Installation of GO-FLOW into the risk monitor being developed at Harbin Engineering University

MATSUOKA Takeshi[1, 2]

1. *Mechanical Systems Engineering, Department of Engineering, Utsunomiya University, 7-1-2 Yoto, Utsunomiya City, 321-8585 Japan (mats@cc.utsunomiya-u.ac.jp)*
2. *College of Nuclear Science and Technology, Harbin Engineering University No.145-1, Nantong Street, Nangang District, Harbin, Heilongjiang Province, 150001 China*

Abstract: A new method of risk monitor system of a nuclear power plant has been proposed by Harbin Engineering University. The Risk Monitor provides a system stability overview and details about events that impact reliability. It calculates the reliability over the lifetime of the system. An important part of the risk monitor is monitoring the dynamic reliability of subsystems, which will help the plant operators to find the problems before real loss of service appears during the plant operation. The GO-FLOW is an important part of the knowledge base system of reliability monitor. In the present paper, available function of the GO-FLOW is explained and discussions are given for how to incorporate the GO-FLOW into the reliability monitor system. An interface between the GO-FLOW and the risk monitor system is a key point of the development of the total system. With well designed interface, operator (=analyst) can easily reflect the change of plant conditions to the evaluation results of risk monitor.

Keyword: risk monitor; reliability monitor; GO-FLOW; common cause failure; dynamical system reliability

1 Introduction

Harbin Engineering University （HEU) is currently developing a risk monitor system. The risk monitor provides an overview of system states and details about events that impact reliability. It calculates the reliability over the lifetime of the system. In this study, the concept of risk monitor is expanded to be applicable for various accident situations ranging from prior to core melt to after core melt.

The basic configuration of the risk monitor system is a two-layer system: “plant DiD (Defense-in-Depth) risk monitor” and “reliability monitor”. The “plant DiD risk monitor” is meant to evaluate the intactness of the whole safety system based on the results of individual reliability monitors. It will monitor the safety functions incorporated in the plant system, which are maintained by multiple barriers of defense-in-depth (DiD).

The "reliability monitors" will show the dynamic reliability of subsystems using specific events that accidentally occurred in a plant system. Monitoring of the dynamic reliability will aid the plant operators to find the problems before real loss of service appears during the plant operation. The risk monitor visualizes risk state intuitively as "dynamic risk monitor”, with the support of knowledge base (KB) system of reliability monitor.

The GO-FLOW analysis framework will be a pivotal part of the KB system. In the present paper, available functions of the GO-FLOW are explained and discussions are given on how to incorporate the GO-FLOW into the reliability monitor system.

2 Risk monitor being develop at HEU

2.1 General definition of Risk monitor

The term “Risk Monitor” has been defined by IAEA [1] 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.”

Received date: August 15, 2012
(Revised date: November 5, 2012)

The word "Risk Monitor" conventionally used in nuclear application has been a specific application of a Living PSA as a real-time analysis tool used to estimate the point-in-time "risk of core melt accident". Here, 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.

2.2 Risk monitor system at HEU

The risk monitor system at HEU deals with the "risk" not by merely "core damage", but by the "radioactive materials" brought about by incidents or accidents. The basic configuration of the risk monitor system is the two-layer system: "plant DiD (Defense-in-Depth) risk monitor" and "reliability monitor" as shown in Fig. 1 (referred from reference [2]).

The "plant DiD risk monitor" is meant to know the potential risk state caused by severe accident phenomena to the plant system as a whole. It can be used to conduct "mind thinking experiment" on what risk will be incurred in the plant if an extraordinary situation happens.

The "reliability monitor" is meant for the daily monitoring of the reliability state of individual subsystems. The reliability monitor systems may be installed either on the main console or the maintainers' handheld computer at their workplace.

The knowledge base system of reliability monitor, that is shown in Fig.1, will comprise various 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[2]. 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 network system over the plant site. The detailed discussions on the knowledge base system of reliability monitor have been presented elsewhere [2, 3].

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, the preconditions for the evaluation by the reliability monitors are all given by plant DiD risk monitor. Those conditions are: (i) target subsystems, (ii) plant operation conditions and mode, (iii) types of accident initiators, (iv) common cause factors, (v) failure

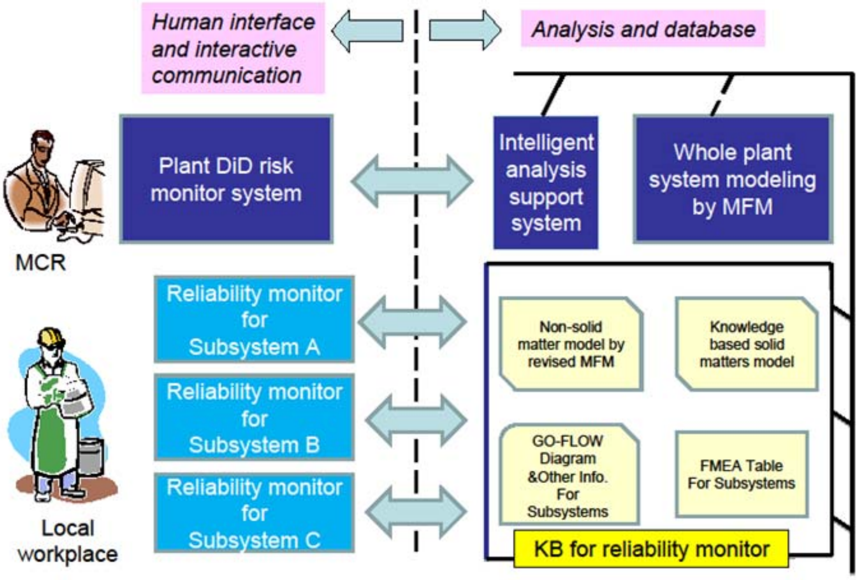
Human interface and interactive communication
Analysis and database
Plant DiD risk monitor system
MCR
Intelligent analysis support system
Whole plant system modeling by MFM
Reliability monitor for Subsystem A
Reliability monitor for Subsystem B
Reliability monitor for Subsystem C
Local workplace
Non-solid matter model by revised MFM
Knowledge based solid matters model
GO-FLOW Diagram &Other Info. For Subsystems
FMEA Table For Subsystems
KB for reliability monitor

Fig. 1 Plant DiD risk monitor and reliability monitor.

mechanism to be considered, etc. As exemplars of reliability monitors for PWR safety sub-systems, two models are being separately developed: one for containment spray system [4] and the other for ECCS system [2].

3 GO-FLOW methodology

3.1 Overview

The GO-FLOW methodology [5] is capable of evaluating system reliability and availability. The modeling technique produces a chart which consists of signal lines and operators, and represents the engineering function of the components / subsystems / system. The operators model function or failure of the physical equipment, and also represent logical gates, signal generators. Fourteen different types of GO-FLOW operators are currently defined as shown in Fig 2. Specific probabilities (point estimates) of component operations or failure are given as input data.

Signals represent some physical quantity or information. The existence of a signal means the existence of a physical quantity or information. In the GO-FLOW methodology, the existence of a signal is interpreted as both the actual and the potential existence of a signal. “Potential existence” means that a signal exists when all the resistances of downstream are removed.

A quantity called “intensity” is associated with a signal. Usually the intensity represents the probability of signal existence. When a signal is used as a sub-input signal to type 35, 37 or 38 operators, the intensity represents a time interval between the successive time points.

A finite number of discrete time values (points) are required to express the system’s operational sequence. The value does not necessarily represent the real time, but correspond to it and represents an ordering.

The first step of the analysis is to construct a GO-FLOW chart, which is a modeling of an engineering system. An analyst interactively constructs a chart on a PC display with the support of GO-FLOW chart editor. During the construction of a chart, component failure data and analysis conditions are assigned in a chart.

An analysis is performed from the upstream to the downstream signal lines. In most cases, only one, or at

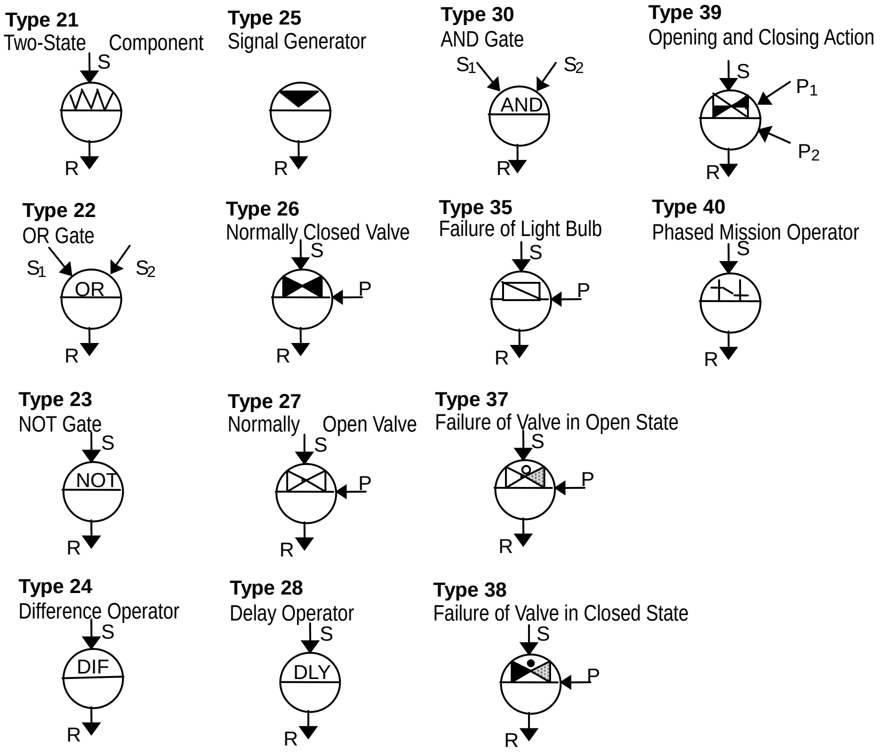

Fig. 2 Operators defined in the GO-FLOW methodology.

most few of all the defined signals are of interest; these signal lines are termed as final signals. An analysis is complete when the intensities of these final signals at all the time points are obtained.

The GO-FLOW methodology possesses the following significant features: (a) The GO-FLOW chart corresponds to the physical layout of the system and is easy to construct and validate, (b) alternations and updates to a GO-FLOW chart are readily accomplished, and (c) GO-FLOW contains all the possible system operational states.

3.2 Available functions of the GO-FLOW

1) Analysis of phased mission problem

Reliability of a subsystem dynamically changes in time sequences on the surrounding conditions, such as, change of mission requirements, occurrence of unexpected events, repair of failed component, or start of axially system. These are typical examples of phased mission problem.

A phased mission is a task to be performed by a system. During the execution of the task, the system configuration is altered such that the failure logic model changes at one or more times. Mission reliability is defined as the probability that the system functions in successive phases. Therefore, it is necessary to calculate the products of success probabilities among different phases. In this case, it is imperative to treat correctly the inclusion or exclusion relation between the failures of shared components in different phases.

The type 40 operator is prepared for the analysis of phased mission problem. This operator freezes signal intensity except during specific time period. With the aid of type 40 operator, the GO-FLOW methodology can correctly treat the dependency between the failures of shared components in different phases. More detailed explanations about the procedure of treating the phased mission problem are given in reference [6], which gives an analysis result of a sample system with the comparison of the result obtained by FT analysis.

2) Analysis of common cause failure

For the prediction of system reliability, information regarding the effects of common cause failure (CCF) is very important. Usually, there are more than one common causes, and also there are many possible combinations of component failures for a specific common cause. If all these failures are treated simultaneously in the reliability analysis, the analysis becomes impractical. An example of CCF analysis [7] showed that the second-order terms of CCF contributed less than 1% of total system unavailability. Therefore, in the GO-FLOW, each common cause is separately evaluated and the total system unavailability is obtained by summing up the contributions from each CCF.

Effects of common causes are well evaluated with parametric CCF models, such as β-factor, MGL model and so on. The selection of component failure model and assignment of failure data can be easily performed in the GO-FLOW analysis framework.

3) Identification of minimal cut sets

The GO-FLOW is a success-oriented system analysis technique. The success probabilities of system states or state at intermediate points in the system are expressed by signal intensities, which are products of success probabilities of components or basic events that contribute to system function.

In the GO-FLOW program, system states expressed in success probability can be converted into the expression in the failure probability, and the minimal cut sets (MCS), which are products of failure probabilities of basic events, are obtained for designated signal lines. The MCSs give the information regarding which failures are major contributors to the total failure probability of a subsystem.

4) Uncertainty analysis

The GO-FLOW handles the parameter value uncertainty. The distribution of failure probabilities are assigned for the basic events in the MCSs, and the distribution of subsystem failure probability is obtained with the Monte Carlo simulation. Failure probabilities of subsystem are calculated by combining values selected by sampling from the probability distribution for selected basic events. By accumulating the calculated failure probabilities, the distribution of subsystem's failure probability can be obtained, which gives the range of uncertainty of subsystem's reliability.

The function of common cause failure analysis together with uncertainty analysis has been provided in the GO-FLOW methodology [8].

5) Aging and maintenance effects

Aging effects are very important and difficult factors in nuclear power plants. However, in the GO-FLOW framework, probabilities and failure rates are not implemented in situations where failure rate changes due to aging effects. Therefore, the functions of the GO-FLOW need to be enhanced by using the time-dependent technique. The technique used here to model the time-dependent availability of aging components is based on the extended renewal equation [9]. The parameters of the aging model for each component are based on the NUREG report [10].

It is often assumed that the component is restored as age 0 by maintenance activity. However, this assumption is not realistic in view of the actual plant operations because: a) surveillance / test may not identify the failure, and b) repair may be imperfect. It is therefore necessary to consider the unavailability caused by imperfection of maintenance. Two causes of imperfection of maintenance must be considered. The first one is that some part of a component cannot be inspected directly. The second one is human error.

By considering aging and maintenance effects, degradation of system reliability can be shown in the reliability curve which may be provided in the risk monitor system.

4 User interface of risk monitor system

As mentioned in chapter 2, the risk monitor system has two-layer configuration: plant DiD risk monitor and reliability monitor systems. Plant DiD risk monitor system shows an overall plant states and risks, and it is also used for identifying preconditions of the plant. Those conditions are: (i) target subsystems, (ii) plant operation conditions and mode, (iii) types of accident initiators, (iv) common cause factors, (v) failure mechanism to be considered, etc. The reliability monitor system has various information and functions for evaluating the risks of subsystems. They include MFM models, knowledge based solid matters models, handling of GO-FLOW Diagram and the related information, and FMEA table, for individual subsystems. Therefore, different kinds of monitor screens have to be prepared for the plant DiD risk monitor and reliability monitor systems.

An integrated analysis framework of the GO-FLOW has been developed [11] for the safety analysis of Elevator systems in Japan. In this system (ELSAT: Elevator Safety Analysis Tool), an analyst can freely handle inter-related information, such as, records of elevator accidents in the past, detailed figures of mechanical structure of elevator, control logic of elevator operation, failure and maintenance data of components, GO-FLOW model and its explanation, analysis results, improved system model and corresponding GO-FLOW model. Framework of ELSAT can be reflected in the design of reliability monitor system being developed in HEU.

Figure 3 shows an example of user interface developed for the handling of GO-FLOW analysis in the reliability monitor system.

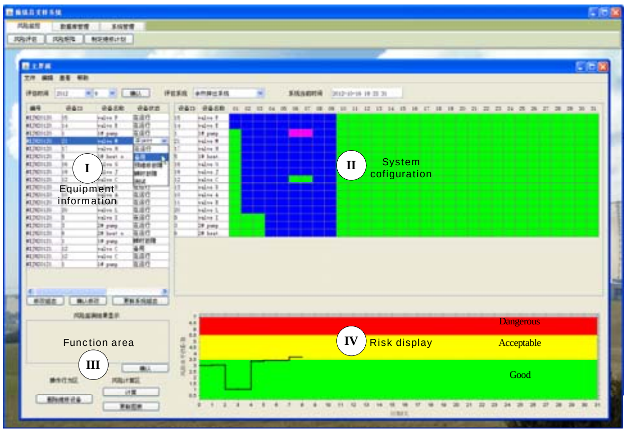

Fig. 3 User interface for GO-FLOW analysis in reliability monitor system.

This monitor screen is divided into four functional areas.

Area I: This area shows the components of a specific subsystem in a table form. The table contains the component ID, component name, component status (operating, standby, failed), start time for maintenance, Mean Time to Repair (MTTR), failure rate and its uncertainty range, and parameters of aging effects. The information about the common cause failure groups, phase boundaries and the mission of subsystem at each phase is also given in area I.

By double clicking the status column, the operator can select the current component status from the predefined status for the analysis of GO-FLOW in order to evaluate the actual or hypothetical subsystem condition. While the actual component state change is realized on the monitor screen of the plant DiD risk monitor system.

Area II: Corresponding to the modified information about component status, the user interface will automatically show the system configuration with the detailed expression of component status in the passage of time. The components in standby state are indicated in light yellow color and the operating state in light blue color. Failed state is expressed in magenta. Components belong to the same common cause failure group are indicated in the same dark color tinged with yellow or blue, depending on whether they are in standby or operating state.

Area III: Instead of rebuilding a new GO-FLOW model, the modified system configuration is realized by a mere change the data information of the original GO-FLOW model. Generation of modified GO-FLOW data is obtained by selecting "New data" button. By selecting the "execution" button in the function area, modified system configuration is evaluated by the GO-FLOW methodology, which can take into account of common cause failures, aging effects and uncertainty analysis. Information of MCSs is also obtained by this analysis.

If the change of subsystem configuration is drastic and thus becoming difficult to use data modification method, a plant personnel(= analyst in this case) at main control room or equivalent place, has to construct new GO-FLOW model.

Area IV: After the calculation, the reliability result of a subsystem is displayed in a curve with three color bands background indicating three reliability levels. The boundaries between these risk bands are predefined according to the safety criteria concerning to a specific subsystem. The red region indicates a high and unacceptable reliability level of subsystem. Hence, immediate action needs to be taken to reduce the risk. The yellow band means that system reliability is moderate and acceptable, so proper actions are preferred to be taken based on cost effective considerations. When the reliability curve lies in the green band, it means the system is normally and safely operated.

An interface between the reliability monitor and operator is therefore very important. With the well-designed interface, an operator (=analyst) can easily identify the change of plant conditions, and can easily re-evaluate the risk level of the system. Thereafter, plant personnel can take proper actions for the prevention of sever accident.

5 Conclusion

A new method of risk monitor system of a nuclear power plant has been proposed by Harbin Engineering University. The Risk Monitor provides an overall plant states and details about events that impact the reliability of plant operation. An important part of the risk monitor is monitoring the dynamic reliability of subsystems, which will help the plant operators to find the problems before real loss of service appears during the plant operation.

The GO-FLOW is an important part of the knowledge base system of reliability monitor. The GO-FLOW has capability to treat the following matters: phased mission problem, common cause failure, identification of MCSs, uncertainty analysis, and aging and maintenance effects.

Explanations were given for the installation of the GO-FLOW into the reliability monitor of the risk monitor system being developed at HEU.

References

[1] IAEA-TECDOC-1106, Living Probabilistic Safety Assessment (LPSA), IAEA (1999).

[2] YOSHIKAWA, H., LIND, M., YANG, M., HASHIM, M., and ZHANG, Z.: Configuration of Risk Monitor system by plant defense-in-depth risk monitor and reliability monitor, International Journal of Nuclear Safety and Simulation, 2012, 3(2): 140-152.

[3] 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.

[4] HASHIM, M., MATSUOKA, T., and ZHANG, Z.: Development of reliability monitor for the safety related subsystem in PWR considering the redundancy and maintenance of components by fault tree and GO-FLOW methodology, International Journal of Nuclear Safety and Simulation, 2012, 3(2): 164-175.

[5] MATSUOKA, T., and KOBAYASHI, M.: GO-FLOW A new reliability analysis methodology, Nuclear Science and Engineering, 1988, 98: 64-78.

[6] MATSUOKA, T., and KOBAYASHI, M.: A phased mission analysis by the GO-FLOW methodology, In: Proceedings of International ANS/ENS Topical Meeting Probability, Reliability and Safety Assessment, Pittsburgh, 1989: 1145-11148.

[7] MOSLEH, A., *et al.*: Procedure for treating common cause failures in safety and reliability studies, EPRI-NP-5613, 1988.

[8] MATSUOKA, T., and KOBAYASHI, M.: The GO-FLOW reliability analysis methodology -Analysis of common cause failures with uncertainty -, Nuclear Engineering and Design, 1997,(175):205-214.

[9] KARLIN, S., and TAYLOR, H. M.: A First Course in Stochastic Processes (Second Edition), Academic Press, New York, 1975.

[10] LEVY, I. S., *et al.*: Prioritization of TIRGALEX – Recommended Components for Further Aging Research, NUREG/CR-5248. US Nuclear Regulatory Commission, Washington DC, 1988

[11] MATSUOKA, T.: GO-FLOW methodology -Basic concept and integrated analysis framework for its applications, International Journal of Nuclear Safety and Simulation, 2010, 1(3): 198-206.