

A method for developing living PSA for NPPs by using the GO-FLOW methodology

YANG Jun¹, YANG Ming², YOSHIKAWA Hidekazu³, and YANG Fangqing⁴

1. College of Nuclear Science and Technology, Harbin Engineering University, 150001, China (youngjun51@hotmail.com)

2. College of Nuclear Science and Technology, Harbin Engineering University, 150001, China (yangming@hrbeu.edu.cn)

3. Symbio Community Forum, Kyoto, Japan(yosikawa@kib.biglobe.ne.jp)

4. China Nuclear Power Research Institute, 518000, China (yfq613@163.com)

Abstract: A living PSA method is developed for nuclear power plants using GO-FLOW method. Unlike conventional fault-tree analysis, the GO-FLOW model is a system reliability analysis method based on a success-tree oriented approach, which can treat time-dependent system reliability analysis including phased-mission problems. A generalized GO-FLOW modeling structure is proposed in this paper, where all the necessary functional modes of the equipment comprising a whole system can be taken into account. Moreover the structure of GO-FLOW modeling can be easily modified in accordance with the changes of plant configuration caused by either equipment failures, or operator interventions, or maintenance activities. The methods on how to build up a generalized GO-FLOW model structure and then how to convert it to a living PSA model by utilizing the GO-FLOW model are validated as illustrated by a case study. An application of the proposed method is also briefly discussed for developing to a risk monitoring system.

Keyword: Living PSA; Risk Monitor; Reliability Analysis; GO-FLOW Methodology;

1 Introduction

Safe operation is the precondition for pursuing higher productivity at nuclear power plants (NPP). Aiming at providing insights on the existing safety margins for event sequences with an integrated risk analysis model, Probabilistic Safety Assessment (PSA) has become a widely used tool for the safety assessment of nuclear power plants.

The system configuration of NPP often changes over time with the change of operation modes such as start-up, steady state operation, power level change, shutdown and refueling and maintenance. Due to the large scale complexity of facilities, such changes may result in repeated physical modifications, and enhancement of operational procedures and organization management^[1]. The PSA model, as a means of valuating plant risk at any given time, must be updated or modified when it is necessary to reflect the plant changes for the understanding of the current state of plant safety.

The above-stated need of evaluating risk state at any time has led to the concept of living PSA^[2] and its application for Risk Monitor^[3-4]. The risk monitor model is based on and updated with higher or at least

the same frequency as living PSA^[5]. While, at the same time risk monitor is significantly different from the model that is used for living PSA. Living PSA is a plant specific PSA that is used for determining the average risk of the plant for some average assumed conditions or simplifications made in the model, with aspects such as average initiating event frequencies, maintenance unavailability and simplified system alignments.

In contrast, risk monitor aims at providing point-in-time risk based on the actual plant configuration^[6]. Hence, the living PSA model needs to be inspected and amended to remove these simplifications and more information of the current state of the plant needs be used in the PSA to make it more suitable for the risk monitor. The core of risk monitor is living PSA which consists of two aspects; developing and updating living PSA models. Living PSA models are built based on Level-1 PSA models with specific considerations reflecting the current design and operation features.

This paper will present a method for developing a living PSA method by using GO-FLOW method. Unlike conventional fault-tree analysis, the GO-FLOW model is a system reliability analysis method based on a success-tree oriented approach, which can treat time-dependent system reliability

Received date: March 11, 2014

(Revised date: May 17, 2014)

analysis including phased-mission problems. In this study, a generalized GO-FLOW model structure will be proposed, which includes the necessary functional modes of equipment and can be easily modified according to the changes of plant configuration caused by either equipment failures, operator interventions, or maintenance activities. The proposed method is expected to provide an effective solution for living PSA development and update in a risk monitoring system.

The rest of the paper is organized as follows. In Section 2, motivation of why GO-FLOW should be applied as well as why generalized GO-FLOW structure is proposed for living PSA development. The methods on how to build up a generalized GO-FLOW model structure and then how to convert it to a living PSA model by utilizing the GO-FLOW model, are demonstrated through a case study in Section 3. Section 4 briefly introduces the framework of a risk monitoring system based on the proposed GO-FLOW modeling method for living PSA development and update. Finally, the conclusions and some future work are summarized in Section 5.

2 Living PSA development by using GO-FLOW method

2.1 The motivation for developing living PSA by GO-FLOW method

PSA models for risk monitoring can be represented in a number of ways. Fault tree (FT) /event tree (ET) are the most conventional methods^[7] used for PSA models. Fault Tree Analysis puts the possible causes for system failure in a logical form that is helpful in identifying weakness in the system. Fault trees can be used in system reliability analysis from both qualitative and quantitative points of view. However, the conventional fault tree has several limitations in order to describe the effects of system configuration changes, especially caused by surveillance test and maintenance activities^[8]. This is because the failure behavior of systems with those different modes of operation is generally dependent on the time stamp or the sequence of events^[9], while time-dependent unavailability analysis cannot be performed by one fault tree analysis^[10]. In addition, a fault tree is difficult to modify or validate as a large complex target system is to be considered.

GO-FLOW methodology^[11] is a success-tree based system reliability analysis technique. Compared to fault tree analysis (FTA), GO-FLOW is more suitable for the availability analysis of repairable systems with phased mission problems^[12-13] and timing consideration^[14]. Reliability analysis by GO-FLOW consists of two steps: first constructing a GO-FLOW chart for the target system and then calculating the system reliability quantitatively. The GO-FLOW model corresponds to the physical layout of the system. The model can be easily constructed from GO-FLOW operators. These operators represent particular functional modes or logical gates. Reliability analysis by GO-FLOW is performed by the approximate method used in the fast fault-tree analysis program^[11]. The GO-FLOW methodology can also be used for common cause failure analysis^[15] and logical loops^[16] evaluation and has been applied to a wide variety of systems, ranging from railways^[17], and elevator systems^[17] to nuclear power plants^[18].

One of the specific applications of living PSA is to use it as a PSA tool to generate risk information for day-to-day management of operational safety at NPPs. These daily operational and maintenance activities on components turn out to be sequence-dependent and time-dependent with dynamic behavior. The time-dependent sequential action order requires continuous-time processes or a finite number of discrete time values to express it, which is indicated to be difficult to handle by conventional fault trees. On the other hand, the system operation sequence with time stamps can be easily analyzed by GO-FLOW method. Apart from the sequential action problem, a component may vary its functional status in different phases of the system life cycle, i.e. operation, standby, maintenance, test and failure. When component status is changing, re-arrangements of system configuration and operation sequence are necessarily made to maintain the objective of system function. By then, the GO-FLOW model must be updated in terms of the the new system configuration. The model update is readily realized with a GO-FLOW modularization modeling method which will be presented in the next Section.










2.2 Development of a generalized GO-FLOW structure for living PSA

In conventional GO-FLOW analysis, the system logic model varies greatly as the component status and system configuration changes. Although sometimes the updated GO-FLOW model may be only subtle alternations to the original system model, the process of update involves many trivial manual operations by either displacing GO-FLOW operators or modifying parameters of operators in conventional GO-FLOW modeling method. Human errors are easily introduced in the process. And this is even more burdensome for those who are not PSA specialists but are required to interact with the PSA model. Therefore, it is most desirable that Living PSA update could be completed in a convenient way by a risk management tool.

In this section, a generalized GO-FLOW structure is proposed for developing living PSA models that contain all possible system and component operational states. The generalized model is presented based on the conventional GO-FLOW modeling method. The generalized model is actually an integrated model of a component with all kinds of functional modes

synthesized in different phased missions. Fig.1 shows the integrated model structure. The structure exhibits all the functional status modes that a component such as pump, valve, actuator, etc. may experience in its lifetime within one single module. In the GO-FLOW module, all component states are arrayed in a parallel structure, which is straightforward for expressing the component state. The state changes among them are easily completed through the switchover of different functional mode lines. The status modes included in the generalized model are presented in individual modules, with each functional module consisting of a set of designated GO-FLOW operators so that different levels of component performance and task demands can be modeled. Each functional mode module is taken as a stand-alone unit. By adding or deleting the corresponding functional mode unit in the integrated model, the reliability characteristics of equipment in different mission profiles and modes are described. The functions of these designated GO-FLOW operators used in the generalized GO-FLOW model are explained in Table 1.

Table 1 Operators in GO-FLOW method

Symbol	Type	Meaning	Symbol	Type	Meaning
	Type-22 Operator	OR Gate		Type-35 Operator	Operator for an Item with Ageing Effect (Operating Failure)
	Type-25 Operator	Signal Generator		Type-37 Operator	Operator for an Item with Ageing Effect (Standby Failure)
	Type-26 Operator	Operator for Normally Closed Item		Type-38 Operator	Operator for an Item in Corrective Maintenance
	Type-28 Operator	Operator for an Item with Delay Impact		Type-39 Operator	Operator for an Item with Opening and Closing Action
	Type-30 Operator	AND Gate			

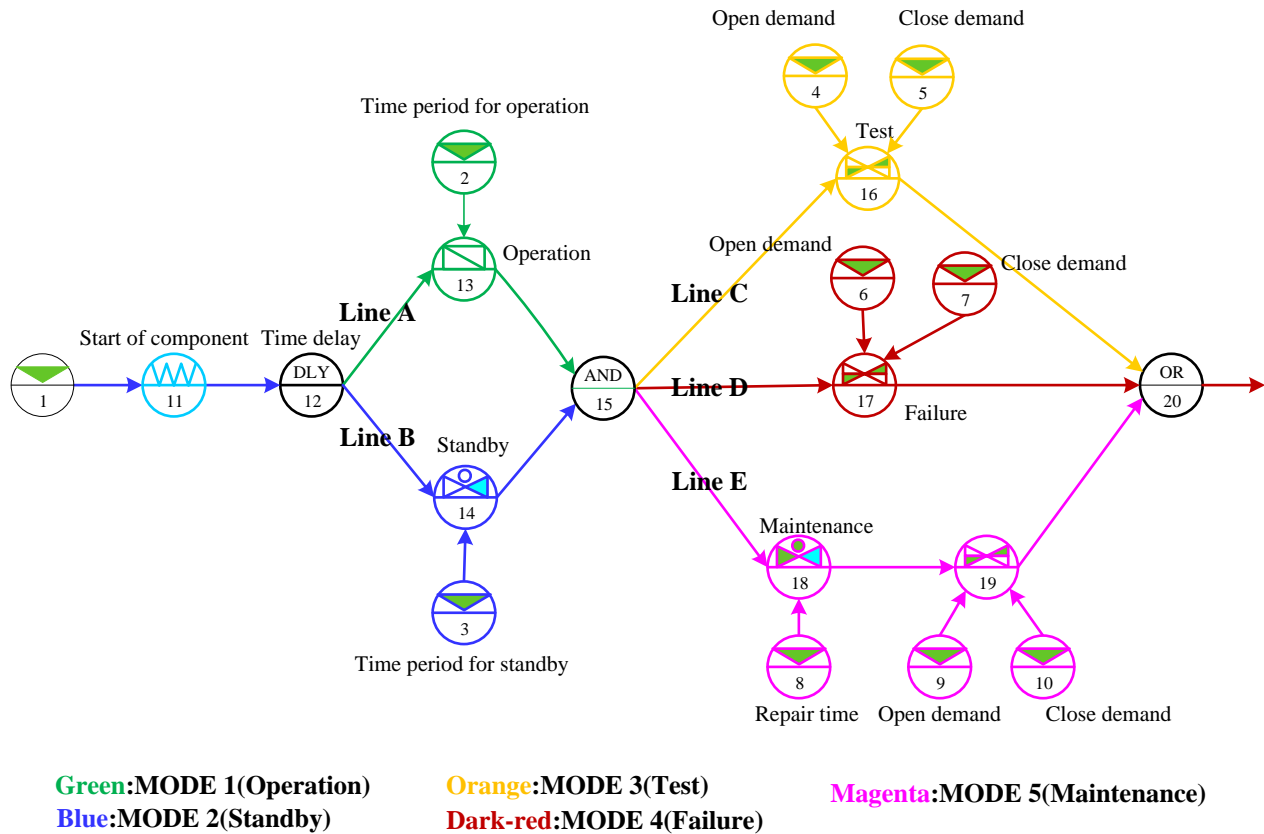


Fig. 1 Generalized GO-FLOW model structure developed for use in living PSA.

The generalized GO-FLOW model covers all functional modes of a component, which are operating, standby, test, failure, and maintenance, respectively as Line A to Line E as shown in Figure.1. The number below the horizontal line of each operator in the model is used to identify operators that may be of the same operator type. These numbers will be given by GO-FLOW editor automatically during the GO-FLOW modeling. The subroutine line drawn in different color in the model is used to guide and distinguish the signal flows of component in different functional modes. The signal flows out of functional operators such as type-21 operator (No.11 operator indicated by cyan) and type-28 operator (No.12 operator indicated by bold black) in the model that represent the basic characteristic and time delay of a component, and it comes to an end at an OR gate through mutually exclusive functional mode lines. Because of the mutual exclusion of component status, Exclusive-OR operation in this generalized GO-FLOW model is hence substituted by combining type-22 operator (OR gate) with the control over open and close demand signal of type-39 operator in each subroutine line. The type-21 operator in the model structure represents a pass/fail type component. It can

be also replaced by a type-26 operator, type-27 operator or type-39 operator depending on the type of products ranging from normally closed component, normally open component to on-off component. Type-28 operator is a delay operator used for describing the delay effect of a component but is not a necessity in every component model. When the time delay of a signal is not being considered, type-28 operator is allowed to be removed from the model so that the signal flow will come out of the basic characteristic operator (in this model, it is indicated by No.12 operator) to a particular subroutine line. The functional modes as well as its subroutine lines are explained in detail as follows.

MODE 1: operating--signal flows through subroutine line A

For a component working in operating mode, type-35 operator (No.13 operator) is used to model the aging impacts of operating failure. The operating failure follows an exponential distribution and is modeled by

$$R(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} \exp[-(\lambda + \mu)t] \quad (1)$$

Where $R(t)$ is the output signal intensity of the operator, λ is failure rate and μ is repair rate, which describes the time to failure and the time to repair of

component as an exponential distribution. The failure rate and repair rate are assumed to be constant. The time period t for operation is represented by a type-25 operator (No.2 operator).

MODE 2: standby--signal flows through subroutine line B

Standby failure of component is modeled by type-37 operator (No.14 operator) in GO-FLOW method. Type-37 operator in the GO-FLOW model also models the preventive maintenance activity with a type-25 operator (No.3 operator) connected which yields negative sub-input values to cancel the age effects of standby failure.

The reliability changes of a component in preventive maintenance is given by

$$R(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} \exp[-(\lambda + \mu)t]$$

$$(\lambda, \mu) = \begin{cases} (\lambda_1, 0) & t \leq t_i \\ (\lambda_2, \mu) & t > t_i \end{cases} \quad (2)$$

Where λ_1 is the failure rate of component under standby state, λ_2 is the failure rate and μ is the repair rate of component in preventive maintenance, and t_i is the time for preventive maintenance.

MODE 3: test--signal flows through subroutine line C
The modeling of a testing activity includes the effects of test downtimes and test overrides. The opening and closing action of a component during testing activity is modeled by type-39 operator (No.16 operator). If the sub-input signal $P_1(t)$ arrives, the operator takes the opening action. Then the output intensity is calculated by

$$R(t) = S(t) \cdot \{O(t') + [1 - O(t')] \cdot P_1(t) \cdot P_o\} \quad (3)$$

If the sub-input signal $P_2(t)$ arrives, closing action is taken. The output intensity becomes

$$R(t) = S(t) \cdot O(t') \cdot [1 - P_2(t) \cdot P_c] \quad (4)$$

Where $S(t)$ is the main input signal, $P_1(t)$ is the probability of generating the open demand, $P_2(t)$ is the probability of generating the close demand, P_o and P_c are probabilities of a component being successfully opened and successfully closed upon demands during test, and the test override can be also modeled by giving a particular value to P_c . $O(t')$ is probability of component in the open state at the time point immediately before time point t .

MODE 4: failure--signal flows through subroutine line D

Failure means a component is out of service and gives no output. In this respect, type-39 operator (No.17

operator) is used as a switch to control output of a component in failure. When it is used as a switch, the expression of type-39 operator becomes

$$R(t) = \begin{cases} 1 & P_1(t)=1, P_2(t)=0 \\ 0 & P_1(t)=0, P_2(t)=1 \end{cases} \quad (P_p=0, P_o=1, P_c=1) \quad (5)$$

Where P_p is the probability of component being prematurely opened before the testing activity. $P_p = 0, P_o = 1, P_c = 1$ setting in the expression is used for modeling "off-on-off" functional state of a switch represented by type-39 operator, $P_1(t)$ is the open demand signal used for turning type-39 operator on, and $P_2(t)$ is the close demand signal which is used to turn type-39 operator off. $P_1(t) = 1, P_2(t) = 0$ means that type-39 operator turns on and the signal can be output as usual. The type-39 operator is normally "on" to represent a component being in service, e.g. operation and standby. Once the component fails, $P_1(t), P_2(t)$ will change to $P_1(t)=0, P_2(t)=1$ and the connected type-39 operator is turned off. The type-39 operator in line of failure mode is reused for state cutover of a component being in-service (operation and/or standby) and failure.

MODE 5: maintenance--signal flows through subroutine line E

With the use of a type-38 operator (No.18 operator), corrective maintenance of a component can be implemented in the GO-FLOW model. Type-38 operator is originally used to model a time dependent valve failure in a closed state by the following formula

$$R(t) = 1.0 - \frac{\mu}{\lambda + \mu} - \frac{\lambda}{\lambda + \mu} \exp[-(\lambda + \mu)t]$$

$$= \frac{\lambda}{\lambda + \mu} - \frac{\lambda}{\lambda + \mu} \exp[-(\lambda + \mu)t] \quad (6)$$

Where λ is failure rate, μ is repair rate, and t stands for time durations.

While the reliability changes of a component in corrective maintenance is exactly given by

$$R(t) = \frac{\mu}{\lambda + \mu} \{1 - \exp[-(\lambda + \mu)t]\} \quad (7)$$

This equation means that the component is initially in failure state, $R(t=0) = 0.0$ and then recovers gradually.

Consider that λ is the repair rate and μ is the failure rate in type-38 operator, then type-38 operator can act as a new operator to represent the component in corrective maintenance.

Now replace λ with μ' , and μ with λ' , then the expression of type-38 operator becomes

$$R(t) = \frac{\mu'}{\mu + \lambda} - \frac{\mu'}{\mu + \lambda} \exp[-(\mu' + \lambda')t] \\ = \frac{\mu}{\lambda + \mu} \{1 - \exp[-(\lambda + \mu)t]\} \quad (8)$$

This new operator defined from type-38 operator can then be used to model the corrective maintenance of a component which recovers gradually from a completely failed state. The repair time is represented by No.8 operator.

In each subroutine line, a type-39 operator is also serially connected to control the signal output of different component status. Each type-39 operator in parallel has two sub-inputs, an open demand signal and close demand signal. The open demand signal is used to turn on the type-39 operator and the corresponding functional state is “on”. The close demand signal turns the component status into “off”. By setting open and close demand signals to type-39 operators in each functional mode unit at different time points, the status change is realized. For example, if a component is under test, the No.4 operator which is connected to the type-39 operator in the test line will take an opening action. After that we can give it a close demand signal to the No.5 operator to stop the testing activity. When component status changes, e.g. from test to operation, then both type-39 operators in test mode and operation mode take actions. The turn-off action of type-39 operator in test parallel and turn-on action of type-39 operator in operation parallel should be fulfilled by inputting a command signal to No.5 operator and No.6 operator simultaneously. By this means, the status changes of component and system are easily realized with the generalized model.

3 A case study of living PSA by GO-FLOW

An example of a simple water supply system is described to illustrate how the proposed generalized model structure is applied to living PSA development and update.

3.1 System description

Figure 2 shows a simple water supply system. The water supply system is designed as two redundant lines to improve the system availability. The system provides water from a tank to the users through two pumps (1#pump and 2#pump). The water tank and at least one of the pumps must function normally to

supply the water to the users. Initially, the water tank supplies water to 1#pump. 1#pump is actuated. Two hours later 2#pump starts up. The system is required to operate for 120 hours following its demand.

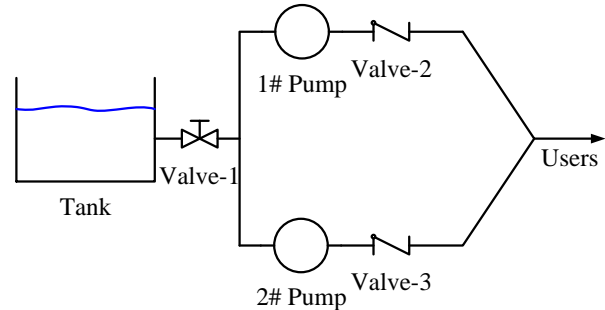


Fig.2 The schematic diagram of a water supply system.

The operational sequence of the system under normal conditions is shown in Figure. 3. A total of nine time points are defined for expressing the sequence of system operation, as well as to describe the system responses under a hypothetical scenario. Time point 1 is an initial time. At time point 2, the water supply system is placed in service as 1#pump and valve-2 is put into operation. The system keeps operating following its demand. Note that time point 3 and time point 4 have the same actual time but with different expression of meanings. Time point 3 is two hours after time point 2 without any other action. Time point 4 immediately follows on time point 3, representing the opening action of 2# pump. As for actual time 50h and 70h, they have the similar definitions of time points with reference to the action sequence shown in Fig.4.

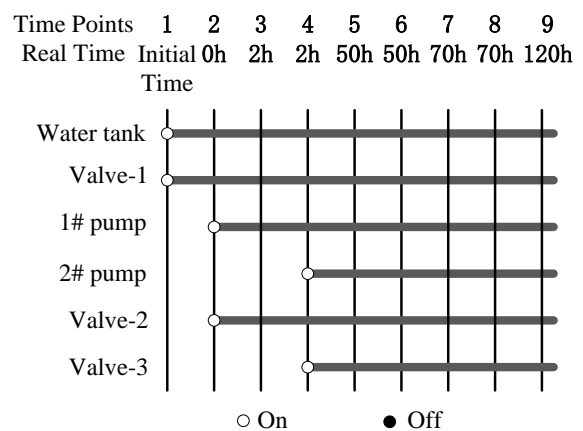


Fig. 3 System configuration under normal operation.

While during the actual operation, the components status and system configuration is usually altered

according to the accident sequence, system responses and the operator's intervention on system. For example, in the analysis of the water supply system it is supposed that the 1# pump breaks down at time 50h (time point 6) for a sudden failure. Following this, 1# pump is taken out of service for repair until its recovery at 70h (time point 7). 1# pump may be put into operation again (at time point 8) to ensure the water supply after its maintenance. Based on the hypothetical system responses, the configuration of water supply system is changed, as shown in Fig. 4. Downtime of 1# pump begins at time point 6 and ends at time point 8, while other components continue operating as normally required.

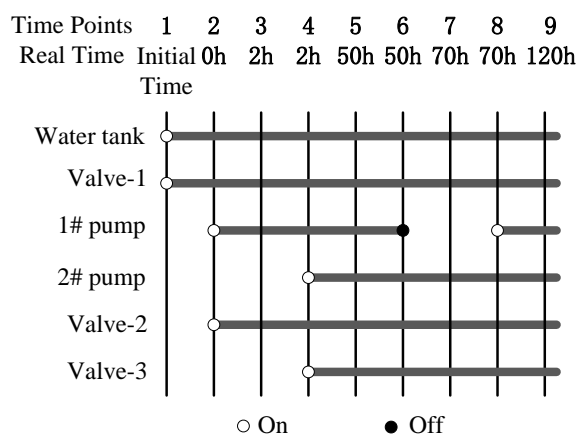


Fig. 4 Hypothetical system configuration.

3.2 Develop living PSA model with the generalized GO-FLOW model structure

The reliability model of the water supply system under different system configurations and components status is built into one GO-FLOW chart by using the generalized model method, as shown in Fig. 5. In the GO-FLOW model of the water supply system, the proposed generalized model is adopted and incorporated to represent the possible pump status changes during the operation.

To identify the components and their functional modes, notations are written by the side of the corresponding operators.

First, the components in the water supply system are classified into three types, pass/fail type, normally-closed type and on-off type.

1. Pass/fail type component

Water tank and check valve-2/valve-3 are treated as a pass/fail type component in the water supply system. GO-FLOW uses the type-21 operator to model the

pass/fail-type component.

2. Normally closed component

Normal valve-1 is treated as a normally-closed type component, which is modeled by type-26 operator in the GO-FLOW chart.

3. On-off component

1# pump, 2# pump are treated as on-off type components. The opening and closing action of an on-off component is modeled by type-39 operator.

Next, aging impacts are considered for 1# pump and 2# pump. The ageing effect model is followed by the basic functional model. Type-35 operators are used for modeling the failure of the pump working in operating mode. The operating failure follows a negative exponential distribution. Standby failures of the 1# pump and 2# pump are modeled by type-37 operator in GO-FLOW chart.

Besides the functional operators introduced above, there are also signal generators and logical operators *e.g.*, type-25 operator (signal generator), AND and OR logic (logical operators) appear in the GO-FLOW model. Type-25 operator has various meanings in the GO-FLOW model according to its uses. Type-25 operator represents water flow from a water tank when it acts as water source. The water flow is treated as a signal in GO-FLOW. The type-25 operator also acts as a trigger signal source when used for opening a normally closed component or opening and closing an on-off component. The ageing effect of 1# pump and 2# pump are also modeled with a sub-input type-25 operator which represents the time interval between successive time points. As sub-input signal connected to a switch which is represented by a type-39 operator for controlling outputs of each functional mode, type-25 operators are taken to turn the switch on and off. The logical relation of system branching lines is expressed in the GO-FLOW chart by using the logic gates "OR". Table 3 shows the reliability data for system analysis.

Table 3 Reliability data for system analysis

Components	Operator Parameters
1# Pump/2# pump	$P_o = P_c = 0.9995$ $\lambda(\text{standby}) = 1 \times 10^{-6}/h$ $\lambda(\text{operating}) = 5 \times 10^{-6}/h$ $\mu = 5 \times 10^{-2}/h$
Normal valve-1	$P_g = 0.999$
Check valve-2/valve-3	$P_g = 0.9999$
Water tank	$P_g = 0.999999$

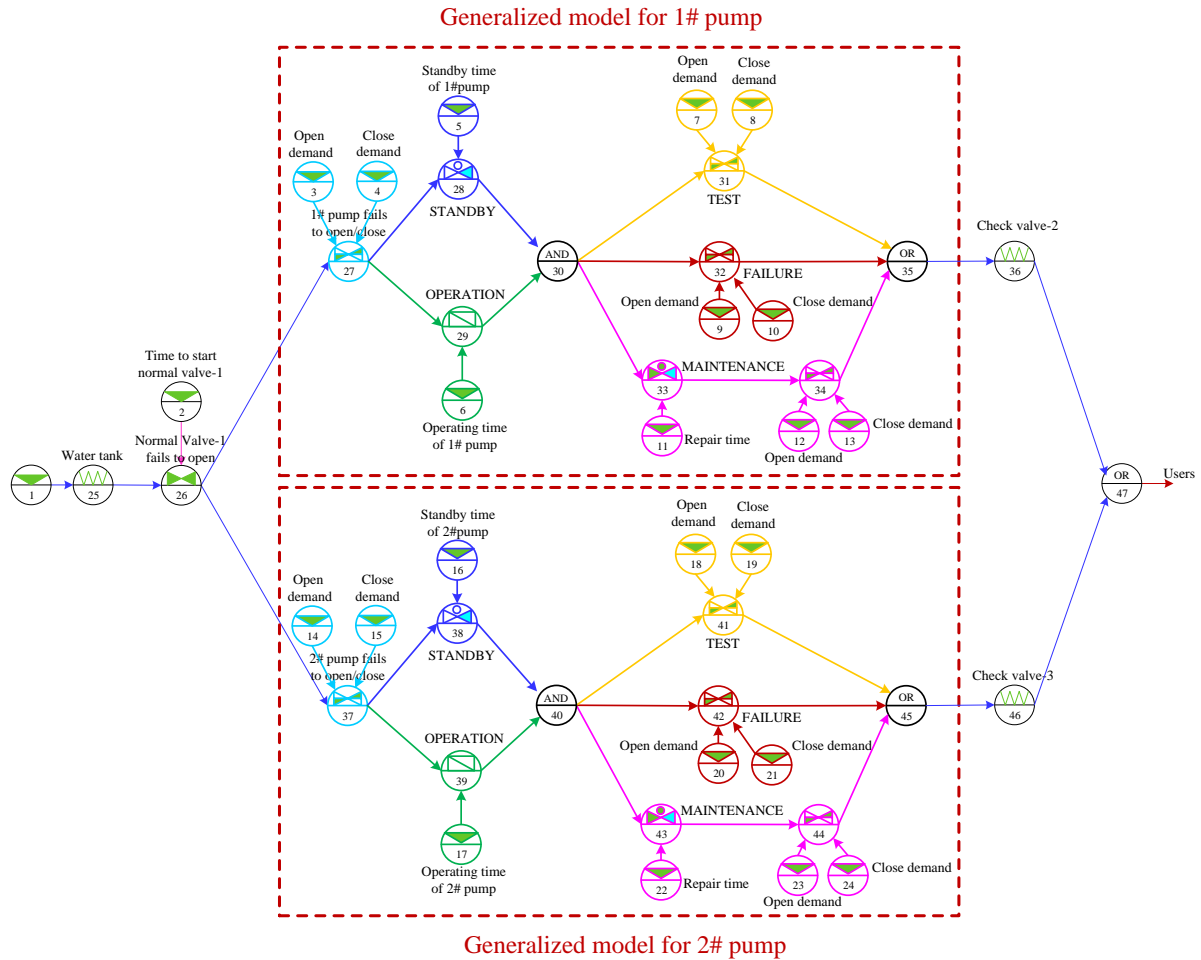


Fig. 5 GO-FLOW chart for water supply system with the proposed generalized structure.

3.3 Living PSA Model update on system GO-FLOW model file

In living PSA by GO-FLOW, the system model is initially setup with average assumptions and values. The generalized GO-FLOW model is applied to the representation of all possible component statuses but without designating any specific functional mode at the beginning. Once the system configuration information has been input, the model will be updated to reflect the current operation of system. The GO-FLOW update can be easily realized using a model file. The GO-FLOW model file is generated by the GO-FLOW program automatically upon the assignment of system parameters to the model. The GO-FLOW model file is a translation of the GO-FLOW model. The data in the system model file contains all possible system operational states and the file itself can be repeatedly modified for model updating. The GO-FLOW model file initially with average assumptions and values is output as the original system model file (also referred to as living PSA model). Every time when performing living PSA

updating, a new file the same as the original system model file will be created for repeated uses. This can be done for a range of plant configuration changes being updated by a system model file.

As shown in Figure. 6, the system model file consists of four sections, which are (i) system logic model, (ii) failure data given to operators, (iii) definition of time points, and (iv) signals output by signal generator(type-25 operator). In section (i), system logic model is represented by various operators which connect to each other with unique numbers allocated. As to each operator, the failure data is then given in part (ii). Time points are predefined in part (iii). The expressions of the signal generated by signal generator in part (iv) range from source signal, trigger signal to time interval in response to the different uses of type-25 operators in GO-FLOW model. Living PSA is updated with modification to the signal intensity in part (iv). *E.g.*, in the analysis of the case study, the system configuration under normal conditions is firstly written into the model file which is shown in the upper left corner of Fig. 7. A new model file will

be updated as hypothetical changes occurring to the system configuration. The new model file is generated and presented in the lower left corner of Fig. 7. with parameters modifications. The data modifications reflect the changes to the system configuration. The

modifications in the GO-FLOW model file are classified into three types, including open and close demand signal of each functional mode, time interval between functional modes and source signal intensity.

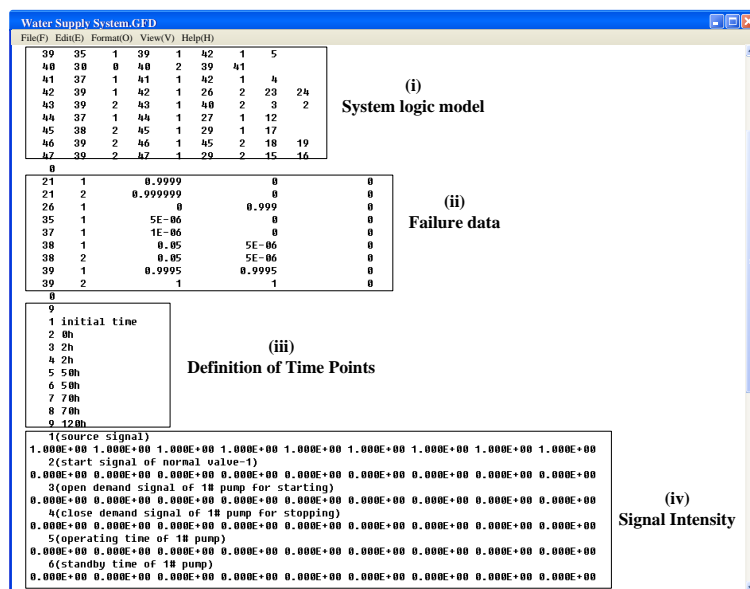


Fig.6 System GO-FLOW model file.

3.4 Living PSA analysis by a remote procedure call

Following system model update, the analysis of the system under the normal configuration and hypothetical scenarios are performed by using a remote procedure call "a.bat". The function "a.bat" is developed as an automatic tool for GO-FLOW analysis. The function will call the GO-FLOW program to evaluate the system model when it is demanded. As shown in Fig.7, the system model file is called directly to update the analysis results. The system GO-FLOW model files are located on the left side while system results are showed to the right of the figure.

The analysis results of the water supply system under normal operation sequence and a hypothetical scenario are listed in Table 3. Results are also shown in Fig.8 and Fig.9 respectively for the possible comparisons. Generally, the system availability decreases over time due to aging effects and accumulative wear. While at time point 4, the 2# pump is started, which results in a dramatic decrease of the system unavailability from 1.61033×10^{-3} to

1.00125×10^{-3} . The system unavailability increases again when the 1# pump is out of its service at time 50h in the hypothetical scenario. The variation of system reliability is mainly caused by the components status and system configuration changes. The changes to the system configuration are easily input into the model file for living PSA update and analysis.

Table 3 Unavailability of water supply system

Time Points	Actual Time/h	System Failure Probability/ 10^{-3}	
		Normal Condition	Hypothetical Scenario
1		0	0
2	0	1.60035	1.60035
3	2	1.61033	1.61033
4	2	1.00125	1.00125
5	50	1.00149	1.00149
6	50	1.00149	1.84193
7	70	1.00154	1.94174
8	70	1.00154	1.00142
9	120	1.00209	1.00182

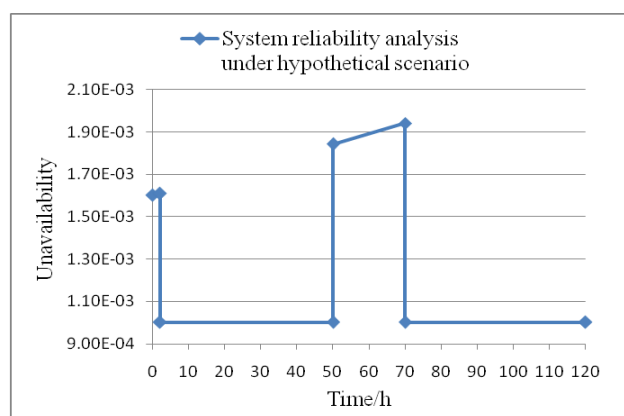


Fig.9 System reliability analysis under hypothetical scenario.

4 Framework of a risk monitoring system by GO-FLOW method

This Section will briefly introduce a risk monitoring system based on the presented GO-FLOW modeling method for living PSA development and update. As shown in Fig.10, the risk monitoring system that the authors have been engaging by utilizing GO-FLOW is designed to receive the information on plant configuration changes resulting from operator interventions on system, maintenance plans or condition monitoring system, and then update the

GO-FLOW model with online modification to the system GO-FLOW model file and perform the GO-FLOW analysis by a remote procedure call, and display risk values graphically. The specific procedures for risk management at NPPs by this proposed risk monitoring system are (i) GO-FLOW modeling, (ii) GO-FLOW updating, (iii) GO-FLOW analysis and (iv) risk information display. The methods employed in those four items are described in the subsequent part of this Section.

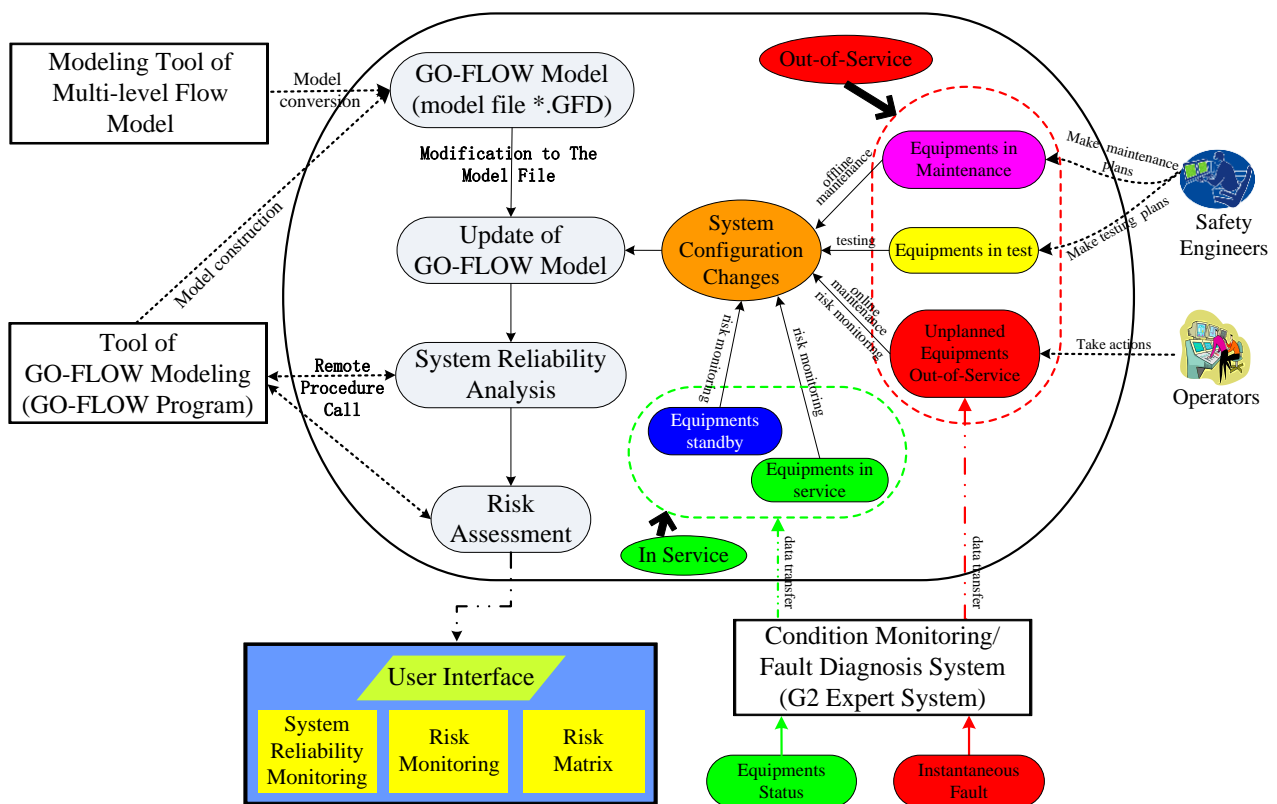


Fig. 10 Framework of risk monitoring system by GO-FLOW.

4.1 GO-FLOW modeling

The GO-FLOW models can be either generated from the tool of GO-FLOW modeling or converted from the tool of Multi-level flow models (MFM) which are graphical models of goals and functions of process systems^[19-20]. Compared to the system GO-FLOW chart modeled by the tool of GO-FLOW modeling, the GO-FLOW models that are converted from MFM are of higher understandability with multiple levels of means-end and whole-part hierarchy for the system configuration. The software tool of mapping the MFM models into GO-FLOW models has been developed

by the authors and a reliability analysis program based on the multilevel flow models is under development^[21-22].

4.2 GO-FLOW updating

When changes occur to system configuration, the corresponding reliability model of the system must be updated and recalculated to reflect the actual risk level of the current plant configuration. Since the component functional mode represented by the proposed GO-FLOW model structure is in one-to-one correspondence with the signal number in system

GO-FLOW model file (file *.gfd), the equipment status changes and system configuration changes can be easily achieved with online modification to the signal information of the system model file (file *.gfd) instead of manual operations on the tool of GO-FLOW modeling. The GO-FLOW models can be online updated through the tool of risk monitoring system by operators. When the tool of the risk monitoring system is connected online, changes to the plant configuration will be automatically input to the system model files via the databases. The model files can also be updated manually by safety engineers for offline uses.

4.3 GO-FLOW analysis

In the risk monitoring system, GO-FLOW analysis will involve the activities of system reliability analysis and risk assessment. The GO-FLOW analysis is performed automatically through a remote procedure call in system reliability analysis. As for risk assessment, an accident sequence model is first represented by a GO-FLOW chart. The GO-FLOW model is the logical equivalent to a dynamic event tree which is conventionally used for accident sequence analysis. The safety systems which are required to operate to prevent or limit core damage are considered as basic heading events appearing in the sequence model. System failure analysis results from GO-FLOW can be directly linked to the headings in the sequence model. Then the sequence model GO-FLOW chart is analyzed to get the quantitative risk level. In this designed risk monitoring system, core damage frequency (CDF) will be taken as a quantitative risk measure.

4.4 Risk information display

The risk information obtained by GO-FLOW analysis will be entered into the user interface of the risk monitoring system tool as a curve that gives the user a clear visual indication of the level of plant risk. The safety margins and values are employed to heighten the awareness of plant personnel as well as resulting in corresponding actions involvement during plant operation or maintenance activities. The risk monitoring system aims at providing assistance for safety engineers and plant operators in their maintenance management and daily operation risk management at NPPs.

5 Conclusions

A method for developing living PSA is proposed based on the GO-FLOW methodology. The methods on how to develop and update living PSA by utilizing the GO-FLOW model are illustrated by a case study. The analysis shows that living PSA by GO-FLOW is easily updated and performed with the model modification as well as remote procedure call technique for model re-quantification.

On the basis of the presented method for living PSA, a brief introduction of the framework of a risk monitoring system by GO-FLOW is also introduced in the paper. The proposed framework will be expected to provide a comprehensive overview of several issues for risk management by the risk monitoring system. It has been shown that the key technologies for realization of a risk monitoring system are readily accessible with GO-FLOW. Future work will mainly focus on the development of various tools which are related with the proposed risk monitoring system.

Acknowledgements

The authors appreciate the financial support from “111” Project on Nuclear Power Safety and Simulation (Grant No.b08047) and Prof. Takeshi Matsuoka of Utsunomiya University for his kind help in this study.

References

- [1] BALFANZ, H. P., VIROLAINEN, R. K.: State of Living PSA and Future Development, NEA/CSNI/R(99)15, 1999.
- [2] COBO, A. G.: Living Probabilistic Safety Assessment (LPSA), IAEA-TECDOC-1106, 1999.
- [3] COBO, A. G.: Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, IAEA-TECDOC-1200, 2001.
- [4] YOSHIKAWA, H., YANG, M., HASHIM, M., *etc*: Design of Risk Monitor for Nuclear Power Plants, Nuclear Safety and Simulation, Vol.2, No.3, pp.266-274, 2011.
- [5] SHEPHEND, C., EVANS, M., BONEHAM, P.: RISK MONITORS—The State of the Art in their Development and Use at Nuclear Power Plants, NEA/CSNI/R(2004)20, 2004.
- [6] KAFKA, P.: Living PSA-risk monitoring—current use and developments, Nuclear Engineering and Design, Vol. 175, pp. 197-204, 1997.
- [7] NELSON, W. R., NOVACK, S. D.: Real-Time Risk and Fault Management in the Mission Evaluation Room for the International Space Station, INEEL/EXT-03-00661, 2003.

- [8] CEPIN, M., MAVKO, B.: a dynamic fault tree, Reliability Engineering and System Safety, Vol.75, pp.83-91, 2002.
- [9] WALKER, M., PAPADOPOULOS, Y.: qualitative temporal analysis: Towards a Full Implementation of the Fault Tree Handbook, Control engineering practice, pp.1-11, 2008.
- [10] REN, Y., DUGAN, J. B.: Optimal Design of Reliable Systems using Static and Dynamic Fault Trees, IEEE Transactions on Reliability, 1998:234-244.
- [11] MATSUOKA, T.: FFTA: A Fast Tree Analysis Program, Nuclear Engineering and Design, Vol.91, pp.93-101, 1986.
- [12] MATSUOKA, T., KOBAYASHI, M.: GO-FLOW: A New Reliability Analysis Methodology, Nuclear Science and Engineering, Vol. 98, No.1, pp. 64-78, 1988.
- [13] MATSUOKA, T., KOBAYASHI, M.: A Phased Mission Analysis by the GO-FLOW Methodology, Proc. Int. ANS/ENS Tropical Meeting Probability, Reliability and Safety Assessment, Pittsburgh, USA, 1989.
- [14] MATSUOKA, T., KOBAYASHI, M.: GO-FLOW Methodology: A Reliability Analysis of the Emergency Core Cooling System of a Marine Reactor Under Accident Conditions, Nuclear Technology, Vol.84, No. 3, pp.285-295, 1989.
- [15] MATSUOKA, T., KOBAYASHI, M.: The GO-FLOW reliability analysis methodology—analysis of common cause failures with uncertainty, Nuclear Engineering and Design, 1997,(175):205-214.
- [16] MATSUOKA, T.: Method for solving logical loops in system reliability analysis, Nuclear Safety and Simulation, Vol.1, No.4, pp.328-339, 2010.
- [17] MATSUOKA, T.: GO-FLOW methodology—Basic concept and integrated analysis framework for its applications, Nuclear Safety and Simulation, Vol.1, No.3, pp.198-206, 2010.
- [18] OKAZAKI, T., MITOMO, N., MATSUOKA, T.: The use of the GO-FLOW methodology to investigate the aging effects in nuclear power plants, Proceedings of PSAM-0113: International Conference on Probabilistic Safety Assessment and Management, New Orleans, Louisiana, USA, 2006.
- [19] LIND, M.: Modeling Goals and Functions of Complex Industrial Plants, Applied Artificial Intelligence, 1994, Vol.18, No.2, pp.259-283.
- [20] LIND, M.: An introduction to multilevel flow modeling, Nuclear Safety and Simulation, 2011, Vol.2, No.1, pp.22-32.
- [21] YANG, M., ZHANG, Z. J.: Study on Quantitative Reliability Analysis by Multilevel Flow Models for Nuclear Power Plants, Nuclear Power Engineering, Vol.32, No.4, pp.72-76, 2011.
- [22] YANG, M., ZHANG, Z. J., PENG, M. J., YAN, S. Y.: Design and Development of A Reliability Analysis Tool Based on Multilevel Flow Models, Proceedings of 16th International Conference on Nuclear Engineering, Orlando, Florida, 2008.