Transition of the mission success probability under severe accident conditions: analysis by the GO-FLOW methodology and the consideration of uncertainty

MATSUOKA Takeshi[1,2]

1. College of Nuclear Science and Technology, Harbin Engineering University, Harbin, 150001, China

2. Center for Fundamental Education, Utsunomiya University, Utsunomiya City, Tochigi Prefecture, 321-8505, Japan (mats@cc.utsunomiya-u.ac.jp)

Abstract: In case of a nuclear power plant accident, the plant configuration drastically changes and required missions also change. The GO-FLOW is applied to estimate mission success probabilities of nuclear power plant system under severe accident conditions. A hypothetical sequence of accident conditions has been settled based on the Fukushima Daiichi accident. Effects of loop structures in nuclear power plant system and common cause failures are considered in reliability analysis. The situation of "phased mission problem" is considered for the operation change from reactor core isolation cooling system (RCIC) to high-pressure coolant injection (HPCI) and during the change of water sources from water tank to sea water for core injection by fire protection pump. Uncertainty analysis is performed and the results are expressed in graphical style with uncertainty ranges. It corresponds to a display window of risk monitor system, which visualizes risk state intuitively. Discussions are given for uncertainty ranges which are important information for judging the safety level of a system.

Keyword: uncertainty analysis; loop structure; phased mission problem; common cause failure; GO-FLOW

1 Introduction

In nuclear power plant accidents in general, and especially in severe accidents, the plant configuration drastically changes dynamically with the progression of accident. Subsequently required missions for safe operation of plant or prevention of escalation of accident will also change [1]. Event trees (ET) and fault trees (FT) are the basic analytical tools that have been most frequently used for probabilistic safety assessments (PSAs). However, in view of their limitation regarding the representation of timing of events and hardware/process/software/human interactions, several system analysis methods may need to be used in addition to, or in support of, ET/FT analyses. The need for more advanced methods of system reliability analysis has grown with the increased complexity of engineering systems in the society.

In this paper, the GO-FLOW methodology [2], which has been developed by the author, is applied to estimate mission success probabilities of a nuclear power plant system under severe accident conditions. Also, considerations are given for the phased mission problems, common cause failure effects, human factors, and loop structure conditions, which are often required in the analyses of complex system behavior.

A hypothetical sequence of accident conditions has been chosen based on the Fukushima Daiichi accident. Starting from a normal operation, the accident progresses by loss of offsite power (LOOP), station blackout (SBO), core cooling by emergency core cooling systems and to core cooling by sea water. Success probabilities of system operation, or prevention of core damage are quantitatively evaluated by the GO-FLOW methodology with uncertainty ranges.

The following conditions are considered in the analysis. Loop structures in nuclear power plant system. The situation of "phased mission problem" during the operation change from reactor core isolation cooling system (RCIC) to high-pressure coolant injection (HPCI) and in the change of water sources from water tank to sea water during core injection by fire protection pump. Common cause failures. It is pointed out the necessity of the estimation of human performance. Discussions are

Received date: October 20, 2016
(Revised date: December 7, 2016)

given that uncertainty ranges are important information for judging the safety level of a system.

2 Systems analyzed under accident conditions

Figure 1 shows a general layout of BWR system. Only essential parts are shown in Fig.1. The system has been also used in [3] for the evaluation of its dynamic behavior. It is seen there are five essential loop structures: main steam and feed water loop, electric power supply, component cooling water supply, steam extraction, and lubricating oil system.

In case of a station blackout, the mission of the plant is to keep the core cooled. The RCIC and HPCI are successively used for this purpose. The layout of these systems are shown in Figs. 2 and 3.

In the progress of plant condition, sometimes required mission and/or system will be changed, for example from power generation to core cooling in mission, from RCIC to HPCI in required system. In this case, if there exist commonly used components among both phases, the situation becomes phased mission problem and the dependency between two phases should be properly treated in reliability analyses.

From Figs. 2 and 3, we can see there are commonly used components for both systems. So the successive operation of two systems becomes a phased mission problem. Also, these two systems have common components with the power generation system of the BWR (Fig.1), including the main steam line, pressure vessel (reactor vessel) and feed water line, but failure rates of these components are very small. Therefore, it is not necessary to consider phased mission condition for the operational change from power generation to core cooling.

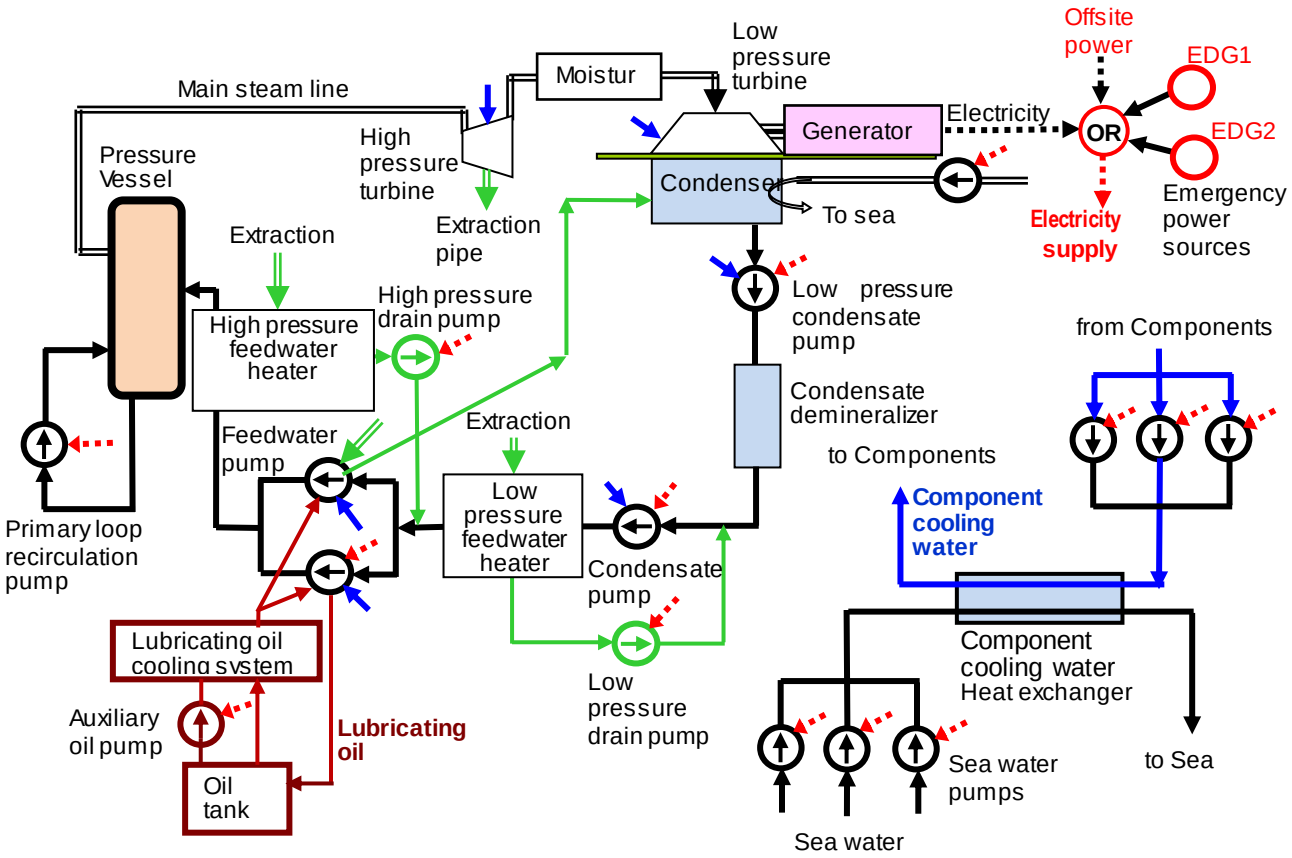

Fig.1 General layout of BWR nuclear power plant.

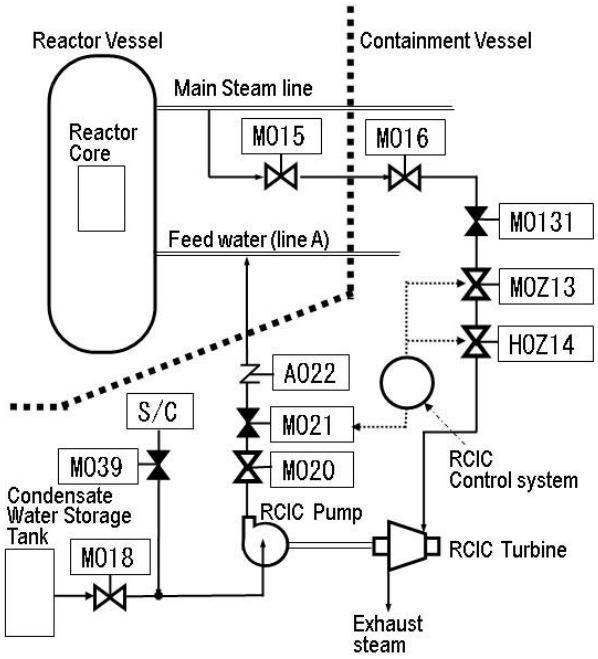

Fig. 2 Reactor core isolation cooling system (RCIC) of Fukushima-Daiichi units 2&3.

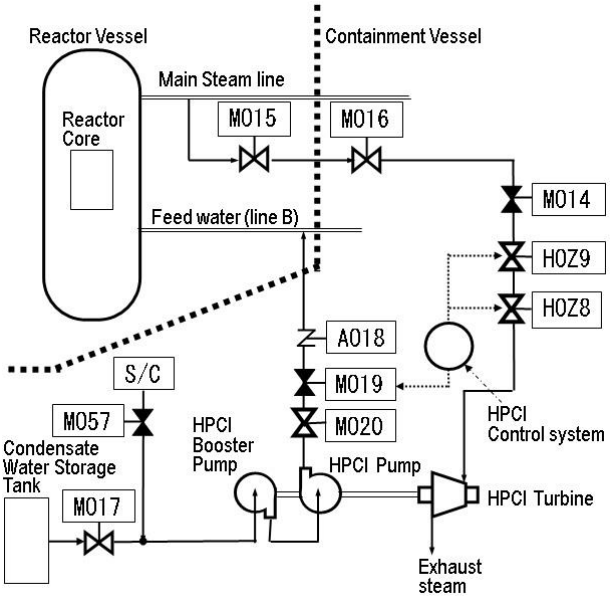

Fig. 3 High pressure coolant injection system (HPCI) of Fukushima-Daiichi units 1,2,3.

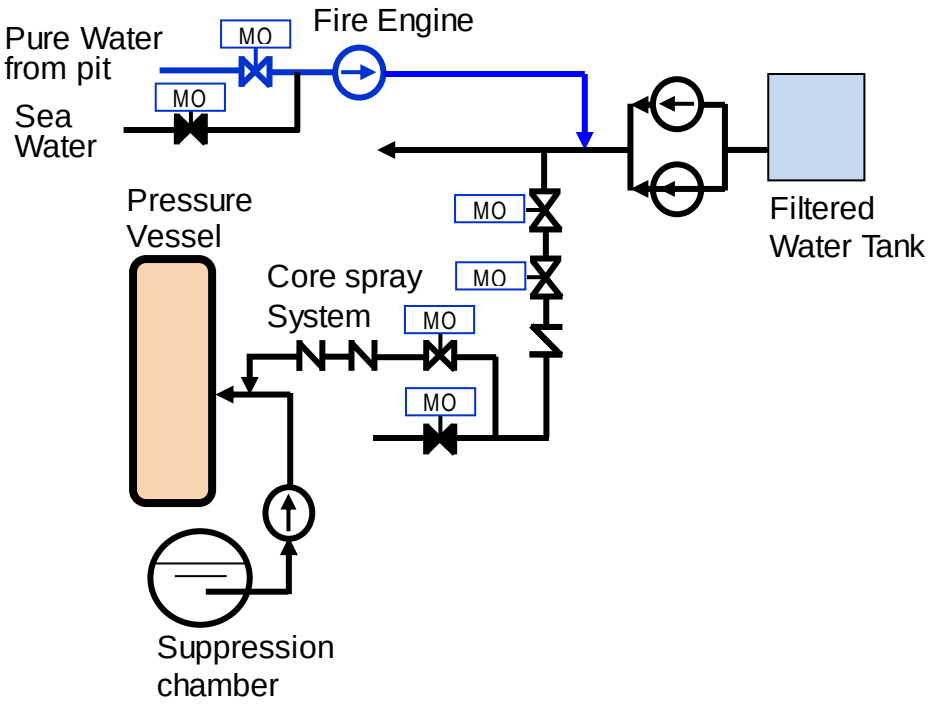

Fig.4 Water injection by fire engine.

After the failure of RCIC and HPCI, fire engine is brought and fire protection pump is used for injection of pure or sea water. The system layout is shown in Fig. 4, which was the actual system layout at the Fukushima Daiichi accident [4].

3 A hypothetical sequence of accident

The following accident sequence is assumed:
Initially, the BWR is in a normal operating state. At a certain point in time, offsite power is lost, but power generation is maintained with the start of emergency

diesel generators (EDGs). Next, one of two emergency generators fails, but power generation is still maintained. Finally, the second generator also fails, but power generation is continued with loop structured condition as shown in Fig. 1.

In the actual operating procedure of the BWR, the operation is immediately stopped if offsite power is lost. But, in this hypothetical sequence, we can see how the nuclear power plant is reliable even in the degraded conditions.

In the next stage, reactor is shut down. There is no AC power source, *i.e.*, plant is placed in SBO condition. The mission of the plant has now changed from power generation to core cooling. The RCIC and HPCI are successively used for core cooling. A small amount of DC power is available for the operation of motor operated valves. The HPCI is designed to inject large amount of coolant, so the reactor pressure rapidly decreases after the start of HPCI. Power of the turbine driven pump (HPCI pump in Fig.3) also rapidly decreases and HPCI cannot continue the injection of coolant for long time. In the accident of Fukushima Daiichi Unit 3, pressure of the reactor vessel decreased under 2MPa about 5hours after the start of HPCI.

After the failure of both systems (RCIC and HPCI), a fire protection pump is connected to the primary cooling system, and the core is cooled by the water from pure water tank on the plant site. The fire pump is driven by diesel generator brought by a car. After the pure water tank is exhausted, the core is cooled by sea water, until external power supply is recovered.

This accident sequence is illustrated in the Fig. 5. Horizontal lines indicate sub systems are in operating conditions. White circles mean the starts of active components.

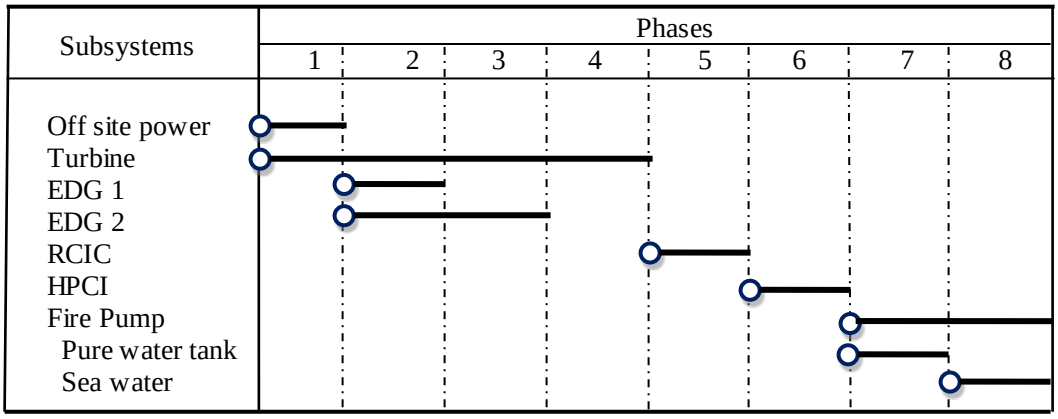

Fig.5 Accident sequence.

4 Failure data

Failure rates of components are assigned as follows based on the data shown in the standard for procedures of Level 1 PSA [5] and component reliability data collected by the International Atomic Energy Agency (IAEA) [6].

Uncertainty ranges for failure rates are estimated based on the error factors given in the Reactor Safety Study [7]. The ranges are assigned as shown in the next lists.

Table 1 Error rates and uncertainty ranges (error factors)

Failure modes	failure rates	Uncertainty ranges (error factors)
Motor/Air operated valve		
failure of open/close action	3.6x10-3/D	3
failure during usage	2.0x10-7/hour	3
failure during standby	2.0x10-8/hour	3
Pump		
fails to start	2.7x10-2/D	3
failure during operation	1.0x10-4/hour	10
Emergency diesel generator		
fails to start	1.0x10-2/D	3
failure during operation	3.0x10-3/hour	10
Fire engine		
Fails to connect	1.4x10-2/D /	10
Fire pump		
fails to start	2.7x10-2/D	3
failure during operation	1.0x10-4/hour	10

Turbine		
fails to start	2.7x10-2/D	3
failure during operation	1.0x10-4/hour	10
Condensate water storage tank		
failure during operation	2.8x10-8/hour	30

5 Procedure for solving a system with loop structures

For a system which has logical loop structure(s), the Boolean relations have to be described with unknown variable(s) "x" as shown in equation (1).

$$x = f(\alpha_1, \cdots, \alpha_n)x + g(\alpha_1, \cdots, \alpha_n) \ . \qquad (1)$$

where α_i be independent Boolean variables (fixed elements of a Boolean algebra). The right hand side is divided into two parts, Boolean algebraic terms including unknown variables x ($f(\alpha_i)x$) and terms without x ($g(\alpha_i)$).

If we try to solve the above equation, we encounter infinite circulation of the unknown variable(s). Logical loop was not generally solved in terms of the arithmetic operators of Boolean algebra. The solution of equation (1) becomes:

$$x = mf(\alpha_1, \cdot\cdot, \alpha_n) + g(\alpha_1, \cdot, \alpha_n). \qquad (2)$$

The unknown element "x" can be expressed by "α_i" and "m" without "x". Where "m" is an indefinite arbitrary element. It has been shown by the author that basically, a loop structure can be solved [8]. An indefinite arbitrary element m is determined by the operating condition of each specific system.

6 Analysis conditions and modeling

6.1 BWR power generation -Loop structured system and CCF-

The GO-FLOW chart for the BWR under consideration is constructed as shown in Fig. 6. The procedure described in Sections 5 was used to resolve the loop structures in the GO-FLOW analysis. The system contains many components and the effect of CCF is expected to be notable. The β-factor method was used for the estimation of the contribution from the CCF of motor operated valves (MOVs) [9]. The GO-FLOW chart does not need to explicitly express the CCF relations [10]. The data used for the CCF analysis are given in Table 2.

Table 2 β–factors for the MOVs in Fig.1.

MOV group	MOV Location (Operator number)	β
1	46,48	0.3
2	20,22	0.3
3	31,39,40	0.3
4	35,37,38	0.3

Uncertainty ranges of mission success probabilities are important information for operators to correspond to accident situation. Uncertainties are produced by failure data distribution, analysis model uncertainty, lack of knowledge and so on.

In the present analysis, uncertainty of failure data distribution is considered. The reactor safety study [7] gives uncertainty ranges as error factors for main components in nuclear power plant. The failure data in Fig. 1 are combined with the error factors and distribution types are assumed by the author. The resultant data used for the uncertainty analysis are given as shown in Table 3.

Table 3 Uncertainty data in Fig.6.

Operator number	Operator Type	Distribution type	μ *Upper bound*	*EF Lower bound*
23	35	Log-normal	1E-8	30
27	35	Log-normal	2.8E-8	10
30	35	Log-normal	2.8E-8	10
44	35	Log-normal	1E-6	3
14	35	Log-normal	1E-4	10
46	35	Log-normal	3E-3	10
48	35	Log-normal	3E-3	10
45	39	Homogeneous	0.9967	0.97
47	39	Homogeneous	0.9967	0.97

In the above table, operator type 35, 39 mean "Failure during operation" and "Opening and closing action", respectively. "μ" and "EF" are median and error factor, respectively. "Lower bound" and "upper bound" are given for Homogeneous distributions.

6.2 Core cooling by RCIC and HPCI -double loop structured system-

It is assumed that the pressure of the pressure vessel decreases under 2MPa about 5hours after the start of HPCI. The HPCI and RCIC have loop structures. The analyses are also performed by using the method described in Section 5 to solve loop structure.

GO-FLOW charts are constructed as shown in Fig. 7 for RCIC and HPCI system. The RCIC and HPCI can be considered as one system with double loop structure, and the chart includes both the RCIC part and HPCI part. The data used for the uncertainty analysis are given in Table 4, which are settled in the same way to Table 3. The CCF is not considered in this case, because components number is not so large and the effects of CCF is expected not notable.

Table 4 Uncertainty data in Fig.7.

Operator number	Operator Type	Distribution type	μ	*EF*
16	35	Log-normal	1E-4	3
18	35	Log-normal	1E-4	3
32	35	Log-normal	1E-4	3
34	35	Log-normal	1E-4	3
42	35	Log-normal	1E-4	3

6.3 Core injection by fire pump -common cause failure-

Core injection by fire pump is started in the late stage of accident progression. Temperature and pressure in the containment vessel may abnormally increase because of insufficient cooling. Then, many components will suffer severe conditions and CCFs will be notable. It is assumed that all the MOVs suffer CCFs. The β-factor method is also used for the estimation of the contribution from CCF. GO-FLOW chart is constructed as shown in Fig. 8. Data used for the CCF of MOVs are shown in Table 5.

Table 5 β–factors for the MOVs in Fig.8.

MOV group	MOV Location (Operator number)	β
1	13,30	0.3
2	21,24,25,26	0.3
3	12,27,29	0.3

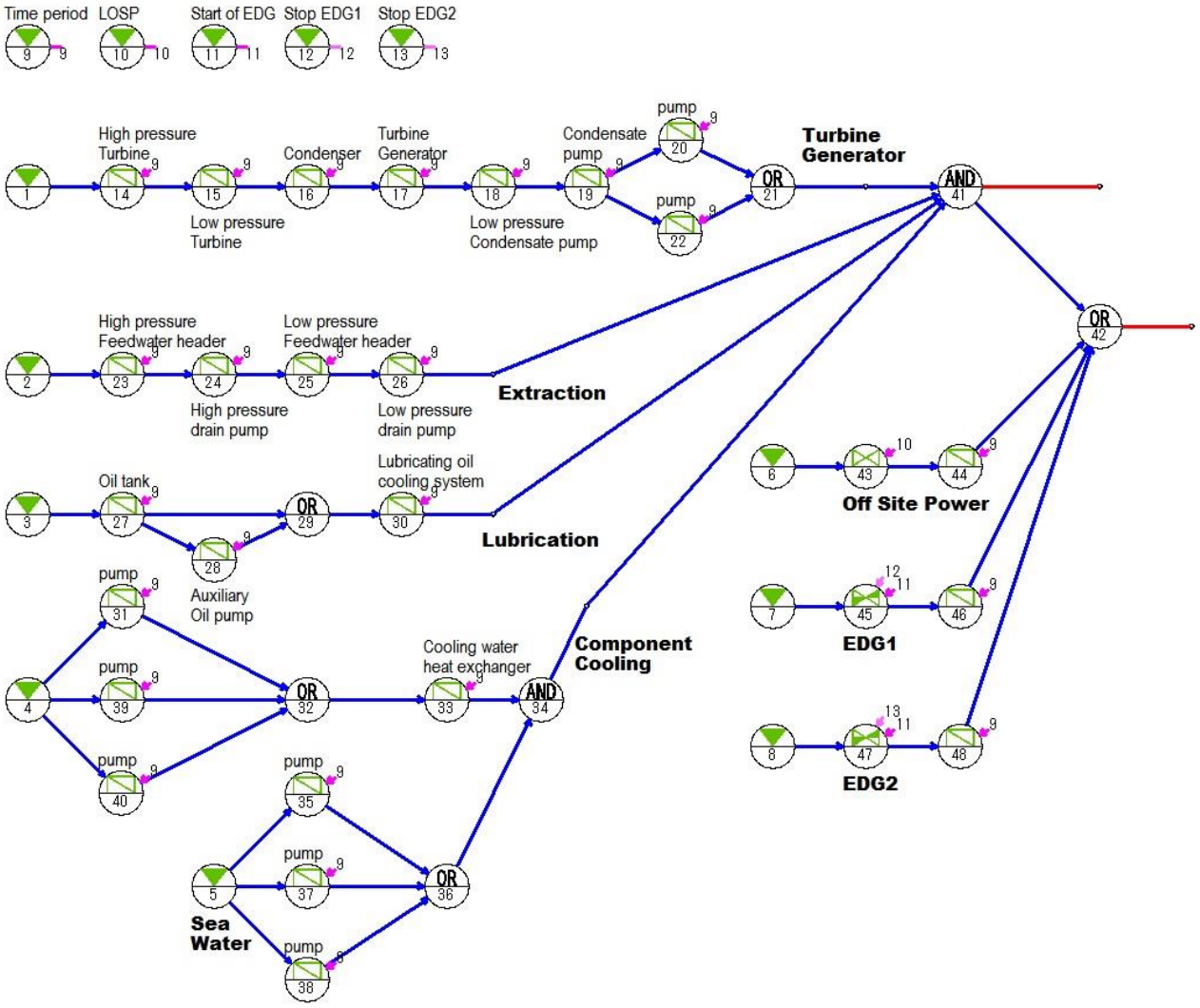

Fig.6 GO-FLOW chart for general layout of BWR nuclear power plant.

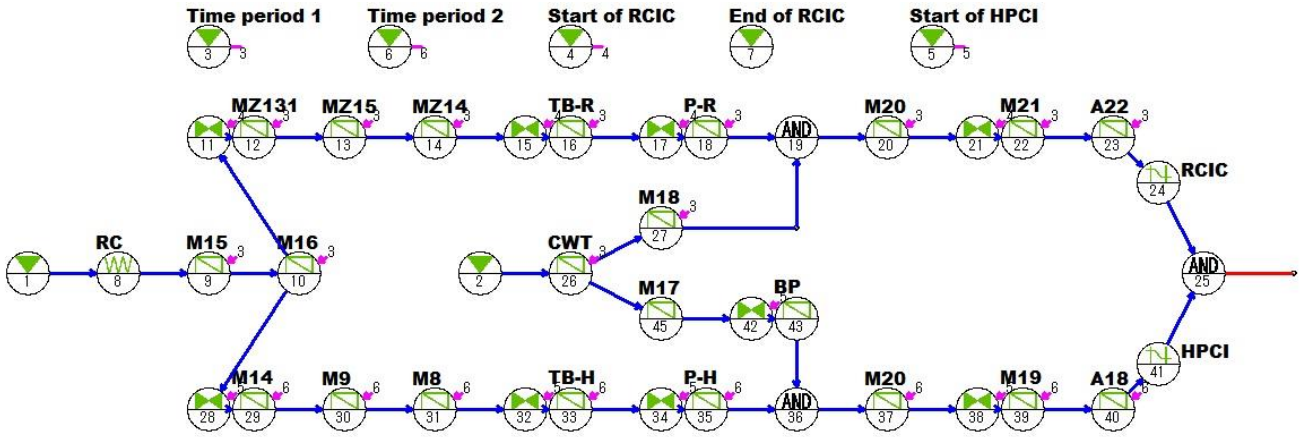

Fig. 7 GO-FLOW chart for the RCIC and HPCI.

The data used for the uncertainty analysis are given in Table 6, which are settled in the same way to Table 3.

Table 6 Uncertainty data in Fig.8.

Operator number	Operator Type	Distribution type	μ *Upper bound*	*EF Lower bound*
17	26	Homogeneous	0.991	0.919
16	26	Homogeneous	0.9986	0.86
28	26	Homogeneous	0.9988	0.9892
30	26	Homogeneous	0.9988	0.9892
12	35	Log-normal	1E-8	30
14	35	Log-normal	2E-7	3
31	35	Log-normal	2E-7	3
18	35	Log-normal	1E-4	10
20	37	Log-normal	2E-8	3
21	37	Log-normal	2E-8	3
22	37	Log-normal	2E-8	3
24	37	Log-normal	2E-8	3
25	37	Log-normal	2E-8	3
26	37	Log-normal	2E-8	3
27	37	Log-normal	2E-8	3
13	39	Homogeneous	0.9988	0.9892

In the above table, operator type 26, 37 mean "Normally closed valve" and "Failure of valve in open state", respectively.

6.4 Consideration of human performance

The emergency procedures at Fukishima Daiichi nuclear power plant did not clearly describe the ventilation of containment vessel without electricity and core injection by fire protection pump in case of severe accident. Accomplishment of these objectives required ad hoc and flexible actions. In that respect, success probabilities of these actions are strongly dependent on human factors.

Evaluation of human performance is an important issue for the safety analysis of engineering systems, because errors directly lead to malfunction or failure of the systems. To evaluate human error probability is a difficult task. Even for a simple action, human failure probability changes in a wide range depending on person's characteristics, surrounding working conditions, relation to other tasks, among a number of other factors.

Failure probabilities of components for water injection by fire pump include human factors. For example, for events such as "Fire engine fails to connect", or "MOV failure of open/close action" strongly depend on human performance. However, in Sections from 6.1 through 6.3, influence of severe and emergency accident conditions to human performance are not explicitly considered.

There is an attempt [11] to estimate human performance by a simplified Step Ladder model and the GO-FLOW framework. With the aid of this technique, it will be possible to estimate the uncertainty and degradation of success probability of the core injection by fire pump due to human factors. To obtain a specific value of the influence by human performance is future work with the support of more definite data.

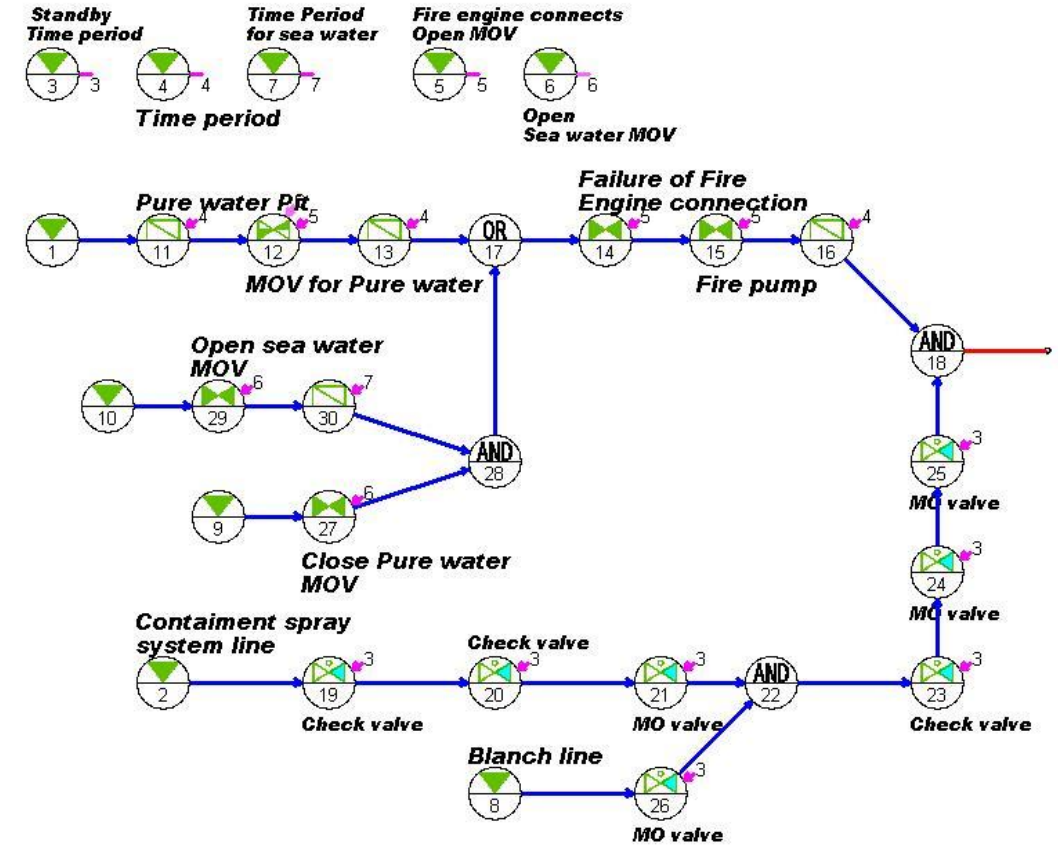

Fig.8 GO-FLOW chart for water injection by fire engine.

7 Results of the analyses

Analysis results are shown in Fig. 9. Uncertainty ranges of 95% upper bound and 5% lower bound are indicated by dotted lines with same color for each operational mode. From time 0 hour to 80 hours, the reactor is operated as normal, that is, continues to generate electricity. After 80 hours, the reactor is shut down and the main purpose becomes to cool the reactor core. The missions have been changed.

During the generation of electricity, the effect of CCF is seen as 11% to 35% increase in mission failure probability. In Fig. 9, the resultant value is indicated and baseline is not given in order to avoid complexity. There are very small uncertainty of the reliability of power generation by three redundant systems, that is, two EDGs and turbine generator (till 40 hours). If one EDG fails, uncertainty range becomes large. Turbine generator has very large uncertainty ranges. This means power generation cannot be relied on only one turbine generator.

Success probabilities discontinuously change when operational condition changes. At 80 hours, large increase of success probability is seen but at this point the mission is also changed from power generation to reactor core cooling. The reactor core cooling can be performed by relatively simple system configurations. Therefore it is not meaningful to make a comparison of the success probabilities before and after the 80 hours. There are very small uncertainty of core cooling by RCIC and HPCI, two redundant systems. Safety of the reactor is assured in this stage.

After the RCIC stops (100hours), the success probability drastically decreases, and uncertainty range also becomes large. This is because of the loss of redundancy of two cooling systems. We cannot much expect for cooling by HPCI. And, HPCI cannot continue effective cooling for long time, because of reactor vessel's pressure drop. This situation is indicated by dotted line around 105 to 120 hours in Fig.9. It is better to change to water injection by the fire pump, as soon as possible.

The water injection is started at 105 hours together with the HPCI operation. The contribution from CCF is estimated as the 2% decrease of failure probability from the results without CCF. This system is simple and almost the series structure. In the -factor model, total failure rate is divided into CCF and independent failure parts. Reduced value is attributed to the decrease in the independent failure rate. Then total system failure probability becomes small compared to a case without CCFs for series structure system.

The reason of the success probability of water injection is larger than that of HPCI is due to the simplicity of the system. However, water injection by the fire engine is an emergency and temporal measure and its functionality is limited. Thus a simple comparison may lead to misinterpretations. Uncertainty ranges gradually increase with time elapse. Only one system is available at this stage. We have to wait the recovery of external electric source.

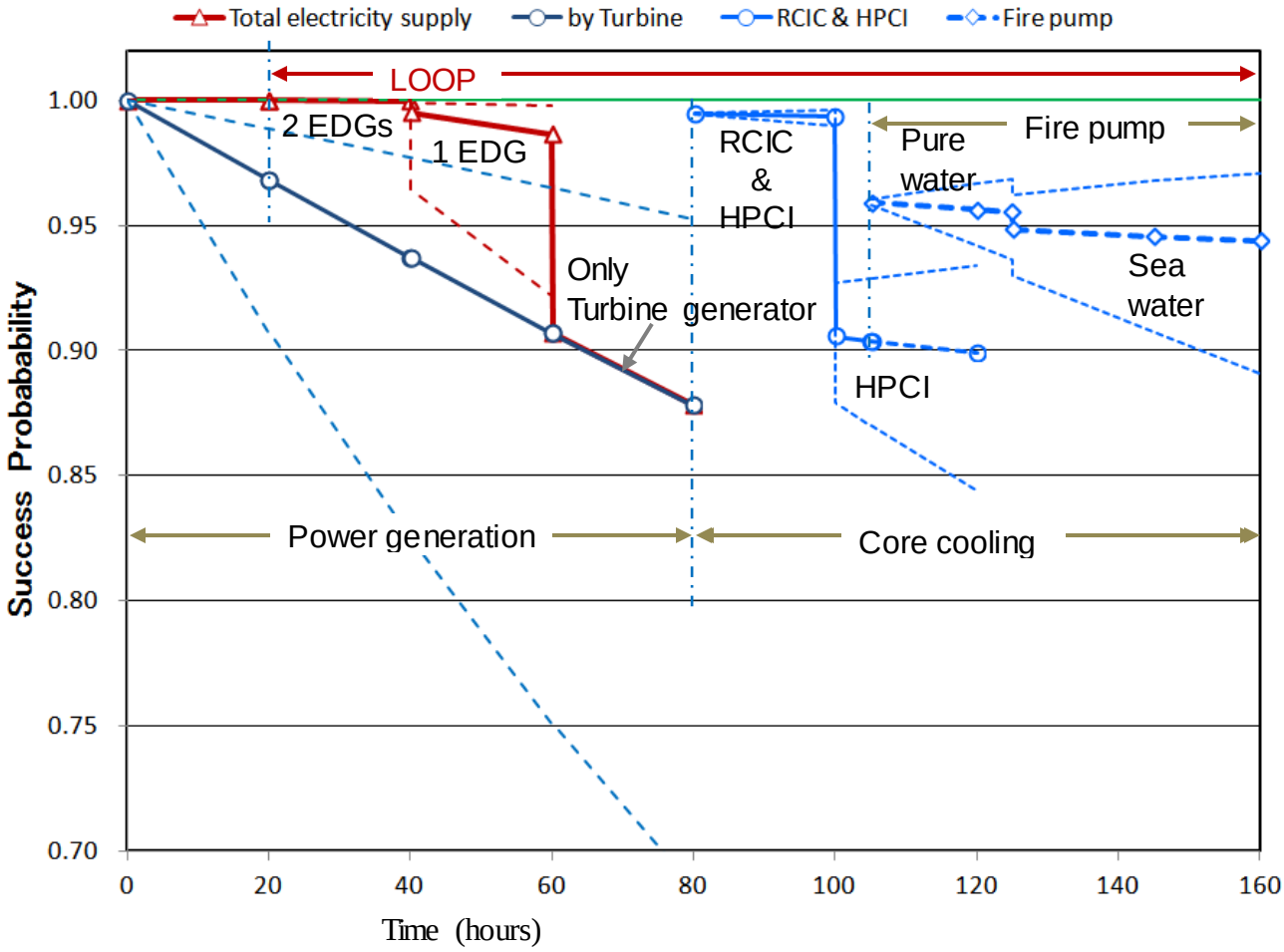

Fig.9 Analysis results.

8 Conclusions

Mission success probability of nuclear power plant system has been evaluated under accident conditions with the consideration of uncertainty. Analyses have been made by the GO-FLOW methodology, which is utilized as key technology to the research activity on going at Harbin Engineering University (HEU) [12].

A hypothetical sequence of accident conditions has been settled based on the Fukushima Daiichi accident. Mission success probabilities have been obtained with the growth of accident.

Success probability of system operation, reliability or availability are obtained with some boundary conditions, such as LOOP condition, unavailable equipment, possible resources, and so on. Furthermore, the mission as “power generation” or “core cooling” changes on a progression of accident.

The analysis results as shown in Fig. 9 could be utilized for visualizing risk state intuitively in "risk monitor" system. In this case, boundary conditions of the analysis should be properly presented to persons who are observing risk monitor. A value itself without analysis or boundary conditions would sometimes make misreading.

Uncertainty ranges of mission success probabilities are important information for operators to correspond to accident situation as shown in this example analysis. Estimation of uncertainty [13] needs to be shown in "risk monitor" system.

The present analyses have shown that mission success probabilities with uncertainty ranges of nuclear power plant will be easily obtained by the GO-FLOW methodology with the growth of accident.

References

[1] MATSUOKA, T.: Estimation of dynamic behavior of nuclear power plant system state under severe accident conditions, International Journal of Nuclear Safety and Simulation, 2014, 5(3):197-204.]

[2] 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.

[3] MATSUOKA, T.: Evaluation of plant operational states with the consideration of loop structures under accident conditions, Nuclear Engineering and Technology, 2015, 47(2):157-164.

[4] Prime minister of Japan and his cabinet: Report of Japanese Government to the IAEA Ministerial Conference on Nuclear Safety - The Accident at TEPCO's Fukushima Nuclear Power Stations –, June 18, 2011.

[5] Japan atomic energy society: A standard for Procedures of Probabilistic Safety Assessment of Nuclear Power Plants during Power Operation 2008(Level 1 PSA): (AESJ-SC-P008:2008).

[6] IAEA: Survey of ranges of Component reliability data for use in probabilistic safety assessment, IAEA-TECDOC-508, 1989.

[7] U. S. NUCLEAR REGULATORY COMMISSION: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400, NUREG-75/014, 1975.

[8] MATSUOKA, T.; Generalized Method for Solving Logical Loops in Reliability Analysis. In: Proceedings of PSAM-11, Helsinki, Finland, June 25-29, 2012.

[9] MOSLEH, A.: Procedures for analysis of common-cause failures in Probabilistic Safety Analysis, NUREG: CR-5801 SAND91-7087 RG, 4. 1993

[10] MATSUOKA, T., and KOBAYASHI, M.: The GO-FLOW reliability analysis methodology—analysis of common cause failures with uncertainty, Nucl. Eng. Des., 1997,175: 205–214.

[11] MATSUOKA, T., and KATO,Y.: Modeling of a Human Performance by the GO-FLOW Methodology. In: First International Symposium on Socially and Technically Symbiotic Systems, Okayama, August 29-31, 2012.

[12] 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.

[13] HASHIM, M., YOSHIKAWA, H., MATSUOKA, T., and YANG, M.: Considerations of uncertainties in evaluating dynamic reliability by GO-FLOW methodology - example study of reliability monitor for PWR safety system in the risk-monitor system, Journal of Nuclear Science and Technology, 2013, 50(7): 695-708.