocks along longitudinal direction stands for a type of system configuration. In landscape orientation, the number of adjacent blocks with same color

indicates the duration in days of equipment in a certain state.

(3) Fault Message Area (Area III): This area shows a list of equipment in fault which is identified by RTFM. Since it is technically impossible for RTFMS diagnosing faults exactly, this message will remind operators or safety engineers to confirm whether the equipment is really in fault and whether correct states of equipment have been updated in the model. A confirmation button is designed for operators to confirm the suspected faults before the fault information is used for system re-configuring.

(4) Operation Execution Area (Area IV): This area offers the functions of calculating system reliability, exporting analysis results, drawing and exporting reliability curve, exporting system configuration data, and updating system reliability calculation. These functions are only used after users manually modify the conditions of model analysis, such as changing equipment states in Equipment Information Area, or remove a faulty status of equipment in Fault Message Area. Users can obtain reliability analysis results and decide whether apply the analysis results into reliability monitoring system by clicking the relevant buttons.

(5) System Reliability Display Area (Area V): This area shows the time history of system reliability in the form of a curve for users. The whole display region of this area is laid out on a grid pattern. Where numeric on the vertical axis indicates system reliability and time frame is marked under the horizontal axis. The timeline is mapped into 31 intervals which represent 31 days. The timelines of System Configuration Area and System Reliability Display Area are consistent with the time and horizontal space. Users not only can be clearly aware of the instantaneous reliability change of systems at any time when operation actions, faulty equipment, and maintenance activities change the failure probability of equipment and the configuration of systems, but also can track along the longitudinal direction upwards to identify the reason of system reliability change. This is very helpful for plant operation condition monitoring, operation strategy decision making, and maintenance plan making.

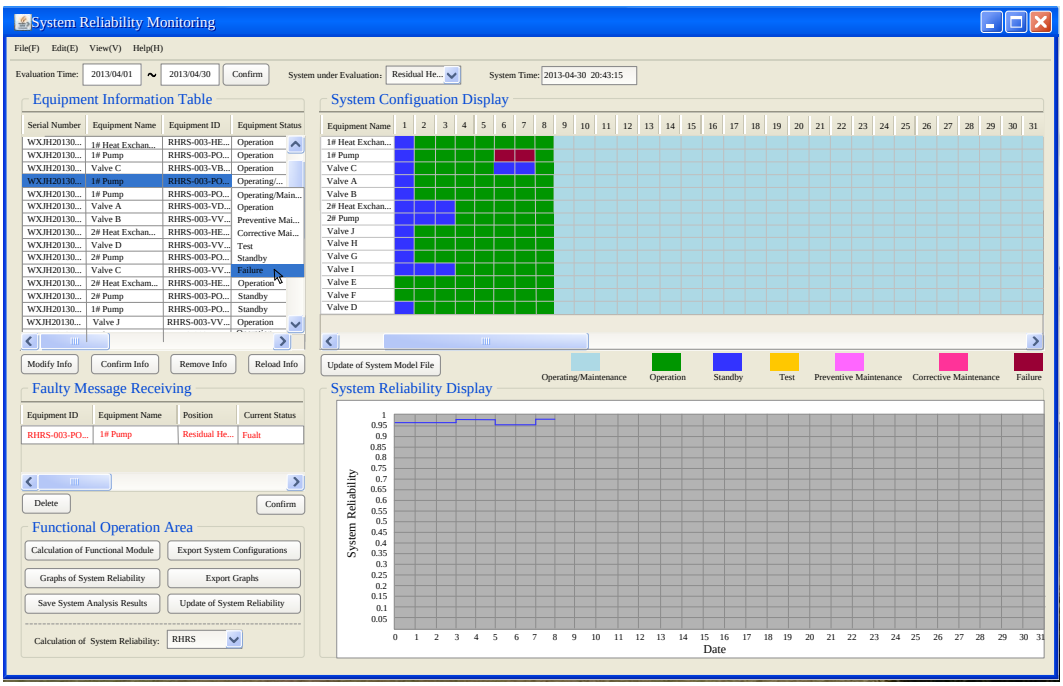

Fig.4 HMI design for reliability monitoring system.

7 Evaluation experiments

Taking a two-loop Pressurized Water Reactor (PWR) system as a target system, a risk monitor has been developed. Totally 434 MFM modules for the systems involved in plant steady state power operation and the engineered safety systems involved the mitigation of three accidents including Loss Of Coolant Accident (LOCA) with small break size, Main Feed Water Line Break (MFWLB) and Main Steam Line Break (MSLB) have been constructed.

Experiments were conducted to test the performance of developed RMS, and evaluate the HMI design of RMS including screen layout, color schemes and information arrangement. Eight students majoring in nuclear engineering are selected as the examinees.

As shown in Fig. 5, SMI HED, an eye tracking system, was utilized for the HMI experiments. SMI HED consists of a head mounted data recorder, a mobile workstation, eye movement data analysis software and video recording software. As shown in Fig.6, the RMS was installed in a desktop computer. The HMI of RMS was presented in a 17 inch LED display with 60Hz display refresh frequency and 1440×900 resolution. The RMS was connected with a full scale simulator which can provide 584 plant parameters

An online maintenance plan was firstly prepared and 8 graduate students majoring in nuclear engineering were required to manually update the models to reflect the configuration changes. During the experiments, the simulator was run into an accidental scenario which was decided by examiner randomly. The examinees will then perform the corresponding Emergency Operating Procedures (EOPs) on the hardware panel to mitigate the sequence of accident with the help of the RMS.

The eye movement data of examinees, including gaze, saccade and blink, were recorded by the head mounted data recorder and analyzed by BeGaze software.

7.1 A case study

In one of the evaluation experiments, the simulator was firstly run at the steady state power operation and then into a Main Steam Line Break (MSLB) accident scenario. Meanwhile, the examinees were asked to manually change the 1#RHR (Residual Heat Removal) pump from in-service to faulty and change the 3#RHR pump from standby to in-service. Finally the examinees were required to monitor the systems, identify the risk level of reactor and find the root cause from the RMS.

7.2 Experimental results

The experimental data is summarized in Table 1 where the No.1-4 examinees are master course students and the No.5-8 examinees are Ph.D. students. The average total gaze time of No.1-4 examinees is 116s which is longer than 82s of No.5-8. It indicates that users with relative less professional knowledge will take more time to obtain plant risk information from the RMS. The average blink time of No.1-4 examinees is 0.032s which is shorter than 0.056s. This is because the blink time will reduce when people gaze at a display for a long time.

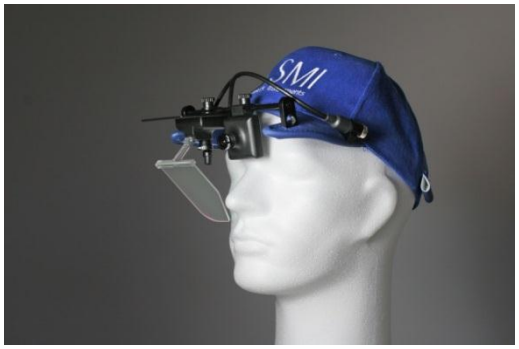

Fig.5 SMI HED eye tracking system.

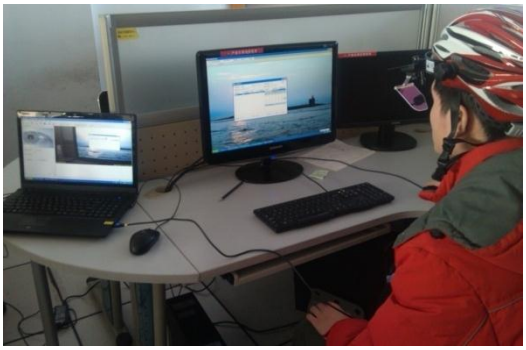

Fig.6 Eye tracking experiment for RMS.

Table 1 Experimental data of eye tracking system

Examinee	Gaze		Blink	
	Number	Total Time (μs)	Number	Total Time (μs)
1	150	104113860	165	7978596
2	131	88630438	141	5717012
3	142	147706135	140	4077859
4	125	12334783	123	3478907
5	142	80642021	152	7918962
6	124	63519297	130	6738967
7	87	86323302	93	6886931
8	96	97503828	109	5159618

The scan rout map and heat map of examinees were also analyzed in order to find the HMI design problems. The scanned rout map of the No.3 examinee who took the longest gaze time during the experiment is as shown in Fig.7. As shown in Fig.7, a polyline in the scan route map indicates that the examinee moved his sightline from one gaze point to another. The corresponding heat map is shown in Fig.8 where the colored parts represent gaze area and time. The longer the gaze time is, the redder a colored part becomes. On the contrary, the colored part will become bluer.

It can be seen that the No.3 examinee quickly obtained the relative information on system reliability changes from the Area V. However, he took a long time to identify the system configuration at the Area II, and update reliability calculation and reliability curve at the Area IV. The interviews for all examinees after the experiment revealed that the examinees confused with the color marked equipment states in the Area II, also the 6 execution buttons in the Area IV.

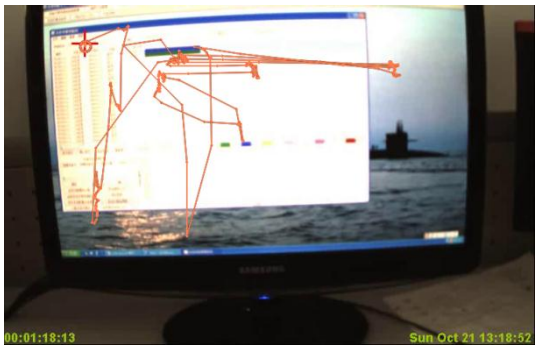

Fig.7 Scanned route map of the No.3 examinee.

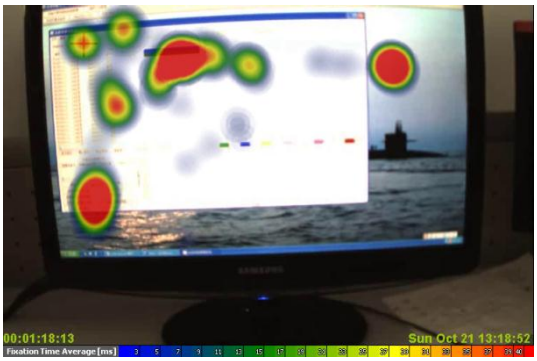

Fig.8 Heat map of the No.3 examinee.

8 Discussion and conclusions

This paper presents the design of a functional modeling platform for risk monitor development based on MFM which is used for analyzing and organizing system knowledge clearly and effectively. The G2 expert system is applied as an automatic reasoning tool. The simulation results showed that G2 expert system can detect equipment condition and identify root cause effectively. In the case of the lack of equipment information, G2 will provide a reasonable, but long list of root causes because G2 utilizes a rule-based reasoning strategy. With the guidance of graphical MFMs of systems operators can clearly understand what functions the systems serve and how a failure of function will may affect the other functions and ultimately endanger the systems to achieve the designed goals. This is very helpful for plant personnel to identify risk in plant operation and maintenance and can complement some limitations of rule-based fault detection and diagnosis.

Furthermore, a fast reliability calculation and updating can be realized by mapping MFMs into GO-FLOW models. The simulation results showed that it took 16 seconds for the risk monitor RMS calculating the reliability changes over time of safety-related systems according to given system configurations in the 31 days by one computer run.

A graphical HMI was developed which can enable operators or safety engineers to evaluate their intended operational actions or maintenance activities effectively without the need of understanding the details of models. The evaluation experiments by eye tracking technology showed that users can be clearly aware of the system risk change from the RMS.

However, the system configuration presented by a combination of different colors is overload for understanding and too many functions of RMS sometimes make the users feel confused.

The authors are now considering to design a new HMI for RMS by considering the problems revealed through evaluation experiments. A new GO-FLOW program is under development which can enable more time points and flexible applications. A navigation system will be developed to guide users to implement model modification.

Acknowledgement

The authors thank Professor Takeshi Matsuoka for his kind help for this research and thank 111 Project on Nuclear Safety and Simulation for providing financial support to this paper.

References

[1] BALFANZ H.P., and VIROLAINEN R.K.: State of Living PSA and Future Development, NEA, 1999

[2] SHEPHERD C.: EVANS M. and BONEHAM P., Risk Monitors-The State of the Art in their Development and Use at Nuclear Power Plants, NEA, 2004

[3] YANG J., YANG M., YOSHIKAWA D., and YANG F.Q.: "Development of a Risk Monitoring System for Nuclear Power Plants based on GO-FLOW Methodology", International Journal of Nuclear Safety and Simulation, Vol. 5, No.1, pp. 70-83, 2014.

[4] MATSUOKA T., and KOBAYASHI M.: "GO-FLOW: A New Reliability Analysis Methodology", Nuclear Science and Engineering, Vol.98, No.1, pp.64-78, 1988.

[5] LIND M., "Modeling Goals and Functions of Complex Industrial Plant", Applied Artificial Intelligence, Vol. 8, No. 2, pp.259-283, 1994.

[6] ZHANG X., and YANG M.: Online Maintenance Support Technology Based on MFM and GO-FLOW, Proceedings of the 7th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2010), Las Vegas, Nevada, U.S.A, Nov. 7-11, 2010.