

The GO-FLOW and the Bayesian Network in PSA

Takeshi Matsuoka^{a*}

^aUtsunomiya University, Utsunomiya City, Japan

Abstract: The same example has been analyzed by the GO-FLOW, BN, and FTA. The modeling procedures and analysis results are compared and the discussions are made on advantages and disadvantages. FTA is very familiar to almost all the system engineers, and is a convenient tool for a simple system, but there are some limitations of function. BN can easily model a complicated situation, with multiple-state variables, and BN is useful for the decision making with the uncertain data. The GO-FLOW is strong for modeling dynamical system behavior and can easily obtain time-dependent system reliability. The GO-FLOW and BN have different features, and they are properly used depending on the analysis purposes in PSA.

Keywords: GO-FLOW, FTA, BN, Dynamic PSA, System reliability analysis

1. INTRODUCTION

In the PSA framework, a Fault Tree Analysis(FTA)[1] is widely used as a system reliability analysis technique. The authors have proposed the GO-FLOW methodology[2], which has advanced function such as to be able to treat time dependency and dynamical behavior.

Bayesian Network(BN) [3] is used as a probabilistic method of reasoning under uncertainty knowledge. Recently, BN has been becoming a popular tool in reliability engineering. BN is represented by a graphical diagram consists of nodes and directed links. The BN diagram is similar to the GO-FLOW chart that has operators and signal lines.

A system reliability analysis is one of the key steps in PSA. These three techniques(FTA, BN, GO-FLOW) can be used as system reliability analysis techniques in PSA, and actually they have been used.

In this presentation, a simple hypothetical system is taken up and is analyzed by these three techniques. The modeling procedures and analysis results are compared and discussions are made on advantages and disadvantages of these analysis tools in the framework of PSA.

2. A SYSTEM FOR ANALYSES

Here, we consider the following simple but a little complicated system as shown in a Block diagram of Figure 1. This system is a hypothetical one and does not correspond any actual system.

Some mechanical or electrical components are represented by X2 and X4. Operator action (X1) plays an alternative role for the function of X2, if some failure occurs to X2. The same relation is given between X3 and X4. Both X2 and X4 function is required. Therefore, X1 and X2 is combined by OR combination, and the output is combined by AND with the output of X3 and X4.

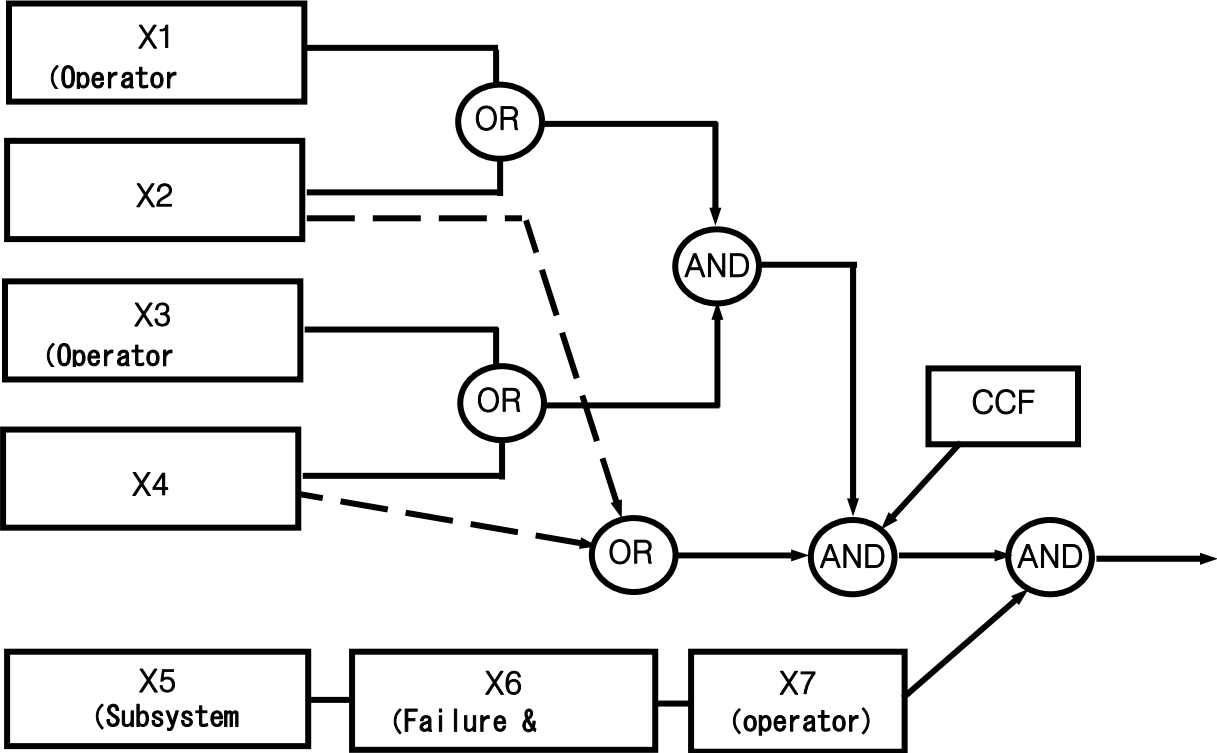
At the same time, X2 and X4 is combined by OR combination. It means at least one hardware component(X2 or X4) must be in sound condition. This condition is also required for the function of X2 and X4 lines. Then the output of OR combination of X2 and X4 is combined with the above output by AND combination.

Contribution from common cause failures is represented by CCF and added to this line by AND combination.

*mats@cc.utsunomiya-u.ac.jp

Remaining part of the total system is represented by sub-system X5. Sub-system failure and repair action are represented by X6 and operational error is represented by X7. The success of total system is represented by the rightmost line.

Figure 1. Block diagram of a hypothetical system.



For the description of system operation, time steps are defined as shown in table 1. Failure data are given as shown in table 2. Failure probabilities of these elements at time step 4 are also given in the table.

Table 1: Time steps

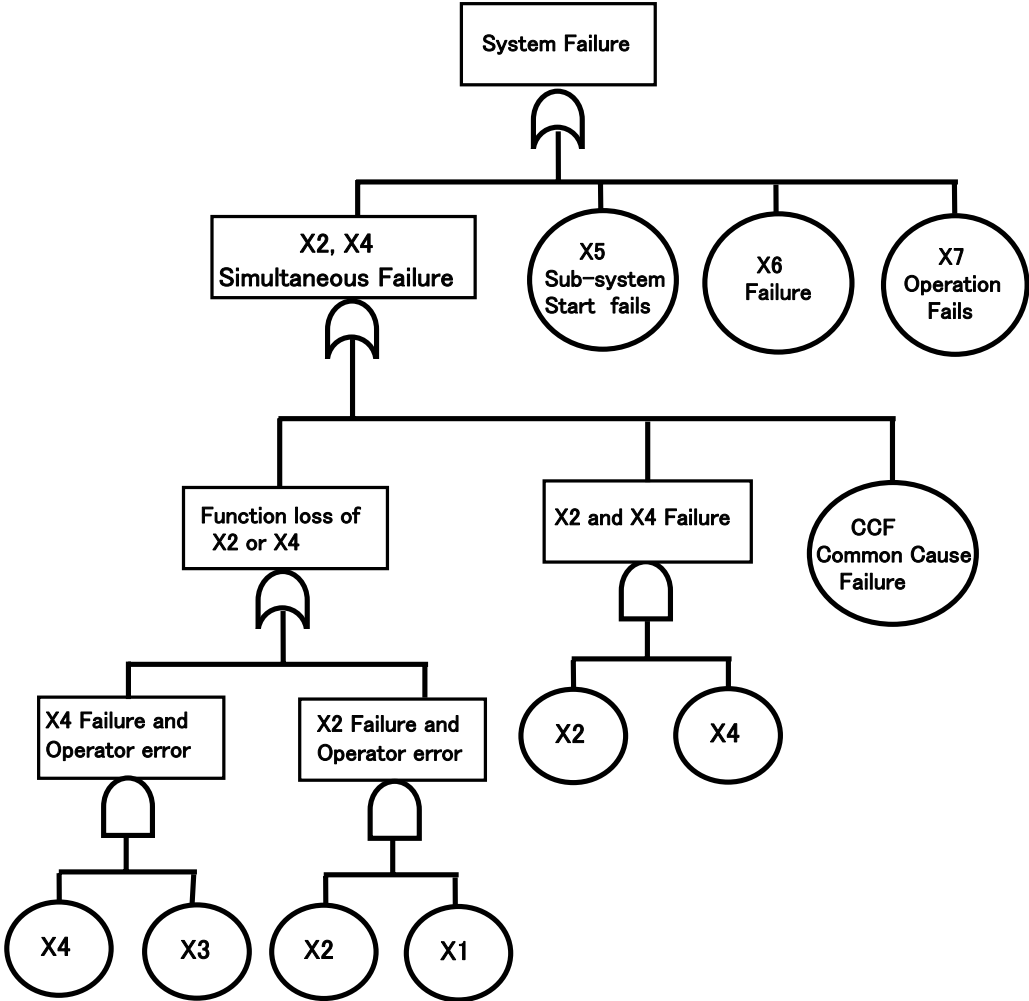
Time step	Meaning	Comments
1	Initial time	Sub-system starts to operate
2	10 hours	
3	30 hours	
4	100 hours	
5	Repair action	Failure is recovered and becomes as new
6	Additional 30 hours	

Table 2: Failure data

Component (Event)	Failure data	Failure probability at time step 4	Comments
X1	$\lambda=1.054 \times 10^{-3}/h$	0.1	
X2	$\lambda=3.567 \times 10^{-3}/h$	0.3	
X3	$\lambda=1.054 \times 10^{-3}/h$	0.1	
X4	$\lambda=3.567 \times 10^{-3}/h$	0.3	
X5	0.1	0.1	Successful start is 0.9
X6	$\lambda=3.567 \times 10^{-3}/h,$	0.3	Failure is repaired at time step 5
X7	$\lambda=1.0 \times 10^{-5}/h$	0.001	
CCF	$\lambda=1.0 \times 10^{-4}/h$	0.01	

3. ANALYSIS BY THE FAULT TREE

Figure 2. Fault tree for the example system.



The FTA is based on the identification of a particular undesired event, that is, system failure in this case, and it is placed as top event. The construction of FT proceeds in a top-down fashion from the top event to basic events. Intermediated events are placed and they can represent logical intermediated states, or logical sub-system. The relations between events are represented by logical AND or OR gates. Events are binary events, success or failure.

For a system shown in figure 1, a fault tree is constructed as shown in figure 2. The logical expression of the top events as a function of the minimal cut sets is given by the following equation.

$$System\ failure = X1 \cdot X2 + X3 \cdot X4 + X2 \cdot X4 + CCF + X5 + X6 + X7 \tag{1}$$

Fault tree analyzes a static state of a system, and can not treat time progress of system failure. Quantitative analysis is done for the time step 4 shown in table 1. The system failure probability is calculated at 0.4592

Many kinds of measures of importance are defined and they are used for the evaluation of system characteristics. Let $P(\text{system}/X=a)$ means the conditional probability of system failure when basic event X has a value "a". The following definitions are given.

$$Risk\ reduction\ worth(RRW) = \frac{P(system)}{P(system / X = 0)} \quad (2)$$

$$Risk\ achievement\ worth(RAW) = \frac{P(system / X = 1)}{P(system)} \quad (3)$$

$$Birnbau\ = \frac{P(system / X = 1)}{P(system / X = 0)} \quad (4)$$

$$Fussell - Vesely = \frac{P(system) - P(system / X = 0)}{P(system)} \quad (5)$$

$$Criticality = \frac{\{P(system / X = 1) - P(system / X = 0)\} P(X)}{P(system)} \quad (6)$$

The values of these importances are easily calculated by the fault tree. Failure and repair of subsystem(X6) shows prominent values; RRW=2.02, RAW=2.18, Birnbaum=4.40, F-V=0.505, Criticality=0.505.

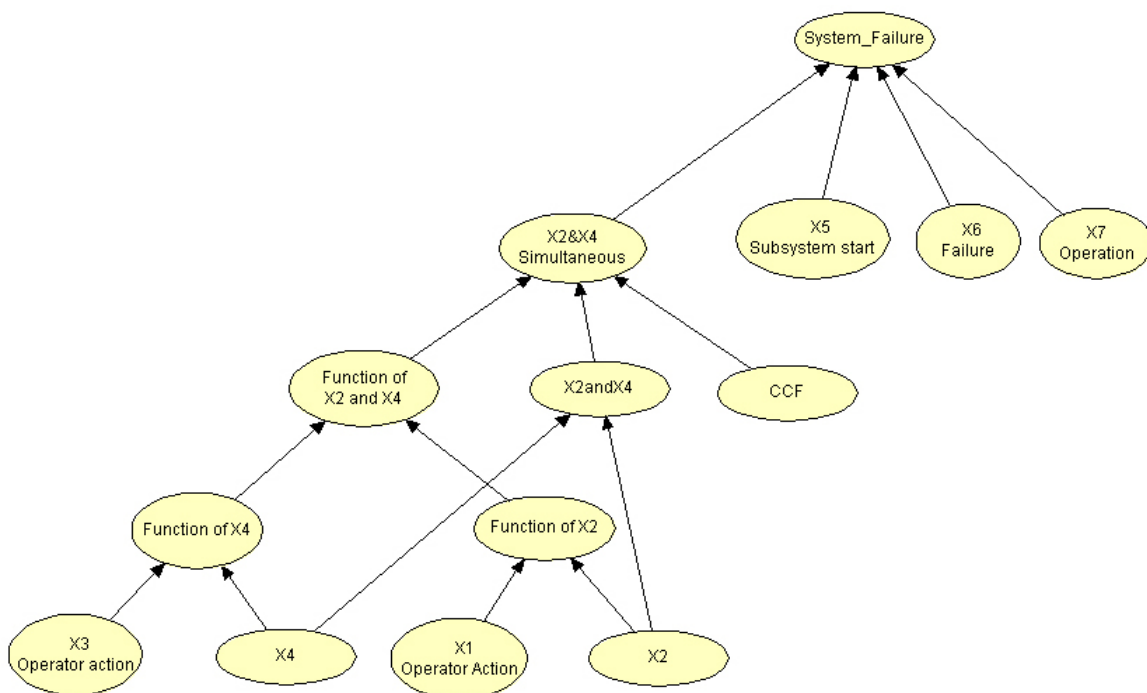
4. ANALYSIS BY THE BAYESIAN NETWORK

A Bayesian network(BN) is constructed as shown in figure 3. Nodes correspond to basic events, intermediate states and top event in fault tree. Nodes are connected by arcs(directed links) and just one node is sufficient for the expression of the basic event appeared at multiple places in fault tree, for example X2 and X4.

There is no gate node in BN, because the function of gate is implemented in conditional probability table (CPT), which belongs to node. In a forward(predictive) analysis, the probability of occurrence of any nodes of the BN is calculated on the basis of the conditional dependence of each node.

Any analysis performed on a FT can be performed on a BN. Exactly the same value is obtained for the system failure, and the measures of importance are also easily calculated in BN.

Figure 3. Bayesian network for the example system.



A specific feature of BN is a backward analysis that concerns the computation of the posterior probability of any given variables, which is given by new observation (evidence, plant specific data, new knowledge, updated data, ...). For example, posterior probability of system failure becomes 0.2817 with an evidence $X_6=0.15$. The posterior probabilities of all other nodes are also shown in BN, and the posterior probability of X_6 becomes 0.0703.

Evidence is not restricted one, multiple evidences can be given in BN at the same time. If an evidence is given to an intermediated node, the relations between calculated posterior probabilities of nodes are not reflected in the conditional dependence given for the calculation of prior distribution.

An evidence can be also given to a top event(system failure itself). The posterior probabilities give us information on the possible explanations of an exhibited system failure. This is a kind of diagnostic analysis, and it is peculiar to BN.

Common cause failure is an important phenomena in a system reliability analysis and PSA. Here we consider the case; events X_2 and X_4 contain common cause failure CCF. Then,

$$X_2 = T_2 + Ind_2 + CCF, \quad X_4 = T_4 + Ind_4 + CCF \quad (7)$$

where T_2 is the state that component is sound, Ind_2 is for independent failure, CCF is for common cause failure. Events T_2 , Ind_2 and CCF are mutually exclusive.

If X_2 and X_4 is combined by AND gate, the CPT in BN must be as shown in table 3 by using multi-state variables, because the joint of events X_2 and X_4 becomes as follows.

$$X_2 \cdot X_4(Truth) = T_2 \cdot T_4 + T_2 \cdot Ind_4 + T_4 \cdot Ind_2, \quad X_2 \cdot X_4(Failure) = Ind_2 \cdot Ind_4 + CCF \quad (8)$$

Table 3: Conditional probability table for common cause failure

X2	TRUE			Independent			CCF		
	TRUE	Ind	CCF	TRUE	Ind	CCF	TRUE	Ind	CCF
TRUE	1	1	0	1	0	0	0	0	0
Failure	0	0	0	0	1	0	0	0	1

In CPT, sum of any column must be more than zero in BN framework. So, the common cause failure is not well treated in BN. Also there is a case that events X_2 and X_4 are combined through other nodes. Some primitive idea to treat the common cause failure in BN is presented[4], but it is not well solved.

5. ANALYSI BY THE GO-FLOW

A GO-FLOW chart is constructed as shown in figure 4. Logical operators (AND or OR gate) appear in the chart. The roles of operators are described on the side of operators. Operators are connected by signal lines and more than one signal lines can be attached to one operator, in which logical combinations of operators can be easily achieved.

Configuration of GO-FLOW chart is well corresponds to the system block diagram shown in figure 1. That is, the GO-FLOW chart is easy to construct, to understand, to validate and to modify.

The GO-FLOW can treat time dependent system reliability analysis. For the sample system, 6 time points are defined and time evolution of system failure probability is analyzed. Any analysis performed on a FT can be performed on a GO-FLOW. Exactly the same value is obtained for the system failure probability at time point 4, and the measures of importance are also easily calculated in GO-FLOW.

The analysis result is shown in figure 5. System failure probability increase with time till 100 hours, and effects of repair is seen at 100 hours. Failure probability is suddenly decreased.

The GO-FLOW can treat the common cause failure[5]. Mutually exclusive relations or inclusion-exclusion relations between basic events is rigorously treated in the analysis procedure.

The GO-FLOW can not make a backward analysis which the BN can do, and diagnostic like analysis can not be directly made by the GO-FLOW.

Figure 4. GO-FLOW chart for the example system.

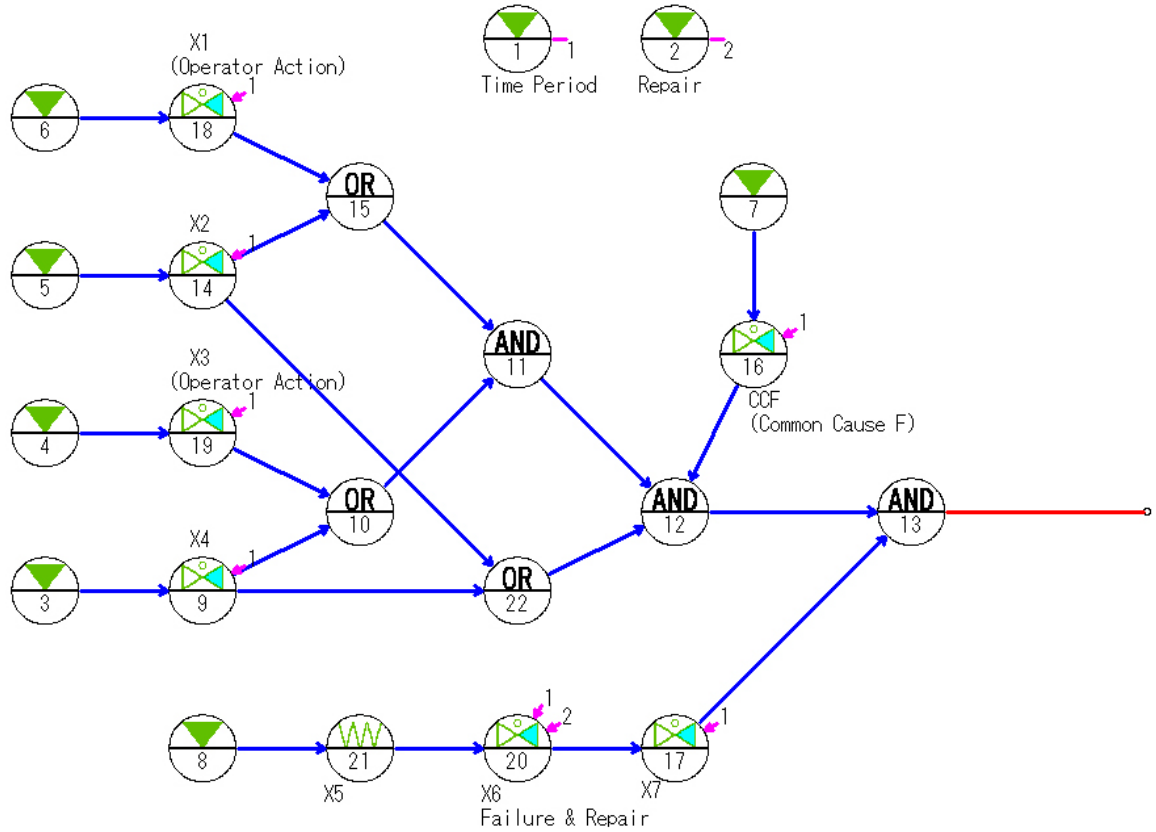
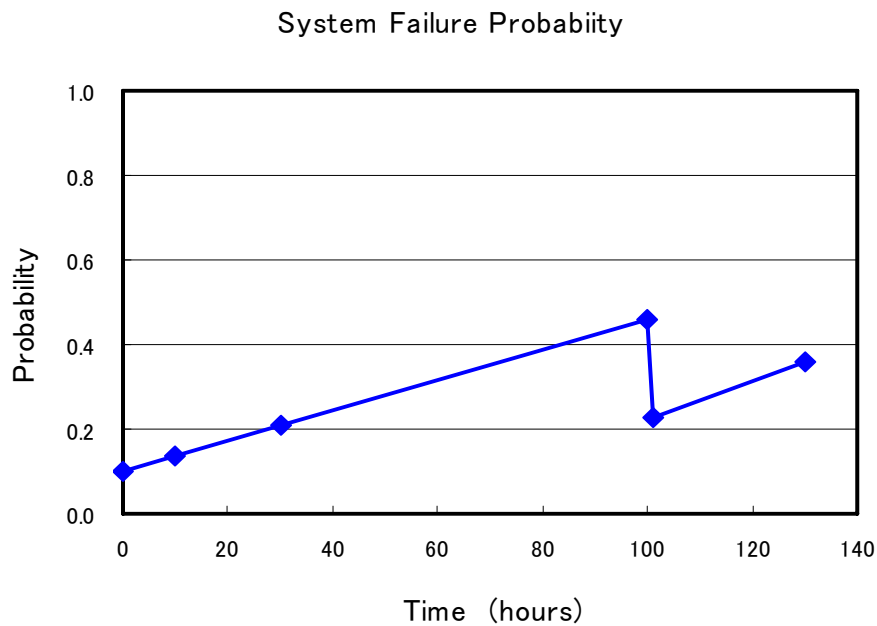


Figure 5. Analysis result by the GO-FLOW.



6. CONCLUSION

The same example has been analyzed by the GO-FLOW, BN, and FTA. The modeling procedures and analysis results are compared and the discussions are made on advantages and disadvantages of these analysis tools.

FTA is very familiar to almost all the system engineers, and is a convenient tool for a simple system, but it requires special skills for the modeling of a complex system or complicated condition. A limited function is provided to the FTA, because only logical OR and AND gates are used, and events are binary events; success or failure, and only a static system can be analyzed.

BN can easily model a complicated situation, such as component's state requires multiple state, and has logical combination which can be flexibly defined. BN gives us the posterior probability of each event in case definite values are given to specific components. So, BN is useful for the decision making with the uncertain data, or after getting a new evidence. But, BN has some difficulty to treat the common cause failure, and can handle only a static system.

The GO-FLOW is strong for modeling dynamical system behavior and can easily obtain time-dependent system reliability. The GO-FLOW provides many kinds of operators, by which complicated system operation is modeled with conventional procedure. The GO-FLOW can rigorously treat the common cause failure.

The GO-FLOW and BN have different features, and both tools give us straightforward procedure for modeling complex systems. They are properly used depending on the analysis purposes in PSA.

References

- [1] E.J. Henry and H. Kumamoto, "*Reliability engineering and risk assessment*", Prentice Hall, 1981, Englewood Cliffs, NJ
- [2] T.Matsuoka and M.Kobayashi, "*GO-FLOW A New Reliability Analysis Methodology*", Nuclear Science and Engineering, Vol.98, pp. 64-78(1988)
- [3] Finn V. Jensen, "*Bayesian Networks and Decision Graphs*", Springer, 2001, New York
- [4] A.Bobbio et al., "*Improving the analysis of dependable systems by mapping fault trees into Bayesian networks*", Reliability engineering and system safety, vol. 71, pp.249-260(2001)
- [5] T.Matsuoka and M.Kobayashi, "*The GO-FLOW Reliability Analysis Methodology -Analysis of Common Cause Failures with Uncertainty-*", Nuclear Engineering and Design Vol.175, pp.205-214 (1997)