NUCLEAR SAFETY

THE GO-FLOW METHODOLOGY: A RELIABILITY ANALYSIS OF THE EMERGENCY CORE COOLING SYSTEM OF A MARINE REACTOR UNDER ACCIDENT CONDITIONS

TAKESHI MATSUOKA and MICHIYUKI KOBAYASHI
Ship Research Institute, Nuclear Technology Division
6-38-1, Shinkawa, Mitaka, Tokyo 181, Japan

KAZUO TAKEMURA *Toyama Mercantile Marine College*
1-2, Ebie-Neriya, Shin-minato, Toyama 933-02, Japan

Received May 9, 1988
Accepted for Publication September 7, 1988

A reliability analysis using the GO-FLOW methodology is given for the emergency core cooling system (ECCS) of a marine reactor experiencing either a collision or a grounding accident. The analysis is an example of a phased mission problem, and the system is a relatively large system with 90 components.

An overview of the GO-FLOW methodology, a description of the ECCS, and the analysis procedure are given. Time-dependent mission unreliabilities under three accident conditions are obtained by one GO-FLOW chart with one computer run.

The GO-FLOW methodology has proved to be a useful tool for probabilistic safety assessments of actual systems.

I. INTRODUCTION

Probabilistic safety assessment (PSA) is important in the safety analysis of nuclear power plants. Event trees and fault trees are the basic analytical tools that have been most frequently used for PSAs (Ref. 1). Several system analysis methods[2] can be used in addition to, or in support of, the event- and fault-tree analysis.

We have developed a new reliability analysis methodology,[3] GO-FLOW, that has a modeling method (chart) and a calculational procedure that are similar to those of the GO method.[4] Its basic concept, however, is different from that of the GO method.

We first present an overview of the GO-FLOW methodology and then deal with a reliability analysis using the GO-FLOW method for the emergency core cooling system (ECCS) of a marine reactor experiencing either a collision or a grounding accident. The present analysis is an example of an analysis of a relatively large system with a complex system operation sequence under multiple accident conditions. The analysis procedure shown in this paper indicates significant, specific features as well as the usefulness of the GO-FLOW methodology.

II. OVERVIEW OF THE GO-FLOW METHODOLOGY

The GO-FLOW methodology, which is a success-oriented system analysis technique, is capable of evaluating system reliability and availability. The modeling technique produces the GO-FLOW chart, which consists of signal lines and operators, and represents the engineering function of a system.

Operators model a function or a failure of physical equipment, a logical gate, and a signal generator. Twelve different types of operators are currently defined, as shown in Fig. 1. (Note that the numbers used in this figure are numbered greater than 20 to avoid being confused with the operators used in the GO method.)

Signals represent some physical quantity or information. The "existence" of a signal necessarily means the existence of a physical quantity or information. In GO-FLOW, the existence of a physical quantity is interpreted as both the actual and the potential existence of a physical quantity. In this case, "the potential existence" means that a physical quantity exists when all the resistance "downstream" is removed.

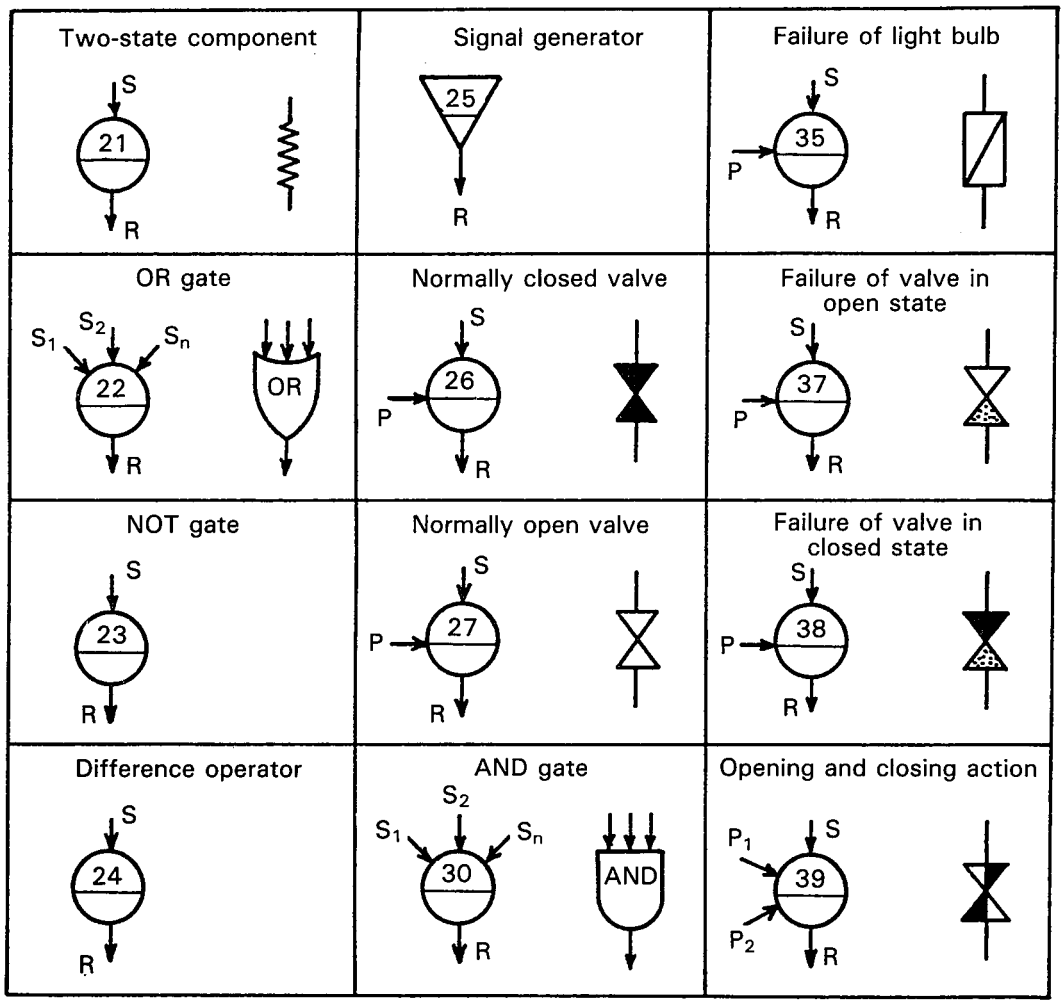

Fig. 1. Operators in the GO-FLOW methodology.

A quantity called "intensity" is associated with a signal. Usually the intensity represents the probability of signal existence. Therefore, intensity is the probability of the actual or potential existence of a physical quantity or the probability that some information or mission exists. When a signal is used as a subinput signal to the type 35, 37, or 38 operator, 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 operation sequence. The values do not necessarily represent real time but correspond to it and represent an ordering. The total number of time points is a user-defined parameter.

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

The GO-FLOW methodology possesses the following significant features:

1. The GO-FLOW chart corresponds to the physical layout of a system and is easy to construct and validate.
2. Alterations and updates to a GO-FLOW chart are readily accomplished.
3. GO-FLOW contains all possible system operational states.
4. The analysis is performed by one GO-FLOW chart with one computer run.

III. SYSTEM DESCRIPTION AND ANALYSIS CONDITIONS

The GO-FLOW methodology is applied to a reliability analysis of the ECCS of a marine reactor experiencing either a collision or a grounding accident. A nuclear propulsion tanker, 80 000 deadweight tonnage, 18-knots speed, was selected for the present analysis. A conceptual design by the Shipbuilding Research Association of Japan[5] and the nuclear ship[6]

Mutsu were used to determine the ship structure, system configurations, and the location of components.

Figure 2 shows the engine section of the nuclear tanker, and Fig. 3 shows a simplified flow diagram of the ECCS. The system is a relatively large system with 90 components. There are two high-pressure core injection (HPCI) loops, two low-pressure core injection (LPCI) loops, and two recirculation cooling loops (RCLs). Each of these loops is separated by a watertight wall and is placed at the starboard or port side of a reactor room, outside of the secondary shielding against the reactor. The LPCI loop and the RCL use a part of the residual heat removal system, and the same pump (A63 or B63 in Fig. 3) is commonly used in these two loops. Two turbine generators and two auxiliary diesel generators are located in the main machinery room. Two emergency diesel generators are located on a bridge deck on the upper part of the ship.

A collision with an ordinary merchant ship and a grounding accident are selected as marine disasters. Furthermore, we assume that a loss-of-coolant accident (LOCA) (100-mm-diam pipe break) occurs at the same time that the marine disaster occurs. After a LOCA has occurred, three phases for ECCS are identified:

1. HPCI (50 s to 10 min)

2. LPCI (10 min to 1 h)

3. recirculation cooling (1 to 150 h).

For phase 1, one HPCI is needed. For phase 2, one HPCI or one LPCI is needed. For phase 3, water in the sump of the containment is used as cooling water. Thus, one RCL is needed. In each phase, sufficient power can be supplied by one of the six electric generators. The zero-duration phase boundaries are assumed for the above phase changes, and all of the components are assumed to be nonreparable.

It is also assumed that any safety system component is not directly damaged by the collision or grounding accident, but is damaged by flooding produced by these accidents.

Three accident conditions are identified:

1. *No flooding*. Flooding does not occur and all the components of the safety system are undamaged by the accident.

2. *Flooding in compartment B*. Flooding occurs in compartment B (port side) of the reactor room, and all the components in compartment B cease to function from the beginning of the LOCA.

3. *Flooding in the main machinery room*. Flooding occurs in the main machinery room, and all the components in the main machinery room cease to function from the beginning of the LOCA.

IV. ANALYSIS BY THE GO-FLOW METHODOLOGY

IV.A. GO-FLOW Chart

The first procedure of the analysis is to construct a GO-FLOW chart that models the configuration and the function of a system. The GO-FLOW chart for the present system is shown in Figs. 4a, 4b, and 4c. This chart is an example of a large GO-FLOW chart, and the total operator number is 195. Each operator is represented by a compound number: The number above the horizontal line represents the operator type, and the number below the line designates each operator. The numbers on the connecting lines identify the signals. Component numbers (A1, B1, . . . , etc., shown in Fig. 3) are written by the side of the corresponding operators. Some components have more than one failure mode: demand failure, standby failure, and operating failure. Therefore, the total operator number is larger than the component number.

The logic of system operation in each phase under three different accident conditions is expressed in one GO-FLOW chart by using the logical operators "OR" (type 22 operator) and "AND" (type 30 operator).

As electric power sources, six generators (two main turbine generators, two auxiliary diesel generators, and two emergency diesel generators) are available under the conditions "no flooding" and "flooding in compartment B." This is expressed by signal line 23 in Fig. 4a.

Under the condition "flooding in the main machinery room," only two generators (two emergency diesel generators) are available. Signal line 24 represents the available power source under this condition.

Under the condition "flooding in compartment B," all the components in compartment B cease to function, and only the A loop (loop in compartment A) is available. Therefore, signal 83 (A loop) and signal 23 (electric power from any of six generators) are combined by the AND gate (operator 84) in Fig. 4b. Output signal 84 represents the probability of system operation if flooding in compartment B in phase 1 occurs.

Operator 92 (OR gate) combines signals 81 (A loop) and 91 (B loop). Output signal 92 indicates that one or both of the A and B loops are available. Signal 94, which is downstream of signal 92, is combined with signal 23 by the AND gate. Output signal 95 represents the probability of system operation under the condition of no flooding in phase 1.

Signal 94 is also combined with signal 24 (electric power from either of two emergency diesel generators). Output signal 96 represents the probability of system operation under the condition of flooding in the main machinery room in phase 1.

In the same way, signals 150, 155, and 156 and signals 166, 171, and 172 represent the probabilities in phases 2 and 3, respectively (see Figs. 4b and 4c).

Many components are commonly used under different accident conditions or in different phases. By

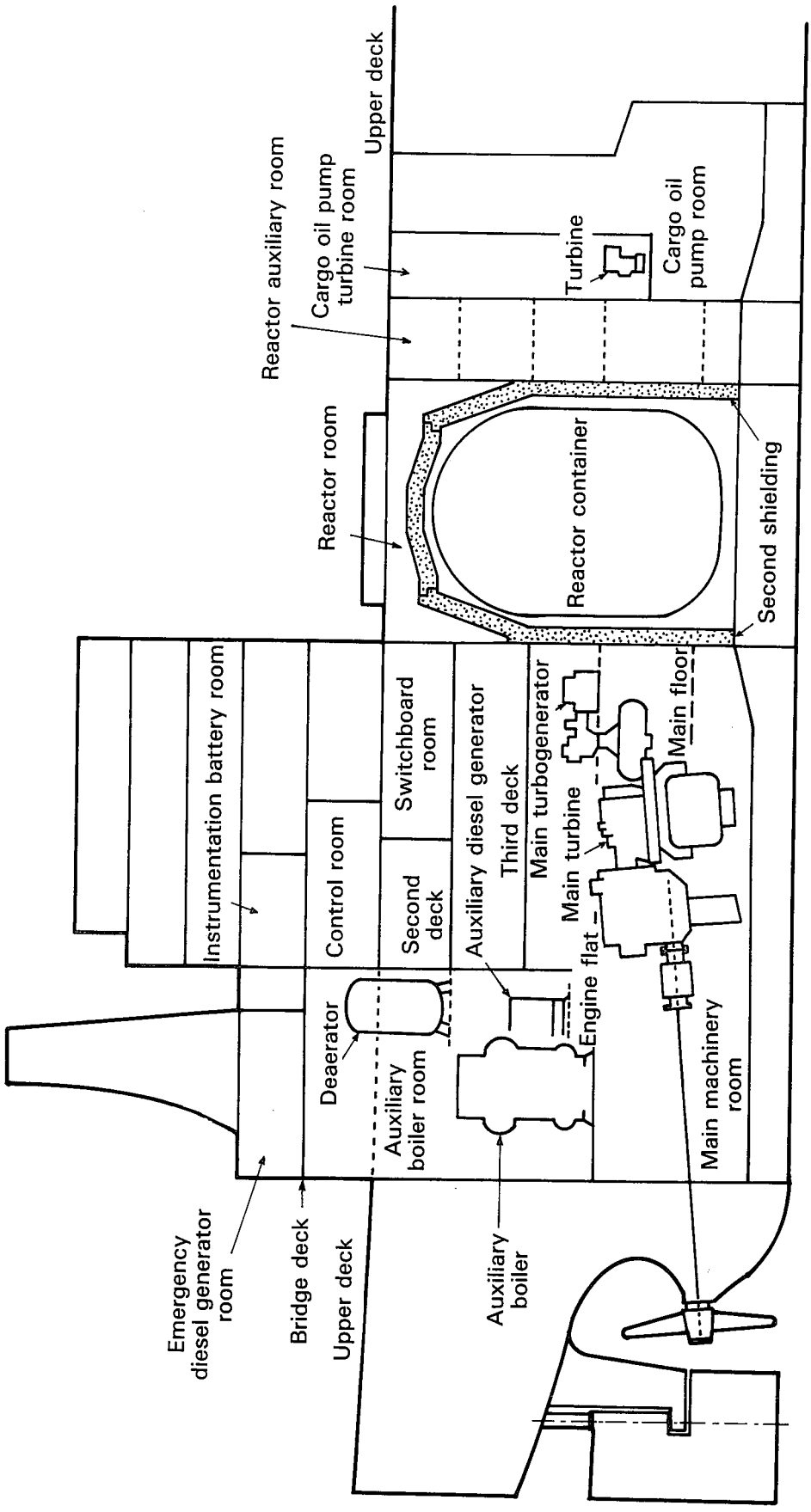

Fig. 2. The engine section of the nuclear tanker.

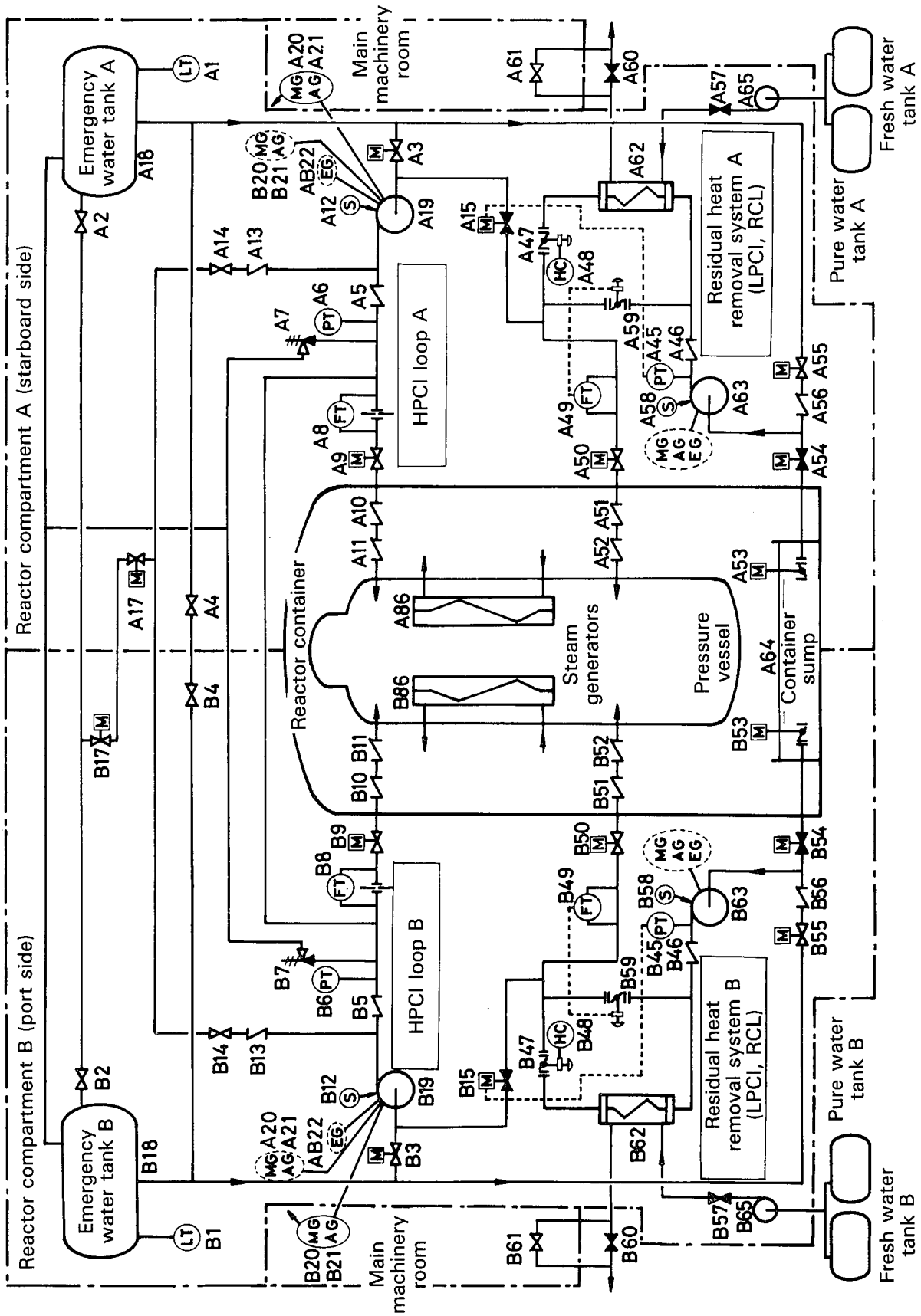

Fig. 3. Flow diagram of the ECCS of a marine reactor.

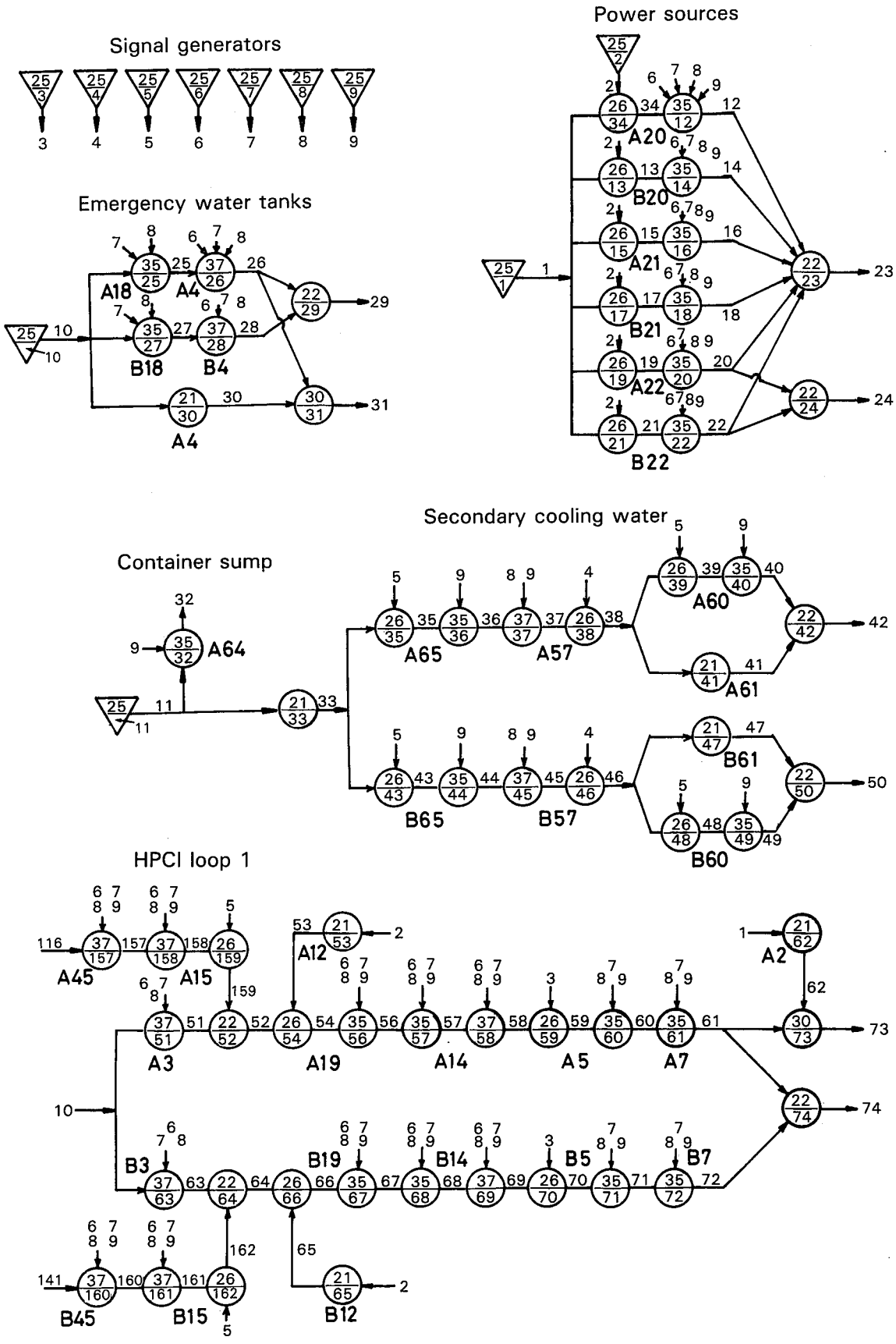

Fig. 4a. GO-FLOW chart for the ECCS of a marine reactor (1).

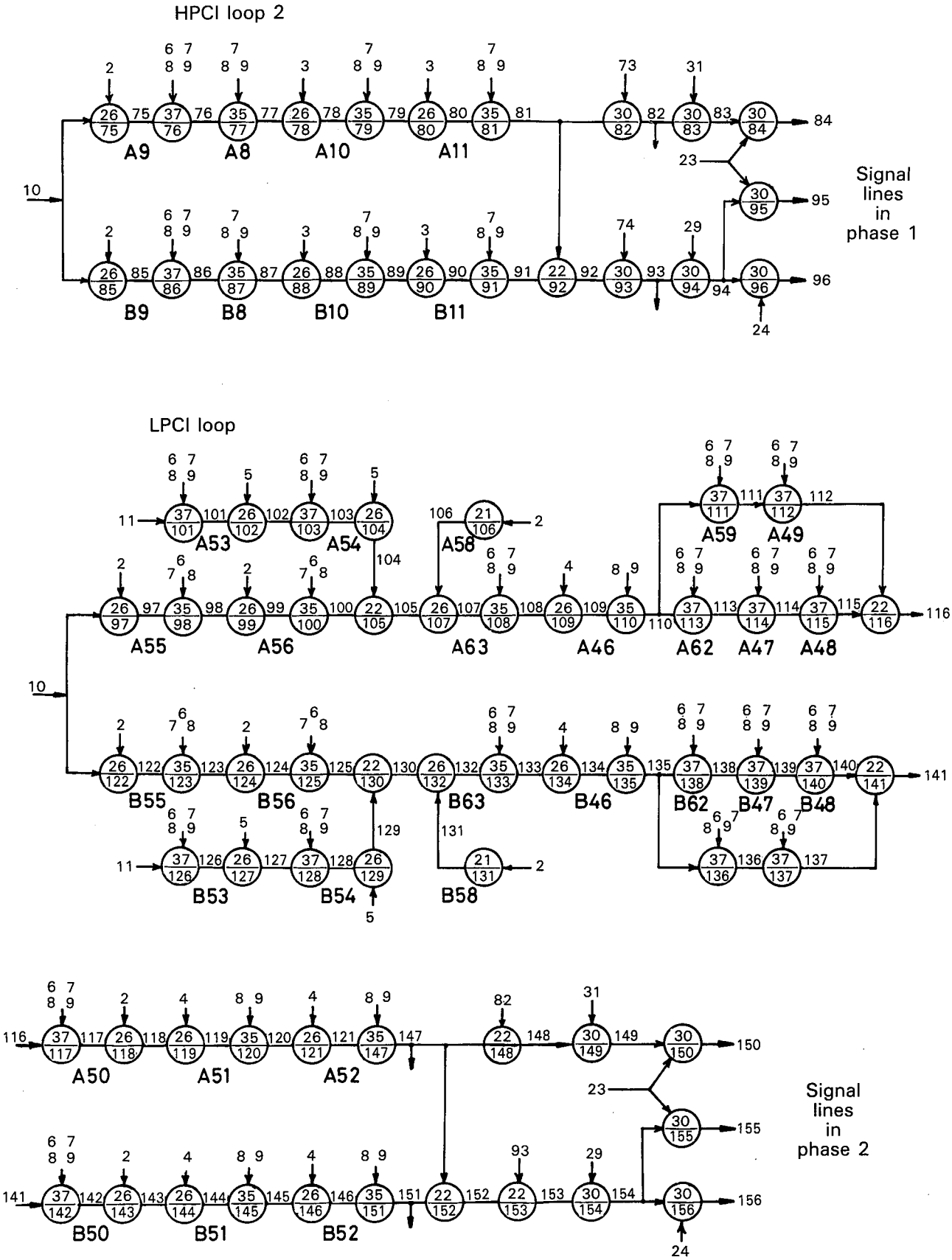

Fig. 4b. GO-FLOW chart for the ECCS of a marine reactor (2).

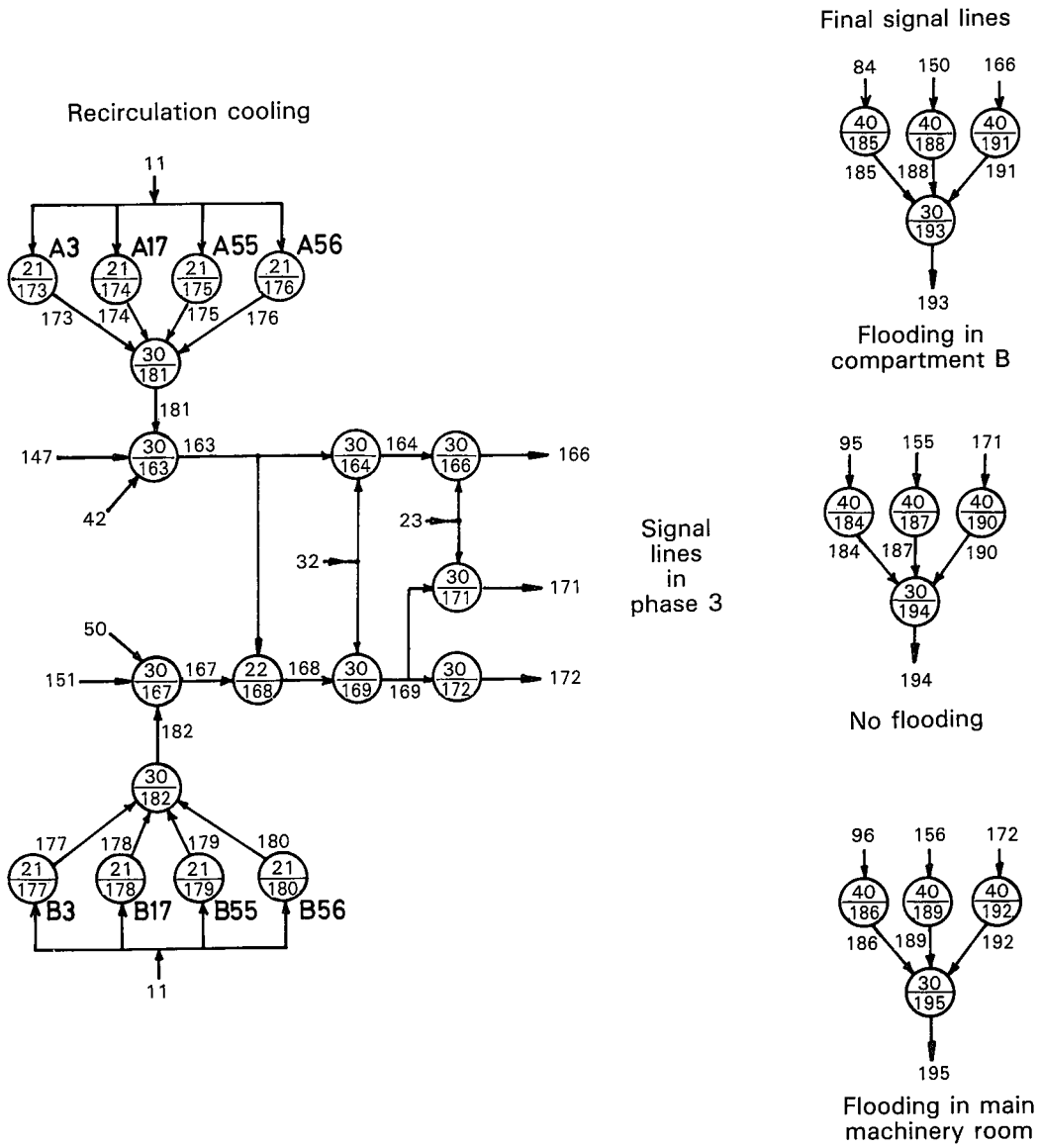

Fig. 4c. GO-FLOW chart for the ECCS of a marine reactor (3).

using branched signal lines and logical gates, it is possible to construct a GO-FLOW chart that contains the signal lines representing the probability of system operation in phases 1, 2, and 3 under three different accident conditions.

The next step is to define time points for the expression of the sequence of system operation. In this analysis, we declare nine time points as shown in Table I. Time intervals between the successive time points are given by the intensities of signals 6, 7, 8, and 9. Signals 2, 3, 4, and 5 represent demand signals for a LOCA to occur, phase 1 to start, phase 2 to start, and phase 3 to start, respectively.

The value of a failure rate or demand probability for each component is deduced from Ref. 7.

TABLE I

Time Points Defined in the Analysis

Time Point	Real Time	Meaning
1		Initial time
2	0	Marine disaster and LOCA occur
3	50 s	Phase 1 starts
4	10 min	Phase 1 ends
5	10 min	Phase 2 starts
6	1 h	Phase 2 ends
7	1 h	Phase 3 starts
8	75 h	Phase 3
9	150 h	Phase 3 ends

IV.B. Treatment of a Phased Mission Problem

The present system is a typical example of a phased mission problem. A phased mission is a task to be performed by a system. 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 successfully in all the preceding phases. Therefore, we have to calculate the product of the success probabilities in successive phases. In other words, it is necessary to calculate the products of signal intensities at different time points (i.e., different phases). If there is a shared component for various phases, it is necessary to treat correctly the inclusion or exclusion relation between the failures of a shared component in different phases.

In the GO-FLOW methodology, the signals, which represent the probabilities of system operation in successive phases, are combined by an AND gate (type 30 operator). At this time, we introduce the type 40 operator, which freezes a signal intensity except during a specific time period, as shown in Fig. 5. In this figure, $S(t)$ is the intensity of an input signal and $R(t)$ is the intensity of an output signal. A specific phase is from t_i to t_j. Before this phase $R(t)$ is always 1.0, and after this phase $R(t)$ holds the value $S(t_j)$ at the end of the phase.

We now consider the case where the signal $R(t)$ is combined with the signal $U(t)$ by an AND gate. Before the time point t_i, the output signal becomes $U(t)$. The signal $R(t)$ has no influence before time point t_i because its intensity equals 1.0. After the time point t_j, $U(t)$ is always combined with $S(t_j)$, the intensity at the end of a specific phase. Therefore, the type 40 operator makes it possible to calculate the product of the success probabilities in successive phases by formally calculating the products of signal intensities at the same time point.

In Fig. 4c, signals 193, 194, and 195 are the final signals, and they represent the mission reliabilities under the accident conditions of flooding in compartment B, no flooding, and flooding in the main machinery room, respectively.

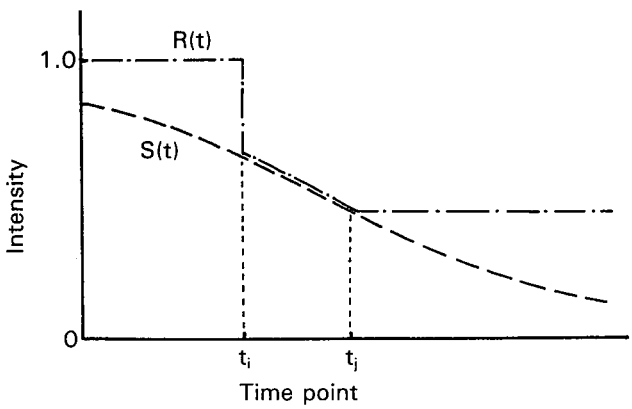

Fig. 5. Function of the type 40 operator.

The calculational procedure of the GO-FLOW methodology can correctly treat the dependency between the failures of a shared component in different phases.

IV.C. Analysis Program

The analysis program of GO-FLOW is written in FORTRAN 77 for the ACOS-910/8 computer at the Ship Research Institute. This program is capable of analyzing GO-FLOW charts with up to 200 operators, 200 signal lines, and 35 time points. Current program dimensions allow the code to load with under 2000 kbytes of memory, and the program does not use external storage devices.

The present analysis has been done with one computer run in 6.883-s CPU time.

V. DISCUSSION OF RESULTS

Table II shows the results of the analysis. Time-dependent mission unreliabilities under three accident conditions are presented for phases 1, 2, and 3.

As described in Sec. III, the systems required in phase 1 form a part of the systems required in phase 2. Therefore, there is no discontinuity of mission unreliabilities at the boundary between phases 1 and 2. The task in phase 3 is recirculation cooling, and the required systems are different from those in phase 2. Then, there is discontinuity of mission unreliabilities at the boundary between phases 2 and 3. Except the phase boundaries, the mission unreliabilities continuously increase with time. If we are interested in more detailed variations of the mission unreliability, we simply define additional time points between the time points that are already defined.

In phases 1 and 2, a nearly three order of magnitude larger mission unreliability is obtained under the condition of flooding occurring simultaneously with a LOCA in comparison with the unreliability under the condition of no flooding. If compartment B of the reactor room is flooded, the redundancy of the HPCI and the LPCI is lost. If the main machinery room is flooded, the main and auxiliary generators are lost and only two emergency generators are available. These are the main reasons that the reliability of the ECCS degrades if flooding occurs simultaneously with a LOCA.

As the operation time lengthens, the reliability of generators mainly determines the reliability of the RCL. Only two emergency generators are available if flooding occurs in the main machinery room. Therefore, at the end of phase 3, an almost one order of magnitude larger mission unreliability is obtained under this condition in comparison with the one under the condition of flooding in compartment B.

TABLE II

Mission Unreliability of the ECCS of Marine Reactor Under Three Accident Conditions

Accident Condition	Phase 1		Phase 2		Phase 3		
	Time Point						
	3	4	5	6	7	8	9
No flooding	2.89×10^{-6}	2.90×10^{-6}	2.90×10^{-6}	2.90×10^{-6}	9.34×10^{-5}	3.98×10^{-4}	3.61×10^{-3}
Flooding in compartment B	2.60×10^{-3}	2.61×10^{-3}	2.61×10^{-3}	2.61×10^{-3}	1.21×10^{-2}	1.89×10^{-2}	2.86×10^{-2}
Flooding in main machinery room	9.05×10^{-4}	9.32×10^{-4}	9.32×10^{-4}	1.09×10^{-3}	1.18×10^{-3}	5.11×10^{-2}	1.46×10^{-1}

The redundancy of the RCL is lost if flooding occurs in compartment B. Then, at the end of phase 3, the mission unreliability is one order of magnitude larger than that under the condition of no flooding.

It should be emphasized that for the evaluation of the safety of a nuclear tanker, it is necessary to evaluate

$$P_A \cdot P_{\text{LOCA}} \cdot P_{SS} ,$$

where

P_{SS} = mission unreliability of a system shown in Table II

P_A = probability that a marine disaster occurs

P_{LOCA} = probability that a LOCA occurs under a marine accident condition.

Our study[8] has shown that the P_A for a collision or grounding accident is $<1.4 \times 10^{-4}$/yr·ship and the P_{LOCA} is negligibly small. The value P_{LOCA} strongly depends on the accident condition, the configuration of a safety system, and the ship structure. The value P_{SS} alone does not have any significant meaning; it should be considered in the product of P_A, P_{LOCA}, and P_{SS}.

VI. COMPARISON WITH FAULT-TREE TECHNIQUE AND GO METHOD

For the analysis of system reliability, a fault-tree technique is most frequently used. A fault tree has only one undesired event of a system (top event), so it is necessary to construct a number of fault trees that correspond to different accident conditions. Furthermore, the time-dependent unreliability analysis cannot be performed by one fault-tree analysis.

Phased mission analysis can be solved by a fault-tree technique, but the procedure is very troublesome. First, make a fault tree for each phase. Then combine these fault trees by the OR gate. At this time, a basic event has to be divided into multiple basic events belonging to each phase. The combined fault tree becomes large and complex.

The GO method can express the different accident conditions in one GO chart. For the time-dependent unreliability analysis, it requires several computer runs with different input data. The GO method determines the time when a system changes state but cannot treat a system that has multiple state changes. Also, the GO method does not have an operator like the type 40 operator of the GO-FLOW methodology. Therefore, the phased mission problem cannot be solved by the GO method within the present framework.

On the other hand, one GO-FLOW chart can express the system function in multiple phases under different accident conditions. With one GO-FLOW chart and a set of input data, an analysis is performed with one computer run. The GO-FLOW method can easily analyze a phased mission problem and a time-dependent unreliability analysis under multiple accident conditions, as shown in Sec. IV.

VII. CONCLUSIONS

This paper has presented a reliability analysis by the GO-FLOW methodology for the ECCS of a marine reactor experiencing a collision or a grounding accident. It has been shown that the GO-FLOW method can be applicable to a relatively large system with a complex system operation sequence. The time-dependent mission unreliabilities under three accident conditions were obtained by one GO-FLOW chart with one computer run.

The GO-FLOW method has proved to be a useful tool for PSAs of actual systems, such as a nuclear power plant or a nuclear propulsion ship.

ACKNOWLEDGMENTS

The authors thank Y. Nikuma, Kawasaki Heavy Industry, and M. Takakura, Ishikawajima-Harima Heavy Industry, for their helpful discussions and suggestions.

This research was supported in part by the RR-30 research committee of the Shipbuilding Research Association of Japan.

REFERENCES

1. "PRA Procedure Guide," NUREG/CR-2300, U.S. Nuclear Regulatory Commission (1983).

2. N. J. McCORMIK, *Reliability and Risk Analysis; Method and Nuclear Applications*, Academic Press, Inc., New York (1981).

3. T. MATSUOKA and M. KOBAYASHI, "GO-FLOW: A New Reliability Analysis Methodology," *Nucl. Sci. Eng.*, **98**, 64 (1988).

4. W. V. GATELY and R. L. WILLIAMS, "GO Methodology—Overview," NP-765, Electric Power Research Institute (1978).

5. "Conceptual Design Study of an Integral Marine Nuclear Reactor," Report, Shipbuilding Research Association of Japan (Oct. 1972) (in Japanese).

6. "The First Nuclear Ship *Mutsu*," Technical Report, Ishikawajima-Harima Heavy Industry (Aug. 1970) (in Japanese).

7. "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, Appendix III Failure Data," WASH-1400, NUREG-75/014, U.S. Nuclear Regulatory Commission (1975).

8. "Study on Practical Application of Safety Criteria for Nuclear Merchant Ships," Draft Report, Shipbuilding Research Association of Japan (Mar. 1988) (in Japanese).