Development of a reliability monitor for the safety related subsystem of a PWR considering the redundancy and maintenance of components by fault tree and GO-FLOW methodologies

HASHIM Muhammad, MATSUOKA Takeshi, and YANG Ming

College of Nuclear Science and Technology, Harbin Engineering University, Heilongjiang, Harbin, 150001 China
(hashimsajid@yahoo.com,mats@cc.utsunomiya-u.ac.jp, myang.heu@gmail.com)

Abstract: A reliability monitor checks the operating performance of each of the individual subsystems that comprise the whole system and display the reliability of the subsystems. By monitoring the reliability of individual subsystems, the operators of the plant can gain insight on potential performance bottlenecks to establish baseline performance. Monitoring the reliability of the subsystems also helps the plant operator to find problems before real loss of service occurs.

The GO-FLOW method is based on success-oriented system analysis technique. This technique is able to evaluate the system reliability and availability. An example analysis is conducted by GO-FLOW to obtain the dynamic reliability curve of the containment spray system in a PWR. It is shown by parametric analysis that the system reliability is increased by the redundant system configuration of the containment spray system.

Keyword: reliability monitor; dynamic reliability; GO-FLOW; containment spray; PWR

1 Introduction

In reliability engineering, the word "reliability" is defined as the ability of a system or component to perform its required functions under certain prescribed conditions for a specified period of time. It is often measured as a probability of failure or a measure of availability.

Maintaining reliability for complex systems requires more elaborate systems approach than for non-complex systems [1]. A nuclear power plant is a complex engineering system, hence it requires special consideration to ensure high reliability of system performance. The reliability of a nuclear power plant decreases with the passage of time because failures increase due to the degradation of components composing the whole system.

In order to maintain high reliability of any complex system, an important issue is to establish a "reliability database" which contains the statistical data of all critical systems and components comprising the whole engineering system. In the case of a nuclear power plant, the reliability can also be improved through daily or periodic activities such as testing, inspections, maintenance and quality assurance activities to maintain the quality of operation [2]. As the failure probabilities of the plant components increase with usage time, the replacement of components can be made before the failure probability exceeds the permissible level. The replacement of components and maintenance is important for maintaining a high level of reliability of nuclear power plant.

In order to evaluate a system's reliability, an effective system reliability model is required. Reliability modeling approaches are largely based on statistical methods. Typical examples of these methods are reliability block diagrams (RBD) [3], fault tree analysis (FTA) [4] and GO-FLOW analysis [5]. These methods can provide system reliability models where individual system components must be defined as either active or failed [6].

The authors of this paper have utilized the GO-FLOW method to evaluate the dynamic reliability of a safety-related subsystem in a PWR by considering the redundancy in the system. An

Received date: May 30, 2012
(Revised date: June 27, 2012)

example is presented for the containment spray system of PWR. The rest of this paper starts from the definition of a reliability monitor, description of the containment spray system and test and maintenance. It then overviews the GO-FLOW method, followed by the evaluation of the dynamic reliability of the containment spray system using GO-FLOW.

2 Definition of a reliability monitor

An important role of the Reliability Monitor of nuclear power plant is monitoring the operating performance of individual subsystems comprising the whole system and displaying the "Reliability" of the subsystems. By monitoring the "Reliability" of individual subsystems, the operator can gain insight into potential bottlenecks to establish baseline performance. The evaluated reliability values can then be used to assess the effectiveness of performance tuning and upgrade of both hardware and software components. Therefore, monitoring reliability helps us to identify problems before the operation of the system causes loss of service. The implemented degree of redundancy and ample safety margins in the designed system provide high reliability of those subsystems and of the components important to safety.

The idea of reliability monitors for individual subsystems has been developed by the authors of this paper and has been presented elsewhere [7] with the complete framework of a "Risk Monitor". In this earlier work, the reliability monitor gives a qualitative evaluation in a way similar to failure mode and effect analysis (FMEA) together with the quantitative reliability evaluation method called GO-FLOW.

3 Overview of GO-FLOW

The GO-FLOW method is a reliability analysis method based on the success-oriented system analysis technique. It is capable of evaluating system reliability and availability by describing the target system with what is called a GO-FLOW chart, which is composed of signal lines and operators. Each operator represents the function or failure of physical equipment, logic gates and a signal generator. There are 14 different types of operators as shown in Fig. 1.These operators are used in making GO-FLOW charts to model a subject system. The signal does not represent a "change of condition" but some physical quantity or information.

A physical quantity called "intensity" is associated with a signal line. The intensity represents the probability of signal existence. In this case, the "Existence" includes "Potential existence" which means that a physical quantity exists when all the resistance "downstream" is removed.

A finite number of discrete time values (points) are given to express the system operational sequence. The values of time points do not represent real time but correspond to the ordering of event occurrences.

The sub-input signal can be given to operators 35, 37 and 38 and the intensity represents a time interval between successive time points. The operators 35, 37 and 38 are light bulb failure, valve failure in an open state and valve failure in a closed state, respectively. These operators require component failure rates λ. The sub-input signal represents the time duration in the same units used for λ [8].

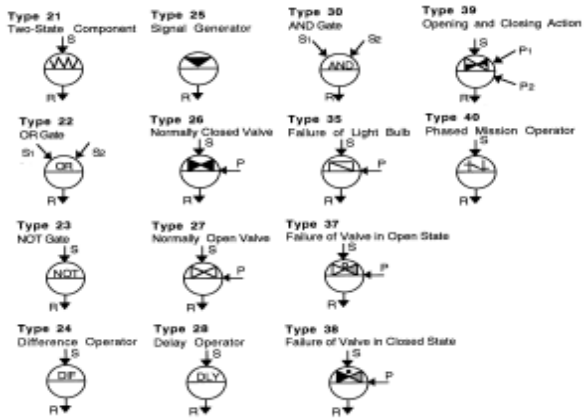

Fig. 1 Operators in the GO-FLOW methodology [8].

The GO-FLOW methodology possesses the following significant features.

(i) The GO-FLOW chart corresponds to the physical layout of a system and is easy to construct and validate,

(ii) Alterations and updates of a GO-FLOW chart are easily made,

(iii) The GO-FLOW chart contains all possible system operational states, and

(iv) The analysis is performed by one GO-FLOW chart and one computer run.

If the system to be analyzed is large-scale, then the construction of a GO-FLOW chart and preparation of input data for the GO-FLOW program requires great effort. To alleviate these constraints, an integrated analysis framework called ELSAT has been developed for easy handling of large, complex systems [9].

4 Description of the containment spray system

4.1 Configuration of the containment spray system

The configuration of the containment spray system employed in the conventional PWR is illustrated in Fig. 2. The containment spray system has the function to decrease the containment pressure during a loss of coolant accident (LOCA) to maintain the design pressure of the containment vessel (atmospheric pressure). The pressure transient during a LOCA is analyzed to determine the maximum required blow-down energy of the reactor coolant system. The containment spray system traps radioactive inorganic iodine washed-down into the containment sump by spraying the reactor vessel with borated cooling water. Sodium hydroxide (NaOH) solution of about 30% concentration is added from a spray additive tank (SAT). The containment spray system is designed to have a single layer of redundancy. During the LOCA, if there is no offsite power, then the necessary electric power is supplied by diesel generators so that it can perform the specified safety function. In the containment spray system there is a test line which is designed to allow periodical tests and inspections to verify the operability and integrity depending on the importance for safety [10].

As shown in Fig. 2, the containment spray system consists of a containment spray pump (CSP), containment heat exchangers (CSHEX), refueling water storage tank (RWST), spray additive tank (SAT) and the containment recirculation sump (CRS). CSHEXs are cooled by components of the cooling water system (CCWS). The RWST is designed to provide the borated water which is pressurized with nitrogen. 100% redundancy capacity of spray pumps

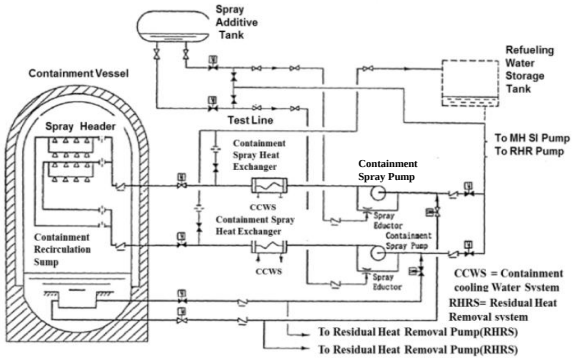

Fig. 2 Containment spray system of PWR plant [10].

and heat exchangers are installed. The NaOH solution makes the water slightly alkaline to enhance absorption of radioactive iodine and to prevent corrosion of the vessel during long-term cooling after the accident. It can minimize the transpiration of radioactive iodine from the recirculation sump water. When the containment pressure increases during the LOCA then a containment high pressure signal is actuated and transmitted to the containment spray system, the CSHEXs outlet valves are opened, the CSP is started, the SAT injection valve is opened and the borated cooling water in the RWST is sprayed into the containment vessel through the spray nozzles attached to the spray headers (injection mode; phase 1).

When the water level in the RWST drops to a certain level, then the water source is switched to the CRS, and after cooling the recirculation water in the CSHEXs, the water will be sprayed into the containment vessel (recirculation mode; phase 2) [10].

In the case of a LOCA, the time span of phase one is 0-1800 sec and for second phase is 1800-3600 sec for the GO-FLOW analysis. The time point 1800 seconds for shifting from phase 1 to 2 is taken by an engineering judgment that water storage should be large enough to cover the needed time for continuous injection of water by both ECCS and containment spray for a large break LOCA in the cold leg.

In subsequent sections 5.1, 5.2 and 5.3, this paper discusses the different redundancy cases for containment spray systems by analyzing the dynamic reliability of individual cases using GO-FLOW.

4.2 Test and maintenance of containment spray system during the operation of the plant

Besides unavailability due to component failure, each containment spray injection system (CSIS) is separately taken out of standby status for monthly flow test of the pumps. During the test only one CSIS spray subsystem is disabled [10].The test duration for each pump is 15 minutes minimum and 4 hours maximum per month. The maintenance of the CSIS pumps is assumed to be performed with an interval ranging from 1 to 12 months. The test and maintenance contribution to CSIS unavailability is estimated by multiplying the sum of test unavailability and maintenance unavailability for one spray subsystem by the hardware failure unavailability of the other subsystem, with a factor of 2 for the two subsystems.

At the monthly test, if one spray subsystem is found to be unavailable, then the other subsystem must be tested for operability [11].

The plant operation continues until its decommission at 40 years and the failure rate of containment spray system components increases during the usage time. In this paper, the functioning of the containment spray system has been considered in the case of a large break LOCA during the normal operation of the nuclear power plant indicated by the yellow block in Fig. 3. The containment spray system works at high containment pressure during the large break LOCA and the large break LOCA occurs in the middle of the yellow block during plant operation

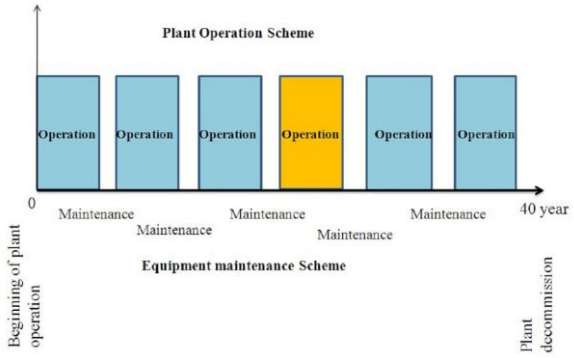

Fig. 3 Plant operation and maintenance Scheme.

The failure rate is the frequency with which an engineering system or component fails and is important in reliability engineering. It is denoted by Greek letter λ (lambda). The failure rate of the system usually depends on time, with the rate varying over the life cycle of the system. The failure rate $\lambda(t)$ is often thought of as the probability that a failure will occur in a specified interval of time in the discrete sense and can be defined with the aid of a reliability function $R(t)$.

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{1}$$

where $f(t)$ is the probability distribution function of failure which is given by:

$$f(t) = \frac{dF}{dt} = -\frac{dR}{dt} \tag{2}$$

since $F(t) = 1 - R(t)$, where $F(t)$ is a cumulative distribution function of failure.

And so Eq. (1) can be approximated by

$$\lambda = \frac{R(t_1) - R(t_2)}{(t_2 - t_1)\ R(t_1)} \tag{3}$$

or it can be

$$\lambda = \frac{R(t) - R(t + \Delta t)}{(\Delta t)\ R(t)} \tag{4}$$

Calculating the failure rate for a small interval of time results in the hazard function $h(t)$ which represents the instantaneous failure rate as Δt tends to zero. Therefore,

$$h(t) = \lim_{\Delta t \to 0} \frac{R(t) - R(t + \Delta t)}{\Delta t\ R(t)} = \lambda(t) \tag{5}$$

The instantaneous failure rate depends on a failure distribution $F(t)$ which is a cumulative distribution function that describes the probability of failure at time t.

$$F(t) = \int_0^t f(\tau) d\tau \tag{6}$$

From Eq.(1), now the hazard function $h(t)$ can be defined as

$$h(t) = \frac{f(t)}{R(t)} \tag{7}$$

Many probability distributions can be used to model the distribution of failure rate. However the exponential distribution is widely used because the

failure rate is given by time independent value. In this case, both Eqs. (1) and (7) are given by

$$h(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda \tag{8}$$

In this case, from Eq. (6) the cumulative distribution function *F(t)* is given by

$$F(t) = \int_0^t \lambda e^{-\lambda \tau} d\tau = 1 - e^{-\lambda t} \tag{9}$$

Both the exponential distribution function *R(t)* and the failure rate $\lambda(t)$ in this case are shown in Fig. 4.

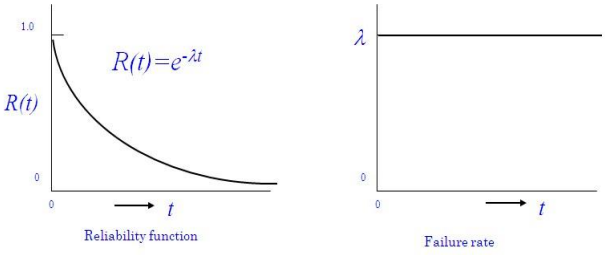

Fig. 4 Exponential distribution and failure rate.

Normally, the failure probability of the safety system of nuclear power plant becomes zero just after maintenance. However, the failure probability of replaced equipment increases in time because of degradation of the whole system with usage. Therefore replacement of components is necessary before the failure probability exceeds the permissible level as shown in Fig. 5.

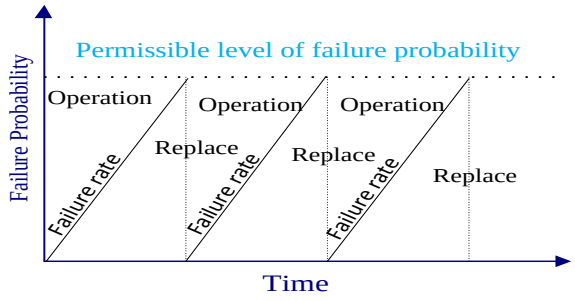

Fig. 5 Failure probability versus time during plant operation and maintenance.

The failure probability of the components which cannot be replaced for the whole plant life simply increases with time. The aims of preventive maintenance are to prevent the failure of equipment before it actually occurs and has been designed to preserve and enhance equipment reliability by replacing worn components before they actually fail. Preventive maintenance activities include equipment checks, oil changes, and lubrication, partial or complete overhauls after specified periods and so on. For maintenance the workers can also record equipment deterioration so they know to replace or repair worn parts before they cause system failure. The ideal preventive maintenance program would prevent all equipment failures before they occur. The long-term benefits of preventive maintenance include: (i) improved system reliability, (ii) decreased cost of replacement, (iii) decreased system downtime, (iv) better spares inventory management.

5 Example practice of GO-FLOW

5.1 Simplified containment spray system

5.1.1 Explanation of single line simplification

For better understanding and ease of GO-FLOW analysis, the authors have considered a simplified containment spray system. As seen in Fig. 2, in the real configuration of the containment spray system there are two parallel lines of injecting water by the CSP from the RWST, and NaOH addition from the SAT and re-circulating water from the CRS. There is also a test line which is designed to allow periodical tests and inspections to verify the operability and integrity. The existence of two parallel lines and the test line enhances the reliability of the containment spray system in both actual operation and maintenance of the system.

However, under the assumption of simplified spray system as shown in Fig. 6, these parallel lines are simplified by a single line. The test line is neglected in the simplified spray system. The CSHEX secondary side is cooled by the CCWS in reality, but this was also neglected in the simplified version. The control of the containment spray system is also explained in Fig. 6. If the containment pressure (P) is abnormally high then the containment pressure activation (CPAS) system will be activated and the containment pressure sensor (CPS) will measure the high containment pressure. The containment spray activation signal (S) will be transmitted to an actuating device (valve or pump) by transmitter (pressure sensing line or electrical wire).

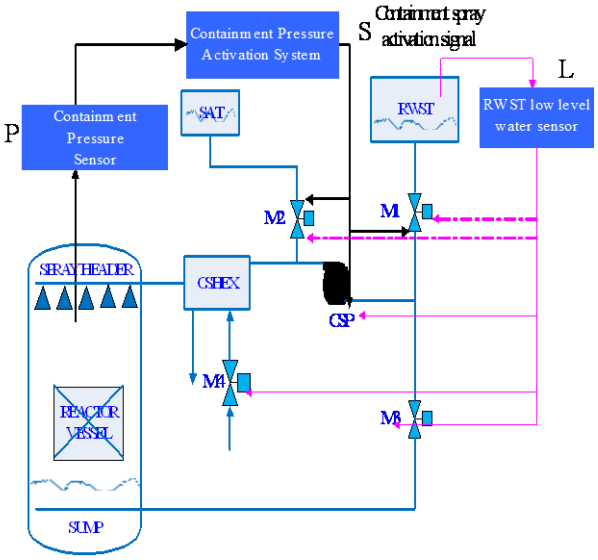

Fig. 6 Simplified containment spray system.

The additional abbreviations M1 to M4 which used in the simplified spray system are motor-operated valves. The components RWST, SAT, CSHEX, and the spray header are passive components while the CSP and motor –operated valves M1 to M4 are active components.

The injection of containment spray will start when "S" is on and then M1, M2 and CSP are on. This is the injection mode which will continue until the water level in the RWST goes down to a certain level. The containment spray system changes to re-circulation mode when the low level water signal (L) of the RWST becomes on. The both valves M1 and M2 will close first and then the both valves M3 and M4 will open followed by the start of containment spray pump (CSP). Thus, the water in the sump will be pumped up by CSP and poured down over reactor vessel in the containment through the spray header after cooling by Containment Spray water Heat Exchanger (CSHEX). This recirculation mode will continue until the containment spray water temperature becomes low enough.

Operation of the active components of the containment spray system (CSS) is explained in Table 1, where major active components in the containment spray system are listed. The changing of the operation mode from injection mode (phase 1) to re-circulation mode (phase 2) is indicated. This is mainly controlled by changing the open-close state of the four motor valves M1 to M4 in the simplified case.

Table 1 Operation of active components and failure rate used in the simplified CSS [12, 13]

Simplified case				
valve	Phase 1	Phase 2	Failure probability	Failure during usage
M1	Open	Close	0.04/demand	1×10^{-5} /sec
M2	Open	Close	0.04/demand	1×10^{-5} /sec
M3	Close	Open	0.04/demand	1×10^{-5} /sec
M4	Close	Open	0.04/demand	1×10^{-5} /sec

5.1.2 Failure mode and failure rate of components used in the containment spray system

There are three different failure modes for both motor-operated valve and pump: (i) failure to open/start (ii) failure to close/stop, and (iii) failure during usage. For each failure mode of safety components there are different failure rates. As the failure of the safety system during operation is degraded in many ways by failure mechanism caused by usage conditions out of the design range - such as high temperature, high moisture / humidity, high pressure, which may cause the material to be disrupted by cracking, wastage, fretting, *etc*.

For the first and second type, the failure rates of motor-operated valve and pump open and close actions should be counted on the demand basis and do not depend on the time duration.

For the third type of failure mode (failure during usage), there are two types of failure mechanism: failure rate λ_o during normal operation and failure rate λ_{acc} during an accident. The both types of failure depend on the time duration. Here special care should be taken for deciding λ_o by considering the regular replacement of equipments as shown in Fig. 5. Especially, the effect of when accident happens should be considered first when you set the failure rate λ_o. The value of λ_o is zero when accident happens just after the replacement while it is almost permissible level when accident happens just prior to replacement.

Logic is used to determine (i) how the control command signal will be generated and (ii) whether or not the generated control command will be successfully transmitted to the actuation device to

start or stop the safety system. The model of this logic is shown in Fig. 7.

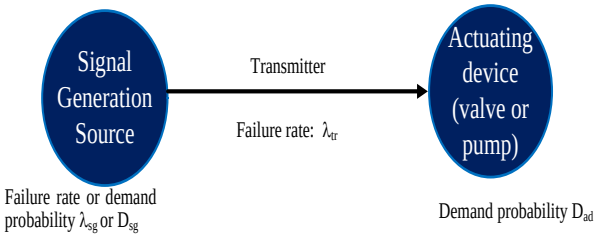

Fig.7 Logical configuration of control command generation and transmit.

This model consists of three steps for the failure of valves and pumps during open/close actions and during operation respectively. These are: (i) command generation process which includes human operator's judgment and proper action (push button), normal operation of command generation equipment, (ii) success of command transmission through electrical wire or pressure sensing line (iii) normal response of the actuating device to a given command.

In the case of the containment spray system there is a containment sensor to detect the high containment pressure during an accident, which for normal operation will generate a command and transmit the high containment pressure signal by transmitter to actuating device (valve or pump).

5.1.3 Fault tree and GO-FLOW analysis for control command generation process

The fault tree analysis is made to find the unreliability (failure probability) in the control command generation process. As seen in Fig. 7 there are three steps for the control command generation and transmitting process. That is (i) signal generation source *e.g.* containment sensor (ii) signal transmitter source *e.g.* signal wire (iii) actuating device *e.g.* valves or pumps. The failure and success probability of these components is given in Table 2. The time duration for fault tree analysis is assumed to be 24 hours or 86400 sec.

The logic for failure of the final system in fault tree analysis is as follows.

(i) "Failure of actuating device" = "failure during run" OR "failure to start"

(ii) "Failure to start" = "failure itself with given signal" OR "failure due to no signal"

(iii) "Failure due to no signal" = "transmitter failure" OR "transmitter has no signal

(iv) "Transmitter has no signal" = "Containment sensor failure"

The fault tree shown in Fig.8 indicates that there are multiple failures that can occur which result in no control command transmitting to the actuating device. However the situation in which there is no control command to the actuating device can result from any one of four failures. The failure probability or opening probability of the final system can be found by using the OR logic Boolean expression for four events.

Table 2 Failure and success probability for fault tree analysis

Components	Failure probability	Success probability	Failure mode
Containment sensor	A1=3.05×10^{-9}	0.99999997 /demand	Fails to operate
Transmitter	5×10^{-9}×86400 A2=4.32×10^{-4}/sec	0.9999136/ sec	Signal failure
Actuating device (valve or pump)	A3=4×10^{-2}	0.96 /demand	Failure to start
	1-exp(-1×10^{-5} ×86400) A4=0.5785/sec	0.4215/sec	Failure during run

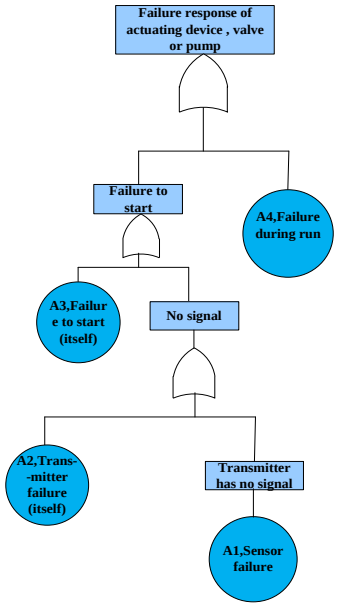

Fig.8 Fault tree model for failure of actuating device.

failure of final system = failure of actuating device+ failure of transmitter + failure of signal generation

P (failure of final system) = P (failure of actuating device + failure of transmitter + failure of signal generation)

P (A1 or A2 or A3 or A4) =

P(A1) + P(A2) + P(A3) + P(A4) –P(A1) × P(A2)- P(A2)× P(A3) - P(A3) × P(A4) - P(A4)× P(A1) – P(A2) × P(A4) - P(A1) × P(A3)+ P(A1) × P(A2) × P(A3) + P(A2) × P(A3) × P(A4) +P (A1) × P (A3) × P (A4) + P (A1) × P(A2) ×P(A4)-P(A1)×P(A2)×P(A3)×P(A4)

Opening probability of final system=0.59577.

The GO-FLOW analysis is made on the control command generation process as shown in Fig.7 The GO-FLOW chart is shown in Fig. 9 where operator 1, 6 and 7 represent the signal generation, transmitter and actuating device. Operator 8 represents the output, which shows the opening or successful probability of the actuating device.

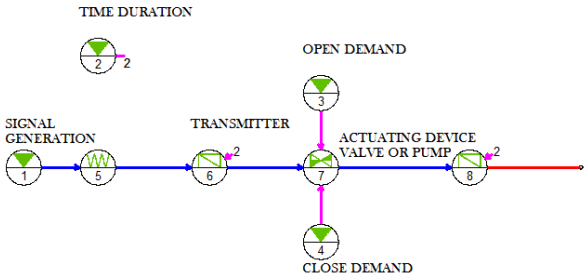

Fig. 9 GO-FLOW chart of control command generation and transmitting model.

The opening probability of the actuating device is given in Table 3. The result of the opening probability of fault tree and GO-FLOW are almost same, with only a slight difference because in the GO-FLOW analysis the failure during run (operation) is modeled by a type 35 operator (operator number 8 in Fig. 9) which models failure proceeding only when the components are in the operating state. But in fault tree analysis, failure proceeds even if the component is not in the operating state. In the fault tree analysis, the opening probability is a little smaller than in the GO-FLOW analysis. The valve opening or successful probability is shown in Fig.10. The analysis is also made for 24 hours or 86400 sec but the valve opening probability shown in Fig.10 is only from 0 to 4200 sec for phase 1 and 2.

Table 3 Opening or successful probability result

Real Time (sec)	Valve Opening Probability
0	4.00000×10^{-2}
0.1	4.00000×10^{-2}
600	3.97606×10^{-2}
1200	3.95226×10^{-2}
1800 (End of phase 1)	3.92861×10^{-2}
1800 (Start of phase 2)	9.60872×10^{-1}
2400	9.55121×10^{-1}
3000	9.49404×10^{-1}
3600	9.43722×10^{-1}
4200	9.38074×10^{-1}
86400	4.12162×10^{-1}

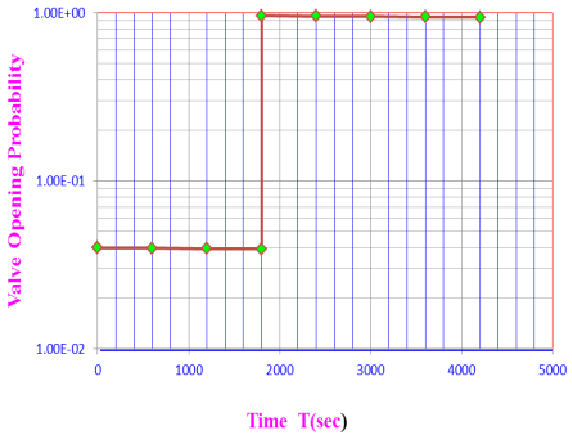

Fig. 10 Opening or successful probability of valve. during open and close action.

The valve successful or opening probability from time 4200 sec to 86400 sec decreases significantly, because the reliability or availability of the nuclear system (components) has been affected adversely by the failure of components with the passage of time.

The failure rate or probability of other safety components such as the RWST, SAT, CSHEX, and sump in the containment spray system increases with the life of the nuclear reactor and the failure rate or probability of these components in different failure modes will be considered in detail in a future study.

5.1.4 GO-FLOW analysis for simplified system (Case 1)

The authors conducted a GO-FLOW analysis to obtain the dynamic reliability curve for the simplified containment spray system. The GO-FLOW chart of the simplified containment spray system is shown in Fig. 11, where each operator represents a component failure, signal generator which controls the operation, or a logic gate.

According to this chart there are two phases. For phase 1 RWST, SAT, CSP M1 and M2 are needed. For phase two CRS, CSHEX, M3 and M4 are required. The connecting lines between every operator identify the signals. The final output signal 19 corresponds to the success probability of the simplified spray system.

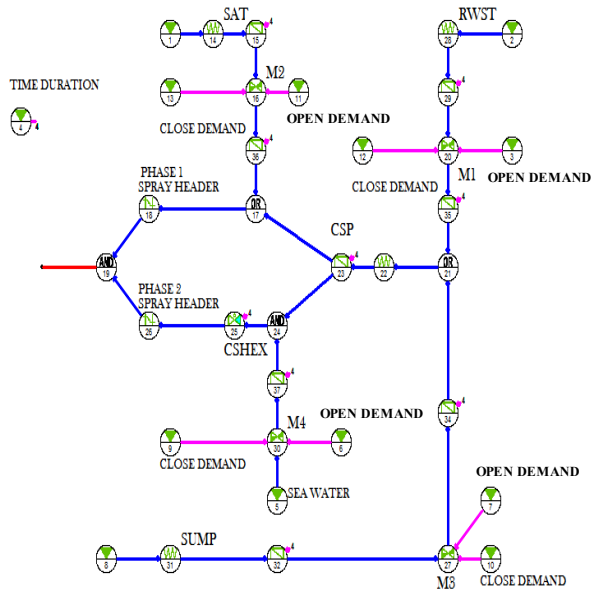

Fig. 11 GO-FLOW chart of simplified spray system.

The reliability data assigned in this study are given in Table 4, where RWST, SAT, CSHEX and CRS are passive components, which have no need of any power source for actuation. The CSP is the active one which needs a power source for actuation and it should open in both phases. But the motor-operated valves from M1 to M8 are active ones which have open and closed states.

In the phased mission problem, 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.

Table 4 Failure rate used in the present analysis [12,13]

Components	Kind	Success probability P failure rate λ
RWST	Passive	Pg= 0.999999, $\lambda o= 1\times10^{-5}$ /sec
SAT	Passive	Pg=0.99, $\lambda o=1\times10^{-5}$ /sec
CRS	Passive	Pg=0.999999, $\lambda o=1\times10^{-5}$/sec
CSHEX	Passive	$\lambda o=1\times10^{-8}$ /sec
CSP	Active	Pg=0.99, $\lambda o=1.5\times10^{-6}$ /sec
M1,M2, M3,M4	Active	Po=0.96/demand , Pc=0.96/demand, Pp=0.96
M5,M6, M7,M8	Active	Po=0.96/demand, Pc=0.96/demand, Pp=0.0

Therefore it is necessary to calculate the products of success probabilities among different phases and to treat correctly the inclusion or exclusion relationship between the failures of shared components [14].

The calculated failure probability versus time for the containment spray system of PWR, will be discussed in 5.5 with the inter-comparison of the three Cases 1, 2, and 3.

5.2 Two parallel lines running simultaneously (Case 2)

In this case, two parallel injection lines are assumed to run simultaneously as shown in Fig. 12 and these two lines are expressed in a GO- FLOW model. This redundancy system of two lines enhances the reliability and can wash-down the radioactive

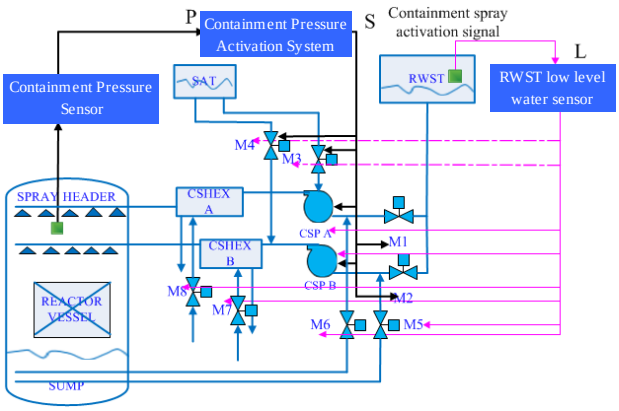

Fig. 12 Containment spray system in case of two lines running simultaneously.

material in the containment more quickly as compared to a single line and also reduce the containment pressure to atmospheric pressure. In this case the following assumptions are made: two CSP pumps and two heat exchangers and 8 motor-operated valves, with a valve corresponding to each line. In the control system of the containment spray system, M1 to M4 and CSP A and B are opened on the receipt of a high containment pressure signal (injection phase) and M5 to M8 and CSP A and B are opened on the receipt of a low level water signal from the RWST (re-circulation phase). The GO-FLOW chart in the case of redundancy is shown in Fig. 13. In the GO-FLOW chart the final signals are 27, 35 and 54. These output signals give the output success probability. The operation of active components and the failure rate used in the case of two parallel lines and hot standby is given in Table 5.

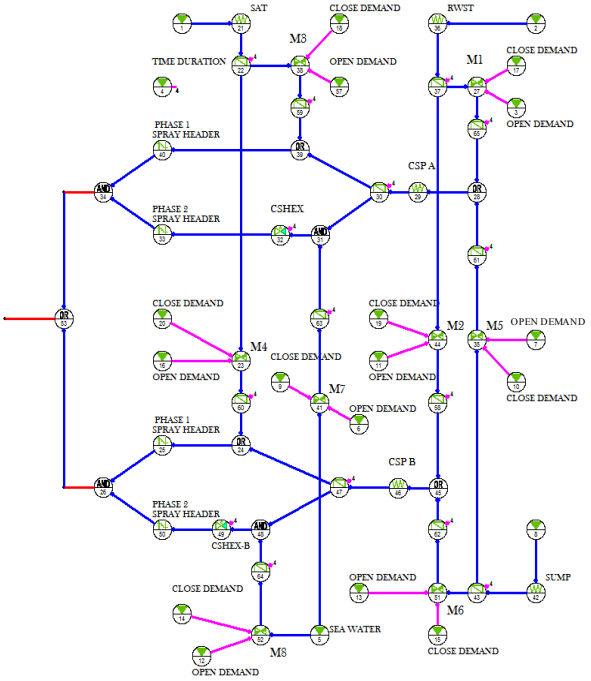

Fig. 13 GO-FLOW chart in case of two lines running simultaneously.

Table 5 Operation of active components and failure rate used in two parallel lines and hot standby case [12, 13]

Two parallel and hot standby case				
Valves	Phase 1	Phase 2	Failure probability(open or close action)	Failure during usage
M1 to M4	Open	Close	0.04/demand	1×10^{-5}/sec
M5 to M6	Close	Open	0.04/demand	1×10^{-5}/sec

5.3 Hot standby case (Case 3)

Hot standby is a redundant method of having one system running simultaneously with another identical system waiting in hot standby mode. Upon failure of the primary system, the hot standby system immediately takes over from the primary system.

The GO-FLOW chart is shown in Fig. 14 where two parallel lines are connected with each other. Each line has a containment spray pump. If the first line fails to supply coolant, the other pump runs. When one line is in use the other line is waiting in hot standby (if working line fails, then operation switches to the waiting line).

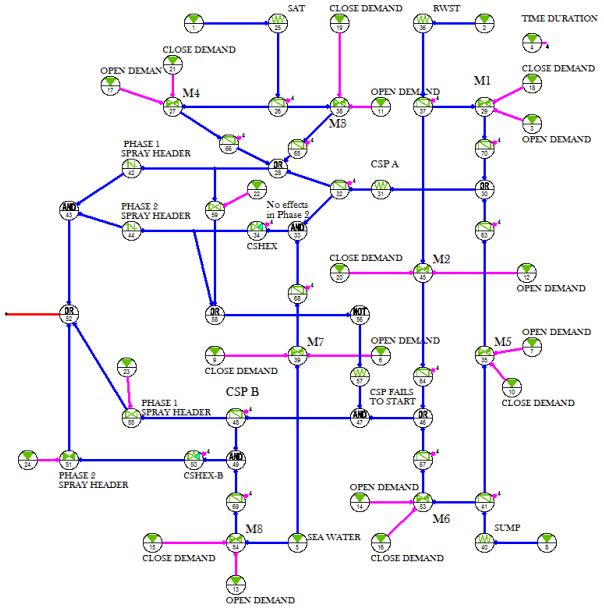

Fig. 14 GO-FLOW chart in hot standby case.

5.4 Inter-comparison of the three cases

The inter-comparison of the three Cases 1, 2 and 3 is shown in Fig. 15, for the calculated failure probability versus time. It shows that Case 1 is larger than that of Cases 2 and 3. The failure probability in case of hot standby (Case 3) gives the smallest value among the three cases. This result shows that the reliability increases with the adoption of redundancy in the design of a containment spray system. However, the above study to evaluate the dynamical reliability of containment spray system does not take into account the following two factors:

(i) what will be the method of changing from injection mode to recirculation mode, *i.e.*, whether by automatic

control or manual control, (ii) what will be the final time of dynamic reliability, *i.e.*, should it be until the time of the hot stand-by condition or until a stable cool-down state is maintained. The evaluation of the failure probability of change control should be elaborated to consider issue (i), while for issue (ii) the operator's procedures to reach the final stage in the recirculation phase should also be taken into account. Human operator's performance can be adequately modeled in the GO-FLOW framework but it requires detailed human action models and human reliability data. In this case the GO-FLOW chart may become much complicated.

Furthermore, if many different failure mechanisms for reliability evaluation are to be considered, then many different sets of statistical data of success probability or failure rate should be prepared, such as in Table 1, 2 and 3. Consider these factors, the resultant failure probability curve given by GO FLOW would be worse than those given in Fig. 15.
This indicates the importance of setting the proper failure data depending upon the problem under consideration in order maintain system reliability.

Further study should expand on the current work to conduct a sensitivity analysis, uncertainty analysis, and common mode failure analysis depending on the objective of reliability monitoring using GO-FLOW analysis.

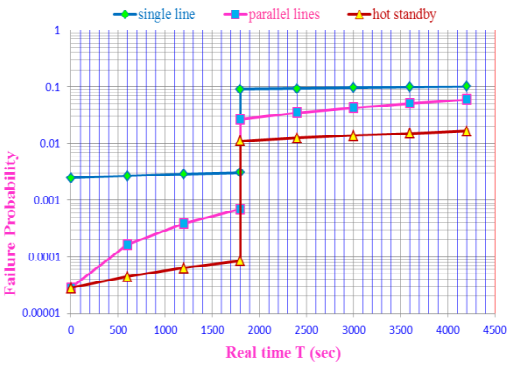

Fig. 15 Calculated failure rate versus time for Case 1, 2, and 3 where the x-axis indicates time in seconds and the y-axis is failure probability.

6 Concluding remarks

A reliability monitor has been developed for safety related subsystems in a PWR, by utilizing GO-FLOW. The discussion started with a definition of reliability monitoring and the explanation of the GO-FLOW methodology.

For the evaluation of dynamic reliability of safety related systems, an example was presented for the containment spray system of a PWR with application of the GO-FLOW methodology. This paper shows that the GO-FLOW methodology can be effectively used if sufficient failure data are given.

The above study to evaluate the dynamic reliability of a real containment spray system in a nuclear power plant does not give sufficient information due to the lack of sufficient failure data as the input parameters for the GO FLOW model.

Further preparation will be needed to conduct studies on common mode failure analysis and uncertainty analysis with the help of GO-FLOW, in order to conduct a practical evaluation of dynamic reliability of the containment spray system in a PWR.

Acknowledgments

This study was supported by the 111 project on Nuclear Power Safety and Simulation (b08047). The authors would like to express their great thanks for the valuable suggestions of Prof. Yoshikawa Hidekazu and Prof. Zhang Zhijian

Nomenclature

CCWS	Component of Cooling Water System
CPAS	Containment Pressure Activation System
CPS	Containment Pressure Sensor
CRS	Containment Recirculation Sump
CSHEX	Containment Spray water Heat EXchanger
CSIS	Containment Spray Injection System
CSP	Containment Spray Pump
CSS	Containment Spray System
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
IAEA	International Atomic Energy Agency
RBD	Reliability Block Diagram
RWST	Refueling Water Storage Tank
SAT	Spray Additive Tank
USNRC	United States Nuclear Regulatory Commission

References

[1] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS: IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries, New York, 1990

[2] IAEA: Reliability of Nuclear Power Plants: IAEA Proceedings Series, 1975.

[3] CHAUDRON, M. R. V.: Reliability Block Diagrams Anallysis and Tactics, Technische Universiteit Eindhoven System Architecture and Networking Group, www.win.tue.nl/~mchaudro/sa2007 (accessed 2012-04-01),2007.

[4] CLEMENS, P. L.: Fault Tree Analysis, 4th Edition, Fault-tree.net, May 1993.

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

[6] ROBIDOUX, R., XU, H., XING, L., and ZHOU, M.C.: Automated modeling of dynamic reliability block diagrams using colored Petri nets, IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans (SMC-A), 2010, 40(2): 337-351.

[7] YOSHIKAWA, H., YANG, M., HASHIM, M., LIND, M., and ZHANG, Z.: Design of risk monitor for nuclear reactor plants, International Journal of Nuclear Safety and Simulation, 2011,2(3): 266-274.

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

[9] MATSUOKA, T.: GO-GLOW methodology –Basic Concept and integrated analysis framework for its applications, International Journal of Nuclear Safety and Simulation, September 2010, 1(3): 198-206.

[10] JAPAN NUCLEAR ENERGY SAFETY ORGANIZATION (JNES): Outline of safety design (case of PWR): JNES Long term training course on Safety Regulation and safety Analysis inspection, 2005.

[11] U.S.NRC: Fault Trees, Appendix II to Reactor Safety Study(WASH-1400), NUREG -75/014, October 1975.

[12] U.S.NRC:Failure Data, Appendix III to Reactor safety Study(WASH-1400), NUREG -75/014, October 1975.

[13] IAEA: Survey of Ranges of Components Reliability data for use in probabilistic safety assessment, IAEA TECDOC-508, 1989.

[14] LA BAND, R. A., and ANDREWS, J D.: Phased mission modelling using fault tree analysis, Journal of Process Mechanical Engineering, 2004, 218(2):83-91.