Vol. 2, No. 1, pp. 50-56, June 2003

INTERNATIONAL JOURNAL OF SAFETY
www.kiis.or.kr

Severe Accident Management Using PSA Event Tree Technology

Young Choi*, Kwang Sub Jeong, and Soo Yong Park

Korea Atomic Energy Search Institute P.O.Box 105, Yusung, Taejon 305-600, Korea

(Received April 28, 2003; Accepted June 15, 2003)

Abstract : There are a lot of uncertainties in the severe accident phenomena and scenarios in nuclear power plants (NPPs) and one of the major issues for severe accident management is the reduction of these uncertainties. The severe accident management aid system using Probabilistic Safety Assessments (PSA) technology is developed for the management staff in order to reduce the uncertainties. The developed system includes the graphical display for plant and equipment status, previous research results by a knowledge-base technique, and the expected plant behavior using PSA. The plant model used in this paper is oriented to identify plant response and vulnerabilities via analyzing the quantified results, and to set up a framework for an accident management program based on these analysis results. Therefore the developed system may play a central role of information source for decision-making for severe accident management, and will be used as a training tool for severe accident management.

Key words : severe accident management guideline, probabilistic safety assessments (PSA), decision support, SPDS, knowledge base

1. Introduction

Since the Three Mile Island (TMI) accident, the importance of a accident management in nuclear power plants has increased. Many countries, including the United States (US), have focused on understanding severe accidents, in order to identify ways to further improve the safety of the plants [1]. It has been recognized that plant-specific probabilistic safety assessments (PSA) can be beneficial in understanding plant-specific vulnerabilities of severe accidents [2].

The objectives of this paper are to describe the PSA analyses of the nuclear power plants, to identify plant response and vulnerabilities via analyzing the quantified results, and to set up a framework for an accident management program based on thse analysis results. Basically the scope and methodology of the analysis used to perform individual plant examination (IPE) are similar to those of PSA. Therefore, a state-of-the-art PSA technique has been used in this study to demonstrate its application feasibility to accident management [3, 4].

Plant damage states (PDSs) are defined as group Level-1 core damage sequences into a manageable size by considering containment failure mode and timing, and the source term characteristics. Also, to model containment responses during severe accidents, containment event trees (CETs) are developed for the plant. Potential containment failure modes including containment bypass, isolation failure, steam explosion, hydrogen combustion and steam overpressurization are also considered in constructing the CETs.

From the viewpoint of severe accident management, the increased sophistication of PSA models and the descriptions of risk results offer the potential for improving the decision-making process [5, 6]. In this study, we investigated methods to utilize the plant-specific PSA results effectively for decision-making in managing accidents in the plant.

To apply the CET to a unique accident initiator, the core damage sequence, containment failure and source term must be correctly identified so that appropriate safety systems in the containment can be used to minimize the accident consequences. This approach will especially help to implement the event oriented procedures of existing emergency operating procedures (EOPs) in dealing with design basis accidents (DBAs) [7].

The CETs are quantified by assigning a probability to each branch (branch fraction) in the CET and propagating the probabilities for each pathway leading to a distinct containment end state. The modeling of complicated containment events can be significantly simplified by the

*Corresponding author: ychoi@kaeri.re.kr

application of decomposition event trees (DETs). DETs allow the use of a generalized CET logic structure for most PDSs while keeping the size of the CET reasonable for scrutability and understanding. All dependencies in the subevents in PDS conditions and prior CET branch point decisions can be rigorously treated. Hence, the combined paths of CETs and DETs are used in prioritizing the success paths for accident management.

Finally, the method we developed for the application of PSA results to accident management is applied to the loss of offsite power (LOOP) accidents in this demonstration. The controllability of the CET headings for LOOP is first identified along with the feasible CET paths. The conditional probabilities of early containment failure are then calculated for possible recovery actions. Based on these calculations, the CET paths are prioritized to help the decision-making of the emergency response team in the plant.

2. Methodology of PSA Application to Accident Management

This section describes the methodology of how to use PSA results in managing accidents occurring in a nuclear power plant. In particular, we are mainly interested in severe accidents because less serious accidents usually evolve more rapidly at the systems level compared to such severe accidents that may involve core damage to some extent. Although level-1 PSA may be somewhat useful for certain accident types, the analysis results of level-2 PSA would be more helpful in managing severe accidents. Hence, in this study we focused on level-2 PSA to develop how to use PSA results for accident management.

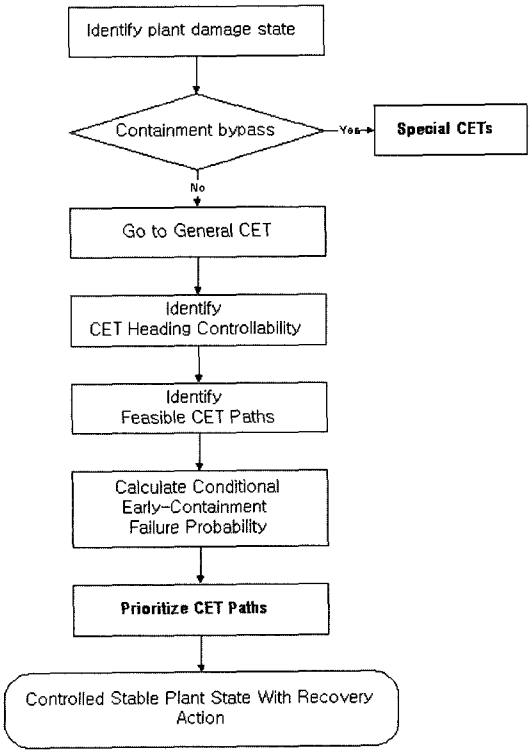

Fig. 1. Procedure for the Application of PSA Results to Severe Accident.

Level-2 PSA covers containment performance analysis and source term analysis. In order to connect the results of level-1 PSA to level-2 PSA, plant damage states (PDSs) are defined and each level-1 sequence is grouped into an appropriate PDS. For each PDS, the accident phenomena are analyzed together with the analysis of containment performance. The failure probability of the containment is then evaluated for all the sequences leading to core damage. Plant-specific source terms are next evaluated for those accident sequences which represent the characteristic source term categories[8].

The flow chart of Fig. 1 shows a procedure by which the PSA results can be applied for managing a severe accident that took place in a nuclear power plant. The procedure consists of 6 steps: 1) identify plant damage state, 2) go to general CET, 3) identify CET heading controllability, 4) identify feasible CET paths, 5) calculate conditional probability of early containment failure, and 6) prioritize CET paths. Each of these steps is described below.

2-1. Identification of Plant Damage State

To use the PSA results for real-time accident management, the current plant damage state (PDS) should be identified from Fig. 2. This figure shows 45 PDSs, among which PDS 1 and 2 represent unisolated containment states, and PDS 44 and 45 indicate containment bypass. Hence these four PDSs are treated as special PDSs for which special containment event trees (CETs) are develeoped. For all other PDSs, i.e., PDS 3~42, general CETs are developed. The PDS characteristics are defined by selecting key system operations considered to be important to the following parameters: accident progression in the containment; time, mode, and location of containment failure; and the radionuclide source term [9]. The parameters used to define the PDSs include the functional status of important systems, variables determined by systems operation (e.g., reactor coolant system (RCS) pressure), accident initiator type, and the timing of key events (e.g., power recovery). (Table 1)

In a real application of the PSA, the plant situation shall be identified as one of the 45 PDSs in view of the eight parameters described above.

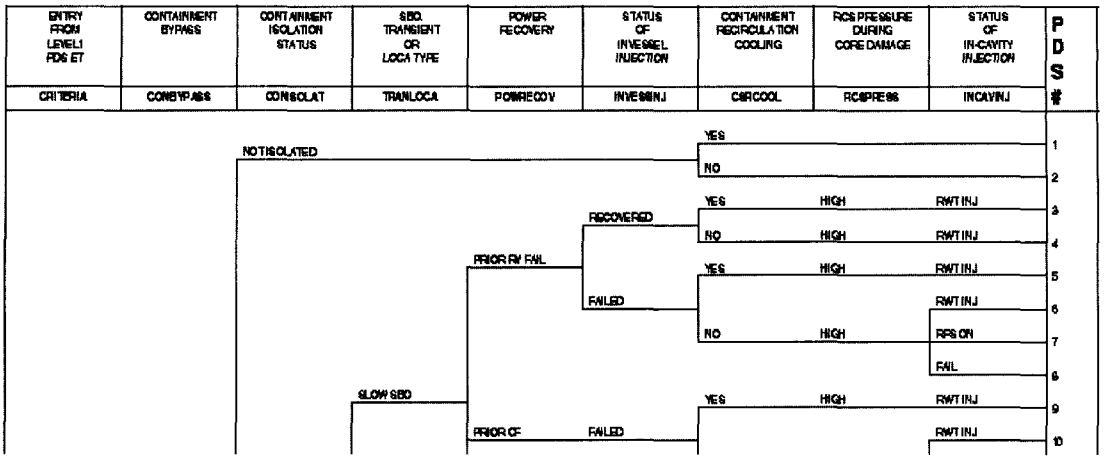

Fig. 2. PDS Grouping Logic Diagram

Table 1. Grouping Parameters of a PDS Event Tree

1) containment bypass
2) containment isolation status
3) station blackout, transient or LOCA
4) power recovery
5) status of in-vessel injection
6) containment recirculation cooling
7) RCS pressure during core damage
8) status of in-cavity injection

2-2. Transfer to General CET

In the quite unusual case where the containment is bypassed or unisolated, special CETs are used. In all other cases where it is not bypassed or isolated, general CETs for PDS 3~42 are used [10]. Figure 3 shows a typical CET for PDS 3~42. These CETs depict various phenomenological processes, containment conditions, and containment failure modes that could occur under severe accident conditions. Each PDS end point represents a unique accident progression starting point with respect to the CET. In principle, each event path has to be quantified separately because of the unique accident progression. Core damage sequences in which the containment is successfully isolated (i.e., not bypassed) would have different modeling requirements compared with those sequences in which the containment is either unisolated or bypassed.

Therefore, it follows that a CET must be developed and quantified for each PDS. In practice, however, there will be many commonalties for most accident sequences, except for the containment bypass and containment isolation failure sequences. To model containment responses for most accident sequences, a general CET is developed. Special CETs are used to model those sequences in which the containment is bypassed or unisolated as discussed above.

The event headings in the CET contain those phenomena expected to have an impact on the accident progression within the containment. To simplify the structure of the CET the number of events is reduced to

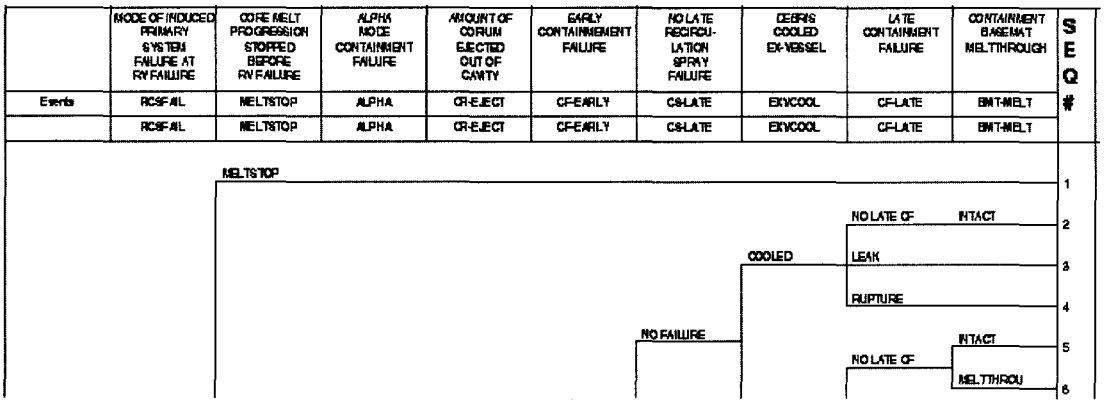

Fig. 3. CET Grouping for PDSs 3~42.

Table 2. Headings of a General Containment ET

1. Mode of Induced Primary System Failure
2. Core-Melt Arrest
3. Alpha Mode Containment Failure
4. Amount of Corium Ejected out of Cavity
5. Mode of Early Containment Failure
6. No Late Recirculation Spray Failure
7. Debris Cooled Ex-vessel
8. Mode of Late Containment Failure
9. Basemat Melt-through

as few as possible. The events that contribute to these top events of CET and/or which aid in the assessment of the event branch probabilities are relegated to decomposition event trees (DETs). Table 2 shows typical nine top events of general CET. Each top event has its own DET. DETs consist of the important "subevents" that contribute to the top event and is used to quantify the branch probability of the top event.

Several major top events of the CET are described below.

Mode of Induced Primary System Failure

This question asks whether the elevated temperatures and pressures within the RCS following core uncovery can result in failure of the RCS pressure boundary outside the vessel prior to failure of the reactor vessel's lower head.

Core-Melt Arrest

This question asks whether the damaged core can be cooled in-vessel by the introduction of cooling water into the reactor vessel, thereby terminating the accident progression before reactor vessel rupture.

Alpha Mode Containment Failure

This question asks whether the extensive in-vessel steam explosion occurs and results in early containment failure. A postulated alpha mode containment failure results from a large coherent in-vessel steam explosion that fails the reactor vessel and generates a missile (from part of the reactor vessel upper head) with sufficient mass and energy to fail the containment.

Mode of Early Containment Failure

This question asks whether the early containment failure occurs. Early containment failure is defined as failure of containment shortly before, at, or soon after reactor vessel failure. Early containment failure can potentially result from a combination of energetic processes and events that may occur at the reactor vessel breach. These processes and events include blowdown of the primary system, direct containment heating (DCH), hydrogen combustion, and rapid steam genera-tion in the cavity.

2-3. Identification of CET Heading Controllability

Modeling complicated containment events can be simplified by the use of decomposition event trees (DETs). DETs offer advantages by allowing the use of a generalized CET logic structure for most PDSs while keeping the size of the CET reasonable for scrutability and understanding. The PDS-specific quantification and additional event phenomenology are then contained in the DETs.

The basic considerations in the construction of a DET are:

1) The last event in the DET is the same event heading as in the CET. Each possible branch pathway shown in the CET for this event must also exist in the DET. After the DET is quantified, the end point probabilities for similar branches in the last event are summed together and these summed probabilities are passed back into the CET as CET branch probabilities.

2) The selected sub-events can be quantified with available data or analyses.

3) All dependencies in the sub-events on PDS conditions and prior CET branch point decisions can be rigorously treated.

The controllability of CET top events or sub-events of their corresponding DET is examined in this step to identify controllable events which will be considered later in prioritizing the CET paths.

2-4. Identification of Feasible Success Paths

Once the controllability of the CET top events and the DET subevents are examined, then feasible CET paths in view of the event controllability and current plant state are identified. These success paths also represent the phenomena, such as ex-vessel steam explosion or hydrogen burning.

The feasible CET paths should be identified from both the CET in Fig. 3. in this study, the aim of accident management is placed on minimizing the likelihood of early containment failure.

The phenomenological branch point probability should be one or zero (i.e., occurrence or non-occurrence). However, because of the current lack of knowledge regarding the phenomenon, it is not possible to identify the correct branch. The branch point probabilities that are assigned must therefore represent the analyst's degree of belief that

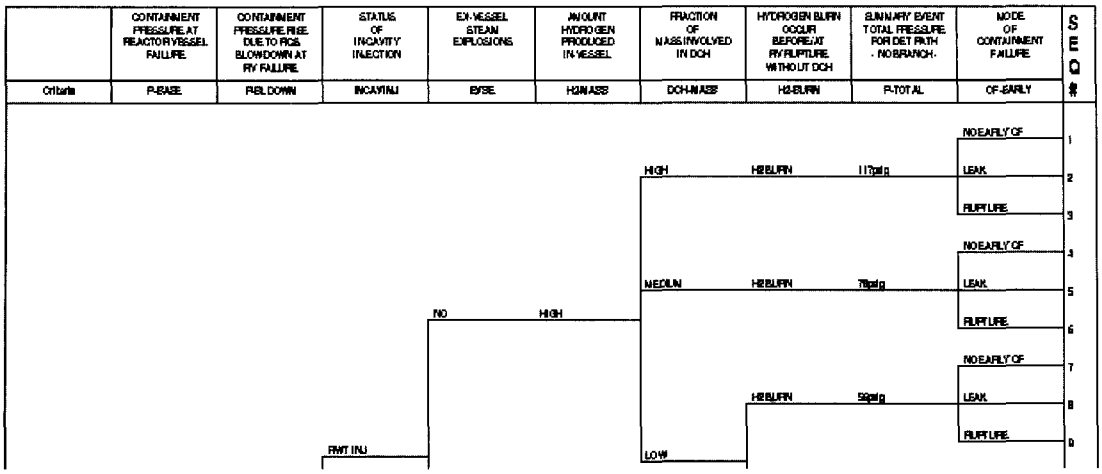

Fig. 4. Mode of Early Containment Failure DET.

the accident will progress along the branch.

2-5. Calculation of Conditional Probability of Early Containment Failure

Early containment failure is one of the most severe cases of plant containment failure modes in terms of radionuclides release. Thus, even though early containment failure is found to take place relatively infrequently, it should be given special attention in accident management. The probability of containment failure and its failure mode is calculated using the containment fragility curve developed by a domain expert.

The early containment failure may occur as a result of either rupture or leakage of containment. Thus, the three modes of early containment failure, namely rupture, leakage, or no early containment failure, can be identified using Fig. 4. Among these, the rupture failure is determined to be the most dominant contributor to the early containment failure.

The conditional probability of early containment failure can be calculated by multiplying the branch probabilities of each feasible CET path, as is done in a typical event tree quantification.

2-6. Prioritization of Success Paths

Once the conditional probabilities of early containment failure are computed, the CET paths can be easily prioritized in terms of the probabilities. Usually recovery actions are not properly credited in level-2 PSAs performed to date. If this is the case, human recovery should be taken into account in the prioritization.

The prioritization also should consider equipment and human performance under severe accident conditions and the availability of information. A further important aspect is the evaluation of the accessibility of equipment which has to be operated or repaired. An examination also has to be made to determine whether the equipment concerned can be operated or repaired without exposing the plant staff to excessive radiation, temperature, etc.

3. Application of PSA Results to Accident Management

Here we present a sample application of the procedure discussed in the previous chapter for the loss of offsite power (LOOP) accident in a nuclear power plant.

3-1. Outline of Loss of Offsite Power

In this study, LOOP is taken as one of the major events. A typical PDS (plant damage state) event tree for LOOP from level-2 PSA given in Fig. 5. The plant technical specifications that govern the required availability of AC power during operations are typical of those in many reactors. After LOOP occurs, the two diesel generators which supply the electric power to the 4.16 kV Class 1E buses (A-PB-001 and B-PB-001) receive a start signal, run up and connect to each bus. The load sequencer automatically loads up each diesel generator by a phased start of all the safety equipment. (Fig. 6)

Then using the results of the above event tree analysis, one can derive success path sets for the operator to take the proper actions which are described.

Electrical Source Requirements

As a minimum, the following AC electric power source shall be operable:

(1) One circuit between the offsite transmission network and onsite class IE distribution system and

(2) One diesel generator

(3) One load group of AC emergency buses consist-

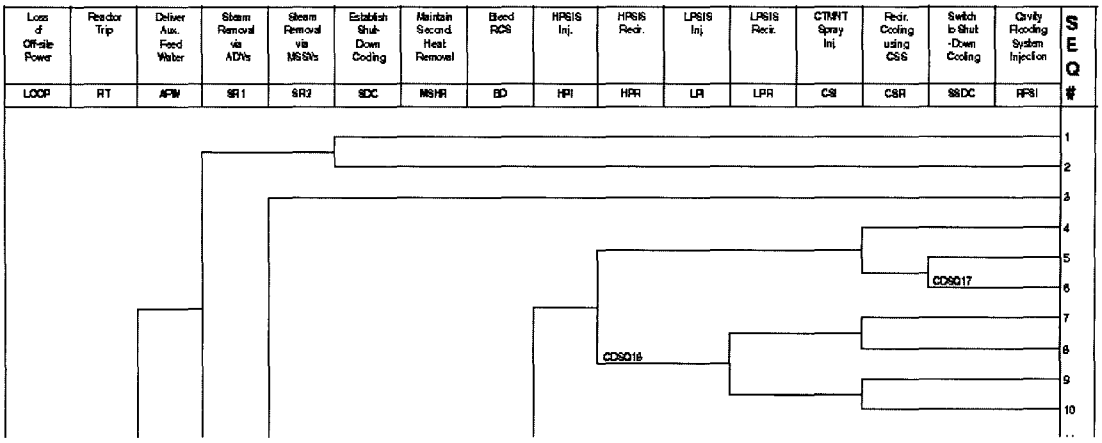

Fig. 5. PDS Event Tree for Loss of Offsite Power

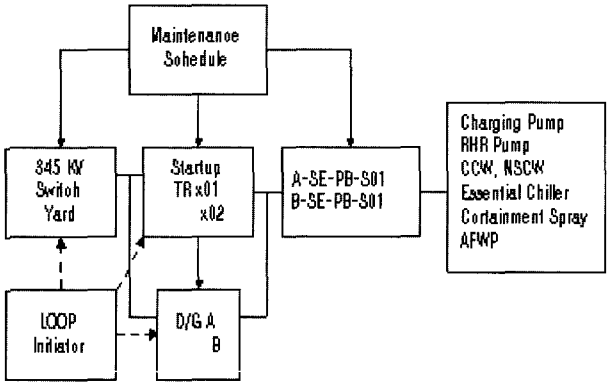

Fig. 6. Electical System Configuration.

ing of one 4.16 kV

3-2. Basic Architecture

A computerized architecture is developed to support the operators in emergency situations of NPPs [11]. This paper suggests incorporation of the LOOP events to those operator support systems. The basic architecture has three functional levels: top, second, and third levels according to the depth and detailed strategy of the mitigating plant transient (Fig. 7).

The top level contains a display of the plant overview and the plant parameter which has boron concentration, RCS level, temperature and flow. Therefore, the operational crew can monitor the overall plant status at a glance. The second level is a computerized software system designed to guide them in emergency conditions. This level is composed of event diagnosis and event analysis.

The event is diagnosed from plant parameters which represent specific symptoms for each event. Event analysis contains system reliability and maintenance status. System reliability comes from a generic fault tree approach with shutdown specific data. Maintenance status gives some limitation to plant configurations which

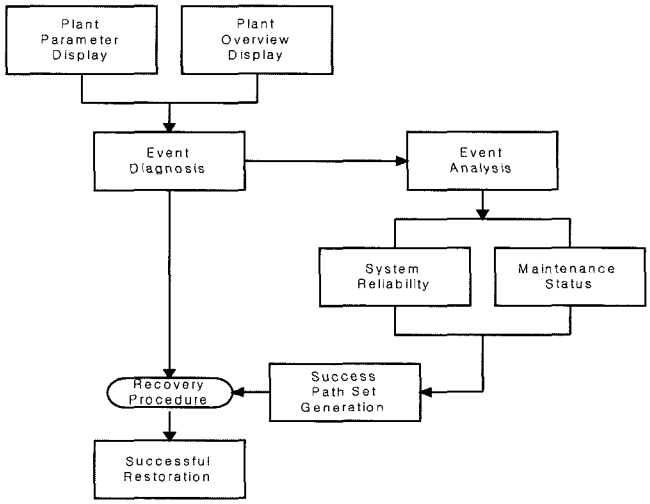

Fig. 7. Basic Architecture for Accident Management.

describe realistic plant states during maintenance.

Third level is a final step which produces generation of a success path set and shows plant restoration guidances according to the measures taken in the recovery procedure[12] with the help of a mimic display of the safety system status.

3-3. Path Monitoring

The suggested paths can be checked by monitoring the plant status with the SAMAT system [13, 14]. The support system for decision-making with severe accident management provides plant parameters to monitor plant status. The path monitor checks the status of the safety system selected by the maintenance status and displays an optimal success path based on each component with a mimic display of the systems drawings. An example display of an optimal success path selected from the integrated reliability rules is shown in Figure 8 for a typical electrical system. Eventually, the operator will

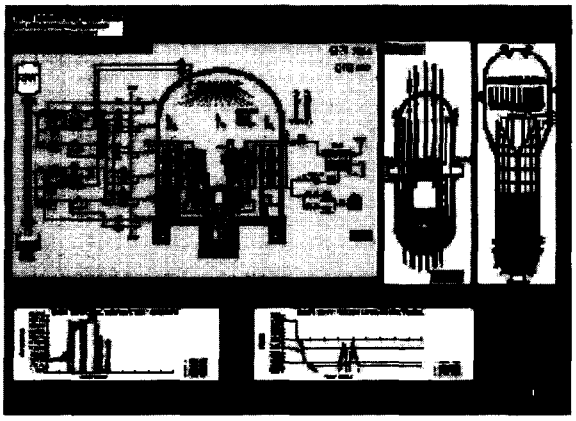

Fig. 8. Display of Optimal Success Path for LOOP in Computer Monitor.

be supported by this generation of success path sets to restore the plant. Then, the operator can make an appropriate decision without ambiguity and complexity.

4. Conclusions

The increased sophistication of PSA models and the descriptions of risk results offer the potential for improving the decision-making process. In this study, we investigated methods to utilize the plant-specific PSA results effectively for decision-making in managing accidents in the plant.

In particular, our approach of applying PSA results to accident management is based on back-end analyse, i.e., level-2 PSA results, because the current emergency operating procedures (EOPs) do not properly cover the severe accident regime involving core damage [15]. The results of back-end analyses help to identify plant vulnerabilities and appropriate plant responses to a specific challenge [16].

Acknowledgements

This work was performed under "The Mid- and Long-Term Nuclear R & D Program" sponsored by Ministry of Science and Technology (MOST), Korea.

References

[1] USNRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants", NUREG-1150, 1989.
[2] USNRC, "Evaluation of Severe Accident Risks: Surry Unit 1", NUREG/CR-4551,, July 1989.
[3] U.S. NRC "Individual Plant Examination for Severe Accident Vulnerabilities - 10 CFR 50. 54(f)", Generic Letter No. 88-20, November 1988.
[4] USNRC, "Individual Plant Examination Program : Perspectives on Reactor Safety and Plant Performance", NUREC-1560, November 1996.
[5] KEPRI, "Preliminary Study for Development of Accident Management Plans in Nuclear Power Plants," TR.96NJ11.97.77, 1997.
[6] H. S. Chang, "A Study on the Development of Framework and Supporting Tools for Severe Accident Management" Ph.D, KAIST,September 1995.
[7] WOG, "Severe Accident Management Guidance", Vol.1, Executive Volume, Westinghouse, June 1994.
[8] USNRC, "PRA Procedure Guide," NUREG/CR-2300, January 1983.
[9] KAERI, CONPAS 1.0 Code Package User's Manual, KAERI/TR-651/96, April 1996.
[10] KEPCO, "PSA for Ulchin Units 1&2," 1993.
[11] Young Choi, et al., "Conceptual Design of Emergency Operation Procedure Advice System by Combining SPDS, ERG, and Success Path Generators", KNS, Korea, October. 10.
[12] KEPCO, "General & Abnormal Operating Procedure for Kori 3&4", 1993.
[13] Jeong, K. S, et al. "Development of Severe Accident Management Advisory and Training Simulator (SAMAT)", annals of NUCLEAR ENERGY 29, 2002.
[14] Jeong, K. S, et al. "Development of Severe Accident Management Advisory and Training Simulator (SAMAT)", KAERI/TR-1789/, 2001.
[15] KAERI, "Development of Accident Management Technology and Computer Code," KAERI/RR-1742/96, 1997.
[16] KEPRI, "Level 2 Probabilistic Safety Assessment for PHWR," TR.93NJ10.97.67-2, 1997.