# Display of Dynamical Behaviour of Nuclear Power Plant States in Risk Monitor System - Use of the GO-FLOW Methodology and Interactive Update -

Takeshi MATSUOKA

*Collaboration Centre for Research and Development, Utsunomiya University, Japan.*
*E-mail: mats@cc.utsunomiya-u.ac.jp*

It is shown how to use the GO-FLOW methodology in "Risk Monitor" system. Operator, faced to risk monitor, gives plant conditions and obtains present plant risk state, interactively. For this purpose, the GO-FLOW analysis can be performed flexibly correspond to the change of plant configuration and required mission. The GO-FLOW framework can automatically give graphical style of analysis results. It corresponds to a display window of risk monitor system, which visualizes risk state intuitively. In this study, take up a BWR nuclear power plant and consider a hypothetical sequence of accident conditions based on the Fukushima Daiichi accident. The applicability of GO-FLOW to risk monitor system has been shown.

*Keywords*: Dynamical behaviour, Risk monitor, GO-FLOW, Nuclear power plant, Fukushima Dai-ichi accident, Mission success probability.

## 1. Introduction

In nuclear power plant accidents, especially in severe accidents, the plant configuration drastically changes with the progression of accident. Consequently, required missions for safe operation of plant or prevention of escalation of accident will also change; Matsuoka (2016). The GO-FLOW methodology; Matsuoka et al. (1988) can estimate mission success probabilities of nuclear power plant system under severe accident conditions.

For safe operation or prevention of accidents, plant operators must instantaneously comprehend the plant state, and the operator use it in support of operational decisions. This paper shows how to use the GO-FLOW methodology in "Risk Monitor" system.

The Risk Monitor model is based on, and is consistent with, the Living PSA. The real-time analysis is based on the actual plant configuration which dynamically changes in accordance with accidents. It is important to show the prediction of mission success probability in future from the present plant state, with several plant conditions supposed to be occurred.

Operator, faced to risk monitor, gives plant conditions and obtains present and future plant risk state, interactively. For this purpose, the GO-FLOW analysis is performed flexibly correspond to the change of plant configuration and required mission. The GO-FLOW framework can automatically give graphical style of analysis results; Matsuoka (2018). It corresponds to a display window of risk monitor system, which visualizes risk state intuitively.

In the present study, take up a BWR nuclear power plant and consider a hypothetical sequence of accident conditions based on the Fukushima Daiichi accident. Starting from a normal operation, the accident progresses by loss of offsite power (LOOP), station blackout (SBO).

When analysis results are shown in risk monitor, boundary conditions of the analysis should be properly presented to operators who are observing risk monitor. A value itself without analysis conditions or boundary conditions would sometimes make misreading. And, uncertainty ranges of analysis results; Matsuoka (2016) needs to be shown in "risk monitor" system, as it is important for decision making.

## 2. Risk Monitor

### 2.1 *Risk Monitor System*

The term risk monitor has been defined by International Atomic Energy Agency (1999) as "a plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components". At any given time, the risk monitor reflects the current plant configuration in terms of the known status of the various systems and/or components.

The Risk-Monitor is based on, and is consistent with, the Living PSA. It is updated with the same frequency as the Living PSA. The risk monitor is used by the plant operators in support of operational decisions.

Real-time analysis is based on the actual plant configuration which dynamically changes in accordance with accidents. The first risk monitor (ESSM) was developed at Heysham 2 in 1988; Holloway (1994). Now there are many risk monitors at various power plants. One example of

*Proceedings of the 30th European Safety and Reliability Conference and*
*the 15th Probabilistic Safety Assessment and Management Conference*
*Edited by* Piero Baraldi, Francesco Di Maio and Enrico Zio
*Published by* Research Publishing, Singapore.
ISBN/DOI: TBA

risk monitor system is developing at Harbin Engineering University; Hashim et al. (2015)

We consider that the range of risk is not limited in core-damage accident but includes all kinds of dangerous states brought by abnormality of plant state. Failure of a required mission during a plant operation leads sometimes to an accident. It is important to show the prediction of mission success probability in future from the present plant state, with several plant conditions supposed to be occurred.

Aside from system availability, prediction of coolant inventory trend, or radiation level at various point around the plant are important information for the operators watching risk monitor.

### 2.2 *Reliability Analysis for Risk Monitor*

In the analysis of dynamically changing complex plant system, the following items are important. They are also required for developing risk monitor system.

Common cause failure. If one accident or single phenomenon affects many components at the same time in redundant and large complex system, the common cause failure must be adequately treated in reliability analysis; Matsuoka et al. (1997).

Phased mission problem. In the progress of accident, required missions change subsequently, so the situation of "phased mission problem" must be also properly treated.

Dependencies between Systems. The dependencies between multiple systems, which are produced by the existence of commonly used components between systems, are also properly considered.

Effects of loop structures. In large complex system, there are sometimes loop structured configuration which supports each other for establishing self-sustained function. It is also needed to consider the effects of loop structures in reliability analysis; Matsuoka (2012).

Uncertainty. Information about the range of uncertainty is important for adequately understanding the analysis results; Matsuoka (2016).

### 2.3 *Necessary Function in Risk Monitor*

We consider the following function is important for risk monitor which shows us dynamical behaviour of plant states.

Operator, faced to risk monitor, gives plant conditions and obtains present plant risk state, interactively. For this purpose, the GO-FLOW analysis has to be performed flexibly correspond to the change of plant configuration and required mission.

Updated analysis result is automatically given in graphical style as a display window of risk monitor system, which visualizes risk state intuitively.

## 3. GO-FLOW methodology

In the present study, mission success probabilities are calculated by the GO-FLOW methodology. So, brief explanations about the GO-FLOW is given in this section.

The GO-FLOW methodology is a reliability analysis methodology, which has been developed by authors; Matsuoka et al. (1988). It is success-oriented system analysis technique and is capable of evaluating system reliability and availability. The modelling technique produces a chart which consists of signal lines and operators and represents engineering function of the components/subsystems/system. The operators (functional elements in GO-FLOW) model function or failure of the physical equipment, and also represent logical gates, signal generators.

Fourteen different types of GO-FLOW operators are currently defined as shown in Fig. 1. Their probability calculation formulas are provided in reference; Matsuoka et al. (1988). The output signal may connect to another operator as its input. Specific probabilities (point estimates) of component operations or failure are given as input data.

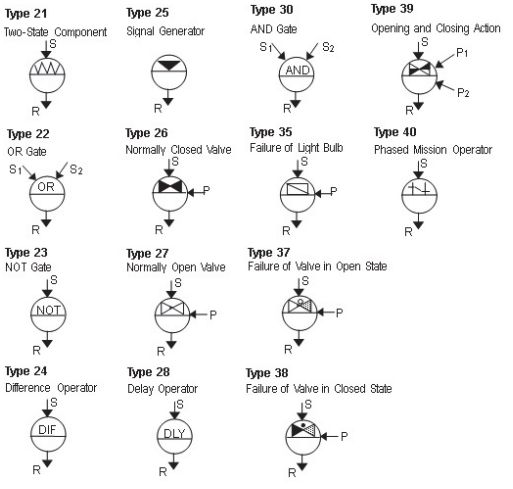


Fig. 1. GO-FLOW operators.

Signals represent some physical quantity or information. The existence of a signal means the existence of a physical quantity or information. In the GO-FLOW methodology, the existence of a signal is interpreted as both the actual and the potential existence of a signal. “Potential

existence" means that a signal exists when all the resistances of downstream are removed.

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

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

First step of the analysis is to construct a GO-FLOW chart, which is a modelling of an engineering system. An analyst interactively constructs a chart on a PC display with the support of the GO-FLOW chart editor as shown in Fig. 2. During the construction of a chart, component failure data and analysis conditions are assigned in a chart.

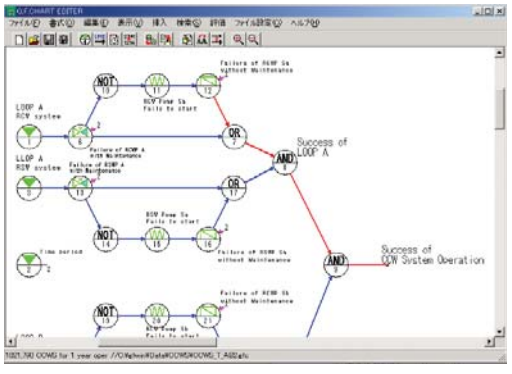


Fig. 2. GO-FLOW Chart Editor.

An analysis is performed from the upstream to the downstream signal lines. In most cases, only one, or at most few of all the defined signals are of interest; these signal lines are termed as final signals. An analysis is completed when the intensities of these final signals at all the time points are obtained.

The GO-FLOW methodology possesses the following significant features: (a) The GO-FLOW chart corresponds to the physical layout of the system and is easy to construct and validate, (b) alternations and updates to a GO-FLOW chart are readily accomplished, and (c) GO-FLOW contains all the possible system operational states. And GO-FLOW methodology can perform following functions such as: (1) analysis of phased mission problem, (2) aging and maintenance effects, (3) identification of minimal cut sets, and parametric studies of (4) common cause failure analysis, (5) uncertainty analysis, and (6) sensitivity analysis.

## 4. Systems Analysed under accident conditions

In the present study, a general layout of BWR system is taken up. 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. The detailed figure is seen in the previous study; Matsuoka (2016).

In case of a station blackout, the mission becomes to keep the core cooled. Reactor Core Isolation Cooling system (RCIC) and High Pressure Coolant Injection (HPCI) are successively used for this purpose. After the failure of RCIC and HPCI, fire engine is brought, and fire protection pump is used for injection of pure or sea water in order to cool the reactor core. The system layout for these systems are also shown in figures of the previous study.

### 4.1 *A Hypothetical Accident Sequence*

The following accident sequence is assumed based on the Fukushima Daiichi accident. 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 (by turbine generator).

In the actual operating procedure of 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) 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 Table 1. Horizontal lines indicate sub systems are in operating conditions. White circles mean the starts of active components.

Table 1. Operational condition of subsystems.

| Subsystems | Phases | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Off Site Power | | | | | | | | |
| Turbine | | | | | | | | |
| EDG 1 | | | | | | | | |
| EDG 2 | | | | | | | | |
| RCIC | | | | | | | | |
| HPCI | | | | | | | | |
| Fire Pump | | | | | | | | |
| Pure Water | | | | | | | | |
| Sea Water | | | | | | | | |

### 4.2 *Failure Data*

Failure rates of components are assigned based on the data shown in the standard for procedures of Level 1 PSA; Japan atomic energy society (2008) and component reliability data collected by the International Atomic Energy Agency (1989).

Uncertainty ranges for failure rates are estimated based on the error factors given in the Reactor Safety Study; U.S.NRC (1975).

## 5. GO-FLOW modelling

A hypothetical accident sequence is expressed by GO-FLOW modelling, in which change of required mission, available systems/components are specified with the passage of time. There are four systems, BWR main part, HPCI, RCIC and water injection by fire engine system. In the previous study, GO-FLOW charts are separately constructed for these systems.

In the present study, one big GO-FLOW chart is constructed, which includes all related systems. With this big GO-FLOW chart, we can obtain "mission success probabilities" by one computer run, along with the change of required mission in the passage of time.

If we need to evaluate different accident sequence or condition, basically we must make recalculation by different GO-FLOW model. But in the present big GO-FLOW chart, change of required subsystem and timing are easily reflected to analysis without changing GO-FLOW chart configuration, just by changing parameter values. Fig. 3 shows a part of input data for GO-FLOW analysis program.

This part defines the signals which control start and stop of the operations of EDG, pump, HPCI, RCIC and so on, at specific time. With the change of these parameter values, we can obtain different accident sequence. If there is no start signal for some specific system, this system is not used in a certain accident sequence.

```
 9
0.000E+00 0.000E+00 0.000E+00 0.000E+00 1.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
 10
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 1.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
 11
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 1.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
 12
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 1.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
 13
1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00
1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00
1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00
1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00 1.000E+00
 14
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 1.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
 15
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 1.000E+00 0.000E+00
0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00 0.000E+00
 16
```

Fig. 3. Input data for GO-FLOW analysis program.

## 6. Analysis Results

### 6.1 *Base case*

Following accident sequence is set for the base case.

1. Loss of offsite power (LOOP) happens at 20 hours, and EDG1 & 2 start immediately after the LOOP.
2. EDG1 stops at 40 hours and EDG2 stops at 60 hours.
3. Turbine generator makes electricity till 80 hours.
4. RCIC starts and HPCI is placed as backup.
5. RCIC stops at 100 hours and HPCI is used for 10 hours.
6. Fire engine is connected at 110 hours, and start the injection of pure water.
7. Water source is changed to sea water at 125 hours.

Mission success probabilities are obtained by a single calculation of big GO-FLOW chart. The result is shown in Fig. 4. In this figure, the range of uncertainty is expressed by dotted lines.

Low success probabilities are seen during turbine generator operation (60 to 80 hours) and HPCI operation (100 to 110 hours). If plant operator watching this analysis result, thinks that future plant risk is a little high, he has to seek other alternatives with different conditions.

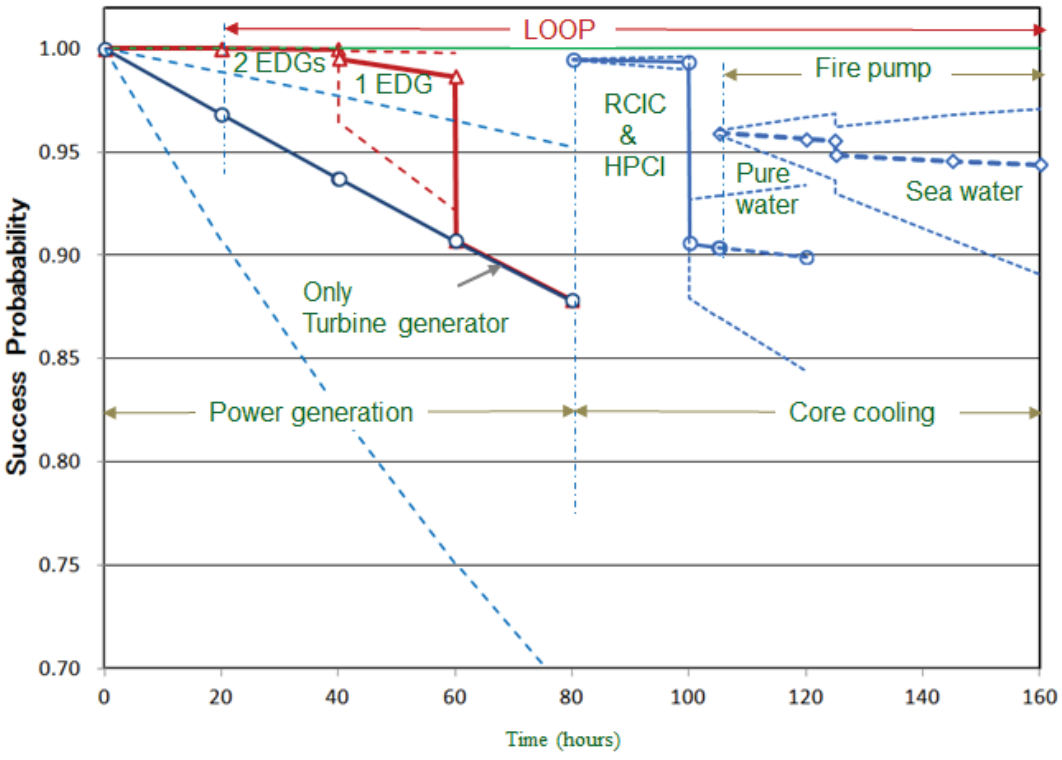


Fig. 4. Mission Success Probability in Base Case.

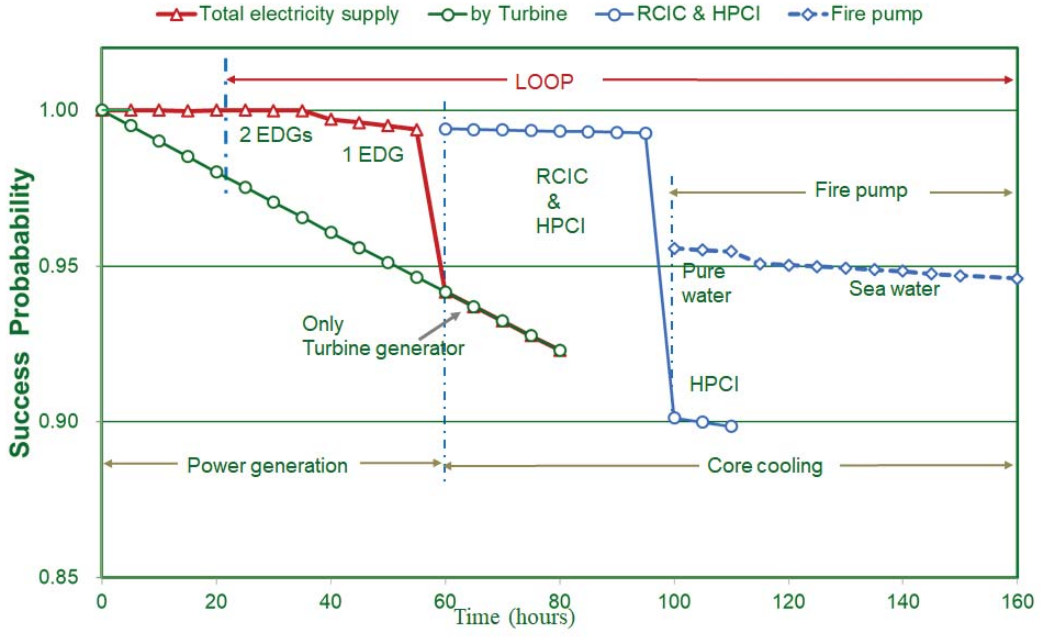


Fig. 5. Mission Success Probability in Modified Base Case.

Then change the timing of the start of RCIC and connection of fire pump. This change is easily accomplished by the change of parameter values of input data for the GO-FLOW analysis program.

The result is shown in Fig. 5. It is seen that the success probabilities are kept at relatively high level during entire time period (from 0 to 160 hours).

### 6.2 *Case 2*

Consider the case that HPCI fails and it cannot be used. Only RCIC is used for core cooling.

Accident sequence becomes as follows.

1. LOOP happens at 20 hours, and EDG1 & 2 start immediately after the LOOP.
2. EDG1 stops soon, and EDG2 also stops soon at 40 hours.
3. Only turbine generator makes electricity till 70 hours, relatively long period.
4. RCIC starts and HPCI fails at 70 hours.
5. RCIC is used for long time and stops at 120 hours.
6. Fire engine is connected at 120 hours, and start the injection of pure water.
7. Water source is changed to sea water at 145 hours.

The same big GO-FLOW chart for base case can be used for the case 2. The analysis is performed by slightly changed input data. The result is shown in Fig. 6.

Low mission success probabilities are observed after 40 hours. This is because of early failure of EDG 1 & 2, and unavailability of HPCI. The case 2 situation is not favourable for the prevention of reactor accident.

### 6.3 *Case 3*

Consider the strategy that EDG and RCIC are used as long as possible. And HPCI is not used because of its low success probability of start, and short operable time duration. HPCI is used as the backup for RCIC.

Accident sequence becomes as follows.

1. LOOP and EDG1 start at 20 hours. EDG2 fails to start.
2. EDG1 runs for long time, and EDG1 stops at 80 hours.
3. Only turbine generator makes electricity for short time duration and stops at 80 hours.
4. RCIC starts and HPCI is placed as backup at 80 hours.
5. RCIC is used for long time and stops at 125 hours. HPCI is not used after the stop of RCIC.
6. Fire engine is connected at 125 hours and start the injection of pure water.
7. Water source is changed to sea water at 145 hours.

Also, the same big GO-FLOW chart can be used for the case 3. The input data can be easily constructed by modifying parameter values of the input data for case 2. The result is shown in Fig. 7.

High mission success probabilities are obtained till 125 hours. Case 3 strategy is effective to prevent the reactor accident.

## 7. Discussions and Conclusions

As indicated in previous sections, it is necessary for updated analysis results to be automatically given in graphical style in risk monitor system. Operators can get plant risk states intuitively.

The present GO-FLOW framework automatically gives graphical style of analysis results; Matsuoka (2018). It is necessary to make some interface system which converts numerical values (analysis results) to graphical figure in risk monitor system.

In the present analysis, a big GO-FLOW chart is made for modelling all the relating systems. With one calculation of the big GO-FLOW model, mission success probabilities can be obtained along with the change of required mission.

Analysis examples (base case to case 3) show that change of required subsystem and timing are easily reflected to the analyses without changing GO-FLOW chart configuration, just by changing parameter values.

It is seen from the results of example cases, analysis results should be properly presented with boundary conditions to operators who are observing risk monitor. A value itself without analysis or boundary conditions would sometimes make misreading.

Uncertainty ranges of analysis results; Matsuoka (2016) needs to be shown in "risk monitor" system, as it is important for decision making.

The real-time analysis can be easily performed corresponding to dynamical accident sequence. The applicability of GO-FLOW to risk monitor system has been shown.

## References

Hashim, M., H. Yoshikawa, T. Matsuoka and Z. Ma (2015). Reliability Monitor Development for Passive Safety System of Ap1000 in New Concept of Risk Monitor System. *ICONE23-2061*

Holloway, N.J. (1994). Risk-Based Management of Safety Systems' Availability. NEA/CSNI/R(94)21.

IAEA (1989). Survey of ranges of Component reliability data for use in probabilistic safety assessment. IAEA-TECDOC-508.

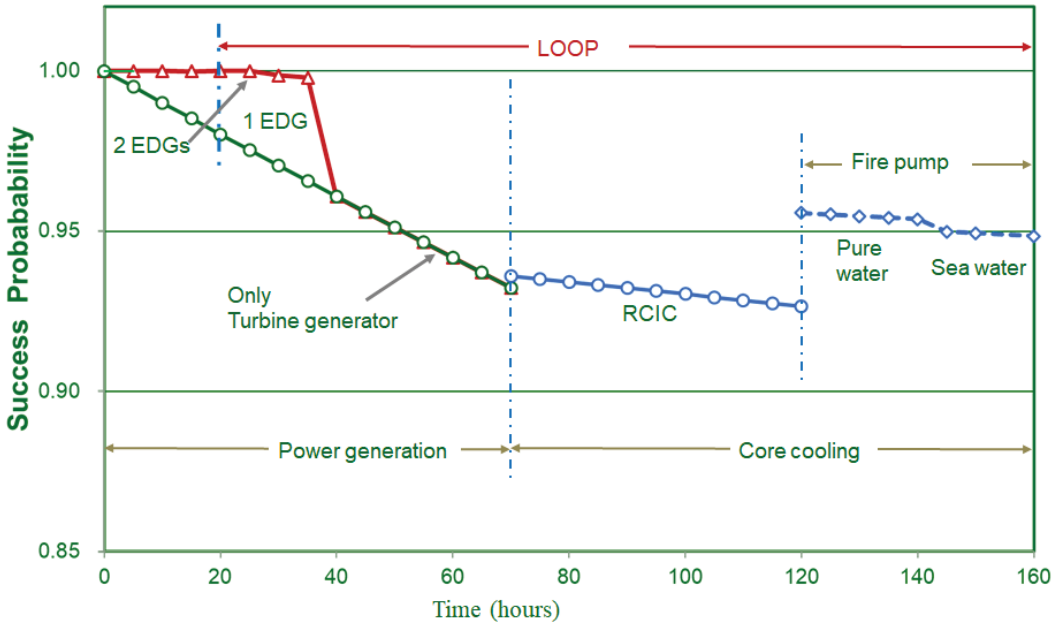


Fig. 6. Mission Success Probability in Case 2.

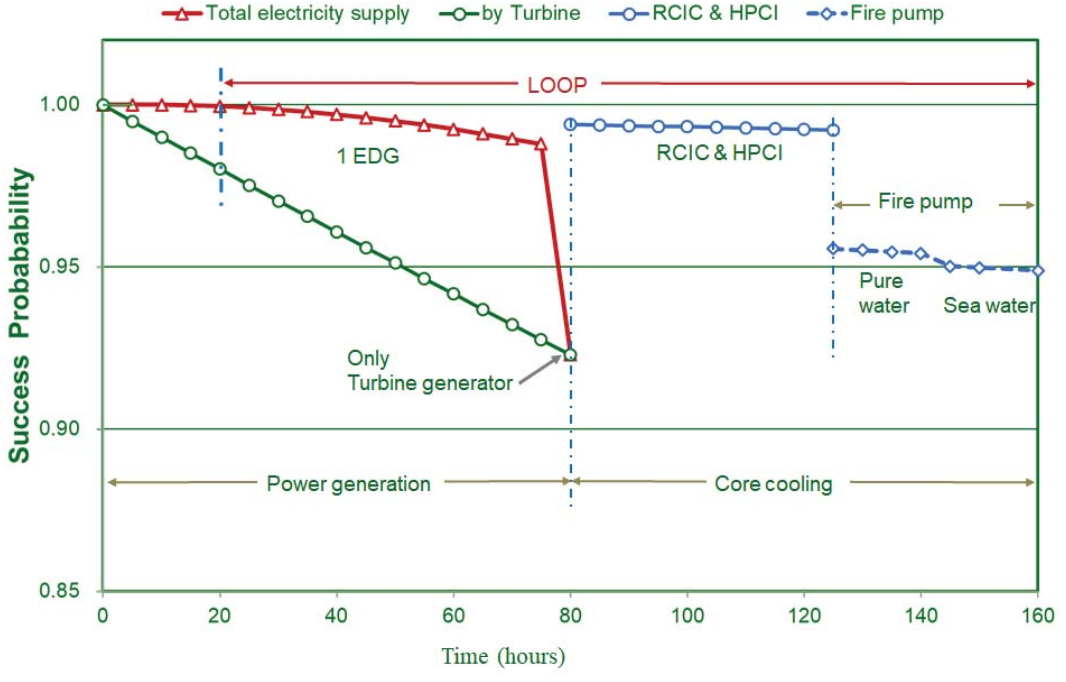


Fig. 7. Mission Success Probability in Case 3.

IAEA (1999). Living Probabilistic Safety Assessment (LPSA). IAEA-TECDOC-1106.

Japan Atomic Energy Society (2008). A standard for Procedures of Probabilistic Safety Assessment of Nuclear Power Plants during Power Operation (Level 1 PSA). AESJ-SC-P008.

Matsuoka, T and Kobayashi M. (1988). GO-FLOW A New Reliability Analysis Methodology. *Nuclear Science and Engineering* 98, 64-78.

Matsuoka, T. and m. Kobayashi (1997). The GO-FLOW reliability analysis methodology—analysis of common cause failures with uncertainty, *Nuclear Engineering and Design.* 175, 205–214.

Matsuoka, T. (2012). Generalized Method for Solving Logical Loops in Reliability Analysis. *PSAM-11*, Helsinki, Finland, June 25-29.

Matsuoka, T. (2016), Transition of the mission success probability under severe accident conditions: analysis by the GO-FLOW methodology and the consideration of uncertainty. *International Journal of Nuclear Safety and Simulation* 7(2),119-128.

Matsuoka, T. (2018). Dynamic Behaviour of Nuclear Power Plant State under Severe Accident Conditions: Analysis by the GO-FLOW Methodology and the Consideration of Loop Structures. In Aldemir, T (Eds.), *Advanced Concepts in Nuclear Energy Risk Assessment and Management*, pp.427-476, World Scientific Publishing Co Pte Ltd.

Prime Minister of Japan and his Cabinet (2011). Report of Japanese Government to the IAEA Ministerial Conference on Nuclear Safety - The Accident at TEPCO's Fukushima Nuclear Power Stations –.

U.S.NRC (1975). An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants Appendix III Failure Data, WASH-1400, NUREG-75/014.